VMware

Enterprise applications

NetApp
January 02, 2026

Inhalt

VMware

VMware vSphere mit ONTAP –

VMware vSphere mit ONTAP –

ONTAP war seit seiner Einführung in das moderne Datacenter im Jahr 2002 eine der führenden Storage-Lösungen für VMware vSphere und in jüngster Zeit auch Cloud-Foundation-Umgebungen. Es werden weiterhin innovative Funktionen eingeführt, die das Management vereinfachen und Kosten senken.

Dieses Dokument stellt die ONTAP Lösung für vSphere vor und hebt die neuesten Produktinformationen und Best Practices hervor, um die Implementierung zu optimieren, Risiken zu minimieren und das Management zu vereinfachen.

Diese Dokumentation ersetzt zuvor veröffentlichte technische Berichte *TR-4597: VMware vSphere for ONTAP*

Andere Dokumente wie Leitfäden und Kompatibilitätslisten werden durch Best Practices ergänzt. Sie werden basierend auf Labortests und umfassenden praktischen Erfahrungen der NetApp Ingenieure und Kunden entwickelt. Es handelt sich hierbei unter Umständen nicht nur um die einzigen unterstützten Praktiken, die in jeder Umgebung funktionieren. Im Allgemeinen sind sie aber die einfachsten Lösungen, die die Anforderungen der meisten Kunden erfüllen.

Der Schwerpunkt dieses Dokuments liegt auf den Funktionen der neuesten Versionen von ONTAP (9.x), die unter vSphere 7.0 oder höher ausgeführt werden. In "Interoperabilitäts-Matrix-Tool (IMT)" und "VMware Compatibility Guide" finden Sie Details zu den jeweiligen Versionen.

Warum ONTAP für VMware vSphere?

Kunden entscheiden sich vertrauensvoll für ONTAP für vSphere sowohl für SAN- als auch für NAS-Speicherlösungen. Die neue vereinfachte disaggregierte Speicherarchitektur, die in den neuesten All SAN Arrays enthalten ist, bietet SAN-Speicheradministratoren eine vereinfachte Erfahrung, die ihnen vertraut ist, während die meisten Integrationen und Funktionen herkömmlicher ONTAP -Systeme erhalten bleiben. ONTAP -Systeme bieten außergewöhnlichen Snapshot-Schutz und robuste Verwaltungstools. Durch die Auslagerung von Funktionen auf dedizierten Speicher maximiert ONTAP die Hostressourcen, senkt die Kosten und sorgt für optimale Leistung. Darüber hinaus können Workloads mithilfe von Storage vMotion problemlos über VMFS, NFS oder vVols migriert werden.

Die Vorteile der Verwendung von ONTAP für vSphere

Zehntausende Kunden haben sich für ONTAP als Storage-Lösung für vSphere entschieden. Dafür gibt es viele Gründe, beispielsweise ein Unified-Storage-System, das sowohl SAN- als auch NAS-Protokolle unterstützt, robuste Datensicherungsfunktionen mittels platzsparender Snapshots und eine Fülle von Tools, die Sie beim Management von Applikationsdaten unterstützen. Wenn Sie ein Storage-System getrennt vom Hypervisor verwenden, können Sie viele Funktionen verlagern und Ihre Investitionen in vSphere Host-Systeme optimal nutzen. Hierdurch wird sichergestellt, dass Ihre Host-Ressourcen schwerpunktmäßig für Applikations-

Workloads verwendet werden. Darüber hinaus werden zufällige Auswirkungen auf die Performance von Applikationen aufgrund des Storage-Betriebs vermieden.

Die Verwendung von ONTAP zusammen mit vSphere ist eine großartige Kombination, mit der Sie die Kosten für Host-Hardware und VMware-Software senken können. Sie können Ihre Daten außerdem zu geringeren Kosten bei gleichbleibend hoher Leistung schützen. Da virtualisierte Workloads mobil sind, können Sie mithilfe von Storage vMotion verschiedene Ansätze erkunden, um VMs zwischen VMFS-, NFS- oder vVols Datenspeichern zu verschieben, und zwar alle auf demselben Speichersystem.

Hier sind die wichtigsten Faktoren, die Kunden heute schätzen:

- **Einheitlicher Speicher.** Systeme, auf denen ONTAP läuft, sind in mehreren wichtigen Punkten vereinheitlicht. Ursprünglich bezog sich dieser Ansatz sowohl auf NAS- als auch auf SAN-Protokolle, und ONTAP ist weiterhin eine führende Plattform für SAN, abgesehen von seiner ursprünglichen Stärke im NAS-Bereich. In der vSphere-Welt könnte dieser Ansatz auch ein einheitliches System für die virtuelle Desktop-Infrastruktur (VDI) zusammen mit der virtuellen Server-Infrastruktur (VSI) bedeuten. Systeme mit ONTAP sind für VSI in der Regel weniger teuer als herkömmliche Enterprise-Arrays und verfügen dennoch über erweiterte Speichereffizienzfunktionen, um VDI im selben System zu verarbeiten. ONTAP vereint außerdem eine Vielzahl von Speichermedien, von SSDs bis SATA, und kann diese problemlos in die Cloud erweitern. Es ist nicht erforderlich, ein Speicherbetriebssystem für die Leistung, ein anderes für Archive und noch ein weiteres für die Cloud zu kaufen. ONTAP verbindet sie alle.
- **All-SAN-Array (ASA).** Die aktuellen ONTAP ASA Systeme (beginnend mit A1K, A90, A70, A50, A30 und A20) basieren auf einer neuen Storage-Architektur, mit der das herkömmliche ONTAP Storage-Paradigma beim Management von Aggregaten und Volumes entfällt. Da es keine Filesystem-Shares gibt, werden keine Volumes benötigt! Sämtlicher Storage, der mit einem HA-Paar verbunden ist, wird als gemeinsame Storage Availability Zone (SAZ) behandelt, in der LUNs und NVMe-Namespaces als „Storage Units“ (Sus) bereitgestellt werden. Die neuesten ASA Systeme sollen einfach zu managen sein und bieten SAN-Storage-Administratoren vertraute Erfahrung. Diese neue Architektur eignet sich ideal für vSphere Umgebungen, da sie das Management von Storage-Ressourcen vereinfacht und den SAN Storage-Administratoren eine vereinfachte Erfahrung bietet. Die ASA Architektur unterstützt darüber hinaus die neueste NVMe over Fabrics (NVMe-of) Technologie, die noch bessere Performance und Skalierbarkeit für vSphere Workloads bietet.
- **Snapshot-Technologie.** ONTAP ist der erste Anbieter von Snapshot-Technologie für die Datensicherung und bleibt auch in der Branche der fortschrittlichste Anbieter. Dieser platzsparende Ansatz für die Datensicherung wurde erweitert und unterstützt nun VMware vSphere APIs for Array Integration (VAAI). Dank dieser Integration können Sie die Snapshot-Funktionen von ONTAP für Backup- und Restore-Vorgänge nutzen und so die Auswirkungen auf Ihre Produktionsumgebung verringern. Dieser Ansatz ermöglicht zudem, Snapshots für die schnelle Wiederherstellung von VMs zu verwenden und so den Zeit- und Arbeitsaufwand für die Wiederherstellung von Daten zu reduzieren. Darüber hinaus ist die Snapshot-Technologie von ONTAP in die Live Site Recovery (VLSR, früher Site Recovery Manager [SRM])-Lösungen von VMware integriert. So erhalten Sie eine umfassende Datensicherungsstrategie für Ihre virtualisierte Umgebung.
- **Virtuelle Volumes und speicherrichtlinienbasierte Verwaltung.** NetApp war einer der ersten Designpartner von VMware bei der Entwicklung von vSphere Virtual Volumes (vVols) und lieferte architektonischen Input und frühzeitigen Support für vVols und VMware vSphere APIs for Storage Awareness (VASA). Dieser Ansatz ermöglichte nicht nur eine granulare VM-Speicherverwaltung für VMFS, sondern unterstützte auch die Automatisierung der Speicherbereitstellung durch eine auf Speicherrichtlinien basierende Verwaltung. Dieser Ansatz ermöglicht es Speicherarchitekten, Speicherpools mit unterschiedlichen Funktionen zu entwerfen, die von VM-Administratoren problemlos genutzt werden können. ONTAP ist in der Speicherbranche führend im vVol-Maßstab und unterstützt Hunderttausende von vVols in einem einzigen Cluster, während Anbieter von Enterprise-Arrays und kleineren Flash-Arrays nur einige Tausend vVols pro Array unterstützen. NetApp treibt mit kommenden Funktionen auch die Entwicklung des granularen VM-Managements voran.

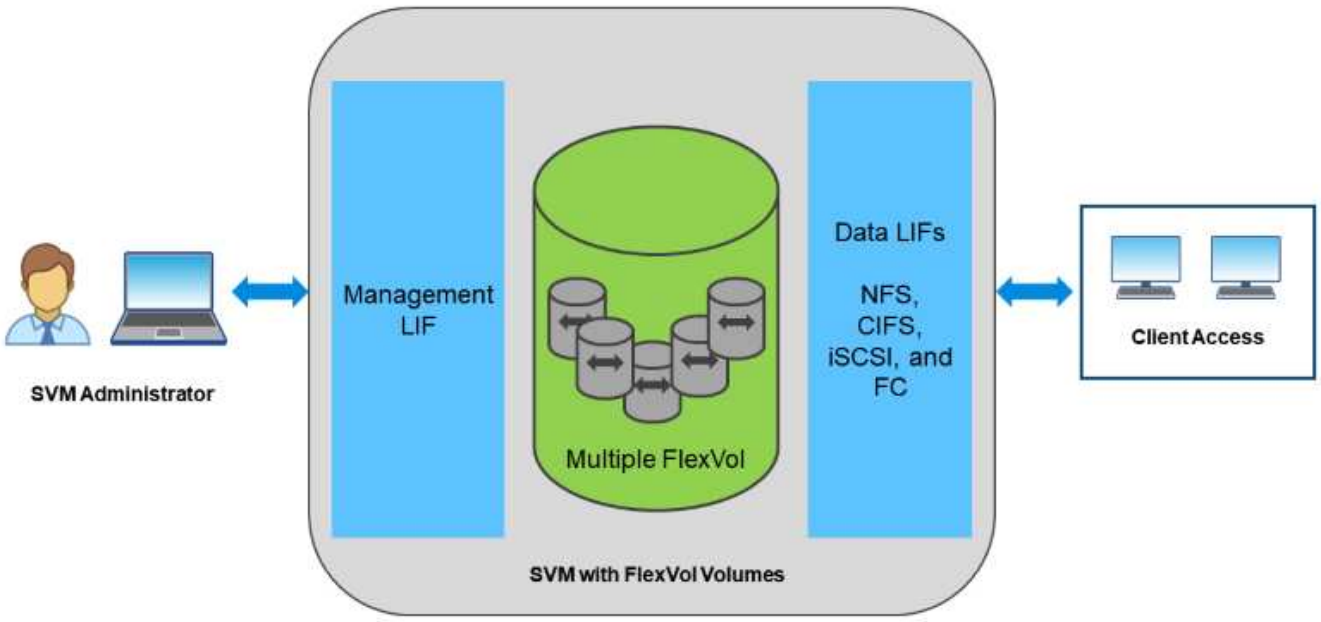
- **Speichereffizienz.** Obwohl NetApp als erstes Unternehmen Deduplizierung für Produktions-Workloads bereitstellte, war diese Innovation weder die erste noch die letzte in diesem Bereich. Es begann mit Snapshots, einem platzsparenden Datenschutzmechanismus ohne Leistungseinbußen, zusammen mit der FlexClone -Technologie zum sofortigen Erstellen von Lese-/Schreibkopien von VMs für die Produktion und Sicherung. NetApp lieferte anschließend Inline-Funktionen, darunter Deduplizierung, Komprimierung und Zero-Block-Deduplizierung, um den größtmöglichen Speicherplatz aus teuren SSDs herauszuholen. ONTAP hat außerdem die Möglichkeit hinzugefügt, kleinere E/A-Vorgänge und Dateien durch Komprimierung in einen Festplattenblock zu packen. Durch die Kombination dieser Funktionen konnten Kunden im Allgemeinen Einsparungen von bis zu 5:1 bei VSI und bis zu 30:1 bei VDI erzielen. Die neueste Generation von ONTAP -Systemen umfasst außerdem hardwarebeschleunigte Komprimierung und Deduplizierung, wodurch die Speichereffizienz weiter verbessert und die Kosten gesenkt werden können. Mit diesem Ansatz können Sie mehr Daten auf weniger Speicherplatz speichern, wodurch die Gesamtkosten für die Speicherung gesenkt und die Leistung verbessert werden. NetApp ist von seinen Speichereffizienzfunktionen so überzeugt, dass es einen Link anbietet:https://www.netapp.com/pdf.html?item=/media/79014-ng-937-Efficiency-Guarantee-Customer-Flyer.pdf [Effizienzgarantie^].
- **Mehrere Mandanten.** ONTAP ist seit langem führend im Bereich Multitenancy und ermöglicht Ihnen die Erstellung mehrerer virtueller Speichermaschinen (SVMs) auf einem einzigen Cluster. Mit diesem Ansatz können Sie Arbeitslasten isolieren und verschiedenen Mandanten unterschiedliche Servicelevel bereitstellen. Dies ist ideal für Dienstanbieter und große Unternehmen. Die neueste Generation von ONTAP -Systemen umfasst auch Unterstützung für das Tenant-Kapazitätsmanagement. Mit dieser Funktion können Sie Kapazitätsgrenzen für jeden Mandanten festlegen und so sicherstellen, dass kein einzelner Mandant alle verfügbaren Ressourcen verbrauchen kann. Dieser Ansatz trägt dazu bei, dass alle Mieter das Serviceniveau erhalten, das sie erwarten, und bietet gleichzeitig ein hohes Maß an Sicherheit und Isolation zwischen den Mietern. Darüber hinaus sind die Multitenancy-Funktionen von ONTAP in die vSphere-Plattform von VMware integriert, sodass Sie Ihre virtualisierte Umgebung einfach verwalten und überwachen können durch "ONTAP Tools für VMware vSphere" Und "Einblicke In Die Dateninfrastruktur" .
- **Hybrid Cloud.** Ganz gleich, ob Sie die Lösung für eine lokale Private Cloud, eine Public Cloud-Infrastruktur oder eine Hybrid Cloud verwenden, die das Beste aus beiden kombiniert: ONTAP -Lösungen unterstützen Sie beim Aufbau Ihrer Datenstruktur, um die Datenverwaltung zu rationalisieren und zu optimieren. Beginnen Sie mit leistungsstarken All-Flash-Systemen und koppeln Sie diese dann mit Festplatten- oder Cloud-Speichersystemen für Datenschutz und Cloud-Computing. Wählen Sie zwischen Azure, AWS, IBM oder Google Cloud, um Kosten zu optimieren und Lock-in-Strategien zu vermeiden. Nutzen Sie bei Bedarf erweiterten Support für OpenStack und Container-Technologien. NetApp bietet außerdem Cloud-basierte Backup- (SnapMirror Cloud, Cloud Backup Service und Cloud Sync) sowie Storage-Tiering- und Archivierungstools (FabricPool) für ONTAP an, um die Betriebskosten zu senken und die große Reichweite der Cloud zu nutzen.
- * Und mehr.* Nutzen Sie die extreme Performance von NetApp AFF A-Series Arrays, um Ihre virtualisierte Infrastruktur zu beschleunigen und gleichzeitig die Kosten im Griff zu haben. Mit horizontal skalierbaren ONTAP Clustern profitieren Sie bei der Wartung, bei Upgrades und selbst beim kompletten Ersatz Ihres Storage-Systems von einem durchgängig unterbrechungsfreien Betrieb. Daten im Ruhezustand werden mit NetApp Verschlüsselungsfunktionen ohne zusätzliche Kosten geschützt. Durch fein abgestimmte Quality-of-Service- Funktionen stellen Sie sicher, dass die Performance den geschäftlichen Service-Levels entspricht. Sie alle sind Bestandteil des umfangreichen Funktionsbereichs, das in ONTAP, der branchenführenden Software für das Enterprise-Datenmanagement, enthalten ist.

Unified Storage

ONTAP vereinheitlicht den Storage durch einen vereinfachten, softwaredefinierten Ansatz für sicheres und effizientes Management, verbesserte Performance und nahtlose Skalierbarkeit. Dieser Ansatz verbessert die Datensicherung und ermöglicht eine effektive Nutzung der Cloud-Ressourcen.

Ursprünglich wurde in diesem einheitlichen Ansatz erwähnt, dass sowohl NAS- als auch SAN-Protokolle auf einem Storage-System unterstützt werden sollten. ONTAP ist dabei weiterhin eine der führenden Plattformen für SAN und bietet in Bezug auf NAS die ursprünglichen Stärken. ONTAP unterstützt jetzt auch S3-Objektprotokolle. Obwohl S3 nicht für Datastores verwendet wird, können Sie es für in-Guest-Applikationen verwenden. Weitere Informationen zur Unterstützung des S3-Protokolls in ONTAP finden Sie in der "S3-Konfigurationsübersicht". Der Begriff Unified Storage hat sich zu einem einheitlichen Ansatz für das Storage Management entwickelt und umfasst die Möglichkeit, alle Storage-Ressourcen über eine einzige Schnittstelle zu managen. Dazu gehört die Möglichkeit, Storage-Ressourcen vor Ort und in der Cloud zu managen, aktuelle All-SAN-Array-Systeme (ASA) zu nutzen und mehrere Storage-Systeme über eine einzige Oberfläche zu managen.

Eine Storage Virtual Machine (SVM) ist die Einheit der sicheren Mandantenfähigkeit in ONTAP. Es handelt sich um ein logisches Konstrukt, das den Client-Zugriff auf Systeme mit ONTAP ermöglicht. SVMs können Daten gleichzeitig über mehrere Datenzugriffsprotokolle über logische Schnittstellen (Logical Interfaces, LIFs) bereitstellen. SVMs ermöglichen den Datenzugriff auf Dateiebene über NAS-Protokolle wie CIFS und NFS sowie den Datenzugriff auf Blockebene über SAN-Protokolle wie iSCSI, FC/FCoE und NVMe. SVMs können SAN- und NAS-Clients unabhängig gleichzeitig sowie mit S3 Daten bereitstellen.



Bei vSphere könnte dieser Ansatz auch für ein einheitliches System für Virtual Desktop Infrastructure (VDI) in Kombination mit einer virtuellen Serverinfrastruktur (VSI) stehen. Systeme mit ONTAP sind bei VSI in der Regel kostengünstiger als herkömmliche Enterprise-Arrays, bieten gleichzeitig aber fortschrittliche Storage-Effizienzfunktionen, mit denen Sie im selben System auch VDI gerecht werden können. ONTAP vereint außerdem eine Reihe von Storage-Medien – von SSDs bis SATA – und kann diese problemlos in die Cloud erweitern. Auf diese Weise müssen Sie nicht ein Flash-Array für Performance-Zwecke, ein SATA-Array für Archive und separate Systeme für die Cloud erwerben. Sie alle sind in ONTAP integriert.

HINWEIS: Weitere Informationen zu SVMs, Unified Storage und Client-Zugriff finden Sie unter "Storage-Virtualisierung" Im Dokumentationszentrum ONTAP 9.

Virtualisierungstools für ONTAP

NetApp bietet mehrere Standalone-Software-Tools, die mit herkömmlichen ONTAP- und ASA-Systemen kompatibel sind. Durch die Integration von vSphere können Sie Ihre virtualisierte Umgebung effektiv managen.

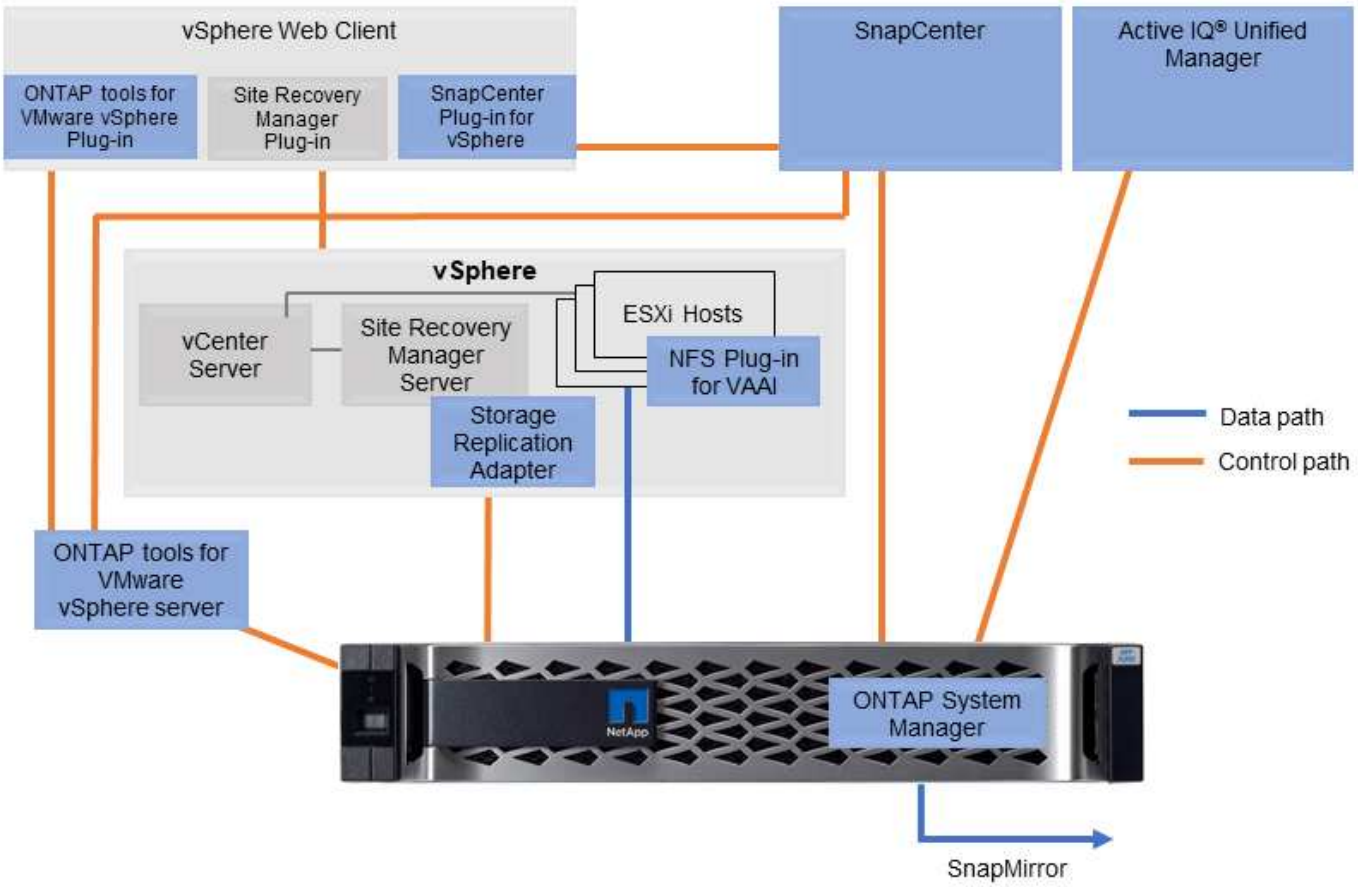
Die folgenden Tools sind ohne Aufpreis in der ONTAP One Lizenz enthalten. In Abbildung 1 sehen Sie eine Darstellung, wie diese Tools in Ihrer vSphere Umgebung zusammenarbeiten.

ONTAP Tools für VMware vSphere

"ONTAP Tools für VMware vSphere" Bietet eine Reihe von Tools zur Verwendung von ONTAP Storage zusammen mit vSphere. Das vCenter Plug-in, ehemals Virtual Storage Console (VSC), vereinfacht Storage-Management- und Effizienzfunktionen, verbessert die Verfügbarkeit und senkt die Storage-Kosten und den Betriebsaufwand – sei es bei SAN oder NAS. Dieses Plug-in nutzt Best Practices für die Bereitstellung von Datastores und optimiert ESXi Hosteinstellungen für NFS- und Block-Storage-Umgebungen. Wegen all dieser Vorteile empfiehlt NetApp, bei der Nutzung von vSphere mit Systemen mit ONTAP diese ONTAP Tools als Best Practice zu verwenden. Sie umfasst eine Server-Appliance, UI-Erweiterungen für vCenter, VASA Provider und Storage Replication Adapter. Nahezu alles in ONTAP Tools lässt sich mithilfe einfacher REST-APIs automatisieren – auch mit den meisten modernen Automatisierungs-Tools nutzbar.

- **VCenter UI-Erweiterungen.** Die UI-Erweiterungen der ONTAP Tools vereinfachen die Arbeit von Operations Teams und vCenter Administratoren, indem benutzerfreundliche, kontextabhängige Menüs für das Management von Hosts und Storage, Informationsportlets und native Alarmfunktionen direkt in die vCenter UI integriert werden, um optimierte Workflows zu erzielen.
- **VASA Provider für ONTAP.** der VASA Provider für ONTAP unterstützt das VMware vStorage APIs for Storage Awareness (VASA) Framework. Er wird im Rahmen von ONTAP Tools für VMware vSphere als eine einzelne virtuelle Appliance zur einfachen Implementierung bereitgestellt. VASA Provider verbindet vCenter Server mit ONTAP und erleichtert so die Bereitstellung und das Monitoring von VM-Storage. Es aktiviert die Unterstützung und das Management von Storage-Funktionsprofilen für VMware Virtual Volumes (VVols) und die VVols Performance für einzelne VMs sowie Alarme für die Monitoring-Kapazität und -Compliance mit den Profilen.
- **Speicherreplikationsadapter.** Der SRA wird zusammen mit VMware Live Site Recovery (VLSR)/Site Recovery Manager (SRM) verwendet, um die Datenreplikation zwischen Produktions- und Notfallwiederherstellungsstandorten mithilfe von SnapMirror für die Array-basierte Replikation zu verwalten. Es kann die Failover-Aufgabe im Katastrophenfall automatisieren und dabei helfen, die DR-Replikate unterbrechungsfrei zu testen, um das Vertrauen in Ihre DR-Lösung sicherzustellen.

In der folgenden Abbildung sind die ONTAP Tools für vSphere dargestellt.



SnapCenter Plug-in für VMware vSphere

Der "SnapCenter Plug-in für VMware vSphere" ist ein Plug-In für vCenter Server, mit dem Sie Backups und Wiederherstellungen von virtuellen Maschinen (VMs) und Datenspeichern verwalten können. Es bietet eine einzige Schnittstelle zum Verwalten von Backups, Wiederherstellungen und Klonen von VMs und Datenspeichern über mehrere ONTAP Systeme hinweg. SnapCenter unterstützt die Replikation auf und Wiederherstellung von sekundären Standorten mithilfe von SnapMirror. Die neuesten Versionen unterstützen auch SnapMirror zur Cloud (S3), manipulationssichere Snapshots, SnapLock und SnapMirror Active Sync. Das SnapCenter -Plug-In für VMware vSphere kann in SnapCenter -Anwendungs-Plug-Ins integriert werden, um anwendungskonsistente Backups bereitzustellen.

NFS-Plug-in für VMware VAAI

Das "NetApp NFS Plug-in für VMware VAAI" ist ein Plug-in für ESXi Hosts, mit dem diese VAAI Funktionen mit NFS-Datastores auf ONTAP verwenden können. Es unterstützt den Copy-Offload für Klonvorgänge, die Speicherplatzreservierung für Thick Virtual Disk Files und Snapshot Offload. Die Verlagerung von Kopiervorgängen in den Storage erfolgt nicht unbedingt schneller, sorgt aber dafür, dass die Anforderungen an die Netzwerkbandbreite reduziert werden und Host-Ressourcen wie CPU-Zyklen, Puffer und Warteschlangen verlagert werden. Sie können das Plug-in mithilfe von ONTAP Tools für VMware vSphere auf ESXi Hosts oder, sofern unterstützt, vSphere Lifecycle Manager (vLCM) installieren.

Premium-Softwareoptionen

Die folgenden Premium-Softwareprodukte sind von NetApp erhältlich. Sie sind nicht in der ONTAP One-Lizenz enthalten und müssen separat erworben werden.

- "NetApp Disaster Recovery (DR)"für VMware vSphere. Dies ist ein Cloud-basierter Dienst, der

Notfallwiederherstellung und Backup für VMware-Umgebungen bereitstellt. Es kann mit oder ohne SnapCenter verwendet werden und unterstützt On-Prem-zu-On-Prem-DR mithilfe von SAN oder NAS sowie On-Prem-zu/von der Cloud mithilfe von NFS, sofern unterstützt.

- "Einblicke in die Dateninfrastruktur (DII)". Dies ist ein Cloud-basierter Dienst, der Überwachung und Analyse für VMware-Umgebungen bereitstellt. Es unterstützt andere Speicheranbieter in heterogenen Speicherumgebungen sowie mehrere Switch-Anbieter und andere Hypervisoren. DII bietet umfassende End-to-End-Einblicke in die Leistung, Kapazität und Integrität Ihrer VMware-Umgebung.

Virtual Volumes (VVols) und richtlinienbasiertes Storage-Management (SPBM)

NetApp wurde erstmals im Jahr 2012 vorgestellt und war bereits ein früher Design-Partner von VMware bei der Entwicklung von VMware vSphere APIs for Storage Awareness (VASA), der Grundlage des Policy-basierten Storage-Managements (SPBM) für Enterprise Storage Arrays. Durch diesen Ansatz wurde das granulare VM-Storage-Management nur noch für VMFS und NFS Storage verfügbar.

Als Technology Design Partner lieferte NetApp Architektureingaben und kündigte 2015 Unterstützung für VVols an. Diese neue Technologie ermöglichte nun die Automatisierung der granularen und Array-nativen Storage-Bereitstellung über SPBM.

Virtuelle Volumes (VVols)

VVols sind eine revolutionäre Storage-Architektur, die das granulare Storage-Management von VMs ermöglicht. Dadurch lässt sich Storage nicht nur pro VM (einschließlich VM-Metadaten) managen, sondern sogar pro VMDK. VVols sind eine Kernkomponente der Strategie des Software Defined Data Center (SDDC), die die Grundlage von VMware Cloud Foundation (VCF) bildet und eine effizientere und skalierbarere Storage-Architektur für virtualisierte Umgebungen bietet.

VVols ermöglichen VMs die Storage-Nutzung pro VM, da jedes VM Storage-Objekt in NetApp ONTAP eine eindeutige Einheit ist. Bei ASA r2-Systemen, für die kein Volume-Management mehr erforderlich ist, ist daher jedes VM-Speicherobjekt eine eindeutige Storage-Einheit (SU) auf dem Array und kann unabhängig gesteuert werden. Dadurch können Storage-Richtlinien erstellt werden, die auf einzelne VMs oder VMDKs (und somit auf einzelne Sus) angewendet werden können und granulare Kontrolle über Storage-Services wie z. B. Performance, Verfügbarkeit und Datensicherung bieten.

Storage Policy Based Management (SPBM)

SPBM bietet ein Framework, das als Abstraktionsebene zwischen den für Ihre Virtualisierungsumgebung verfügbaren Storage-Services und den über Richtlinien bereitgestellten Storage-Elementen dient. Storage-Architekten können mit diesem Ansatz Storage-Pools mit unterschiedlichen Funktionen entwerfen. Diese Pools können von VM-Administratoren problemlos genutzt werden. Administratoren können dann die Workload-Anforderungen der Virtual Machine an die bereitgestellten Storage-Pools anpassen. Dieser Ansatz vereinfacht das Storage-Management und ermöglicht eine effizientere Nutzung der Storage-Ressourcen.

SPBM ist eine zentrale Komponente von VVols und bietet ein richtlinienbasiertes Framework für das Management von Storage-Services. Die Richtlinien werden von vSphere Administratoren anhand von Regeln und Funktionen erstellt, die vom VASA Provider (VP) des Anbieters offengelegt werden. Richtlinien für verschiedene Storage-Services wie Performance, Verfügbarkeit und Datensicherung können erstellt werden. Richtlinien können individuellen VMs oder VMDKs zugewiesen werden, wodurch Storage-Services granular kontrolliert werden können.

NetApp ONTAP und VVols

Bei VVols ist NetApp ONTAP eine der führenden Lösungen in der Storage-Branche, da es Hunderttausende VVols in einem einzigen Cluster unterstützt*. Im Gegensatz dazu unterstützen Anbieter von Enterprise-Arrays und kleineren Flash-Arrays nur wenige Tausend VVols pro Array. ONTAP bietet eine skalierbare und effiziente Storage-Lösung für VMware vSphere Umgebungen, die VVols mit einer umfassenden Auswahl an Storage-Services unterstützt, darunter Datendeduplizierung, Komprimierung, Thin Provisioning und Datensicherung. SPBM ermöglicht die nahtlose Integration mit VMware vSphere Umgebungen.

Zuvor haben wir erwähnt, dass VM-Administratoren Kapazitäten als Storage-Pools belegen können. Dies wird durch die Verwendung von Storage-Containern erreicht, die in vSphere als logische Datastores dargestellt werden.

Storage-Container werden von Storage-Administratoren erstellt und gruppiert, um Storage-Ressourcen zu gruppieren, die von VM-Administratoren belegt werden können. Storage-Container können je nach verwendetem ONTAP-System unterschiedlich erstellt werden. Bei einem herkömmlichen ONTAP 9 Cluster werden Containern ein oder mehrere FlexVol-Volumes zugewiesen, die gemeinsam den Storage-Pool bilden. Bei ASA r2-Systemen ist der gesamte Cluster der Storage-Pool.

Weitere Informationen zu VMware vSphere Virtual Volumes, SPBM und ONTAP finden Sie unter "TR-4400: VMware vSphere Virtual Volumes with ONTAP".

*Abhängig von Plattform und Protokoll

Datenspeicher und Protokolle

Übersicht über vSphere Datastore- und Protokollfunktionen

Sechs Protokolle können für die Anbindung von VMware vSphere an Datastores auf einem System mit ONTAP genutzt werden:

- FCP
- NVMe/FC
- NVMe/TCP
- ISCSI
- NFS v3
- NFS 4.1

FCP, NVMe/FC, NVMe/TCP und iSCSI sind Blockprotokolle, die das vSphere Virtual Machine File System (VMFS) verwenden, um VMs in ONTAP LUNs oder NVMe-Namespaces, die in einem ONTAP FlexVol volume enthalten sind, zu speichern. NFS ist ein File-Protokoll. Hierbei werden die Datastores nicht zusätzlich mit VMFS formatiert. VMs laufen direkt auf dem ONTAP Volume. SMB (CIFS), iSCSI, NVMe/TCP oder NFS kann direkt aus einem Gastbetriebssystem für ONTAP genutzt werden.

In der folgenden Tabelle sind die Funktionen herkömmlicher Datastores dargestellt ONTAP, die von vSphere unterstützt werden. Diese Informationen gelten nicht für VVols Datastores, sie gelten jedoch im Allgemeinen für vSphere 6.x bzw. neuere Versionen, bei denen unterstützte ONTAP Versionen verwendet werden. Im können Sie auch "Tool „VMware Konfigurationsmaxima“"Informationen zu bestimmten vSphere Versionen einsehen, um bestimmte Limits zu überprüfen.

Funktion/Feature	FC	ISCSI	NVMe-of	NFS
Formatieren	VMFS oder Raw Device Mapping (RDM)	VMFS oder RDM	VMFS	k. A.
Maximale Anzahl an Datastores oder LUNs	1024 LUNs pro Host	1024 LUNs pro Server	256 Namespeces pro Server	256 NFS-Verbindungen pro Host (betroffen von nconnect und Session Trunking) Standard-NFS. MaxVolumes ist 8. Erhöhen Sie mit den ONTAP Tools für VMware vSphere auf 256.
Maximale Datastore-Größe	64 TB	64 TB	64 TB	300 TB FlexVol Volume oder mehr mit FlexGroup Volume
Maximale Datastore-Dateigröße	62 TB	62 TB	62 TB	62 TB mit ONTAP 9.12.1P2 und höher
Optimale „Queue depth“ pro LUN oder Filesystem	64-256	64-256	Autonegotiation Ist Eingeschaltet	Siehe NFS.MaxQueueDepth in "Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen".

In der folgenden Tabelle sind die unterstützten Funktionen in Bezug auf VMware Storage aufgeführt.

Kapazität/Funktion	FC	ISCSI	NVMe-of	NFS
VMotion	Ja.	Ja.	Ja.	Ja.
Storage vMotion	Ja.	Ja.	Ja.	Ja.
VMware HA	Ja.	Ja.	Ja.	Ja.
Storage Distributed Resource Scheduler (SDRS)	Ja.	Ja.	Ja.	Ja.
VMware vStorage APIs for Data Protection (VADP)-fähige Backup-Software	Ja.	Ja.	Ja.	Ja.

Kapazität/Funktion	FC	ISCSI	NVMe-of	NFS
Microsoft Cluster Service (MSCS) oder Failover Clustering in einer VM	Ja.	Ja [1]	Ja [1]	Nicht unterstützt
Fehlertoleranz	Ja.	Ja.	Ja.	Ja.
Live Site Recovery/Site Recovery Manager	Ja.	Ja.	Nein [2]	V3 nur [2]
VMs (virtuelle Festplatten) mit Thin Provisioning	Ja.	Ja.	Ja.	Ja. Diese Einstellung ist der Standard für alle VMs im NFS, wenn nicht VAAI verwendet wird.
Natives VMware Multipathing	Ja.	Ja.	Ja.	Für das NFS v4.1 Session-Trunking ist ONTAP 9.14.1 und höher erforderlich

In der folgenden Tabelle werden die unterstützten ONTAP Storage-Managementfunktionen aufgeführt.

Funktion/Feature	FC	ISCSI	NVMe-of	NFS
Datendeduplizierung	Einsparungen im Array	Einsparungen im Array	Einsparungen im Array	Einsparungen im Datastore
Thin Provisioning	Datenspeicher oder RDM	Datenspeicher oder RDM	Datenspeicher	Datenspeicher
Datenspeichergröße ändern	Erweitern Sie nur	Erweitern Sie nur	Erweitern Sie nur	Vergrößerung, Autogrow und Verkleinerung
SnapCenter Plug-ins für Windows, Linux Applikationen (in Gast-BS)	Ja.	Ja.	Ja.	Ja.
Monitoring und Host-Konfiguration mit ONTAP Tools für VMware vSphere	Ja.	Ja.	Ja.	Ja.
Bereitstellung mit ONTAP Tools für VMware vSphere	Ja.	Ja.	Ja.	Ja.

In der folgenden Tabelle sind die unterstützten Backup-Funktionen aufgeführt.

Funktion/Feature	FC	ISCSI	NVMe-of	NFS
ONTAP Snapshots	Ja.	Ja.	Ja.	Ja.
Durch replizierte Backups unterstütztes SRM	Ja.	Ja.	Nein [2]	V3 nur [2]
Volume SnapMirror	Ja.	Ja.	Ja.	Ja.
VDMK Image-Zugriff	Backup-Software für SnapCenter und VADP	Backup-Software für SnapCenter und VADP	Backup-Software für SnapCenter und VADP	SnapCenter- und VADP-fähige Backup-Software, vSphere Client und vSphere Web Client Datastore-Browser
VDMK-Zugriff auf Dateiebene	SnapCenter- und VADP-fähige Backup-Software, nur Windows	SnapCenter- und VADP-fähige Backup-Software, nur Windows	SnapCenter- und VADP-fähige Backup-Software, nur Windows	Backup-Software und Applikationen von Drittanbietern, die SnapCenter und VADP unterstützt
NDMP-Granularität	Datenspeicher	Datenspeicher	Datenspeicher	Datastore oder VM

[1] **NetApp empfiehlt** die Verwendung von in-Guest iSCSI für Microsoft Cluster anstelle von VMDKs mit Multiwriter-Aktivierung in einem VMFS Datastore. Dieser Ansatz wird von Microsoft und VMware vollständig unterstützt. Er bietet mit ONTAP ein hohes Maß an Flexibilität (SnapMirror auf ONTAP Systeme vor Ort oder in der Cloud), lässt sich leicht konfigurieren und automatisieren und kann mit SnapCenter gesichert werden. VSphere 7 bietet außerdem eine neue Clustered VMDK-Option. Dies unterscheidet sich von VMDKs mit Multiwriter-Funktion, die einen VMFS 6 Datastore mit aktivierter Clustered VMDK-Unterstützung benötigen. Weitere Einschränkungen sind möglich. Konfigurationsrichtlinien finden Sie in der Dokumentation von VMware"Einrichtung für Windows Server Failover Clustering".

[2] Datastores, die NVMe-of und NFS v4.1 verwenden, erfordern eine vSphere-Replizierung. Die Array-basierte Replizierung für NFS v4.1 wird derzeit von SRM nicht unterstützt. Die Array-basierte Replizierung mit NVMe-of wird derzeit nicht von den ONTAP Tools für den VMware vSphere Storage Replication Adapter (SRA) unterstützt.

Auswahl eines Storage-Protokolls

Systeme mit ONTAP unterstützen alle wichtigen Storage-Protokolle, sodass die Kunden abhängig von der vorhandenen und geplanten Netzwerkinfrastruktur und den Fähigkeiten der Mitarbeiter das für ihre Umgebung am besten geeignete Protokoll auswählen können. In der Vergangenheit zeigten NetApp-Tests im Allgemeinen nur geringe Unterschiede zwischen Protokollen, die mit ähnlichen Übertragungsgeschwindigkeiten ausgeführt werden, und der Anzahl der Verbindungen. NVMe-of (NVMe/TCP und NVMe/FC) bietet jedoch einen bemerkenswerten Anstieg bei den IOPS, eine Verringerung der Latenz und eine Reduzierung des Host-CPU-Verbrauchs um bis zu 50 % und mehr durch Storage-I/O. Auf der anderen Seite bietet NFS die höchste Flexibilität und ein einfaches Management, besonders bei einer großen Anzahl von VMs. All diese Protokolle können mit ONTAP Tools für VMware vSphere genutzt und gemanagt werden, wodurch Datastores einfach über eine Benutzeroberfläche erstellt und gemanagt werden können.

Die folgenden Faktoren könnten bei Überlegungen zur Auswahl eines Protokolls hilfreich sein:

- **Aktuelle Betriebsumgebung.** Obwohl IT-Teams normalerweise erfahren im Management von Ethernet-IP-Infrastrukturen sind, haben nicht alle die Kompetenz, eine FC-SAN-Fabric zu managen. Die Nutzung eines nicht auf Storage-Traffic ausgelegten dedizierten IP-Netzwerks ist jedoch unter Umständen keine gute

Lösung. Berücksichtigen Sie Ihre vorhandene Netzwerkinfrastruktur, alle geplanten Optimierungen sowie die Fähigkeiten und die Verfügbarkeit von Mitarbeitern, die diese managen.

- **Einfache Einrichtung.** über die Erstkonfiguration der FC-Fabric hinaus (zusätzliche Switches und Kabel, Zoning und die Verifizierung der Interoperabilität von HBA und Firmware) müssen Blockprotokolle auch LUNs erstellen und zuordnen sowie vom Gastbetriebssystem Erkennung und Formatierung vornehmen. Nach der Erstellung und dem Export der NFS-Volumes werden sie vom ESXi Host gemountet und sind dann betriebsbereit. Für NFS sind keine besonderen Hardwarequalifizierungen oder Firmware für das Management erforderlich.
- **Einfaches Management.** Falls bei SAN-Protokollen mehr Speicherplatz erforderlich ist, müssen verschiedene Schritte durchgeführt werden. Dazu gehören das vergrößern einer LUN, das erneute Scannen zur Ermittlung der neuen Größe und das anschließende Wachstum des Filesystems.) Eine LUN kann erweitert werden, aber eine Reduzierung der Größe einer LUN ist es nicht. NFS ermöglicht eine problemlose Größenanpassung, die durch das Storage-System automatisiert werden kann. SAN bietet eine Rückgewinnung von Speicherplatz über Befehle des Gast-OS, die ZUORDNUNG/TRIM/UNMAP ermöglichen. So kann Speicherplatz von gelöschten Dateien wieder an das Array zurückgegeben werden. Diese Art von Speicherplatzrückgewinnung ist bei NFS-Datenspeichern nicht schwierig möglich.
- **Storage-Speicherplatztransparenz.** die Storage-Auslastung ist in NFS-Umgebungen in der Regel einfacher zu erkennen, da Thin Provisioning unmittelbare Einsparungen ermöglicht. In ähnlicher Form sind Einsparungen durch Deduplizierung und Klonen unmittelbar für andere VMs im selben Datastore oder für Storage-System-Volumes verfügbar. Die VM-Dichte ist typischerweise ebenfalls größer als in einem NFS-Datastore. Hierdurch können höhere Einsparungen bei der Deduplizierung sowie eine Senkung der Managementkosten erzielt werden, da weniger Datastores gemanagt werden müssen.

Datenspeicher-Layout

ONTAP Storage-Systeme bieten beim Erstellen von Datastores für VMs und virtuelle Festplatten ein hohes Maß an Flexibilität. Wenn Datastores für vSphere mit ONTAP Tools bereitgestellt werden, werden viele ONTAP Best Practices angewendet (siehe Abschnitt "Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen"). Darüber hinaus sind einige zusätzliche Richtlinien zu berücksichtigen:

- Der Einsatz von vSphere mit ONTAP-NFS-Datastores sorgt für eine hochperformante, einfach zu managende Implementierung mit VM/Datastore-Verhältnissen, die mit blockbasierten Storage-Protokollen nicht erreicht werden können. Diese Architektur kann zu einer Verzehnfachung der Datastore-Dichte und einer damit korrelierenden Verringerung der Datastore-Anzahl führen. Obwohl ein größerer Datastore die Storage-Effizienz begünstigen und betriebliche Vorteile bieten kann, sollten Sie mindestens vier Datastores (FlexVol Volumes) pro Node verwenden. Durch die ONTAP Verteilung der Datastores auf die Controller kann so die bestmögliche Ausnutzung der Hardware erreicht werden. Mit diesem Ansatz können Sie auch Datastores mit unterschiedlichen Recovery-Richtlinien erstellen. Einige können je nach den geschäftlichen Anforderungen häufiger gesichert oder repliziert werden als andere. Da FlexGroup Volumes eine Skalierung pro Design durchführen, sind für mehrere Datastores nicht erforderlich.
- **NetApp empfiehlt** die Verwendung von FlexVol-Volumes für die meisten NFS-Datastores. Ab ONTAP 9.8 werden FlexGroup Volumes auch für die Nutzung als Datastores unterstützt und für bestimmte Anwendungsfälle im Allgemeinen empfohlen. Andere ONTAP Storage-Container wie qtrees werden im Allgemeinen nicht empfohlen, da diese derzeit weder durch ONTAP Tools für VMware vSphere noch durch das NetApp SnapCenter Plug-in für VMware vSphere unterstützt werden.
- Eine gute Größe für einen FlexVol Volume-Datastore liegt bei etwa 4 TB bis 8 TB. Diese Größe bildet einen guten Ausgleichspunkt im Hinblick auf Performance, einfaches Management und Datensicherung. Beginnen Sie mit einem kleinen Datastore (beispielsweise 4 TB) und vergrößern Sie diesen nach Bedarf (bis auf maximal 300 TB). Kleinere Datenspeicher lassen sich nach einem Backup oder nach einem Ausfall schneller wiederherstellen und können schnell im Cluster verschoben werden. Die automatische Größenanpassung von ONTAP kann sinnvoll sein, um das Volume bei wechselnder Speicherplatzbelegung automatisch zu vergrößern oder zu verkleinern. Der ONTAP-Assistent für die Bereitstellung von VMware

vSphere Datastores verwendet standardmäßig Autosize für neue Datastores. Eine weitere Anpassung der Vergrößerungs- und Verkleinerungsschwellenwerte sowie der maximalen und minimalen Größe kann mit System Manager oder über die Befehlszeile erfolgen.

- Alternativ können VMFS Datastores mit LUNs oder NVMe-Namespaces (so genannte Storage-Einheiten in neuen ASA-Systemen) konfiguriert werden, auf die FC, iSCSI, NVMe/FC oder NVMe/TCP zugreifen. Bei VMFS können alle ESX Server in einem Cluster gleichzeitig auf Datenspeicher zugreifen. VMFS Datastores können eine Größe von bis zu 64 TB haben und bestehen aus bis zu 32 2TB LUNs (VMFS 3) oder einer einzelnen 64-TB-LUN (VMFS 5). Die maximale LUN-Größe von ONTAP beträgt auf AFF-, ASA- und FAS-Systemen 128 TB. NetApp empfiehlt immer, für jeden Datastore eine einzelne, große LUN zu verwenden, anstatt zu versuchen, Extents zu verwenden. Analog zu dem NFS Ansatz, verteilen Sie ebenfalls die Datastores (Volumes oder Storage-Einheiten), um die Performance auf einem einzelnen ONTAP Controller zu maximieren.
- Ältere Gastbetriebssysteme (OS) mussten an das Storage-System angeglichen werden (Alignment), um die bestmögliche Performance und Storage-Effizienz zu erzielen. Bei modernen Betriebssystemen mit Anbieterunterstützung von Microsoft und Linux Distributoren wie Red hat sind jedoch keine Anpassungen mehr erforderlich, um die Filesystem-Partition mit den Blöcken des zugrunde liegenden Storage-Systems in einer virtuellen Umgebung zu alignen. Wenn Sie ein altes Betriebssystem verwenden, für das unter Umständen ein Alignment erforderlich ist, suchen Sie in der NetApp Support Knowledgebase nach Artikeln, in denen VM Alignment verwendet wird, oder fordern Sie bei einem NetApp Ansprechpartner für den Vertrieb oder für Partner ein Exemplar des technischen Berichts TR-3747 an.
- Vermeiden Sie die Verwendung von Defragmentierungsprogrammen innerhalb des Gast-Betriebssystems, da dies keinen Performance-Vorteil bietet und die Speichereffizienz und Snapshot-Speicherplatznutzung beeinträchtigt. Zudem sollten Sie die Suchindizierung im Gastbetriebssystem für virtuelle Desktops deaktivieren.
- ONTAP ist eines der branchenweit führenden Unternehmen mit innovativen Storage-Effizienzfunktionen, mit denen Sie Ihren nutzbaren Festplattenspeicherplatz maximal ausschöpfen können. AFF Systeme sind durch Inline-Deduplizierung und -Komprimierung sogar noch effizienter. Die Daten werden über alle Volumes hinweg in einem Aggregat dedupliziert. Daher müssen zur Maximierung der Einsparungen keine ähnlichen Betriebssysteme und ähnlichen Applikationen in einem einzelnen Datastore mehr gruppieren.
- In einigen Fällen benötigen Sie eventuell nicht einmal einen Datastore. Die Filesystems des Gastsystems wie NFS, SMB, NVMe/TCP oder iSCSI werden vom Gastsystem gemanagt. Eine Anleitung zu bestimmten Applikationen finden Sie in den technischen Berichten von NetApp für die jeweilige Applikation. Beispielsweise "Oracle-Datenbanken auf ONTAP"enthält einen Abschnitt zur Virtualisierung mit nützlichen Details.
- Festplatten der ersten Klasse (oder verbesserte virtuelle Festplatten) ermöglichen über vCenter gemanagte Festplatten unabhängig von einer VM mit vSphere 6.5 und höher. Sie werden zwar primär durch API gemanagt, sind aber auch mit VVols nützlich, insbesondere bei dem Management mit OpenStack oder Kubernetes-Tools. Sie werden von ONTAP unterstützt sowie ONTAP Tools für VMware vSphere.

Datastore und VM-Migration

Wenn Sie VMs aus einem bestehenden Datastore in einem anderen Storage-System zu ONTAP migrieren, sollten Sie die folgenden Praktiken berücksichtigen:

- Verwenden Sie Storage vMotion, um den Großteil Ihrer Virtual Machines in ONTAP zu verschieben. Dieser Ansatz ermöglicht nicht nur einen unterbrechungsfreien Betrieb der VMs, sondern auch die Nutzung von ONTAP Storage-Effizienzfunktionen wie Inline-Deduplizierung und -Komprimierung zur Verarbeitung der Daten während der Migration. Es empfiehlt sich unter Umständen, mithilfe von vCenter Funktionen mehrere VMs aus der Bestandsliste auszuwählen und die Migration dann zu einem geeigneten Zeitpunkt zu planen (dazu klicken Sie mit gedrückter Strg-Taste auf „Actions“).

- Sie können eine Migration auf geeignete Ziel-Datastores zwar genau planen, doch es ist oft einfacher, große Datenmengen zu migrieren und diese anschließend nach Bedarf zu organisieren. Vielleicht möchten Sie diesen Ansatz nutzen, um Ihre Migration in verschiedene Datastores zu steuern, wenn Sie spezielle Datensicherungsanforderungen, z. B. unterschiedliche Snapshot Zeitpläne, haben. Sobald sich die VMs im NetApp Cluster befinden, kann Storage vMotion VAAI Offloads verwenden, um VMs zwischen Datastores im Cluster zu verschieben, ohne dass eine Host-basierte Kopie erforderlich ist. Beachten Sie, dass NFS Storage vMotion nicht auslagert, wenn VMs eingeschaltet sind, VMFS hingegen.
- Virtual Machines, bei denen eine präzisere Migration erforderlich ist, sind unter anderem Datenbanken und Applikationen mit Nutzung von Attached Storage. Bei diesen sollten Sie die Migration im Allgemeinen mit den Applikationstools managen. Für Oracle empfiehlt sich zur Migration der Datenbankdateien die Nutzung von Oracle-Tools wie RMAN oder ASM. Weitere Informationen finden Sie unter "Migration von Oracle Datenbanken auf ONTAP Storage-Systeme" . Ganz ähnlich kommen für SQL Server entweder SQL Server Management Studio oder NetApp Tools wie SnapManager für SQL Server oder SnapCenter in Betracht.

ONTAP Tools für VMware vSphere

Wenn Sie vSphere mit Systemen mit ONTAP verwenden, ist es eine Best Practice, das ONTAP Tools für VMware vSphere Plug-in (früher Virtual Storage Console) zu installieren und zu verwenden. Dieses vCenter Plug-in vereinfacht das Storage-Management, steigert die Verfügbarkeit und senkt die Storage-Kosten und den Betriebsaufwand – sei es bei SAN oder NAS, auf ASA, AFF, FAS oder sogar ONTAP Select (eine softwaredefinierte Version von ONTAP, die in einer VMware oder KVM VM ausgeführt wird). Dieses Plug-in nutzt Best Practices für die Bereitstellung von Datastores und optimiert die ESXi Hosteinstellungen für Multipath- und HBA-Timeouts (diese sind in Anhang B beschrieben). Da es sich um ein vCenter Plug-in handelt, ist es für alle vSphere Webclients verfügbar, die eine Verbindung mit dem vCenter Server herstellen.

Das Plug-in hilft Ihnen auch bei der Nutzung anderer ONTAP Tools in vSphere Umgebungen. Damit können Sie das NFS-Plug-in für VMware VAAI installieren, das einen Copy-Offload zu ONTAP für VM-Klonvorgänge, eine Speicherplatzreservierung für Thick Virtual Disk Files und ONTAP Snapshot Offload ermöglicht.

> Auf abbildbasierten vSphere-Clustern sollten Sie das NFS-Plug-in dennoch zu Ihrem Image hinzufügen, damit die Compliance bei der Installation mit ONTAP-Tools nicht darunter fällt.

ONTAP Tools sind auch die Managementoberfläche für viele Funktionen von VASA Provider für ONTAP und unterstützen das richtlinienbasierte Storage-Management mit VVols.

Im Allgemeinen empfiehlt **NetApp** die Verwendung der Schnittstelle ONTAP Tools für VMware vSphere in vCenter zur Bereitstellung herkömmlicher und VVols Datastores, um die Einhaltung von Best Practices sicherzustellen.

Allgemeines Networking

Wenn Sie vSphere mit Systemen mit ONTAP verwenden, ist die Konfiguration von Netzwerkeinstellungen einfach und erfolgt ähnlich wie andere Netzwerkkonfigurationen. Folgende Punkte sind dabei zu berücksichtigen:

- Separater Storage-Netzwerk-Traffic aus anderen Netzwerken. Ein separates Netzwerk kann mithilfe eines dedizierten VLANs oder separater Switches für Storage eingerichtet werden. Falls im Storage-Netzwerk physische Pfade wie Uplinks geteilt werden, sind eventuell QoS oder zusätzliche Uplink-Ports erforderlich, um eine ausreichende Bandbreite sicherzustellen. Stellen Sie keine direkte Verbindung zwischen Hosts und Storage her. Verwenden Sie Switches, um redundante Pfade zu verwenden und VMware HA ohne Eingriff von Microsoft HA zu arbeiten. Siehe "Direkte Netzwerkverbindung" Finden Sie weitere Informationen.
- Jumbo Frames können genutzt werden, sofern dies gewünscht ist und von Ihrem Netzwerk unterstützt

wird, insbesondere bei Verwendung von iSCSI. Vergewissern Sie sich bei ihrem Einsatz, dass sie auf allen Netzwerkgeräten, VLANs etc. Im Pfad zwischen Storage und dem ESXi Host gleich konfiguriert sind. Anderenfalls kann es zu Performance- oder Verbindungsproblemen kommen. Auf dem virtuellen ESXi Switch, dem VMkernel Port, sowie den physischen Ports oder den Interface Groups muss für jeden ONTAP Node auch jeweils dieselbe MTU festgelegt sein.

- NetApp empfiehlt eine Deaktivierung der Netzwerk- Flusssteuerung nur an den Cluster-Interconnect-Ports innerhalb eines ONTAP Clusters. Für die übrigen Netzwerkports, die für Daten-Traffic verwendet werden, gibt NetApp im Hinblick auf Best Practices keine weiteren Empfehlungen. Diese Ports sollten Sie nach Bedarf aktivieren oder deaktivieren. Weitere Informationen zur Flusssteuerung finden Sie unter "TR-4182".
- Wenn ESXi- und ONTAP-Speicher-Arrays mit Ethernet-Speichernetzwerken verbunden werden, empfiehlt **NetApp** die Konfiguration der Ethernet-Ports, mit denen diese Systeme verbunden werden, als RSTP-Edge-Ports (Rapid Spanning Tree Protocol) oder mit der Cisco-PortFast-Funktion. **NetApp empfiehlt** die Aktivierung der Spanning-Tree PortFast Trunk-Funktion in Umgebungen, in denen die Cisco PortFast-Funktion verwendet wird und die 802.1Q VLAN-Trunking entweder für den ESXi-Server oder die ONTAP-Speicher-Arrays aktiviert haben.
- **NetApp empfiehlt** die folgenden Best Practices für die Link Aggregation:
  - Verwenden Sie Switches, die die Link-Aggregation von Ports in zwei separaten Switch-Chassis durch einen Ansatz mit einer Multi-Chassis-Link-Aggregationsgruppe wie Virtual PortChannel (vPC) von Cisco unterstützen.
  - Deaktivieren Sie LACP für mit ESXi verbundene Switch Ports, es sei denn, Sie verwenden dvSwitches ab 5.1 mit konfiguriertem LACP.
  - Erstellen Sie mit LACP Link-Aggregate für ONTAP Storage-Systeme mit dynamischen Multimode-Schnittstellengruppen mit Port- oder IP-Hash. Siehe "Netzwerkmanagement" Für weitere Hinweise.
  - Verwenden Sie eine IP-Hash-Teaming-Richtlinie für ESXi bei Verwendung von statischer Link-Aggregation (z. B. EtherChannel) und Standard-vSwitches oder LACP-basierter Link-Aggregation mit vSphere Distributed Switches. Wenn die Link-Aggregation nicht verwendet wird, verwenden Sie stattdessen „Weiterleiten basierend auf der ursprünglichen virtuellen Port-ID“.

SAN (FC, FCoE, NVMe/FC, iSCSI), RDM

Mit vSphere gibt es vier Möglichkeiten, Block-Storage-Geräte zu nutzen:

- Mit VMFS Datastores
- Mit Raw Device Mapping (RDM)
- Als eine über iSCSI verbundene LUN oder ein NVMe/TCP-verbundener Namespace, auf den ein Software-Initiator über ein VM-Gastbetriebssystem zugegriffen und gesteuert wird
- Als VVols Datastore

VMFS ist ein hochperformantes geclustertes Filesystem, das Datastores bereitstellt, bei denen es sich um Shared-Storage-Pools handelt. VMFS Datastores können mit LUNs konfiguriert werden, auf die über FC, iSCSI, FCoE zugegriffen wird. Zudem können NVMe-Namespaces, auf die über NVMe/FC- oder NVMe/TCP-Protokolle zugegriffen wird, verwendet werden. Bei VMFS können alle ESX Server in einem Cluster gleichzeitig auf den Speicher zugreifen. Die maximale LUN-Größe beträgt normalerweise 128 TB ab ONTAP 9.12.1P2 (und früher bei ASA Systemen). Daher kann ein VMFS 5 oder ein Datastore mit einer maximalen Größe von 6 TB mit einer einzigen LUN erstellt werden.

Extents sind ein vSphere Speicherkonzept, in dem Sie mehrere LUNs „zusammenfügen“ können, um einen einzelnen größeren Datastore zu erstellen. Sie sollten niemals Extents verwenden, um die gewünschte Datastore-Größe zu erreichen. Eine einzelne LUN ist die Best Practice für einen VMFS Datastore.

VSphere bietet integrierte Unterstützung für mehrere Pfade zu Speichergeräten. VSphere kann den Typ des Speichergeräts für unterstützte Speichersysteme erkennen und konfiguriert automatisch den Multipathing-Stack zur Unterstützung der Funktionen des verwendeten Speichersystems, zur Unterstützung der Regarldess des verwendeten Protokolls oder bei Verwendung von ASA, AFF, FAS oder softwaredefiniertem ONTAP.

Sowohl vSphere als auch ONTAP unterstützen Asymmetric Logical Unit Access (ALUA) zur Einrichtung von aktiv-/optimierten und aktiv-/nicht-optimierten Pfaden für Fibre Channel und iSCSI sowie Asymmetric Namespace Access (ANA) für NVMe-Namespaces unter Verwendung von NVMe/FC und NVMe/TCP. In ONTAP folgt ein ALUA- oder ANA-optimierter Pfad auf einen direkten Datenpfad. Dabei wird ein Zielport auf dem Node verwendet, der die LUN oder den Namespace hostet, auf die zugegriffen wird. ALUA/ANA ist sowohl in vSphere als auch in ONTAP standardmäßig aktiviert. Die Multipathing-Software in vSphere erkennt den ONTAP Cluster als ALUA oder ANA und verwendet das entsprechende native Plug-in zur Round-Robin-Load-Balancing-Richtlinie.

Bei den ASA Systemen von NetApp werden die LUNs und Namespaces den ESXi Hosts mit symmetrisches Pathing bereitgestellt. Das bedeutet, dass alle Pfade aktiv und optimiert sind. Die Multipathing-Software in vSphere erkennt das ASA System als symmetrisch und verwendet das entsprechende native Plug-in für die Richtlinie zum Round Robin-Lastausgleich.

Weitere Informationen zu optimierten Multipathing-Einstellungen finden Sie unter"Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen".

ESXi erkennt keine LUNs, Namespaces oder Pfade, die über seine Grenzen hinausgehen. In einem größeren ONTAP Cluster ist es möglich, dass das Pfadlimit vor dem LUN-Limit erreicht wird. Zur Beseitigung dieser Beschränkung unterstützt ONTAP ab Version 8.3 die selektive LUN-Zuordnung (Selective LUN Map, SLM).

In finden Sie die "Tool „VMware Konfigurationsmaxima“"aktuellsten unterstützten Grenzwerte in ESXi.

SLM beschränkt die Nodes, die Pfade an eine bestimmte LUN weitergeben. Als NetApp Best Practice wird empfohlen, pro Node pro SVM mindestens zwei LIFs zu verwenden und SLM zu verwenden, um die weitergegebenen Pfade auf den Node zu beschränken, der die LUN hostet, und auf seinen HA-Partner. Es sind zwar noch andere Pfade vorhanden, doch werden diese standardmäßig nicht weitergegeben. Die weitergegebenen Pfade können mit den Node-Argumenten zum Hinzufügen oder Entfernen der Berichterstellung in SLM geändert werden. Beachten Sie, dass in Versionen vor 8.3 erstellte LUNs alle Pfade weitergeben. Sie müssen geändert werden, damit nur die Pfade zum Hosting-HA-Paar weitergegeben werden. Weitere Informationen zu SLM finden Sie in Abschnitt 5.9 von "TR-4080". Um die für eine LUN verfügbaren Pfade weiter zu reduzieren, kann auch die frühere Portsatzmethode verwendet werden. Portsätze tragen dazu bei, die Anzahl der sichtbaren Pfade zu verringern, durch die Initiatoren in einer Initiatorgruppe LUNs ausfindig machen können.

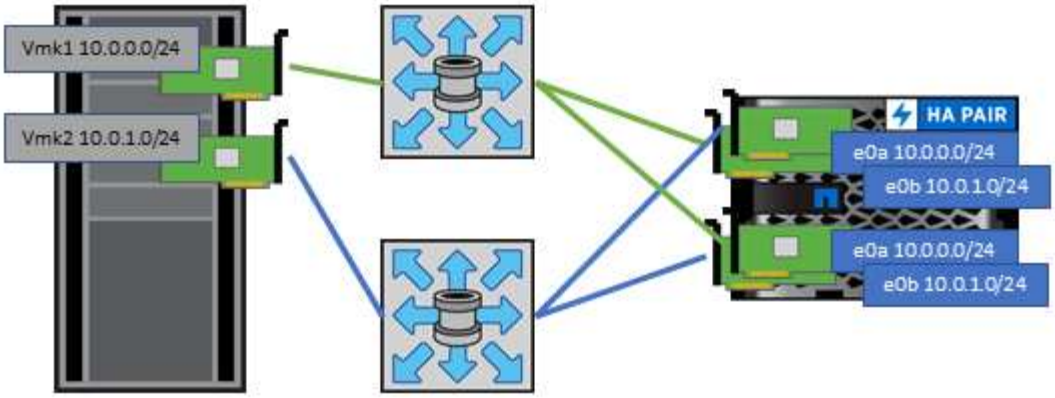
- SLM ist standardmäßig aktiviert. Sofern Sie keine Portsätze verwenden, ist keine weitere Konfiguration erforderlich.
- Für LUNs, die vor Data ONTAP 8.3 erstellt wurden, wenden Sie SLM manuell an. Dazu führen Sie den Befehl aus, um die LUN-Nodes für die Berichterstellung zu entfernen und den LUN-Zugriff auf den LUN-Eigentümer-Node und dessen HA-Partner zu beschränken. `lun mapping remove-reporting-nodes`

SCSI-basierte Blockprotokolle (iSCSI, FC und FCoE) greifen mithilfe von LUN-IDs und Seriennummern sowie

mit eindeutigen Namen auf LUNs zu. FC und FCoE verwenden weltweite Namen (WWNNs und WWPNs). ISCSI verwendet qualifizierte iSCSI-Namen (IQNs), um Pfade basierend auf LUN-zu-igroup-Zuordnungen festzulegen, die nach Portsätzen und SLM gefiltert sind. NVMe-basierte Block-Protokolle werden gemanagt, indem einem NVMe-Subsystem einen Namespace mit einer automatisch generierten Namespace-ID zugewiesen und dieses Subsystem dem NVMe Qualified Name (NQN) der Hosts zugeordnet wird. Unabhängig von FC oder TCP werden NVMe-Namespaces mit dem NQN und nicht mit dem WWPN oder WWNN zugeordnet. Der Host erstellt dann einen softwaredefinierten Controller, damit das zugeordnete Subsystem auf seine Namespaces zugreifen kann. Der Pfad zu LUNs und Namespaces in ONTAP hat für die Blockprotokolle keine Bedeutung und wird nirgendwo im Protokoll angegeben. Daher muss ein Volume, das nur LUNs enthält, nicht intern gemountet werden. Zudem ist für Volumes, die in Datastores verwendete LUNs enthalten, kein Verbindungspfad erforderlich.

Weitere Best Practices, die berücksichtigt werden sollten:

- Prüfen Sie"Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen", ob die von NetApp in Zusammenarbeit mit VMware empfohlenen Einstellungen vorhanden sind.
- Vergewissern Sie sich, dass für jede SVM auf jedem Node im ONTAP Cluster eine logische Schnittstelle (LIF) erstellt wird, um maximale Verfügbarkeit und Mobilität zu gewährleisten. Als Best Practice empfiehlt sich für ONTAP SANs die Verwendung von zwei physischen Ports und LIFs pro Node, einer für jede Fabric. Mit ALUA werden Pfade geparst und aktive optimierte (direkte) Pfade im Gegensatz zu aktiven nicht optimierten Pfaden identifiziert. ALUA wird für FC, FCoE und iSCSI verwendet.
- Nutzen Sie für iSCSI-Netzwerke mehrere VMkernel Netzwerkschnittstellen für verschiedene Subnetze mit NIC-Teaming, wenn mehrere virtuelle Switches vorhanden sind. Darüber hinaus können Sie mehrere physische NICs nutzen, die mit mehreren physischen Switches verbunden sind, um Hochverfügbarkeit und einen höheren Durchsatz bereitzustellen. Die folgende Abbildung zeigt ein Beispiel für Multipath-Konnektivität. Konfigurieren Sie in ONTAP entweder eine Single-Mode-Schnittstellengruppe für Failover mit zwei oder mehr Links, die mit zwei oder mehreren Switches verbunden sind, oder nutzen Sie LACP oder eine andere Link-Aggregationstechnologie mit Multimode-Schnittstellengruppen, um Hochverfügbarkeit und die Vorteile der Link-Aggregation bereitzustellen.
- Wenn das Challenge-Handshake Authentication Protocol (CHAP) in ESXi für die Zielauthentifizierung verwendet wird, muss es auch in ONTAP über die CLI konfiguriert werden (`vserver iscsi security create`) Oder mit System Manager (bearbeiten Sie die Initiatorsicherheit unter „Storage“ > „SVMs“ > „SVM-Einstellungen“ > „Protocols“ > „iSCSI“).
- Verwenden Sie ONTAP Tools für VMware vSphere, um LUNs und Initiatorgruppen zu erstellen und zu managen. Das Plug-in bestimmt automatisch die WWPNs von Servern und erstellt entsprechende Initiatorgruppen. Darüber hinaus konfiguriert er LUNs gemäß Best Practices und ordnet sie den richtigen Initiatorgruppen zu.
- Setzen Sie RDMs mit Bedacht ein, da ihr Management schwieriger sein kann. Zudem verwenden sie auch Pfade, die wie bereits beschrieben beschränkt sind. ONTAP LUNs unterstützen beide "Kompatibilitätsmodus für physischen und virtuellen Modus" RDMs:
- Weitere Informationen zur Verwendung von NVMe/FC mit vSphere 7.0 finden Sie im hier "ONTAP NVMe/FC-Host-Konfigurationsleitfaden" Und "TR-4684"Die folgende Abbildung zeigt die Multipath-Konnektivität von einem vSphere Host zu einer ONTAP LUN.



NFS

Bei ONTAP handelt es sich unter anderem um ein horizontal skalierbares NAS-Array der Enterprise-Klasse. ONTAP ermöglicht VMware vSphere den gleichzeitigen Zugriff auf NFS-verbundene Datastores von vielen ESXi Hosts und übertrifft dabei die für VMFS Dateisysteme auferlegten Grenzen bei Weitem. Die Verwendung von NFS mit vSphere bietet einige Vorteile in Bezug auf Benutzerfreundlichkeit, Storage-Effizienz und Sichtbarkeit, wie im Abschnitt erwähnt"Datenspeicher".

Für die Verwendung von ONTAP NFS mit vSphere werden folgende Best Practices empfohlen:

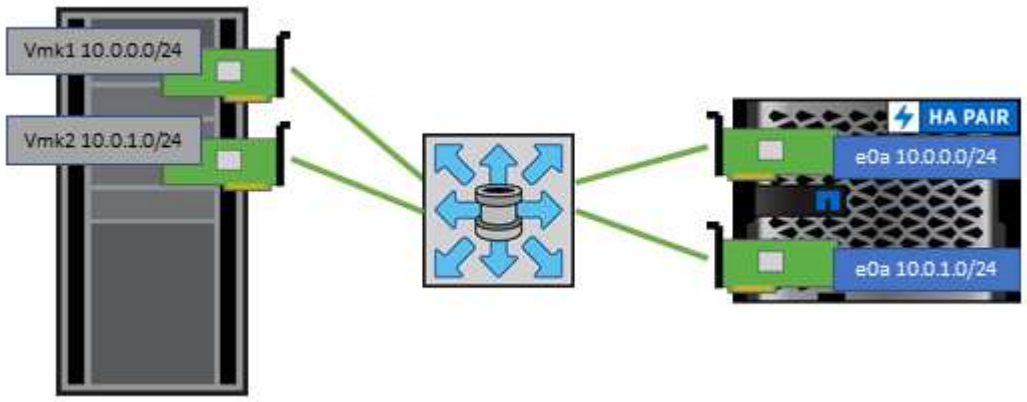
- Verwenden Sie ONTAP Tools für VMware vSphere (die wichtigste Best Practice):
  - Mit den ONTAP Tools für VMware vSphere können Sie Datastores bereitstellen, da es das Management von Richtlinien für den Export automatisch vereinfacht.
  - Wählen Sie beim Erstellen von Datastores für VMware Cluster mithilfe des Plug-ins das Cluster anstelle eines einzelnen ESX Servers aus. Bei dieser Auswahl mountet der Datastore automatisch auf alle Hosts im Cluster.
  - Wenden Sie mithilfe der Plug-in-Mount-Funktion vorhandene Datastores auf neue Server an.
  - Wenn Sie die ONTAP Tools nicht für VMware vSphere verwenden, verwenden Sie eine Exportrichtlinie für alle Server oder für jeden Server-Cluster, wo eine zusätzliche Zugriffs-Kontrolle erforderlich ist.
- Verwenden einer einzelnen logischen Schnittstelle (LIF) für jede SVM auf jedem Node im ONTAP-Cluster Die bisherigen Empfehlungen eines LIF pro Datenspeicher sind nicht mehr erforderlich. Der direkte Zugriff (LIF und Datastore auf demselben Node) ist zwar am besten, aber indirekte Zugriffe müssen sich keine Sorgen machen, da die Performance-Auswirkungen im Allgemeinen minimal sind (Mikrosekunden).
- Wenn Sie fpolicy verwenden, sollten Sie .lck-Dateien ausschließen, da diese von vSphere zum Sperren verwendet werden, wenn eine VM eingeschaltet ist.
- Alle aktuell unterstützten Versionen von VMware vSphere können sowohl NFS v3 als auch v4.1 verwenden. Die offizielle Unterstützung für nconnect wurde für vSphere 8.0 Update 2 für NFS v3 und Update 3 für NFS v4.1 hinzugefügt. Für NFS v4.1 unterstützt vSphere weiterhin Session-Trunking, Kerberos-Authentifizierung und Kerberos-Authentifizierung mit Integrität. Beachten Sie, dass für das Session-Trunking ONTAP 9.14.1 oder eine neuere Version erforderlich ist. Mehr über die nconnect-Funktion und wie sie die Leistung verbessert, erfahren Sie unter "NFSv3 nconnect Funktion mit NetApp und VMware".

- Der Höchstwert für nconnect in vSphere 8 ist 4 und der Standardwert ist 1. Das Maximalwert-Limit in vSphere kann durch erweiterte Einstellungen auf Host-Basis angehoben werden, allerdings ist es in der Regel nicht erforderlich.
- Für Umgebungen, die eine höhere Performance als eine einzelne TCP-Verbindung liefern können, wird der Wert 4 empfohlen.
- Beachten Sie, dass ESXi 256 NFS-Verbindungen hat, und jede nconnect-Verbindung zählt zu diesem Gesamtwert. Beispielsweise würden zwei Datenspeicher mit nconnect=4 als insgesamt acht Verbindungen gezählt.
- Es ist wichtig, die Performance-Auswirkungen von nconnect auf Ihre Umgebung zu testen, bevor Sie umfangreiche Änderungen in Produktionsumgebungen implementieren.

- Erwähnenswert ist, dass NFSv3 und NFSv4.1 verschiedene Sperrmechanismen verwenden. NFSv3 verwendet „Client-side locking“, während in NFSv4.1 „Server-side locking“ verwendet wird. Ein ONTAP Volume kann zwar mit beiden Protokollen exportiert werden, doch ESXi kann einen Datastore nur durch ein Protokoll mounten. Dies bedeutet jedoch nicht, dass andere ESXi-Hosts nicht denselben Datastore über eine andere Version mounten können. Um Probleme zu vermeiden, ist es wichtig, die beim Mounten verwendete Protokollversion anzugeben, um sicherzustellen, dass alle Hosts dieselbe Version und somit auch denselben Sperrungsstil anwenden. Es ist entscheidend, zu vermeiden, dass NFS-Versionen über Hosts hinweg gemischt werden. Wenn möglich, verwenden Sie Hostprofile, um die Compliance zu überprüfen.
  - Da keine automatische Datastore-Konvertierung zwischen NFSv3 und NFSv4.1 stattfindet, erstellen Sie einen neuen Datastore für NFSv4.1 und migrieren Sie die VMs mithilfe von Storage vMotion zum neuen Datastore.
  - In den Tabellenhinweisen zu NFS v4.1 Interoperabilität in "NetApp Interoperabilitäts-Matrix-Tool" finden Sie Informationen zu den spezifischen ESXi Patch-Leveln, die für die Unterstützung erforderlich sind.
- Wie in erwähnt"Einstellungen", sollten Sie, wenn Sie vSphere CSI für Kubernetes nicht verwenden, das newSyncInterval per einstellen "VMware KB 386364"
- Zur Steuerung des Zugriffs durch vSphere Hosts kommen die NFS-Exportrichtlinien zur Anwendung. Sie können eine Richtlinie für mehrere Volumes (Datastores) nutzen. Bei NFS verwendet ESXi den Sicherheitsstil „sys“ (UNIX). Zur Ausführung von VMs ist dabei die Root-Mount-Option erforderlich. In ONTAP wird diese Option als Superuser bezeichnet. Wenn die Option Superuser verwendet wird, ist es nicht erforderlich, die anonyme Benutzer-ID anzugeben. Beachten Sie, dass Regeln für die Exportrichtlinie mit unterschiedlichen Werten für `-anon -allow-suid` die SVM-Erkennungsprobleme mit ONTAP Tools verursachen können. Die IP-Adressen sollten durch Kommas getrennt sein und keine Leerzeichen der vmkernel-Port-Adressen enthalten, durch die die Datenspeicher gemountet werden. Hier sehen Sie eine Beispielrichtlinie:
  - Access Protocol: nfs (schließt nfsv3 und NFSv4 ein)
  - Liste der Hostnamen, IP-Adressen, Netzwerkgruppen oder Domänen von Client Match: 192.168.42.21,192.168.42.22
  - RO-Zugriffsregel: Beliebig
  - RW-Zugriffsregel: Beliebig
  - Benutzer-ID, der anonyme Benutzer zugeordnet werden: 65534
  - Superuser-Sicherheitstypen: Beliebig
  - Ehrensetuid Bits in SETATTR: Wahr
  - Erzeugung von Geräten zulassen: True
- Wenn das NetApp-NFS-Plug-in für VMware VAAI verwendet wird, sollte das Protokoll beim Erstellen oder

Ändern der Regel für die Exportrichtlinie auf eingestellt `nfs` werden. Damit der Copy-Offload funktioniert, wird das NFSv4-Protokoll benötigt. Wenn das Protokoll als angegeben wird, `nfs` schließt dies automatisch beide Versionen – NFSv3 und NFSv4 – ein. Dies ist auch dann erforderlich, wenn der Datenspeichertyp als NFS v3 erstellt wird.

- NFS-Datastore-Volumes werden aus dem Root-Volume der SVM heraus verbunden. Daher muss ESXi zum Navigieren und Mounten von Datastore Volumes auch Zugriff auf das Root-Volume haben. Die Exportrichtlinie für das Root-Volume und für alle anderen Volumes, in denen die Verbindung des Datastore Volumes geschachtelt ist, muss eine oder mehrere Regeln für die ESXi Server einschließen, die ihnen schreibgeschützten Zugriff gewähren. Hier sehen Sie eine Beispielrichtlinie für das Root-Volume, bei der auch das VAAI Plug-in genutzt wird:
  - Zugriffsprotokoll: nfs
  - Client-Match-Spezifikation: 192.168.42.21,192.168.42.22
  - RO-Zugriffsregel: Sys
  - RW Access Rule: Never (höchste Sicherheit für Root-Volume)
  - Anonyme UID
  - Superuser: Sys (auch für Root-Volume mit VAAI erforderlich)
- Obwohl ONTAP eine flexible Namespace-Struktur für Volumes bietet, in der Volumes mithilfe von Verbindungen in einer Baumstruktur angeordnet werden können, ist dieser Ansatz für vSphere nicht praktikabel. Für jede VM im Root-Verzeichnis des Datastores wird unabhängig von der Namespace-Hierarchie des Storage ein Verzeichnis erstellt. Daher besteht die Best Practice darin, den Verbindungspfad für Volumes für vSphere im Root-Volume der SVM zu erstellen. Dies entspricht auch der Art und Weise, wie ONTAP Tools für VMware vSphere Datastores bereitstellt. Ohne geschachtelte Verbindungspfade besteht bei Volumes zudem nur eine Abhängigkeit zum Root-Volume. Wenn ein Volume dann offline geschaltet oder sogar absichtlich zerstört wird, wirkt sich dies also nicht auf den Pfad zu den anderen Volumes aus.
- Eine Blockgröße von 4 KB ist für NTFS-Partitionen auf NFS-Datenspeichern gut. In der folgenden Abbildung ist die Konnektivität eines vSphere Hosts zu einem ONTAP NFS-Datastore dargestellt.



In der folgenden Tabelle sind NFS-Versionen und unterstützte Funktionen aufgeführt.

Funktionen von vSphere	NFSv3	NFSv4.1
VMotion und Storage vMotion	Ja.	Ja.
Hochverfügbarkeit	Ja.	Ja.
Fehlertoleranz	Ja.	Ja.

Funktionen von vSphere	NFSv3	NFSv4.1
DRS	Ja.	Ja.
Hostprofile	Ja.	Ja.
Storage DRS	Ja.	Nein
Storage-I/O-Steuerung	Ja.	Nein
SRM	Ja.	Nein
Virtual Volumes	Ja.	Nein
Hardwarebeschleunigung (VAAI)	Ja.	Ja.
Kerberos Authentifizierung	Nein	Ja (Erweiterung mit vSphere 6.5 und höher zur Unterstützung von AES, krb5i)
Multipathing-Unterstützung	Nein	Ja (ONTAP 9.14.1)

FlexGroup Volumes

Verwenden Sie ONTAP und FlexGroup Volumes mit VMware vSphere für einfache und skalierbare Datastores, die das volle Potenzial eines gesamten ONTAP Clusters ausschöpfen.

ONTAP 9.8 sowie die ONTAP Tools für VMware vSphere 9.8-9.13 und das SnapCenter Plug-in für VMware 4.4 sowie neuere Versionen unterstützten zusätzlich FlexGroup Volume-gestützte Datastores in vSphere. FlexGroup Volumes vereinfachen die Erstellung großer Datenspeicher und erstellen automatisch die erforderlichen verteilten zusammengehörigen Volumes im gesamten ONTAP Cluster, um die maximale Performance eines ONTAP Systems zu erzielen.

Verwenden Sie FlexGroup Volumes mit vSphere, wenn Sie einen einzelnen, skalierbaren vSphere Datastore mit der Leistung eines vollständigen ONTAP Clusters benötigen oder wenn Sie sehr große Klon-Workloads haben, die vom FlexGroup Klonmechanismus profitieren können, indem Sie den Klon-Cache konstant warm halten.

Copy-Offload

Zusätzlich zu umfangreichen Systemtests mit vSphere Workloads hat ONTAP 9.8 einen neuen Copy-Offload-Mechanismus für FlexGroup Datastores hinzugefügt. Das neue System verwendet eine verbesserte Copy Engine, um Dateien zwischen Komponenten im Hintergrund zu replizieren und gleichzeitig Zugriff auf Quelle und Ziel zu ermöglichen. Dieser konstituierende lokale Cache wird dann zur schnellen Instanziierung von VM-Klonen nach Bedarf verwendet.

Informationen zum Aktivieren des für FlexGroup optimierten Copy-Offload finden Sie unter "Konfigurieren von ONTAP FlexGroup Volumes für VAAI Copy-Offload"

Wenn Sie VAAI klonen, aber nicht genug klonen, um den Cache warm zu halten, können Sie feststellen, dass Ihre Klone möglicherweise nicht schneller als eine Host-basierte Kopie sind. In diesem Fall können Sie das Cache-Timeout auf Ihre Bedürfnisse abstimmen.

Betrachten wir das folgende Szenario:

- Sie haben eine neue FlexGroup mit 8 Komponenten erstellt

- Das Cache-Zeitlimit für die neue FlexGroup ist auf 160 Minuten festgelegt

In diesem Szenario sind die ersten 8 Klone vollständig vollständige Kopien anstatt lokale Dateiklone. Für jedes weitere Klonen dieser VM vor Ablauf der 160-Sekunden-Zeitüberschreitung wird die Datei-Klon-Engine innerhalb jeder Komponente nach dem Round-Robin-Verfahren verwendet, um nahezu sofortige Kopien zu erstellen, die gleichmäßig über die einzelnen Volumes verteilt sind.

Bei jedem neuen Klonjob, der ein Volume erhält, wird die Zeitüberschreitung zurückgesetzt. Wenn ein konstituierendes Volume in der Beispiel-FlexGroup vor dem Timeout keine Klonanforderung erhält, wird der Cache für diese bestimmte VM gelöscht und das Volume muss erneut ausgefüllt werden. Wenn sich auch die Quelle des ursprünglichen Klons ändert (z. B. Sie haben die Vorlage aktualisiert), wird der lokale Cache jeder Komponente ungültig, um Konflikte zu vermeiden. Wie bereits erwähnt, kann der Cache an die Anforderungen Ihrer Umgebung angepasst werden.

Weitere Informationen zur Verwendung von FlexGroup Volumes mit VAAI finden Sie in diesem KB-Artikel: "VAAI: Wie funktioniert Caching mit FlexGroup Volumes?"

In Umgebungen, in denen Unternehmen nicht alle Vorteile des FlexGroup Cache ausschöpfen können, aber trotzdem schnelles standortübergreifendes Klonen benötigen, ist die Verwendung von VVols eine erwägen. Das Volume-übergreifende Klonen mit VVols erfolgt viel schneller als bei herkömmlichen Datastores und ist nicht auf einen Cache angewiesen.

QoS-Einstellungen

Das Konfigurieren von QoS auf FlexGroup-Ebene mit ONTAP System Manager oder der Cluster Shell wird unterstützt, allerdings bietet es keine VM-Erkennung oder vCenter-Integration.

QoS (IOPS-Maximum/Min.) kann auf einzelnen VMs oder auf allen VMs in einem Datastore eingerichtet werden. Zu diesem Zeitpunkt in der vCenter UI oder über REST-APIs mithilfe von ONTAP Tools. Die Festlegung der QoS auf allen VMs ersetzt alle separaten Einstellungen pro VM. Einstellungen erweitern nicht auch künftig auf neue oder migrierte VMs. Sie können entweder QoS auf den neuen VMs festlegen oder QoS neu auf alle VMs im Datastore anwenden.

Zu beachten ist, dass VMware vSphere alle I/O-Vorgänge für einen NFS-Datastore als eine einzelne Warteschlange pro Host behandelt. Eine QoS-Drosselung für eine VM kann die Performance für andere VMs im selben Datastore für diesen Host beeinträchtigen. Dies steht im Gegensatz zu VVols, die ihre QoS-Richtlinieneinstellungen beibehalten können, wenn sie zu einem anderen Datastore migriert werden und bei einer Drosselung die I/O anderer VMs nicht beeinträchtigen.

Metriken

ONTAP 9.8 hat außerdem neue dateibasierte Performance-Kennzahlen (IOPS, Durchsatz und Latenz) für FlexGroup-Dateien hinzugefügt. Diese Metriken können über das Dashboard von ONTAP Tools für VMware vSphere sowie VM-Berichte eingesehen werden. Die ONTAP Tools für VMware vSphere Plug-in ermöglichen Ihnen darüber hinaus die Festlegung von QoS-Regeln (Quality of Service) über eine Kombination aus dem Maximum und/oder dem Minimum von IOPS. Diese können über alle VMs in einem Datenspeicher oder individuell für bestimmte VMs hinweg festgelegt werden.

Best Practices in sich vereint

- Erstellen Sie mit den ONTAP Tools FlexGroup Datastores, damit Ihre FlexGroup optimal erstellt wird und die Exportrichtlinien entsprechend Ihrer vSphere Umgebung konfiguriert werden. Nachdem Sie jedoch das FlexGroup Volume mit ONTAP Tools erstellt haben, wird festgestellt, dass alle Nodes im vSphere-Cluster eine einzige IP-Adresse zum Mounten des Datenspeichers verwenden. Dies kann zu einem Engpass am Netzwerkport führen. Um dieses Problem zu vermeiden, mounten Sie den Datastore ab und mounten Sie

ihn dann mit dem standardmäßigen vSphere Datastore-Assistenten unter Verwendung eines Round-Robin-DNS-Namens, der die Last über LIFs auf der SVM verteilt. Nach der erneuten Montage können ONTAP Tools den Datastore wieder managen. Wenn keine ONTAP-Tools verfügbar sind, verwenden Sie die FlexGroup-Standardeinstellungen, und erstellen Sie entsprechend den Richtlinien in Ihre Exportrichtlinie "Datenspeicher und Protokolle – NFS".

- Beachten Sie bei der Dimensionierung eines FlexGroup-Datenspeichers, dass die FlexGroup aus mehreren kleineren FlexVol-Volumes besteht, die einen größeren Namespace erstellen. Daher sollten Sie die Größe des Datenspeichers mindestens 8x (bei Annahme der 8 Standard-Komponenten) der Größe Ihrer größten VMDK-Datei plus 10 bis 20 % ungenutzte Reserven aufweisen, um Flexibilität bei der Ausbalancierung zu ermöglichen. Wenn Sie beispielsweise eine 6 TB VMDK in Ihrer Umgebung haben, müssen Sie den FlexGroup Datenspeicher nicht kleiner als 52,8 TB (6 x 8 + 10 %) dimensionieren.
- VMware und NetApp unterstützen das NFSv4.1 Session Trunking ab ONTAP 9.14.1. Spezifische Versionsinformationen finden Sie in den IMT-Hinweisen (NetApp NFS 4.1 Interoperabilitäts-Matrix-Tool). NFSv3 unterstützt nicht mehrere physische Pfade zu einem Volume, sondern beginnend mit vSphere 8.0U2 nconnect. Weitere Informationen zu nconnect finden Sie unter "NFSv3 nConnect Funktion mit NetApp und VMware".
- Nutzen Sie das NFS-Plug-in für VMware VAAI für den Offloaded Data Transfer. Beachten Sie, dass das Klonen innerhalb eines FlexGroup-Datastore verbessert wird, wie bereits erwähnt, aber ONTAP beim Kopieren von VMs zwischen FlexVol und/oder FlexGroup Volumes keine wesentlichen Performance-Vorteile gegenüber ESXi Hostkopien bietet. Berücksichtigen Sie daher Ihre Klon-Workloads bei der Entscheidung, VAAI oder FlexGroup Volumes zu verwenden. Die Änderung der Anzahl zusammengebender Volumes ist eine Möglichkeit zur Optimierung des FlexGroup-basierten Klonens. Ebenso wie die Anpassung der zuvor erwähnten Cache-Zeitüberschreitung.
- ONTAP Tools für VMware vSphere 9.8-9.13 ermöglichen die Überwachung der Performance von FlexGroup VMs mithilfe von ONTAP Kennzahlen (Dashboard und VM-Berichte) und das Management von QoS auf einzelnen VMs. Diese Metriken sind derzeit nicht über ONTAP-Befehle oder APIs verfügbar.
- Das SnapCenter Plug-in für VMware vSphere Version 4.4 und höher unterstützt das Backup und die Recovery von VMs in einem FlexGroup Datastore auf dem primären Storage-System. SCV 4.6 bietet zusätzliche SnapMirror Unterstützung für FlexGroup-basierte Datastores. Array-basierte Snapshots und Replizierung sind die effizienteste Methode zum Schutz Ihrer Daten.

Netzwerkkonfiguration

Wenn Sie vSphere mit Systemen mit ONTAP verwenden, ist die Konfiguration von Netzwerkeinstellungen einfach und erfolgt ähnlich wie andere Netzwerkkonfigurationen.

Folgende Punkte sind dabei zu berücksichtigen:

- Separater Storage-Netzwerk-Traffic aus anderen Netzwerken. Ein separates Netzwerk kann mithilfe eines dedizierten VLANs oder separater Switches für Storage eingerichtet werden. Falls im Storage-Netzwerk physische Pfade wie Uplinks geteilt werden, sind eventuell QoS oder zusätzliche Uplink-Ports erforderlich, um eine ausreichende Bandbreite sicherzustellen. Verbinden Sie Hosts nicht direkt mit Storage, es sei denn, Ihr Lösungsleitfaden fordert ausdrücklich darauf an. Verwenden Sie Switches mit redundanten Pfaden, und lassen Sie VMware HA ohne Eingriffe arbeiten.
- Jumbo Frames sollten verwendet werden, wenn sie von Ihrem Netzwerk unterstützt werden. Vergewissern Sie sich bei ihrem Einsatz, dass sie auf allen Netzwerkgeräten, VLANs etc. Im Pfad zwischen Storage und dem ESXi Host gleich konfiguriert sind. Anderenfalls kann es zu Performance- oder Verbindungsproblemen kommen. Auf dem virtuellen ESXi Switch, dem VMkernel Port, sowie den physischen Ports oder den Interface Groups muss für jeden ONTAP Node auch jeweils dieselbe MTU festgelegt sein.

- NetApp empfiehlt eine Deaktivierung der Netzwerk- Flusssteuerung nur an den Cluster-Interconnect-Ports innerhalb eines ONTAP Clusters. NetApp gibt im Hinblick auf Best Practices zur Flusskontrolle für die übrigen Netzwerkports, die für Daten-Traffic verwendet werden, keine weiteren Empfehlungen. Sie sollten diese Funktion nach Bedarf aktivieren oder deaktivieren. Weitere Informationen zur Flusssteuerung finden Sie unter "TR-4182".
- Wenn ESXi und ONTAP Storage-Arrays mit Ethernet-Storage-Netzwerken verbunden werden, empfiehlt NetApp, die Ethernet-Ports, mit denen diese Systeme verbunden werden, mit der Cisco PortFast Funktion oder als Rapid Spanning Tree Protocol (RSTP)-Edge-Ports zu konfigurieren. NetApp empfiehlt die Aktivierung der Spanning Tree PortFast Trunk-Funktion in Umgebungen mit Verwendung der Cisco PortFast Funktion und 802.1Q VLAN-Trunking entweder für den ESXi Server oder für die ONTAP Storage-Arrays.
- Für die Link-Aggregation empfiehlt NetApp die folgenden Best Practices:
  - Verwenden Sie Switches, die die Link-Aggregation von Ports in zwei separaten Switch-Chassis durch einen Ansatz mit einer Multi-Chassis-Link-Aggregationsgruppe wie Virtual PortChannel (vPC) von Cisco unterstützen.
  - Deaktivieren Sie LACP für mit ESXi verbundene Switch Ports, es sei denn, Sie verwenden dvSwitches ab 5.1 mit konfiguriertem LACP.
  - Erstellen Sie mit LACP Link-Aggregate für ONTAP Storage-Systeme mit dynamischen Multimode-Schnittstellengruppen mit IP-Hash.
  - Verwenden Sie eine IP-Hash-Teaming-Richtlinie für ESXi.

Die folgende Tabelle enthält eine Zusammenfassung der Netzwerkkonfigurationselemente sowie Angaben dazu, wo die Einstellungen angewendet werden.

Element	ESXi	Switch	Knoten	SVM
IP-Adresse	VMkernel	Nein**	Nein**	Ja.
Link-Aggregation	Virtueller Switch	Ja.	Ja.	Nein*
VLAN	VMkernel und VM-Portgruppen	Ja.	Ja.	Nein*
Flusskontrolle	NIC	Ja.	Ja.	Nein*
Spanning Tree	Nein	Ja.	Nein	Nein
MTU (für Jumbo Frames)	Virtueller Switch und VMkernel Port (9000)	Ja (auf Maximalwert eingestellt)	Ja (9000)	Nein*
Failover-Gruppen	Nein	Nein	Ja (erstellen)	Ja (auswählen)

*SVM-LIFs werden mit Ports, Schnittstellengruppen oder VLAN-Schnittstellen verbunden, die über VLAN-, MTU- und andere Einstellungen verfügen. Diese Einstellungen werden jedoch nicht auf SVM-Ebene gemanagt.

**Diese Geräte haben eigene IP-Adressen für das Management, aber diese Adressen werden nicht im Zusammenhang mit ESXi Storage Networking verwendet.

SAN (FC, NVMe/FC, iSCSI, NVMe/TCP), RDM

ONTAP bietet Block-Storage der Enterprise-Klasse für VMware vSphere unter Verwendung des traditionellen iSCSI- und Fibre-Channel-Protokolls (FCP) sowie des hocheffizienten und performanten NVMe-of (Next-

Generation Block-Protokoll), das sowohl NVMe/FC als auch NVMe/TCP unterstützt.

Detaillierte Best Practices zur Implementierung von Blockprotokollen für VM-Storage mit vSphere und ONTAP finden Sie unter "Datenspeicher und Protokolle – SAN"

NFS

Bei vSphere können Kunden mithilfe von NFS-Arrays der Enterprise-Klasse gleichzeitigen Zugriff auf Datastores auf allen Nodes in einem ESXi Cluster ermöglichen. Wie im Abschnitt erwähnt"Datenspeicher", gibt es bei der Verwendung von NFS mit vSphere einige Vorteile im Hinblick auf Benutzerfreundlichkeit, Storage-Effizienz und Sichtbarkeit.

Empfohlene Best Practices finden Sie in "Datenspeicher und Protokolle – NFS"

Direkte Netzwerkverbindung

Storage-Administratoren ziehen es manchmal vor, ihre Infrastruktur zu vereinfachen, indem sie Netzwerk-Switches von der Konfiguration entfernen. Dies kann in einigen Szenarien unterstützt werden. Allerdings gibt es einige Einschränkungen und Einschränkungen, die zu beachten sind.

ISCSI und NVMe/TCP

Ein Host, der iSCSI oder NVMe/TCP verwendet, kann direkt mit einem Storage-System verbunden werden und ordnungsgemäß ausgeführt werden. Der Grund dafür ist Pathing. Direkte Verbindungen zu zwei verschiedenen Storage Controllern ergeben zwei unabhängige Pfade für den Datenfluss. Der Verlust von Pfad, Port oder Controller verhindert nicht, dass der andere Pfad verwendet wird.

NFS

Direct-Connected NFS Storage kann genutzt werden, aber mit einer erheblichen Einschränkung - Failover funktioniert nicht ohne einen erheblichen Scripting-Aufwand, der in der Verantwortung des Kunden liegt.

Der Grund, warum ein unterbrechungsfreier Failover mit direkt verbundenem NFS-Storage kompliziert ist, ist das Routing auf dem lokalen Betriebssystem. Angenommen, ein Host hat eine IP-Adresse von 192.168.1.1/24 und ist direkt mit einem ONTAP-Controller mit einer IP-Adresse von 192.168.1.50/24 verbunden. Während eines Failovers kann diese 192.168.1.50-Adresse ein Failover auf den anderen Controller durchführen, und sie wird für den Host verfügbar sein. Wie erkennt der Host jedoch sein Vorhandensein? Die ursprüngliche 192.168.1.1-Adresse ist noch auf der Host-NIC vorhanden, die keine Verbindung mehr zu einem Betriebssystem herstellt. Der für 192.168.1.50 bestimmte Datenverkehr würde weiterhin an einen nicht funktionsfähigen Netzwerkport gesendet.

Die zweite BS-NIC könnte als 19 konfiguriert werden 2.168.1.2 und wäre in der Lage, mit der Failed Over 192.168.1.50-Adresse zu kommunizieren, aber die lokalen Routing-Tabellen würden standardmäßig eine **und nur eine**-Adresse verwenden, um mit dem Subnetz 192.168.1.0/24 zu kommunizieren. Ein Sysadmin könnte ein Skript-Framework erstellen, das eine fehlerhafte Netzwerkverbindung erkennt und die lokalen Routing-Tabellen ändert oder Schnittstellen hoch- und herunterfahren würde. Das genaue Verfahren hängt vom verwendeten Betriebssystem ab.

In der Praxis haben NetApp-Kunden NFS direkt verbunden, aber normalerweise nur für Workloads, bei denen IO-Pausen während Failover akzeptabel sind. Wenn harte Mounts verwendet werden, sollte es während solcher Pausen keine IO-Fehler geben. Die E/A-Vorgänge sollten so lange anhalten, bis Dienste wiederhergestellt werden, entweder durch ein Failback oder durch einen manuellen Eingriff, um IP-Adressen zwischen NICs auf dem Host zu verschieben.

FC Direct Connect

Es ist nicht möglich, einen Host direkt über das FC-Protokoll mit einem ONTAP Storage-System zu verbinden. Der Grund dafür ist die Verwendung von NPIV. Der WWN, der einen ONTAP FC-Port mit dem FC-Netzwerk identifiziert, verwendet eine Art Virtualisierung, die als NPIV bezeichnet wird. Jedes Gerät, das an ein ONTAP-System angeschlossen ist, muss einen NPIV-WWN erkennen können. Es gibt derzeit keine HBA-Anbieter, die einen HBA anbieten, der auf einem Host installiert werden kann, der ein NPIV-Ziel unterstützen könnte.

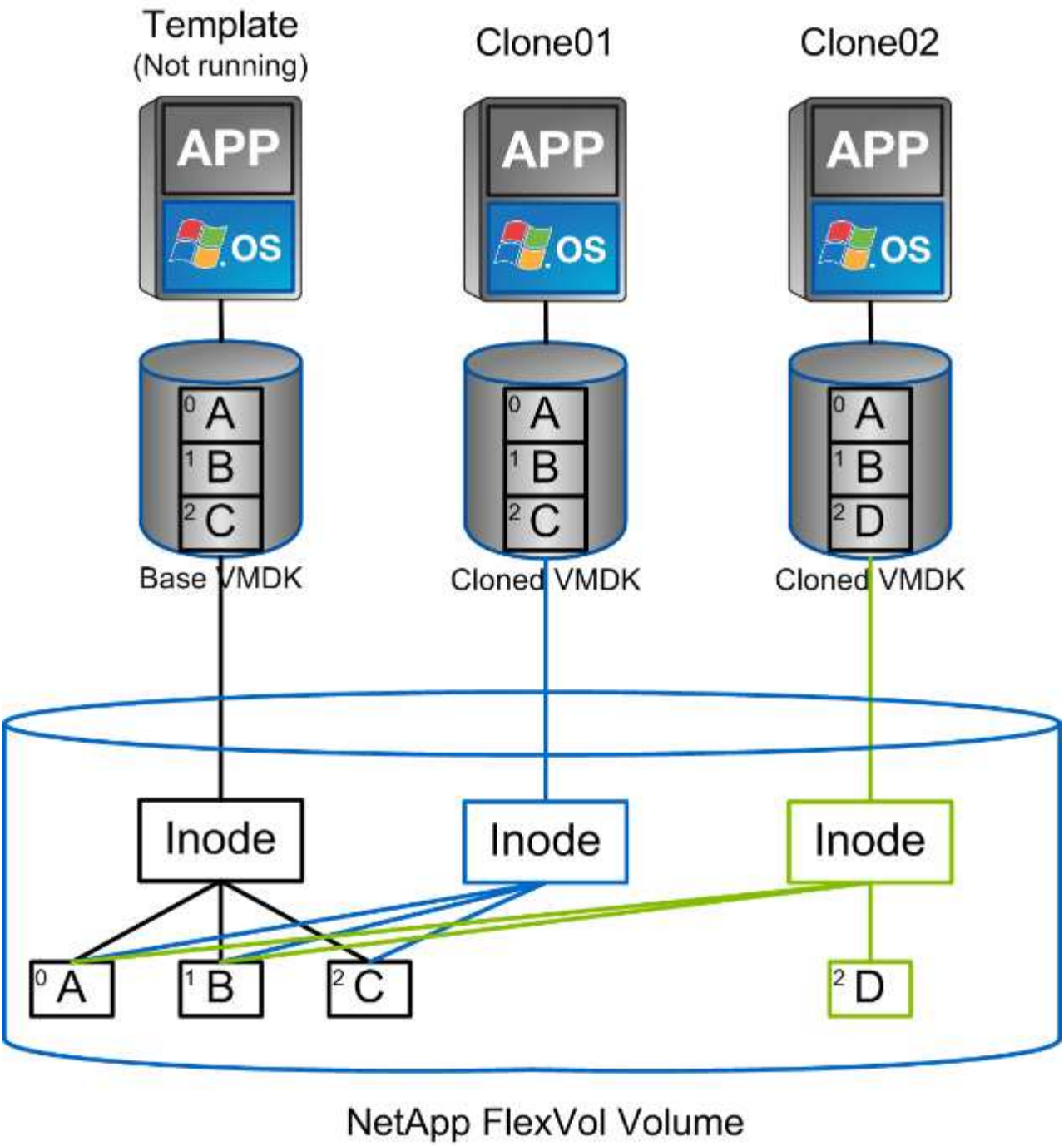
Klonen von VMs und Datastores

Durch das Klonen eines Storage-Objekts können Sie schnell Kopien für andere Zwecke erstellen, beispielsweise zum Provisionieren weiterer VMs, für Backup- und Recovery-Vorgänge usw.

In vSphere können Sie VMs, virtuelle Festplatten, vVol oder Datastores klonen. Nach dem Klonen kann das betreffende Objekt weiter angepasst werden. Dies geschieht häufig durch einen automatisierten Prozess. VSphere unterstützt sowohl vollständige Klone als auch Linked Clones, bei denen Änderungen separat vom ursprünglichen Objekt verfolgt werden.

Linked Clones eignen sich sehr gut, um Speicherplatz zu sparen, aber sie erhöhen die Menge der I/O-Vorgänge, die vSphere für die VM verarbeitet. Dies wirkt sich auf die Performance der betreffenden VM und vielleicht auch des gesamten Hosts aus. Aus diesem Grund nutzen NetApp Kunden häufig Klone, die auf Storage-Systemen basieren, um das Beste aus beiden Welten zu erhalten: Effiziente Storage-Nutzung und höhere Performance.

In der folgenden Abbildung ist das Klonen von ONTAP dargestellt.



Das Klonen kann – in der Regel auf VM-, vVol- oder Datastore-Ebene – durch mehrere Verfahren auf Systeme mit ONTAP verlagert werden. Hierzu zählen:

- VVols, die den NetApp vSphere APIs for Storage Awareness (VASA) Provider verwenden. ONTAP Klone unterstützen von vCenter gemanagte vVol Snapshots, die platzsparend sind und bei der Erstellung und Löschung eine minimale I/O-Auswirkung haben. VMs können auch mit vCenter geklont werden. Sie werden dann auch zu ONTAP verlagert, sei es innerhalb eines einzelnen Datastores/Volumes oder zwischen Datastores/Volumes.
- VSphere Klone und Migration mit vSphere APIs – Array Integration (VAAI). VM-Klonvorgänge können in SAN- und NAS-Umgebungen zu ONTAP verlagert werden (NetApp stellt ein ESXi Plug-in zur Aktivierung von VAAI für NFS bereit). VSphere verlagert lediglich Vorgänge auf kalte (ausgeschaltet) VMs in einem NAS-Datastore, während Vorgänge auf heißen VMs (Klonen und Storage vMotion) auch für SAN verlagert werden. ONTAP nutzt je nach Quelle und Ziel den effizientesten Ansatz. Diese Funktion wird auch von

verwendet "Omnissa Horizon View".

- SRA (wird mit VMware Live Site Recovery/Site Recovery Manager verwendet). Hier werden Klone zum unterbrechungsfreien Testen der Recovery des DR-Replikats herangezogen.
- Backup und Recovery mit NetApp Tools wie SnapCenter. Mit VM-Klonen werden Backup-Vorgänge sichergestellt. Darüber hinaus können VM-Backups gemountet werden, so dass einzelne Dateien wiederhergestellt werden können.

Verlagerte ONTAP Klone können durch VMware, NetApp und Drittanbietertools aufgerufen werden. Zu ONTAP verlagerte Klone haben mehrere Vorteile. Sie sind in den meisten Fällen platzsparend, da sie nur für Änderungen am Objekt Storage benötigen. Es entstehen keine zusätzlichen Performance-Einbußen, wenn sie gelesen und geschrieben werden, und in einigen Fällen wird die Performance durch die Freigabe von Blöcken in High-Speed-Caches erhöht. Zudem verlagern sie CPU-Zyklen und Netzwerk-I/O-Vorgänge vom ESXi Server. Der Copy-Offload innerhalb eines herkömmlichen Datastores mit einem FlexVol volume kann mit einer lizenzierten FlexClone schnell und effizient sein (in der ONTAP One Lizenz enthalten), doch die Kopien zwischen FlexVol Volumes können langsamer sein. Wenn Sie VM-Vorlagen als Klonquelle bereithalten, sollten Sie sie in Betracht ziehen, sie im Datastore-Volume zu platzieren (Ordner oder Inhaltsbibliotheken zur Organisation dieser Klone einsetzen), um schnelle, platzsparende Klone zu erstellen.

Zum Klonen eines Datastores können Sie ein Volume oder eine LUN auch direkt in ONTAP klonen. Mithilfe der FlexClone Technologie kann bei NFS-Datastores ein gesamtes Volume geklont und der Klon anschließend aus ONTAP exportiert und von ESXi als weiterer Datastore gemountet werden. Bei VMFS Datastores kann in ONTAP eine LUN innerhalb eines Volumes oder das gesamte Volume (einschließlich einer oder mehrerer darin enthaltener LUNs) geklont werden. Eine LUN, die ein VMFS enthält, muss einer ESXi Initiatorgruppe zugeordnet und dann von ESXi neu signiert werden, damit sie gemountet und als regulärer Datastore verwendet werden kann. Ein geklontes VMFS kann für einige temporäre Anwendungsfällte ohne erneute Signatur gemountet werden. Nachdem ein Datastore geklont wurde, können die darin enthaltenen VMs registriert, neu konfiguriert und angepasst werden, als wären sie einzeln geklonte VMs.

In einigen Fällen kann das Klonen durch zusätzliche lizenzierte Funktionen wie SnapRestore für Backups oder FlexClone optimiert werden. Diese Lizenzen sind oft in Lizenz-Bundles ohne zusätzliche Kosten enthalten. Für vVol Klonvorgänge und zur Unterstützung gemanagter Snapshots eines vVol (die vom Hypervisor zu ONTAP verlagert werden) ist eine FlexClone Lizenz erforderlich. Durch eine FlexClone Lizenz können auch bestimmte VAAI basierte Klone optimiert werden, wenn sie in einem Datastore/Volume verwendet werden. Dabei werden sofortige platzsparende Kopien anstelle von Blockkopien erstellt. Sie wird zudem von SRA beim Testen der Recovery eines DR-Replikats sowie von SnapCenter für Klonvorgänge und zum Durchsuchen von Backup-Kopien zum Wiederherstellen einzelner Dateien genutzt.

Datensicherung

Backups und schnelle Wiederherstellung von Virtual Machines (VMs) sind die wichtigsten Vorteile von ONTAP für vSphere. Diese Funktionalität lässt sich über das SnapCenter Plug-in für VMware vSphere bequem in vCenter managen. Viele Kunden erweitern ihre Backup-Lösungen von Drittanbietern mit SnapCenter, um die Snapshot-Technologie von ONTAP zu nutzen, da diese die schnellste und unkomplizierte Möglichkeit bietet, eine VM mit ONTAP wiederherzustellen. Kunden, die über eine ONTAP One Lizenz verfügen, ist SnapCenter kostenlos erhältlich. Unter Umständen sind auch andere Lizenzpakete erhältlich.

Darüber hinaus kann das SnapCenter Plug-In für VMware integriert werden mit "NetApp Backup and Recovery für virtuelle Maschinen", wodurch effektive 3-2-1-Backup-Lösungen für die meisten ONTAP Systeme ermöglicht werden. Beachten Sie, dass bei der Verwendung von Backup und Recovery für virtuelle Maschinen mit Premiumdiensten, wie z. B. Objektspeichern für zusätzlichen Sicherungsspeicher, Gebühren anfallen

können. In diesem Abschnitt werden die verschiedenen Optionen zum Schutz Ihrer VMs und Datenspeicher beschrieben.

NetApp ONTAP-Volume-Snapshots

Mit Snapshots können Sie ohne Auswirkungen auf die Performance schnell Kopien Ihrer VMs oder Datastores erstellen und diese dann zur längerfristigen externen Datensicherung mit SnapMirror an ein sekundäres System senden. Durch diesen Ansatz werden der Storage-Platzbedarf und die Netzwerkbandbreite minimiert, da nur geänderte Informationen gespeichert werden.

Snapshots sind eine Schlüsselfunktion von ONTAP, mit der Sie zeitpunktgenaue Kopien Ihrer Daten erstellen können. Sie sind platzsparend und schnell erstellbar – ideal für die Sicherung von VMs und Datenspeichern. Snapshots können für verschiedene Zwecke verwendet werden, einschließlich Backup, Recovery und Tests. Diese Snapshots unterscheiden sich von VMware (Konsistenz-)Snapshots und sind für längerfristige Sicherung geeignet. Die von VMware vCenter gemanagten Snapshots werden aufgrund von Performance und anderen Auswirkungen nur für den kurzfristigen Einsatz empfohlen. "Einschränkungen Bei Snapshots"Weitere Informationen finden Sie unter.

Snapshots werden auf Volume-Ebene erstellt und können zur Sicherung aller VMs und Datenspeicher innerhalb dieses Volumes eingesetzt werden. Das bedeutet, dass Sie einen Snapshot eines gesamten Datastores erstellen können, der alle VMs in diesem Datastore umfasst.

Bei NFS-Datastores können Sie VM-Dateien in Snapshots ganz einfach anzeigen, indem Sie das Verzeichnis .Snapshots durchsuchen. So können Sie schnell auf Dateien von einem Snapshot zugreifen und diese wiederherstellen, ohne dass eine bestimmte Backup-Lösung verwendet werden muss.

Für VMFS-Datastores können Sie eine FlexClone des Datastore auf der Grundlage des gewünschten Snapshots erstellen. Damit können Sie einen neuen Datastore erstellen, der auf dem Snapshot basiert und für Test- oder Entwicklungszwecke verwendet werden kann. Das FlexClone verbraucht nur Speicherplatz für die nach der Snapshot-Erstellung vorgenommenen Änderungen und ist somit eine platzsparende Möglichkeit, eine Kopie des Datastore zu erstellen. Sobald die FlexClone erstellt wurde, können Sie die LUN oder den Namespace einem ESXi-Host zuordnen, wie ein normaler Datastore. So können Sie nicht nur spezifische VM-Dateien wiederherstellen, sondern schnell auch Test- oder Entwicklungsumgebungen auf Basis von Produktionsdaten erstellen, ohne die Performance der Produktionsumgebung zu beeinträchtigen.

Weitere Informationen zu Snapshots finden Sie in der ONTAP Dokumentation. Weitere Details finden Sie unter den folgenden Links: "Lokale ONTAP Snapshot Kopien" "ONTAP SnapMirror Replikationsworkflow"

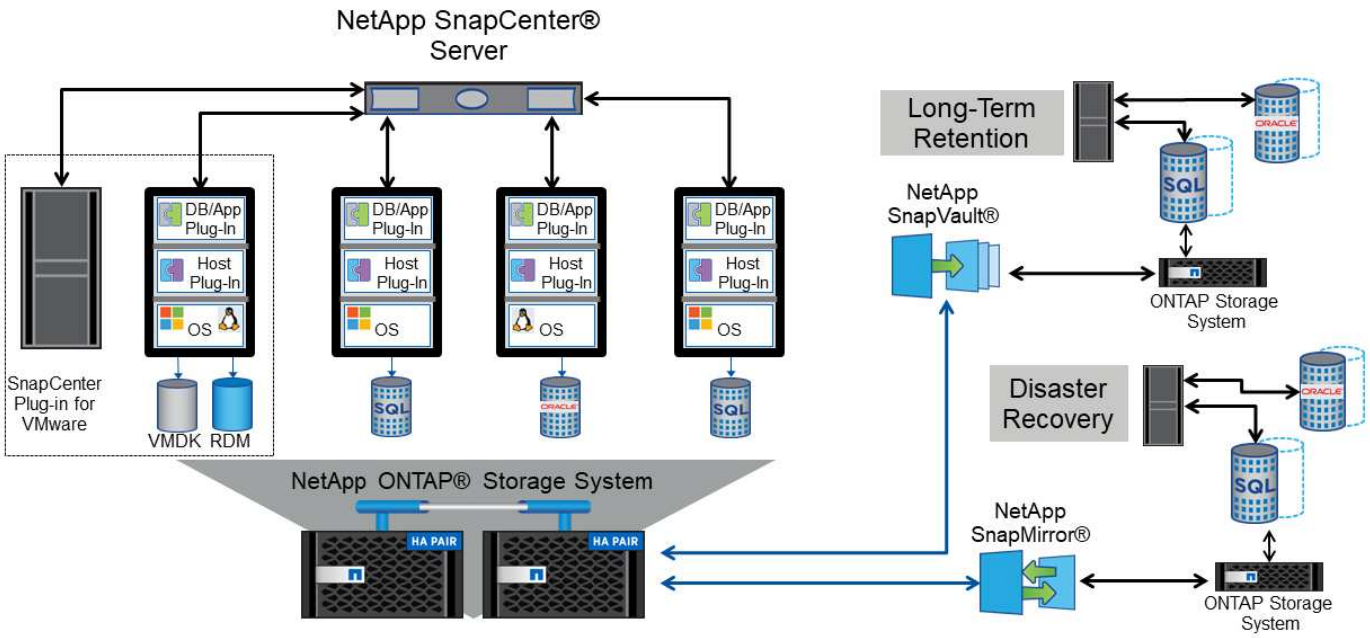
SnapCenter Plug-in für VMware vSphere

Mit SnapCenter können Sie Backup-Richtlinien erstellen, die auf mehrere Jobs angewendet werden können. In diesen Richtlinien können ein Zeitplan, die Aufbewahrung, die Replizierung und andere Funktionen definiert werden. Damit ist es weiterhin möglich, optional VM-konsistente Snapshots auszuwählen und dadurch die Fähigkeit des Hypervisors auszuschöpfen, das I/O vor dem Erstellen eines VMware Snapshots stillzulegen. Aufgrund der Performance-Auswirkungen von VMware Snapshots werden diese jedoch im Allgemeinen nicht empfohlen, es sei denn, Sie müssen das Gast-Betriebssystem stilllegen. Verwenden Sie stattdessen Snapshots für die allgemeine Sicherung und Applikationstools wie SnapCenter Applikations-Plug-ins, um transaktionsorientierte Daten – beispielsweise SQL Server oder Oracle Daten – zu sichern.

Diese Plug-ins bieten erweiterte Funktionen zur Sicherung von Datenbanken in physischen und virtuellen Umgebungen. Bei vSphere können Sie sie zur Sicherung von SQL Server oder Oracle Datenbanken heranziehen, in denen die Daten in RDM-LUNs, VVols oder NVMe/TCP-Namespaces und direkt mit dem Gastbetriebssystem verbundenen iSCSI-LUNs oder VMDK-Dateien in VMFS oder NFS-Datastores gespeichert werden. Mit den Plug-ins können unterschiedliche Typen von Datenbank-Backups angegeben, Online- oder Offline-Backups unterstützt und neben Protokolldateien auch Datenbankdateien gesichert

werden. Neben Backup und Recovery unterstützen die Plug-ins auch das Klonen von Datenbanken für Entwicklungs- oder Testzwecke.

Die folgende Abbildung zeigt ein Beispiel für die Implementierung von SnapCenter.



Informationen zur Dimensionierung finden Sie im "Dimensionierungsleitfaden für SnapCenter Plug-in für VMware vSphere"

ONTAP Tools für VMware vSphere mit VMware Live Site Recovery

Die ONTAP Tools für VMware vSphere (OT4VS) sind ein kostenloses Plug-in, das eine nahtlose Integration zwischen VMware vSphere und NetApp ONTAP bietet. Sie können Ihren ONTAP Storage direkt über den vSphere Web Client managen und Aufgaben wie die Bereitstellung von Storage, das Management von Replizierung und das Monitoring der Performance vereinfachen.

Bessere Disaster-Recovery-Funktionen sollten Sie in Betracht ziehen, NetApp SRA für ONTAP zu verwenden, das Teil von ONTAP Tools für VMware vSphere ist, zusammen mit VMware Live Site Recovery (ehemals Site Recovery Manager). Dieses Tool unterstützt nicht nur die Replizierung von Datastores an einen Disaster-Recovery-Standort mithilfe von SnapMirror, sondern ermöglicht auch unterbrechungsfreie Tests in der DR-Umgebung, indem die replizierten Datastores geklont werden. Darüber hinaus wird das Recovery nach einem Ausfall und der erneute Schutz der Produktion nach einem Ausfall dank integrierter Automatisierungsfunktionen optimiert.

NetApp Disaster Recovery

Disaster Recovery (DR) ist ein Cloud-basierter Dienst, der eine umfassende Lösung zum Schutz Ihrer Daten und Anwendungen im Katastrophenfall bietet. Es bietet eine Reihe von Funktionen, darunter automatisiertes Failover und Failback, mehrere zeitpunktbezogene Wiederherstellungspunkte, anwendungskonsistente Notfallwiederherstellung und Unterstützung sowohl für lokale als auch für Cloud-basierte ONTAP Systeme. NetApp Disaster Recovery ist für die nahtlose Zusammenarbeit mit ONTAP und Ihrer VMware vSphere-Umgebung konzipiert und bietet eine einheitliche Lösung für die Notfallwiederherstellung.

VSphere Metro Storage-Cluster (vMSC) mit NetApp MetroCluster und aktiver SnapMirror-Synchronisierung

Um ein Höchstmaß an Datensicherung zu gewährleisten, ziehen Sie eine VMware vSphere Metro Storage Cluster (vMSC) Konfiguration mit NetApp MetroCluster in Erwägung. VMSC ist eine von VMware zertifizierte, von NetApp unterstützte Lösung mit synchroner Replizierung, die dieselben Vorteile eines Hochverfügbarkeits-Clusters bietet, aber zum Schutz vor Standortausfällen auf separate Standorte verteilt ist. Active Sync mit ASA und AFF sowie MetroCluster mit AFF bietet kostengünstige Konfigurationen für synchrone Replizierung mit transparentem Recovery nach dem Ausfall einer einzelnen Storage-Komponente. Außerdem bietet NetApp SnapMirror Active Sync transparentes Recovery bei SnapMirror Active Sync oder Recovery mit nur einem Befehl im Falle eines Standortausfalls mit MetroCluster. VMSC wird im weiteren Details beschrieben. "TR-4128"

Servicequalität (QoS)

Durchsatzbegrenzungen sind bei der Steuerung von Service-Levels, dem Management unbekannter Workloads oder beim Testen von Applikationen vor der Implementierung nützlich, um sicherzustellen, dass sie sich nicht auf andere Workloads in der Produktion auswirken. Sie können auch zur Beschränkung eines als problematisch identifizierten Workloads eingesetzt werden.

Unterstützung von ONTAP QoS-Richtlinien

Systeme mit ONTAP können die Storage QoS-Funktion nutzen, um den Durchsatz in Megabit pro Sekunde und/oder die Anzahl der I/O-Vorgänge pro Sekunde (IOPS) für unterschiedliche Storage-Objekte wie Dateien, LUNs, Volumes oder ganze SVMs zu beschränken.

Minimale Service-Level auf Basis der IOPS werden ebenfalls unterstützt, um SAN-Objekten in ONTAP 9.2 und NAS-Objekten in ONTAP 9.3 eine konsistente Performance bereitzustellen.

Die maximale QoS-Durchsatzbegrenzung für ein Objekt kann in Megabit pro Sekunde und/oder IOPS festgelegt werden. Wenn beide verwendet werden, wird das erste erreichte Limit von ONTAP durchgesetzt. Ein Workload kann mehrere Objekte umfassen. Auf einen oder mehrere Workloads kann eine QoS-Richtlinie angewendet werden. Wird eine Richtlinie auf mehrere Workloads angewendet, teilen diese das in der Richtlinie zulässige Gesamtlimit. Geschachtelte Objekte werden nicht unterstützt (so können beispielsweise nicht jede Datei in einem Volume eine eigene Richtlinie aufweisen). QoS-Mindestwerte können nur als IOPS angegeben werden.

Derzeit sind folgende Tools für das Management von ONTAP QoS-Richtlinien und deren Anwendung auf Objekte verfügbar:

- CLI VON ONTAP
- ONTAP System Manager
- OnCommand Workflow-Automatisierung
- Active IQ Unified Manager
- NetApp PowerShell Toolkit für ONTAP
- ONTAP-Tools für VMware vSphere VASA Provider

Wenn Sie eine QoS-Richtlinie einschließlich VMFS und RDM einer LUN zuweisen möchten, können Sie die ONTAP SVM (angezeigt als „vServer“), den LUN-Pfad und die Seriennummer auf der ONTAP Tools für VMware vSphere Startseite aus dem Menü „Storage Systems“ abrufen. Wählen Sie das Storage-System

(SVM) und anschließend „Related Objects“ > „SAN“ aus. Verwenden Sie diesen Ansatz, wenn Sie die QoS mit einem der ONTAP Tools angeben.

Siehe "Performance Monitoring und Management – Überblick" Finden Sie weitere Informationen.

Nicht-VVols NFS-Datastores

Eine ONTAP QoS-Richtlinie kann auf den gesamten Datenspeicher oder auf einzelne VMDK-Dateien darin angewendet werden. Es ist jedoch wichtig zu beachten, dass alle VMs eines herkömmlichen NFS-Datenspeichers (ohne VVols) eine gemeinsame I/O-Warteschlange von einem bestimmten Host verwenden. Wenn eine VM durch eine ONTAP QoS-Richtlinie gedrosselt ist, werden in der Praxis alle I/O-Vorgänge für diesen Datastore scheinbar für diesen Host gedrosselt.

Beispiel:
* Sie konfigurieren eine QoS-Begrenzung auf vm1.vmdk für ein Volume, das als herkömmlicher NFS-Datenspeicher durch Host esxi-01 gemountet wird.
* Der gleiche Host (esxi-01) verwendet vm2.vmdk und es ist auf dem gleichen Volume.
* Wenn vm1.vmdk gedrosselt wird, dann wird vm2.vmdk auch scheinen gedrosselt zu sein, da es sich die gleiche IO-Warteschlange mit vm1.vmdk teilt.

Dies gilt nicht für VVols.

Ab vSphere 6.5 können Sie bei Datastores, die nicht über VVols verfügen, granulare Dateilimits managen. Sie nutzen dazu Storage Policy-basiertes Management (SPBM) mit Storage I/O Control (SIOC) v2.

Weitere Informationen zum Leistungsmanagement mit SIOC- und SPBM-Richtlinien finden Sie unter den folgenden Links.

"SPBM Host-basierte Regeln: SIOC v2"
"Managen Sie Storage-I/O-Ressourcen mit vSphere"

Beachten Sie folgende Vorgaben, wenn Sie eine QoS-Richtlinie auf eine VMDK in NFS anwenden:

- Die Politik muss auf das angewendet werden `vmname-flat.vmdk` Die das tatsächliche Image des virtuellen Laufwerks enthält, nicht das `vmname.vmdk` (Deskriptordatei für virtuelle Festplatten) oder `vmname.vmx` (VM-Deskriptordatei).
- Wenden Sie keine Richtlinien auf andere VM-Dateien wie virtuelle Swap-Dateien an (`vmname.vswp`).
- Wenn Sie Dateipfade mithilfe des vSphere Webclients ermitteln („Datastore“ > „Files“), denken Sie daran, dass dieser die Informationen der zusammenfasst `- flat.vmdk` Und `. vmdk` Und zeigt einfach eine Datei mit dem Namen des an `. vmdk` Aber die Größe der `- flat.vmdk`. Zusatz `-flat` In den Dateinamen, um den richtigen Pfad zu erhalten.

FlexGroup Datastores bieten erweiterte QoS-Funktionen, wenn ONTAP Tools für VMware vSphere 9.8 und höher verwendet werden. Sie können ganz einfach QoS für alle VMs in einem Datastore oder für bestimmte VMs festlegen. Weitere Informationen finden Sie im Abschnitt „FlexGroup“ dieses Berichts. Beachten Sie, dass die zuvor erwähnten Einschränkungen von QoS bei herkömmlichen NFS-Datastores weiterhin gelten.

VMFS-Datastores

Die QoS-Richtlinien können mithilfe von ONTAP LUNs auf das FlexVol Volume, das die LUNs enthält, oder auf einzelne LUNs angewendet werden, jedoch nicht auf einzelne VMDK-Dateien, weil ONTAP das VMFS Filesystem nicht erkennt.

VVols Datastores

Die minimale und/oder maximale QoS kann problemlos auf einzelnen VMs oder VMDKs festgelegt werden, ohne dass andere VMs oder VMDK durch das richtlinienbasierte Storage-Management und VVols beeinträchtigt werden.

Wenn Sie das Storage-Funktionsprofil für den vVol Container erstellen, geben Sie unter der Performance-Funktion einen IOPS-Wert für max und/oder min an und verweisen dann mit der Storage-Richtlinie der VM auf dieses Storage-Funktionsprofil. Verwenden Sie diese Richtlinie beim Erstellen der VM oder beim Anwenden der Richtlinie auf eine vorhandene VM.

VVols erfordert die Verwendung von ONTAP Tools für VMware vSphere, die als VASA Provider für ONTAP fungiert. Weitere Informationen zu VVols finden Sie unter "VMware vSphere Virtual Volumes (VVols) mit ONTAP"Best Practices.

ONTAP QoS und VMware SIOC

ONTAP QoS und VMware vSphere Storage I/O Control (SIOC) sind Technologien, die sich gegenseitig ergänzen und die vSphere und Storage-Administratoren gemeinsam nutzen können, um die Performance von vSphere VMs zu managen, die auf Systemen mit ONTAP ausgeführt werden. Wie in der folgenden Tabelle zu sehen ist, hat jedes Tool seine eigenen Stärken. Aufgrund des unterschiedlichen Umfangs von VMware vCenter und ONTAP kann es sein, dass einige Objekte von einem System erkannt und gemanagt werden können, vom anderen jedoch nicht.

Eigenschaft	ONTAP-QoS	VMware SIOC
Wenn aktiv	Richtlinie ist immer aktiv	Aktiv, wenn ein Konflikt besteht (Datastore-Latenz über Schwellenwert)
Einheiten	IOPS, MB/Sek.	IOPS, Freigaben
Umfang von vCenter oder Applikation	Mehrere vCenter Umgebungen, andere Hypervisoren und Applikationen	Einzelner vCenter Server
QoS auf VM festlegen?	VMDK nur auf NFS	VMDK auf NFS oder VMFS
QoS auf LUN festlegen (RDM)?	Ja.	Nein
QoS auf LUN festlegen (VMFS)?	Ja.	Ja (der Datastore kann gedrosselt werden)
QoS auf Volume festlegen (NFS-Datastore)?	Ja.	Ja (der Datastore kann gedrosselt werden)
QoS auf SVM festlegen (Mandant)?	Ja.	Nein
Richtlinienbasierter Ansatz?	Ja – kann von allen Workloads in der Richtlinie geteilt oder vollständig auf jeden Workload in der Richtlinie angewendet werden.	Ja, mit vSphere 6.5 und höher.
Lizenz erforderlich	In ONTAP enthalten	Enterprise Plus

VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler (SDRS) ist eine Funktion von vSphere, die VMs auf Storage basierend auf der aktuellen I/O-Latenz und der Speicherplatznutzung platziert. Danach werden die VM oder VMDKs unterbrechungsfrei zwischen den Datastores in einem Datastore-Cluster (auch Pod genannt) verschoben und es wird der beste Datastore ausgewählt, in dem die VM oder die VMDKs im Datastore-Cluster platziert werden sollen. Ein Datastore-Cluster ist eine Sammlung ähnlicher Datastores, die aus Sicht des vSphere Administrators in einer einzigen Verbrauchseinheit aggregiert werden.

Wenn Sie SDRS mit ONTAP Tools für VMware vSphere verwenden, müssen Sie zuerst einen Datastore mit dem Plug-in erstellen, das Datastore-Cluster mithilfe von vCenter erstellen und diesem dann den Datastore hinzufügen. Nach der Erstellung des Datastore-Clusters können diesem direkt aus dem Assistenten für die Datastore-Bereitstellung auf der Seite „Details“ weitere Datastores hinzugefügt werden.

Weitere ONTAP Best Practices für SDRS:

- Alle Datastores im Cluster sollten denselben Storage-Typ (beispielsweise SAS, SATA oder SSD) verwenden. Zudem sollte es sich bei allen entweder um VMFS oder NFS-Datastores handeln und sie sollten dieselben Replizierungs- und Sicherungseinstellungen aufweisen.
- Sie sollten SDRS eventuell im Standardmodus (manuell) verwenden. Mit diesem Ansatz können Sie die Empfehlungen prüfen und entscheiden, ob Sie sie anwenden oder nicht. Beachten Sie diese Auswirkungen von VMDK Migrationen:
  - Wenn VMDKs VON SDRS zwischen Datastores verschoben werden, gehen sämtliche Speicherersparnisse durch ONTAP Klone oder Deduplizierung verloren. Sie können die Deduplizierung erneut ausführen, um diese Einsparungen zurückzugewinnen.
  - Nachdem SDRS die VMDKs verschoben hat, empfiehlt NetApp, die Snapshots im Quell-Datastore neu zu erstellen, da der Speicherplatz andernfalls von der verschobenen VM gesperrt wird.
  - Die Verschiebung von VMDKs zwischen Datastores im selben Aggregat bietet nur wenige Vorteile. Zudem sind andere Workloads, die das Aggregat möglicherweise teilen, FÜR SDRS nicht sichtbar.

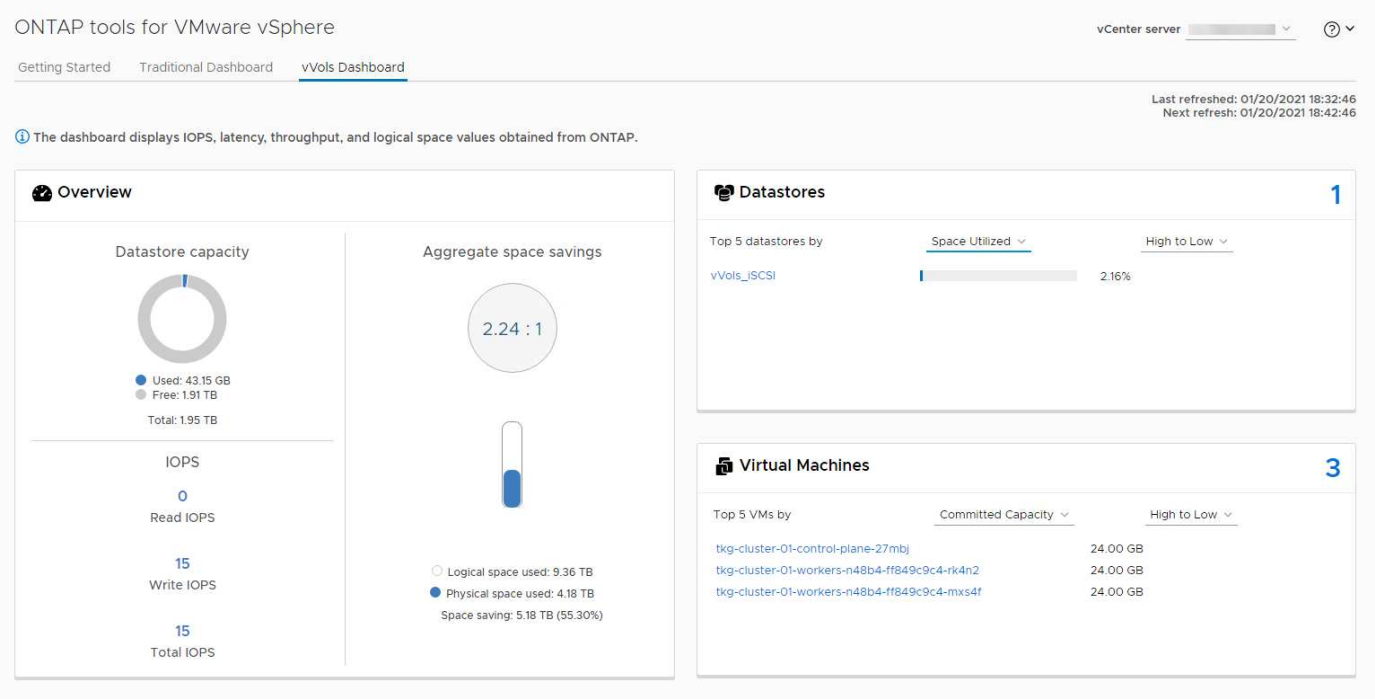
Richtlinienbasiertes Storage-Management und VVols

VMware vSphere APIs for Storage Awareness (VASA) erleichtern einem Storage-Administrator die Konfiguration von Datastores mit klar definierten Funktionen. Der VM-Administrator kann sie zudem im Bedarfsfall jederzeit nutzen, um VMs bereitzustellen, ohne dass eine Interaktion stattfinden muss. Eine genauere Betrachtung dieses Ansatzes lohnt sich für Sie, wenn Sie feststellen möchten, wie er Ihre Storage-Virtualisierungsvorgänge optimieren und Ihnen viele banale Arbeiten ersparen kann.

Vor VASA konnten VM-Administratoren VM-Storage-Richtlinien definieren, mussten aber gemeinsam mit dem Storage-Administrator geeignete Datastores ermitteln – oft anhand der Dokumentation oder von Namenskonventionen. Mit VASA kann der Storage-Administrator eine Reihe von Storage-Funktionen definieren, darunter Performance, Tiering, Verschlüsselung und Replizierung. Ein Satz von Funktionen für ein Volume oder eine Gruppe von Volumes wird als Storage-Funktionsprofil (Storage Capability Profile, SCP) bezeichnet.

Das SCP unterstützt die minimale und/oder maximale QoS für die Daten-VVols einer VM. Minimale QoS wird nur auf AFF Systemen unterstützt. ONTAP Tools für VMware vSphere umfassen ein Dashboard, in dem die granulare VM-Performance und logische Kapazität für VVols auf ONTAP Systemen angezeigt werden.

In der folgenden Abbildung sind die ONTAP Tools für das Dashboard von VMware vSphere 9.8 VVols dargestellt.



Nachdem ein Storage-Funktionsprofil definiert wurde, können damit anhand der Storage-Richtlinie, in der die entsprechenden Anforderungen angegeben sind, VMs bereitgestellt werden. Durch die Zuordnung zwischen der VM-Storage-Richtlinie und dem Datastore-Storage-Funktionsprofil kann in vCenter eine Liste kompatibler Datastores zur Auswahl angezeigt werden. Dieser Ansatz wird als richtlinienbasiertes Storage-Management bezeichnet.

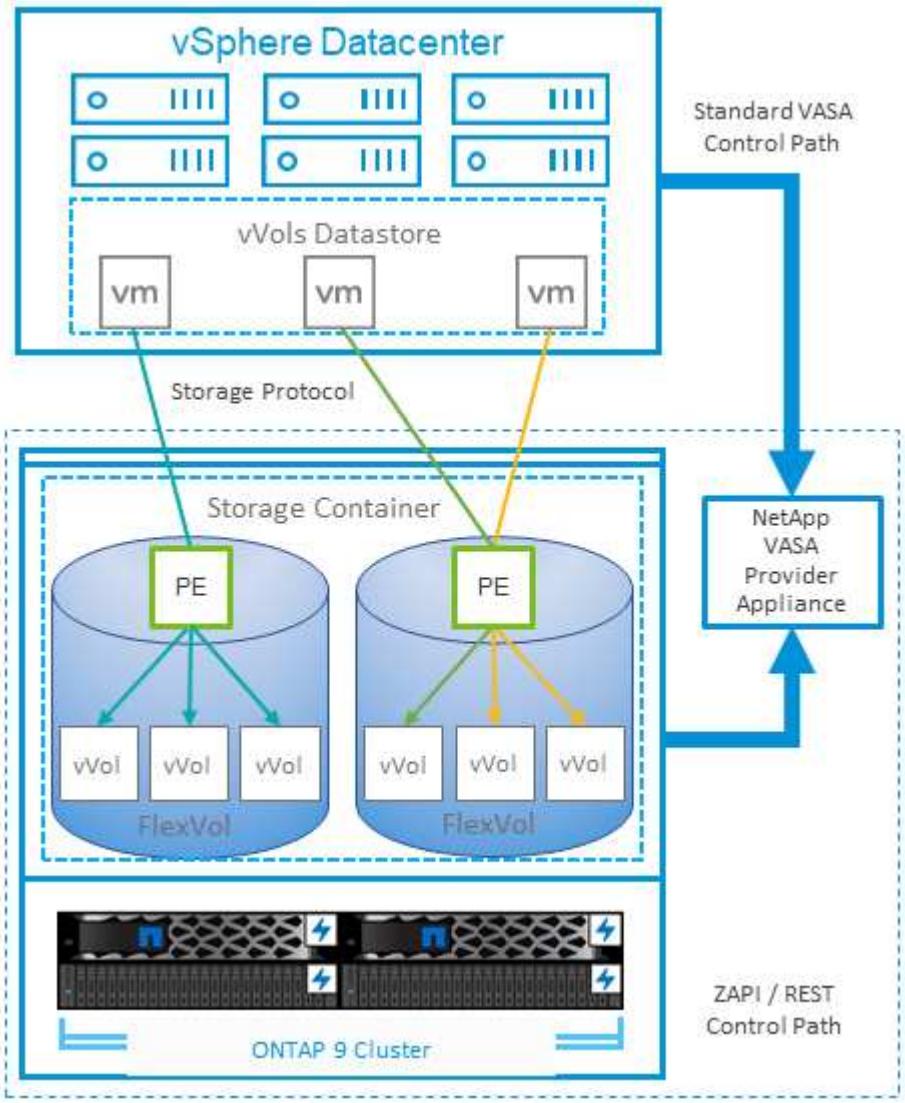
VASA stellt die Technologie bereit, mit der der Storage abgefragt und eine Reihe von Storage-Funktionen an vCenter zurückgegeben werden können. VASA Provider stellen die Übersetzung zwischen den Storage-System-APIs und -Konstrukten einerseits und den von vCenter erkannten VMware APIs bereit. NetApp VASA Provider für ONTAP wird als Teil der ONTAP Tools für die VMware vSphere Appliance VM angeboten. Das vCenter Plug-in bietet die Schnittstelle zum Bereitstellen und Managen von vVol Datastores und bietet die Möglichkeit, Storage-Funktionsprofile zu definieren.

ONTAP unterstützt sowohl VMFS als auch NFS vVol Datastores. Bei gemeinsamer Verwendung von VVols und SAN-Datastores profitieren Sie von einigen der Vorteile von NFS, beispielsweise von Granularität auf VM-Ebene. Im Folgenden werden einige der zu berücksichtigende Best Practices beschrieben. Weitere Informationen finden Sie unter "TR-4400":

- Ein vVol Datastore kann aus mehreren FlexVol Volumes auf mehreren Cluster-Nodes bestehen. Den einfachsten Ansatz stellt ein einzelner Datastore dar, selbst wenn die Volumes unterschiedliche Funktionen haben. SPBM stellt sicher, dass ein kompatibles Volume für die VM verwendet wird. Die Volumes müssen allerdings alle einer einzigen ONTAP SVM angehören und es muss über ein einziges Protokoll auf sie zugegriffen werden. Für jedes Protokoll reicht eine logische Schnittstelle pro Node aus. Es empfiehlt sich nicht, mehrere ONTAP Versionen in einem einzelnen vVol Datastore zu nutzen, da sich die Storage-Funktionen in verschiedenen Versionen unter Umständen unterscheiden.
- Verwenden Sie die ONTAP Tools für VMware vSphere Plug-in, um vVol Datastores zu erstellen und zu managen. Neben dem Management des Datastores und dessen Profil erstellt es bei Bedarf automatisch einen Protokollendpunkt für den Zugriff auf die VVols. Falls LUNs verwendet werden, werden LUN-Protokollendpunkte (PES) mit LUN-IDs ab 300 zugeordnet. Vergewissern Sie sich, dass die erweiterte Systemeinstellung des ESXi-Hosts aktiviert ist `Disk.MaxLUN` Ermöglicht eine LUN-ID-Nummer, die über 300 liegt (Standard ist 1,024). Wählen Sie diesen Schritt aus: ESXi Host in vCenter, dann Registerkarte „Configure“ und suchen Sie `Disk.MaxLUN` In der Liste der erweiterten Systemeinstellungen.

- Installieren oder migrieren Sie VASA Provider, vCenter Server (Appliance oder Windows basierte Version) oder ONTAP Tools für VMware vSphere selbst nicht auf einem VVols Datastore, da diese dann voneinander abhängen. Im Falle eines Stromausfalls oder einer anderen Störung im Datacenter könnten Sie sie dann nur begrenzt managen.
- Sichern Sie die VASA Provider VM in regelmäßigen Abständen. Erstellen Sie mindestens stündlich Snapshots des herkömmlichen Datastores, der VASA Provider umfasst. Weitere Informationen zum Sichern und Wiederherstellen von VASA Provider finden Sie in diesem Abschnitt "KB-Artikel".

In der folgenden Abbildung werden die VVols Komponenten angezeigt.



Cloud-Migration und -Backup

Eine weitere Stärke von ONTAP ist die umfassende Unterstützung für die Hybrid Cloud, bei der Systeme in Ihrer Private Cloud vor Ort mit Public-Cloud-Funktionen vereint werden. Im Folgenden sind einige NetApp Cloud-Lösungen aufgeführt, die gemeinsam mit vSphere verwendet werden können:

- **Angebote von Erstanbietern.** Amazon FSx for NetApp ONTAP, Google Cloud NetApp Volumes und Azure NetApp Files bieten leistungsstarke, multiprotokollverwaltete Speicherdienste in den führenden öffentlichen Cloud-Umgebungen. Sie können direkt von VMware Cloud on AWS (VMC on AWS), Azure

VMware Solution (AVS) und Google Cloud VMware Engine (GCVE) als Datenspeicher oder Speicher für Gastbetriebssysteme (GOS) und Compute-Instanzen verwendet werden.

- **Cloud-Dienste.** Verwenden Sie NetApp Backup and Recovery oder SnapMirror Cloud, um Daten von lokalen Systemen mithilfe von öffentlichem Cloud-Speicher zu schützen. NetApp Copy and Sync unterstützt Sie bei der Migration und Synchronisierung Ihrer Daten über NAS und Objektspeicher hinweg. NetApp Disaster Recovery bietet eine kostengünstige und effiziente Lösung zur Nutzung von NetApp -Technologien als Grundlage für eine robuste und leistungsfähige Disaster Recovery-Lösung für DR in die Cloud, DR vor Ort und vor Ort zu vor Ort.
- **FabricPool.** FabricPool bietet schnelles und einfaches Tiering für ONTAP Daten. Selten genutzte, „kalte“ Blöcke können zu einem Objektspeicher in Public Clouds oder zu einem privaten StorageGRID Objektspeicher migriert werden und beim erneuten Zugriff auf die ONTAP-Daten automatisch wieder abgerufen werden. Alternativ können Sie die Objekt-Tier als dritte Schutzebene für Daten verwenden, die bereits von SnapVault gemanagt werden. Dieser Ansatz kann Ihnen ermöglichen "Speichern Sie mehr Snapshots Ihrer VMs" Auf primären und/oder sekundären ONTAP-Storage-Systemen.
- **ONTAP Select.** mit softwaredefiniertem NetApp Storage erweitern Sie Ihre Private Cloud über das Internet auf Remote-Einrichtungen und Niederlassungen, in denen Sie ONTAP Select zur Unterstützung von Block- und Fileservices sowie denselben vSphere Datenmanagementfunktionen nutzen können, die Sie in Ihrem Unternehmens-Datacenter haben.

Berücksichtigen Sie beim Entwerfen Ihrer VM-basierten Anwendungen die zukünftige Cloud-Mobilität. Anstatt beispielsweise Anwendungs- und Datendateien zusammen zu platzieren, verwenden Sie einen separaten LUN- oder NFS-Export für die Daten. Dadurch können Sie die VM und die Daten separat zu Cloud-Diensten migrieren.

In den folgenden Ressourcen erhalten Sie ausführliche Informationen zu weiteren Sicherheitsthemen.

- "ONTAP Select-Dokumentation"
- "Dokumentation zu Sicherung und Wiederherstellung"
- "Disaster Recovery-Dokumentation"
- "Amazon FSX für NetApp ONTAP"
- "VMware Cloud auf AWS"
- "Was ist Azure NetApp Files?"
- "Azure VMware Lösung"
- "Google Cloud VMware Engine"
- "Was ist Google Cloud NetApp Volumes?"

Verschlüsselung für vSphere Daten

Heute besteht eine wachsende Nachfrage, Daten im Ruhezustand durch Verschlüsselung zu sichern. Obwohl der Schwerpunkt anfänglich auf Informationen im Finanz- und Gesundheitswesen lag, gibt es ein zunehmendes Interesse an der Sicherung sämtlicher Informationen – seien sie in Dateien, Datenbanken oder in anderen Datentypen gesichert.

Systeme mit ONTAP vereinfachen die Sicherung sämtlicher Daten durch Verschlüsselung im Ruhezustand. Die NetApp Storage-Verschlüsselung (NSE) verwendet Self-Encrypting Drives (SEDs) mit ONTAP, um SAN- und NAS-Daten zu sichern. NetApp bietet darüber hinaus NetApp Volume Encryption und NetApp Aggregate Encryption als einen einfachen, softwarebasierten Ansatz zur Verschlüsselung von Volumes auf

Festplattenlaufwerken. Für diese Softwareverschlüsselung sind keine speziellen Festplatten oder externen Schlüsselmanager erforderlich. Es ist für ONTAP Kunden kostenlos verfügbar. Ihre Clients oder Applikationen sind mit Upgrades und deren Nutzung ohne Unterbrechung startbereit. Die Systeme sind nach FIPS 140-2 Level 1 validiert, einschließlich Onboard Key Manager.

Für die Sicherung der Daten virtualisierter Applikationen unter VMware vSphere gibt es verschiedene Ansätze. Einer besteht darin, die Daten mit Software innerhalb der VM auf der Ebene des Gastbetriebssystems zu sichern. Alternativ dazu unterstützen neuere Hypervisoren wie vSphere 6.5 jetzt auch Verschlüsselung auf VM-Ebene. Die NetApp Softwareverschlüsselung ist jedoch eine einfache und bietet folgende Vorteile:

- **Keine Auswirkung auf die virtuelle Server-CPU.** in einigen virtuellen Server-Umgebungen ist jeder verfügbare CPU-Zyklus für ihre Anwendungen erforderlich, aber Tests haben ergeben, dass bei Verschlüsselung auf Hypervisor-Ebene bis zu 5x CPU-Ressourcen benötigt werden. Selbst wenn die Verschlüsselungssoftware zur Verlagerung von Verschlüsselungs-Workloads den AES-NI Befehlssatz von Intel unterstützt (wie es bei der NetApp-Softwareverschlüsselung der Fall ist), ist dieser Ansatz aufgrund der Notwendigkeit neuer CPUs, die nicht mit älteren Servern kompatibel sind, unter Umständen nicht realisierbar.
- **Onboard Key Manager inbegriffen.** Die NetApp Softwareverschlüsselung umfasst einen Onboard Key Manager ohne zusätzliche Kosten. So ist der Einstieg ohne hochverfügbare Verschlüsselungsmanagement-Server leicht, die sich aufgrund der komplexen Anschaffung und Nutzung auszahlen lassen.
- **Keine Auswirkungen auf die Storage-Effizienz.** Storage-Effizienztechniken wie Deduplizierung und Komprimierung werden heute weit verbreitet und sind für eine kostengünstige Nutzung von Flash-Speicher von zentraler Bedeutung. Verschlüsselte Daten können in der Regel jedoch nicht dedupliziert oder komprimiert werden. Die Hardware- und Storage-Verschlüsselung von NetApp arbeitet auf niedrigerer Ebene und ermöglicht im Gegensatz zu anderen Ansätzen die vollständige Nutzung der branchenführenden NetApp Storage-Effizienzfunktionen.
- **Einfache granulare Datastore-Verschlüsselung.** mit NetApp Volume Encryption erhält jedes Volume einen eigenen AES 256-Bit-Schlüssel. Wenn Sie diesen ändern müssen, müssen Sie dazu nur einen einzigen Befehl ausführen. Dieser Ansatz eignet sich ideal, wenn Sie mehrere Mandanten haben oder für unterschiedliche Abteilungen oder Apps eine unabhängige Verschlüsselung nachweisen müssen. Diese Verschlüsselung wird auf Datastore-Ebene gemanagt, was viel einfacher ist als das Management einzelner VMs.

Die ersten Schritte mit Softwareverschlüsselung sind ganz einfach. Nach der Installation der Lizenz konfigurieren Sie einfach den Onboard Key Manager, indem Sie eine Passphrase angeben und dann entweder ein neues Volume erstellen oder ein Storage-seitiges Volume verschieben, um die Verschlüsselung zu aktivieren. NetApp arbeitet daran, künftige Versionen seiner VMware Tools um zusätzliche integrierte Unterstützung von Verschlüsselungsfunktionen zu erweitern.

In den folgenden Ressourcen erhalten Sie ausführliche Informationen zu weiteren Sicherheitsthemen.

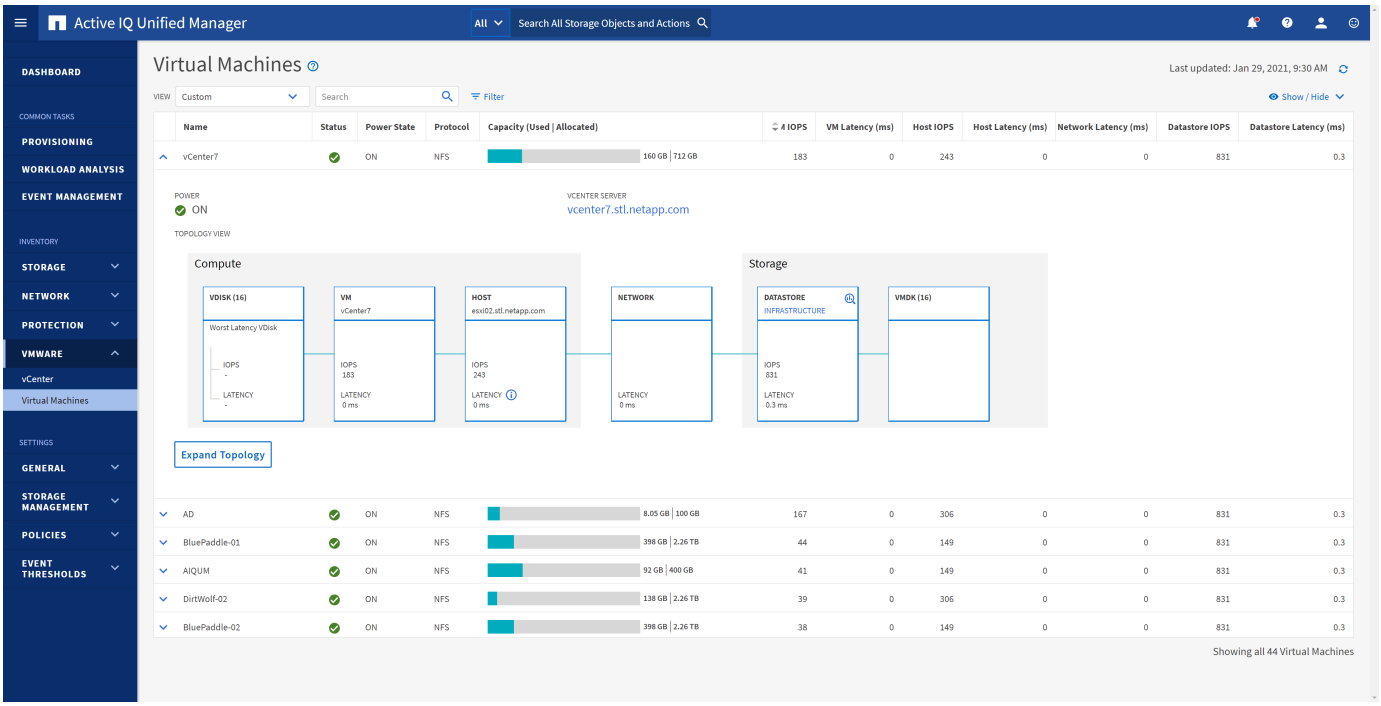
- "Technische Sicherheitsberichte"
- "Leitfäden zur Erhöhung der Sicherheit"
- "Produktdokumentation zu ONTAP Sicherheit und Datenverschlüsselung"

Active IQ Unified Manager

Active IQ Unified Manager bietet einen Überblick über die VMs in Ihrer virtuellen Infrastruktur und ermöglicht die Überwachung und Fehlerbehebung von Storage- und Performance-Problemen in Ihrer virtuellen Umgebung.

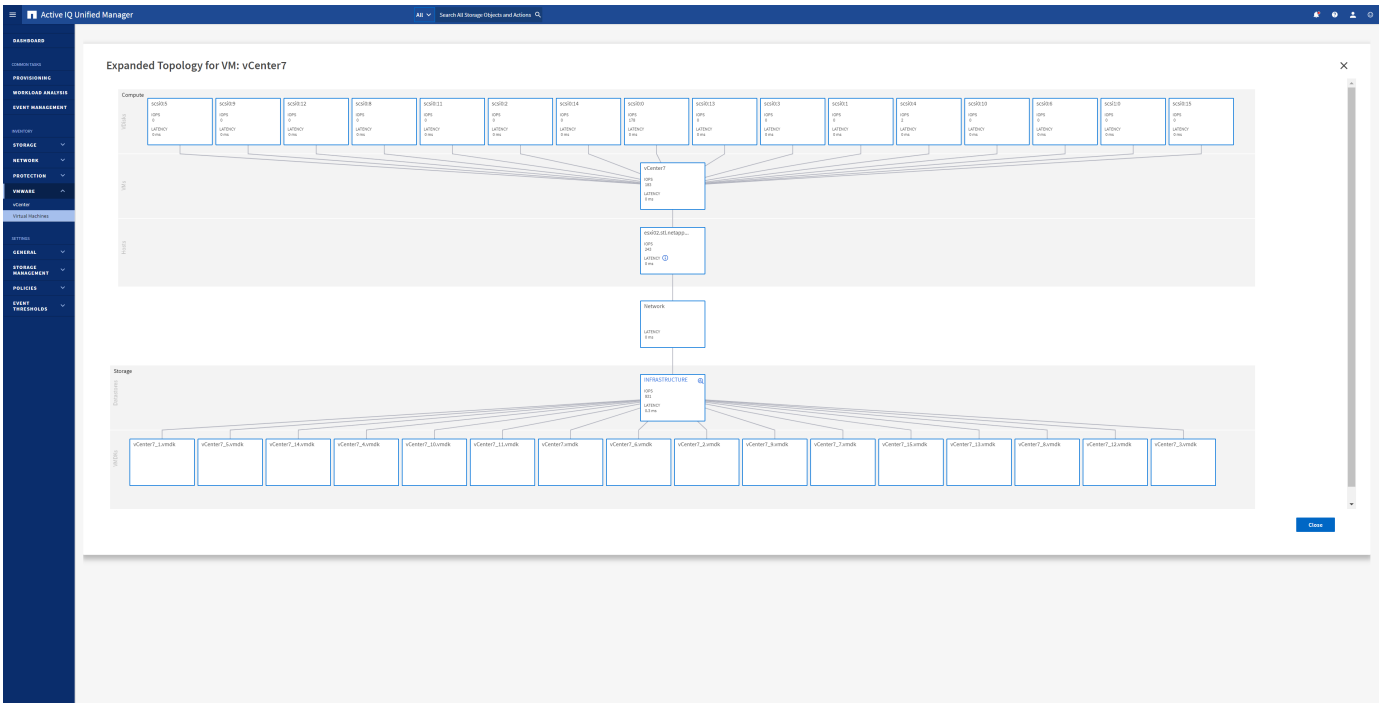
Eine typische Implementierung einer virtuellen Infrastruktur auf ONTAP setzt auf verschiedene Komponenten, die auf Computing-, Netzwerk- und Storage-Ebenen verteilt sind. Alle Performance-Einbußen bei einer VM-Applikation können aufgrund einer Kombination aus Latenzen auftreten, die bei den verschiedenen Komponenten auf den jeweiligen Ebenen auftreten.

Der folgende Screenshot zeigt die Ansicht der virtuellen Active IQ Unified Manager Machines.



Unified Manager stellt das zugrunde liegende Untersystem einer virtuellen Umgebung in einer topologischen Übersicht vor, um zu ermitteln, ob beim Computing-Node, Netzwerk oder Storage ein Latenzproblem aufgetreten ist. Die Ansicht zeigt außerdem das spezifische Objekt, das aufgrund der Performance-Verzögerung Korrekturmaßnahmen ergreifen und das zugrunde liegende Problem lösen kann.

Der folgende Screenshot zeigt die erweiterte AIQUM-Topologie.



Richtlinienbasiertes Storage-Management und VVols

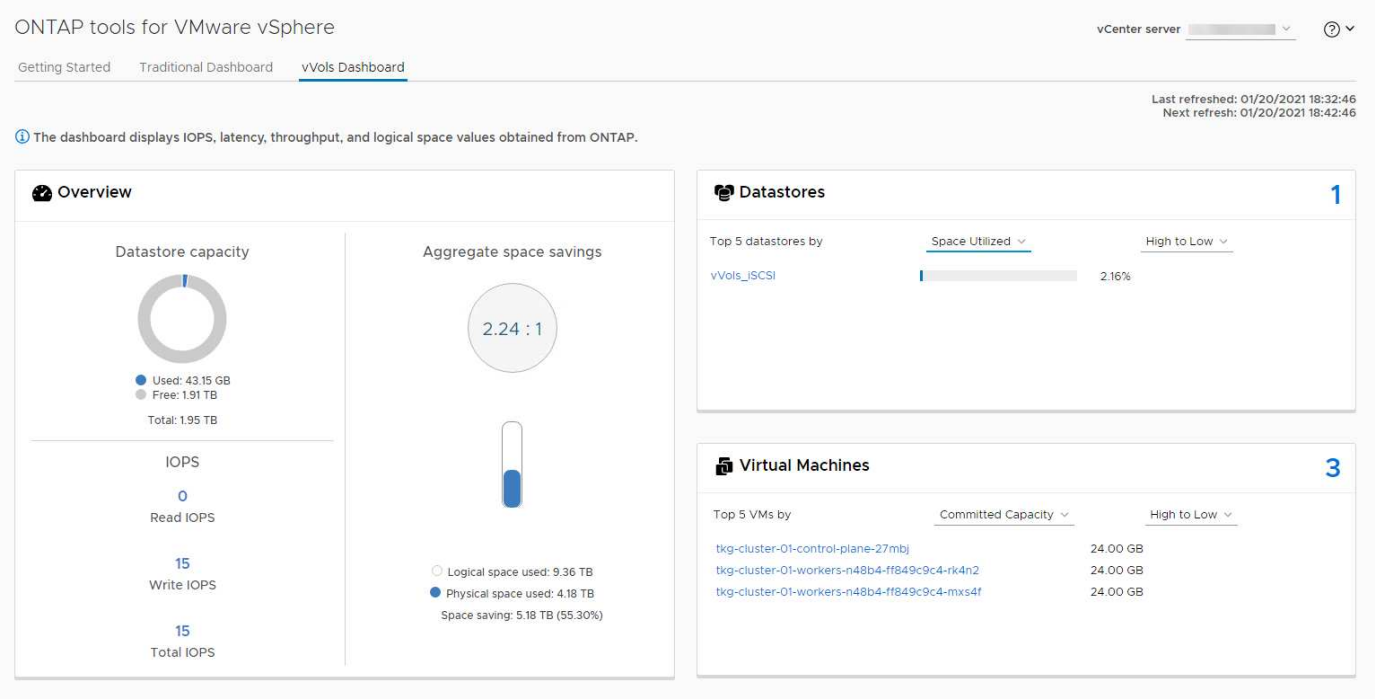
VMware vSphere APIs for Storage Awareness (VASA) erleichtern einem Storage-Administrator die Konfiguration von Datastores mit klar definierten Funktionen. Der VM-Administrator kann sie zudem im Bedarfsfall jederzeit nutzen, um VMs bereitzustellen, ohne dass eine Interaktion stattfinden muss.

Eine genauere Betrachtung dieses Ansatzes lohnt sich für Sie, wenn Sie feststellen möchten, wie er Ihre Storage-Virtualisierungsvorgänge optimieren und Ihnen viele banale Arbeiten ersparen kann.

Vor VASA konnten VM-Administratoren VM-Storage-Richtlinien definieren, mussten aber gemeinsam mit dem Storage-Administrator geeignete Datastores ermitteln – oft anhand der Dokumentation oder von Namenskonventionen. Mit VASA kann der Storage-Administrator eine Reihe von Storage-Funktionen definieren, darunter Performance, Tiering, Verschlüsselung und Replizierung. Ein Satz von Funktionen für ein Volume oder eine Gruppe von Volumes wird als Storage-Funktionsprofil (Storage Capability Profile, SCP) bezeichnet.

Das SCP unterstützt die minimale und/oder maximale QoS für die Daten-VVols einer VM. Minimale QoS wird nur auf AFF Systemen unterstützt. ONTAP Tools für VMware vSphere umfassen ein Dashboard, in dem die granulare VM-Performance und logische Kapazität für VVols auf ONTAP Systemen angezeigt werden.

In der folgenden Abbildung sind die ONTAP Tools für das Dashboard von VMware vSphere 9.8 VVols dargestellt.



Nachdem ein Storage-Funktionsprofil definiert wurde, können damit anhand der Storage-Richtlinie, in der die entsprechenden Anforderungen angegeben sind, VMs bereitgestellt werden. Durch die Zuordnung zwischen der VM-Storage-Richtlinie und dem Datastore-Storage-Funktionsprofil kann in vCenter eine Liste kompatibler Datastores zur Auswahl angezeigt werden. Dieser Ansatz wird als richtlinienbasiertes Storage-Management bezeichnet.

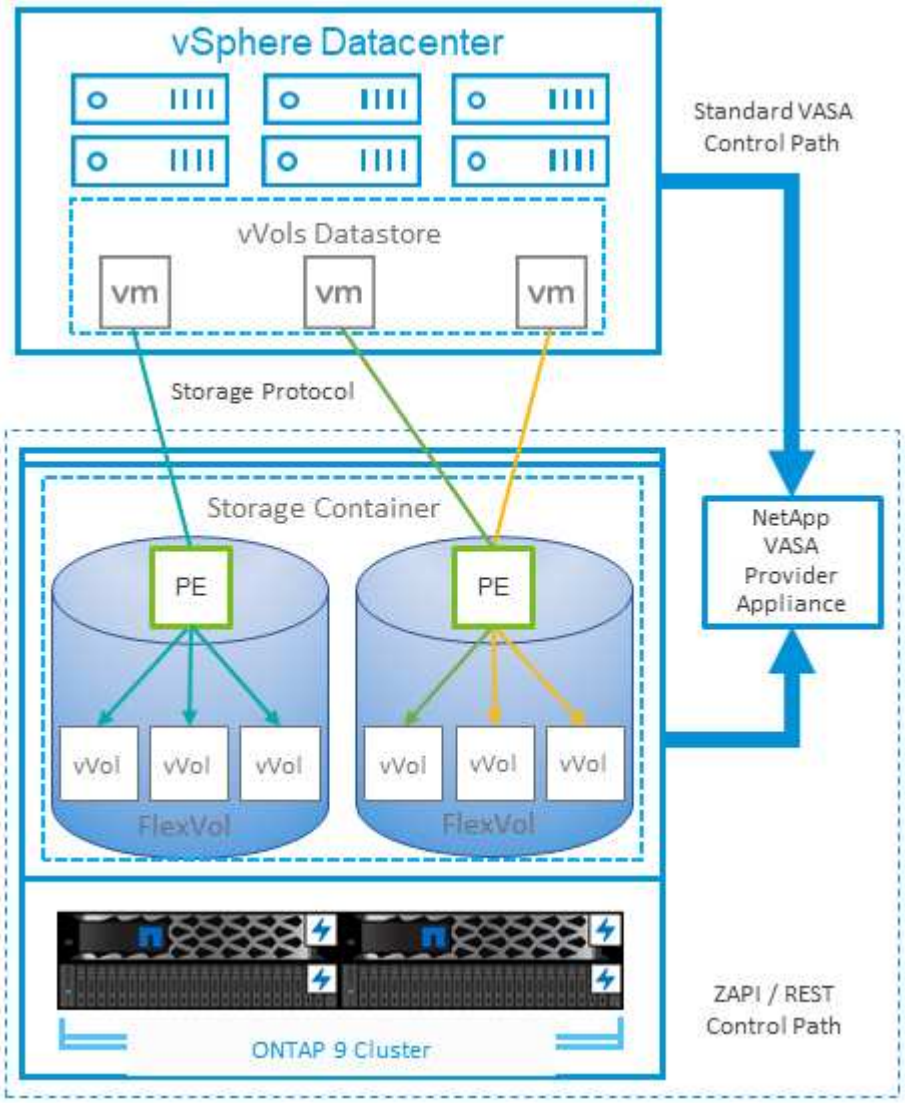
VASA stellt die Technologie bereit, mit der der Storage abgefragt und eine Reihe von Storage-Funktionen an vCenter zurückgegeben werden können. VASA Provider stellen die Übersetzung zwischen den Storage-System-APIs und -Konstrukten einerseits und den von vCenter erkannten VMware APIs bereit. NetApp VASA Provider für ONTAP wird als Teil der ONTAP Tools für die VMware vSphere Appliance VM angeboten. Das vCenter Plug-in bietet die Schnittstelle zum Bereitstellen und Managen von vVol Datastores und bietet die Möglichkeit, Storage-Funktionsprofile zu definieren.

ONTAP unterstützt sowohl VMFS als auch NFS vVol Datastores. Bei gemeinsamer Verwendung von VVols und SAN-Datastores profitieren Sie von einigen der Vorteile von NFS, beispielsweise von Granularität auf VM-Ebene. Im Folgenden werden einige der zu berücksichtigende Best Practices beschrieben. Weitere Informationen finden Sie unter "TR-4400":

- Ein vVol Datastore kann aus mehreren FlexVol Volumes auf mehreren Cluster-Nodes bestehen. Den einfachsten Ansatz stellt ein einzelner Datastore dar, selbst wenn die Volumes unterschiedliche Funktionen haben. SPBM stellt sicher, dass ein kompatibles Volume für die VM verwendet wird. Die Volumes müssen allerdings alle einer einzigen ONTAP SVM angehören und es muss über ein einziges Protokoll auf sie zugegriffen werden. Für jedes Protokoll reicht eine logische Schnittstelle pro Node aus. Es empfiehlt sich nicht, mehrere ONTAP Versionen in einem einzelnen vVol Datastore zu nutzen, da sich die Storage-Funktionen in verschiedenen Versionen unter Umständen unterscheiden.
- Verwenden Sie die ONTAP Tools für VMware vSphere Plug-in, um vVol Datastores zu erstellen und zu managen. Neben dem Management des Datastores und dessen Profil erstellt es bei Bedarf automatisch einen Protokollendpunkt für den Zugriff auf die VVols. Falls LUNs verwendet werden, werden LUN-Protokollendpunkte (PES) mit LUN-IDs ab 300 zugeordnet. Vergewissern Sie sich, dass die erweiterte Systemeinstellung des ESXi-Hosts aktiviert ist `Disk.MaxLUN` Ermöglicht eine LUN-ID-Nummer, die über 300 liegt (Standard ist 1,024). Wählen Sie diesen Schritt aus: ESXi Host in vCenter, dann Registerkarte „Configure“ und suchen Sie `Disk.MaxLUN` In der Liste der erweiterten Systemeinstellungen.

- Installieren oder migrieren Sie VASA Provider, vCenter Server (Appliance oder Windows basierte Version) oder ONTAP Tools für VMware vSphere selbst nicht auf einem VVols Datastore, da diese dann voneinander abhängen. Im Falle eines Stromausfalls oder einer anderen Störung im Datacenter könnten Sie sie dann nur begrenzt managen.
- Sichern Sie die VASA Provider VM in regelmäßigen Abständen. Erstellen Sie mindestens stündlich Snapshots des herkömmlichen Datastores, der VASA Provider umfasst. Weitere Informationen zum Sichern und Wiederherstellen von VASA Provider finden Sie in diesem Abschnitt "KB-Artikel".

In der folgenden Abbildung werden die VVols Komponenten angezeigt.



VMware Storage Distributed Resource Scheduler

VMware Storage Distributed Resource Scheduler (SDRS) ist eine vSphere Funktion, die VMs automatisch in einem Datastore-Cluster platziert, basierend auf der aktuellen I/O-Latenz und Speicherplatznutzung.

Danach werden die VM oder VMDKs unterbrechungsfrei zwischen den Datastores in einem Datastore-Cluster (auch Pod genannt) verschoben und es wird der beste Datastore ausgewählt, in dem die VM oder die VMDKs im Datastore-Cluster platziert werden sollen. Ein Datastore-Cluster ist eine Sammlung ähnlicher Datastores, die aus Sicht des vSphere Administrators in einer einzigen Verbrauchseinheit aggregiert werden.

Wenn Sie SDRS mit ONTAP Tools für VMware vSphere verwenden, müssen Sie zuerst einen Datastore mit dem Plug-in erstellen, das Datastore-Cluster mithilfe von vCenter erstellen und diesem dann den Datastore hinzufügen. Nach der Erstellung des Datastore-Clusters können diesem direkt aus dem Assistenten für die Datastore-Bereitstellung auf der Seite „Details“ weitere Datastores hinzugefügt werden.

Weitere ONTAP Best Practices für SDRS:

- Verwenden Sie SDRS nicht, es sei denn, Sie haben dazu eine bestimmte Anforderung.
  - SDRS ist bei Verwendung von ONTAP nicht erforderlich. SDRS kennt die Storage-Effizienzfunktionen von ONTAP wie Deduplizierung und Komprimierung nicht und kann daher Entscheidungen treffen, die für Ihre Umgebung nicht optimal sind.
  - SDRS kennt die QoS-Richtlinien von ONTAP nicht und kann daher Entscheidungen treffen, die für die Performance nicht optimal sind.
  - SDRS kennt ONTAP Snapshot Kopien nicht und kann daher Entscheidungen treffen, die dazu führen, dass Snapshots exponentiell wachsen. Beispielsweise erstellt das Verschieben einer VM in einen anderen Datastore neue Dateien in dem neuen Datastore, was zu einer Vergrößerung des Snapshots führt. Dies gilt insbesondere für VMs mit großen Disks oder vielen Snapshots. Sollte die VM dann wieder zurück in den ursprünglichen Datenspeicher verschoben werden, wird der Snapshot im ursprünglichen Datenspeicher noch größer.

Bei der Verwendung von SDRS sollten Sie die folgenden Best Practices berücksichtigen:

- Alle Datastores im Cluster sollten denselben Storage-Typ (beispielsweise SAS, SATA oder SSD) verwenden. Zudem sollte es sich bei allen entweder um VMFS oder NFS-Datastores handeln und sie sollten dieselben Replizierungs- und Sicherungseinstellungen aufweisen.
- Sie sollten SDRS eventuell im Standardmodus (manuell) verwenden. Mit diesem Ansatz können Sie die Empfehlungen prüfen und entscheiden, ob Sie sie anwenden oder nicht. Beachten Sie diese Auswirkungen von VMDK Migrationen:
  - Wenn VMDKs von SDRS zwischen Datastores verschoben werden, können jegliche Speicherersparnisse durch ONTAP Klone oder Deduplizierung je nach der Deduplizierungsrate oder Komprimierung auf dem Zielsystem reduziert werden.
  - Nachdem SDRS die VMDKs verschoben hat, empfiehlt NetApp, die Snapshots im Quell-Datastore neu zu erstellen, da der Speicherplatz andernfalls von der verschobenen VM gesperrt wird.
  - Die Verschiebung von VMDKs zwischen Datastores im selben Aggregat bietet nur wenige Vorteile. Zudem sind andere Workloads, die das Aggregat möglicherweise teilen, FÜR SDRS nicht sichtbar.

Weitere Informationen zu SDRS finden Sie in der VMware Dokumentation unter "FAQ zu Storage DRS".

Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen

NetApp hat optimale ESXi Host-Einstellungen für NFS- und Blockprotokolle entwickelt. Des Weiteren finden Sie spezielle Anleitungen zu Multipathing- und HBA-Zeitüberschreitungseinstellungen, um ein angemessenes Verhalten gegenüber ONTAP auf der Grundlage interner Tests von NetApp und VMware zu gewährleisten.

Diese Werte lassen sich mit den ONTAP-Tools für VMware vSphere problemlos einstellen: Scrollen Sie auf der Übersichtsseite der ONTAP-Tools nach unten und klicken Sie im Portlet „ESXi-Host-Compliance“ auf empfohlene Einstellungen anwenden.

Im Folgenden finden Sie die empfohlenen Host-Einstellungen für alle derzeit unterstützten Versionen von

ONTAP.

Hosteinstellung	Von NetApp empfohlener Wert	Neustart Erforderlich
ESXi Advanced Configuration		
VMFS3.HardwareAcceleratLocking	Standard beibehalten (1)	Nein
VMFS3.EnableBlockDelete	Behalten Sie die Standardeinstellung (0) bei, können sie jedoch bei Bedarf geändert werden. Weitere Informationen finden Sie unter "Speicherplatzrückgewinnung für virtuelle VMFS5-Maschinen"	Nein
VMFS3.EnableVMFS6Entmappen	Behalten Sie die Standardeinstellung (1) bei. Weitere Informationen finden Sie unter "VMware vSphere APIs – Array-Integration (VAAI)"	Nein
NFS-Einstellungen		
NewSyncInterval	Wenn Sie vSphere CSI für Kubernetes nicht verwenden, setzen Sie per ein "VMware KB 386364"	Nein
NET.TcpipHeapSize	VSphere 6.0 oder höher: Auf 32 einstellen. Alle anderen NFS-Konfigurationen: Auf 30 einstellen	Ja.
NET.TcpipHeapMax	Sind die meisten vSphere 6.X Versionen auf 512 MB eingestellt. Für 6.5U3, 6.7U3 und 7.0 oder höher auf Standard (1024 MB) gesetzt.	Ja.
MaxVolumes: NFS	VSphere 6.0 oder höher: Auf 256 einstellen Alle anderen NFS-Konfigurationen auf 64 eingestellt.	Nein
NFS41.MaxVolumes	VSphere 6.0 oder höher: Auf 256 einstellen.	Nein
NFS.MaxQueueDepth[1]	VSphere 6.0 oder höher: Auf 128 einstellen	Ja.
NFS.HeartbeatMaxFailures	Alle NFS-Konfigurationen: Auf 10 einstellen	Nein
HeartbeatFrequency NFS.HeartbeatFrequency	Alle NFS-Konfigurationen: Auf 12 einstellen	Nein
HeartbeatTimeout NFS.HeartbeatTimeout	Alle NFS-Konfigurationen: Auf 5 einstellen.	Nein

Hosteinstellung	Von NetApp empfohlener Wert	Neustart Erforderlich
SunRPC.MaxConnPerIP	vSphere 7.0 bis 8.0, auf 128 eingestellt. Diese Einstellung wird in ESXi-Versionen nach 8.0 ignoriert.	Nein
FC/FCoE-Einstellungen		
Pfadauswahl-Richtlinie	Wenn FC-Pfade mit ALUA verwendet werden: Auf RR (Round Robin) einstellen. Alle anderen Konfigurationen: Auf FIXED einstellen. Wenn Sie diesen Wert auf RR einstellen, ist für alle aktiven/optimierten Pfade ein besserer Lastausgleich möglich. Der Wert FIXED wird für ältere Konfigurationen ohne ALUA verwendet und verhindert Proxy-I/O-Vorgänge Er trägt also dazu bei, dass I/O-Vorgänge bei einem HA-Paar in einer Umgebung, in der Data ONTAP im 7-Mode ausgeführt wird, nicht auf den anderen Node verlagert werden	Nein
Disk.QFullSampleSize	Alle Konfigurationen: Auf 32 einstellen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.	Nein
Disk.QFullThreshold	Alle Konfigurationen: Auf 8 einstellen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.	Nein
Emulex FC-HBA-Zeitüberschreitungen	Standardwert verwenden.	Nein
QLogic FC-HBA-Zeitüberschreitungen	Standardwert verwenden.	Nein
ISCSI-Einstellungen		
Pfadauswahl-Richtlinie	Alle iSCSI-Pfade: Auf RR (Round Robin) einstellen. Wenn Sie diesen Wert auf RR einstellen, ist für alle aktiven/optimierten Pfade ein besserer Lastausgleich möglich.	Nein

Hosteinstellung	Von NetApp empfohlener Wert	Neustart Erforderlich
Disk.QFullSampleSize	Alle Konfigurationen: Auf 32 einstellen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert	Nein
Disk.QFullThreshold	Alle Konfigurationen: Auf 8 einstellen. Durch die Festlegung dieses Wertes werden I/O-Fehler verhindert.	Nein

Die erweiterte NFS-Konfigurationsoption MaxQueueDepth funktioniert möglicherweise nicht wie vorgesehen, wenn VMware vSphere ESXi 7.0.1 und VMware vSphere ESXi 7.0.2 verwendet werden. Referenz "VMware KB 86331" für weitere Informationen.

ONTAP-Tools legen beim Erstellen von ONTAP FlexVol Volumes und LUNs bestimmte Standardeinstellungen fest:

ONTAP-Tool	Standardeinstellung
Snapshot-Reserve (-percent-Snapshot-space)	0
Fraktionale Reserve (-fractional-Reserve)	0
Aktualisierung der Zugriffszeit (-atime-Update)	Falsch
Minimales Vorauslesen (-min-readahead)	Falsch
Geplante Snapshots	Keine
Storage-Effizienz	Aktiviert
Volume-Garantie	Keine (Thin Provisioning)
Automatische Volumengröße	Vergrößern_verkleinern
LUN-Speicherplatzreservierung	Deaktiviert
Zuweisung von LUN-Speicherplatz	Aktiviert

Multipath-Einstellungen für die Performance

Obwohl NetApp derzeit nicht durch verfügbare ONTAP-Tools konfiguriert ist, empfiehlt es folgende Konfigurationsoptionen:

- Wenn Sie Nicht- ASA -Systeme in Hochleistungsumgebungen verwenden oder die Leistung mit einem einzelnen LUN-Datenspeicher testen, sollten Sie die Lastausgleichseinstellung der Round-Robin-Pfadauswahlrichtlinie (VMW_PSP_RR) von der IOPS-Standardeinstellung von 1000 auf den Wert 1 ändern. Sehen"VMware KB 2069356" für weitere Informationen.
- In vSphere 6.7 Update 1 hat VMware einen neuen Latenz-Lastausgleichsmechanismus für das Round Robin PSP eingeführt. Die Latenzoption ist jetzt auch bei Verwendung des HPP (High Performance Plugin) mit NVMe-Namespaces und mit vSphere 8.0u2 und höher, über iSCSI und FCP verbundenen LUNs verfügbar. Die neue Option berücksichtigt die E/A-Bandbreite und die Pfadlatenz bei der Auswahl des optimalen Pfads für die E/A. NetApp empfiehlt die Verwendung der Latenzoption in Umgebungen mit nicht

äquivalenter Pfadkonnektivität, beispielsweise in Fällen, in denen auf einem Pfad mehr Netzwerk-Hops vorhanden sind als auf einem anderen, oder bei Verwendung eines NetApp ASA -Systems. Sehen "Standardparameter für Latenzrunde Robin ändern" für weitere Informationen.

Zusätzliche Dokumentation

Für FCP und iSCSI mit vSphere 7 finden Sie weitere Informationen unter "Verwenden Sie VMware vSphere 7.x mit ONTAP" für FCP und iSCSI mit vSphere 8. Weitere Informationen finden Sie unter für NVMe-of mit vSphere 7. Weitere Details finden Sie unter "Verwenden Sie VMware vSphere 8.x mit ONTAP"für NVMe-of mit vSphere 8. Weitere Details finden Sie unter "Für NVMe-of finden Sie weitere Details unter NVMe-of Host Configuration for ESXi 7.x with ONTAP""Für NVMe-of finden Sie weitere Details unter NVMe-of Host Configuration for ESXi 8.x with ONTAP"

Virtual Volumes (VVols) mit ONTAP Tools 10

Überblick

ONTAP ist seit über zwei Jahrzehnten eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich mit innovativen Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen.

Dieses Dokument behandelt die ONTAP Funktionen für VMware vSphere Virtual Volumes (VVols), einschließlich der neuesten Produktinformationen und Anwendungsfälle sowie Best Practices und andere Informationen, um die Implementierung zu optimieren und Fehler zu reduzieren.

Diese Dokumentation ersetzt zuvor veröffentlichte technische Berichte *TR-4400: VMware vSphere Virtual Volumes (VVols) durch ONTAP*

Andere Dokumente wie Leitfäden und Kompatibilitätslisten werden durch Best Practices ergänzt. Sie werden basierend auf Labortests und umfassenden praktischen Erfahrungen der NetApp Ingenieure und Kunden entwickelt. Es handelt sich hierbei unter Umständen nicht nur um geeignete oder unterstützte Praktiken, sondern im Allgemeinen um die einfachsten Lösungen, die die Anforderungen der meisten Kunden erfüllen.

Dieses Dokument wurde mit neuen VVols Funktionen aus vSphere 8.0 Update 3, der Version ONTAP Tools 10.4 und den neuen NetApp ASA Systemen aktualisiert.

Virtual Volumes (VVols) – Übersicht

NetApp begann 2012 die Zusammenarbeit mit VMware zur Unterstützung von vSphere APIs for Storage Awareness (VASA) für vSphere 5. Dieser frühe VASA Provider ermöglichte die Definition von Storage-Funktionen in einem Profil, das zur Filterung von Datastores bei der Bereitstellung und zur Überprüfung der Einhaltung der Richtlinie anschließend verwendet werden konnte. Im Laufe der Zeit wurden neue Funktionen hinzugefügt, um eine stärkere Automatisierung der Bereitstellung zu ermöglichen. Zudem wurden Virtual Volumes oder VVols hinzugefügt, bei denen individuelle Storage-Objekte für Dateien von Virtual Machines und Virtual Disks verwendet werden. Es können sich bei diesen Objekten um LUNs, Dateien und jetzt um vSphere 8 – NVMe Namespaces (in Verbindung mit ONTAP Tools 9.13P2) handelt. NetApp hat 2015 eng mit VMware als Referenzpartner für VVols zusammengearbeitet, die im Bereich vSphere 6 und erneut als Designpartner für VVols unter Verwendung von NVMe over Fabrics in vSphere 8 veröffentlicht wurden. NetApp erweitert VVols kontinuierlich, um die Vorteile der neuesten Funktionen von ONTAP zu nutzen.

Es gibt mehrere Komponenten, die zu beachten sind:

VASA Provider

Dies ist die Softwarekomponente, die die Kommunikation zwischen VMware vSphere und dem Speichersystem übernimmt. Bei ONTAP wird VASA Provider in einer Appliance ausgeführt, bekannt als ONTAP Tools für VMware vSphere (kurz ONTAP Tools). Die ONTAP Tools enthalten außerdem ein vCenter Plug-in, einen Storage Replication Adapter (SRA) für VMware Site Recovery Manager und REST-API-Server zum Erstellen Ihrer eigenen Automatisierung. Sobald ONTAP Tools bei vCenter konfiguriert und registriert sind, besteht kaum noch Bedarf für eine direkte Interaktion mit dem ONTAP System, da sich Ihre Storage-Anforderungen nahezu vollständig über die vCenter UI oder ÜBER REST-API-Automatisierung managen lassen.

Protokollendpunkt (PE)

Der Protokollendpunkt ist ein Proxy für I/O zwischen den ESXi Hosts und dem VVols Datastore. ONTAP VASA Provider erstellt diese automatisch, entweder eine Protokollendpunkt-LUN (4 MB Größe) pro FlexVol Volume des VVols Datastores oder ein NFS-Bereitstellungspunkt pro NFS-Schnittstelle (LIF) auf dem Storage-Node, der ein FlexVol Volume im Datastore hostet. Der ESXi-Host mountet diese Protokollendpunkte direkt statt einzelner vVol-LUNs und Dateien mit virtuellen Laufwerken. Die Protokollendpunkte müssen nicht verwaltet werden, da sie vom VASA Provider zusammen mit den erforderlichen Schnittstellengruppen oder Exportrichtlinien automatisch erstellt, gemountet, unmountet und gelöscht werden.

Virtual Protocol Endpoint (VPE)

Neu in vSphere 8 ist bei Verwendung von NVMe over Fabrics (NVMe-of) mit VVols, das Konzept eines Protokollendpunkts in ONTAP nicht mehr relevant. Stattdessen wird ein virtueller PE automatisch vom ESXi-Host für jede ANA-Gruppe instanziiert, sobald die erste VM eingeschaltet ist. ONTAP erstellt automatisch ANA-Gruppen für jedes vom Datenspeicher verwendete FlexVol Volume.

Ein weiterer Vorteil bei der Nutzung von NVMe-of für VVols besteht darin, dass vom VASA Provider keine Bind-Anfragen erforderlich sind. Stattdessen verarbeitet der ESXi-Host die vVol-Bindungsfunktion intern basierend auf dem VPE. Dies verringert die Möglichkeit, dass ein vVol BIND-Ansturm den Service beeinträchtigt.

Weitere Informationen finden Sie unter "NVMe und Virtual Volumes" Ein "VMware.com"

Datastore für virtuelle Volumes

| Der Virtual Volume-Datenspeicher ist eine logische Datenspeicherdarstellung eines vVols Containers, die von einem VASA-Provider erstellt und verwaltet wird. Der Container repräsentiert einen Pool an Speicherkapazität, der von Speichersystemen bereitgestellt wird, die vom VASA-Anbieter verwaltet werden. ONTAP tools unterstützt die Zuordnung mehrerer FlexVol Volumes (die als Backing-Volumes bezeichnet werden) zu einem einzigen vVols Datenspeicher. Diese vVols Datenspeicher können sich über mehrere Knoten in einem ONTAP Cluster erstrecken und kombinieren Flash- und Hybridsysteme mit unterschiedlichen Fähigkeiten. Der Administrator kann neue FlexVol Volumes mithilfe des Bereitstellungsassistenten oder der REST-API erstellen oder, falls verfügbar, bereits erstellte FlexVol Volumes als Speichermedium auswählen.

Virtuelle Volumes (VVols)

vVols sind die eigentlichen virtuellen Maschinendateien und -datenträger, die im vVols Datenspeicher abgelegt sind. Der Begriff vVol (Singular) bezieht sich auf eine einzelne spezifische Datei, LUN oder einen Namensraum. ONTAP erstellt NVMe-Namespaces, LUNs oder Dateien, je nachdem, welches Protokoll der Datenspeicher verwendet. Es gibt verschiedene Arten von vVols; die gängigsten sind Konfigurationsvolumes (das einzige mit VMFS, es enthält Metadatendateien wie die VMX-Datei der VM), Datenvolumes (virtuelle Festplatte oder VMDK) und Auslagerungsvolumes (werden beim Einschalten der VM erstellt). Durch VMware-VM-Verschlüsselung geschützte vVols gehören zum Typ „Sonstige“. Die VMware VM-Verschlüsselung sollte nicht mit der ONTAP -Volume- oder Aggregatverschlüsselung verwechselt werden.

Richtlinienbasiertes Management

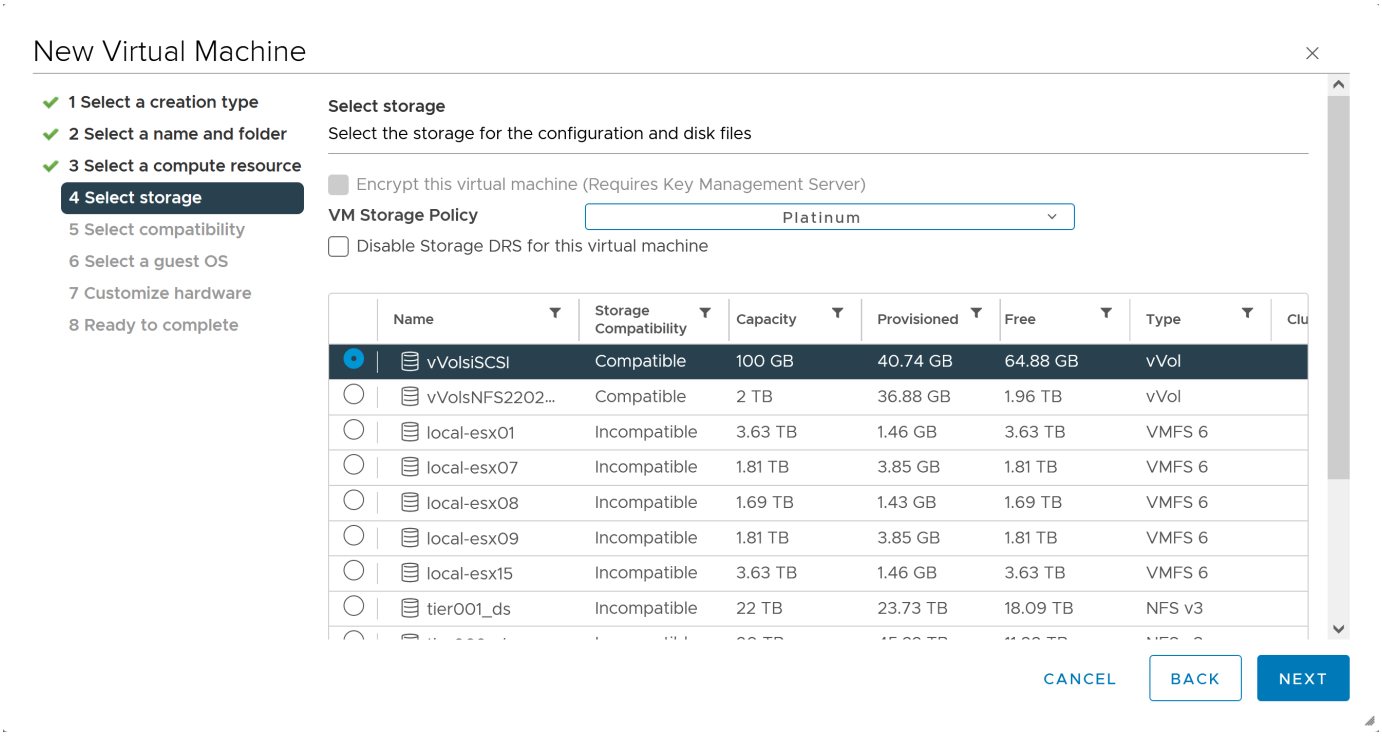
VMware vSphere APIs for Storage Awareness (VASA) erleichtern es VM-Administratoren, die benötigten Speicherfunktionen zur Bereitstellung von VMs zu nutzen, ohne mit ihrem Speicherteam interagieren zu müssen. Vor VASA konnten VM-Administratoren zwar VM-Speicherrichtlinien definieren, mussten aber mit ihren Speicheradministratoren zusammenarbeiten, um geeignete Datenspeicher zu identifizieren, oft anhand von Dokumentationen oder Namenskonventionen. Mit VASA können vCenter-Administratoren mit den entsprechenden Berechtigungen eine Reihe von Speicherkapazitäten definieren, die vCenter-Benutzer dann zum Bereitstellen von VMs verwenden können. Die Zuordnung zwischen VM-Speicherrichtlinie und Datenspeicherfunktionen ermöglicht es vCenter, eine Liste kompatibler Datenspeicher zur Auswahl anzuzeigen und anderen Technologien wie VCF (früher bekannt als Aria und vRealize) Automation oder VMware vSphere Kubernetes Service (VKS) die automatische Auswahl von Speicher aus einer zugewiesenen Richtlinie zu ermöglichen. Dieser Ansatz wird als speicherrichtlinienbasierte Verwaltung bezeichnet. Obwohl VASA Provider-Regeln und VM-Speicherrichtlinien auch mit herkömmlichen Datenspeichern verwendet werden können, konzentrieren wir uns hier auf vVols -Datenspeicher.

VM-Storage-Richtlinien

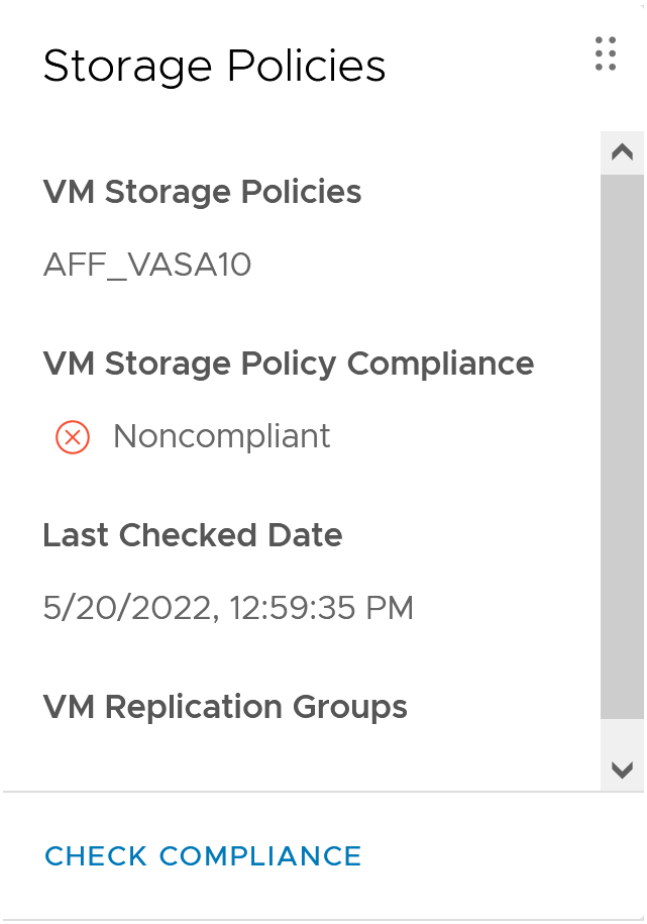
VM Storage-Richtlinien werden in vCenter unter Richtlinien und Profile erstellt. Erstellen Sie für VVols mithilfe von Regeln des NetApp VVols Storage-Typ-Providers ein Regelwerk. ONTAP Tools 10.X bietet jetzt einen einfacheren Ansatz als ONTAP Tools 9.X, da Sie Storage-Attribute direkt in der VM Storage-Richtlinie selbst angeben können.

Wie bereits erwähnt, vereinfacht der Einsatz von Richtlinien die Bereitstellung von VMs oder VMDK. Wählen Sie einfach eine entsprechende Richtlinie aus. VASA Provider zeigt VVols Datastores, die diese Richtlinie unterstützen, und platziert das vVol in einer individuellen, konformen FlexVol volume.

Bereitstellung der VM mithilfe der Storage-Richtlinie



Sobald eine VM bereitgestellt ist, überprüft der VASA-Anbieter weiterhin die Einhaltung der Richtlinien und benachrichtigt den VM-Administrator mit einem Alarm in vCenter, wenn das zugrunde liegende Volume nicht mehr den Richtlinien entspricht.



NetApp VVols Unterstützung

ONTAP unterstützt die VASA-Spezifikation seit ihrer ersten Veröffentlichung im Jahr 2012. Obwohl auch andere NetApp Speichersysteme VASA unterstützen, konzentriert sich dieses Dokument auf die aktuell unterstützten Versionen von ONTAP 9.

ONTAP

Zusätzlich zu ONTAP 9 auf AFF, ASA und FAS -Systemen unterstützt NetApp VMware-Workloads auf ONTAP Select, Amazon FSx für NetApp mit VMware Cloud auf AWS, Azure NetApp Files mit Azure VMware Solution, Google Cloud NetApp Volumes mit Google Cloud VMware Engine und NetApp Private Storage in Equinix. Die spezifische Funktionalität kann jedoch je nach Dienstanbieter und verfügbarer Netzwerkkonnektivität variieren.

Zum Zeitpunkt der Veröffentlichung sind Hyperscaler-Umgebungen auf traditionelle NFS v3-Datenspeicher beschränkt; daher sind vVols nur mit On-Premises ONTAP Systemen oder Cloud-verbundenen Systemen verfügbar, die den vollen Funktionsumfang eines On-Premises-Systems bieten, wie beispielsweise Systeme, die von NetApp -Partnern und Serviceanbietern weltweit gehostet werden.

Weitere Informationen zu ONTAP finden Sie unter "ONTAP Produktdokumentation"

Weitere Informationen zu den Best Practices von ONTAP und VMware vSphere finden Sie unter "TR-4597"

Vorteile der Verwendung von VVols mit ONTAP

Als VMware 2015 mit VASA 2.0 die vVols Unterstützung einführte, beschrieben sie diese als „ein Integrations- und Management-Framework, das ein neues Betriebsmodell für externe Speicher (SAN/NAS) liefert“. Dieses

Betriebsmodell bietet in Verbindung mit ONTAP Speicherung mehrere Vorteile.

Richtlinienbasiertes Management

Wie in Abschnitt 1.2 erläutert, ermöglicht die richtlinienbasierte Verwaltung die Bereitstellung und anschließende Verwaltung von VMs mithilfe vordefinierter Richtlinien. Dies kann den IT-Betrieb in mehrfacher Hinsicht unterstützen:

- **Geschwindigkeit erhöhen.** Mit ONTAP tools entfällt für den vCenter-Administrator die Notwendigkeit, Tickets beim Speicherteam für Speicherbereitstellungsaktivitäten zu eröffnen. Allerdings ermöglichen die RBAC-Rollen der ONTAP Tools in vCenter und im ONTAP System weiterhin unabhängige Teams (z. B. Speicherteams) oder unabhängige Aktivitäten desselben Teams, indem der Zugriff auf bestimmte Funktionen bei Bedarf eingeschränkt wird.
- **Intelligentere Bereitstellung.** die Funktionen des Storage-Systems können über die VASA APIs zugänglich gemacht werden. So können Workflows für die Bereitstellung von erweiterten Funktionen profitieren, ohne dass der VM-Administrator ein Verständnis für das Management des Storage-Systems benötigt.
- **Schnellere Bereitstellung.** verschiedene Storage-Funktionen können in einem einzelnen Datastore unterstützt und anhand der VM-Richtlinie automatisch für eine VM ausgewählt werden.
- **Vermeiden von Fehlern.** Storage- und VM-Richtlinien werden vorab entwickelt und bei Bedarf angewendet, ohne dass bei jeder Bereitstellung einer VM Storage angepasst werden muss. Wenn sich die Storage-Funktionen von den festgelegten Richtlinien abdriften, werden Compliance-Alarme ausgelöst. Wie bereits erwähnt, ist die Erstbereitstellung durch SCPs vorhersehbar und wiederholbar, wobei die korrekte Platzierung durch die Verwendung von VM-Speicherrichtlinien auf den SCPs gewährleistet ist.
- **Besseres Kapazitätsmanagement.** VASA- und ONTAP-Tools ermöglichen bei Bedarf eine Anzeige der Storage-Kapazität bis auf die einzelne Aggregatebene und ermöglichen bei geringer Kapazität mehrere Alarmebenen.

Granulares VM-Management auf dem modernen SAN

SAN-Speichersysteme mit Fibre Channel und iSCSI waren die ersten, die von VMware für ESX unterstützt wurden, aber es fehlte ihnen die Möglichkeit, einzelne VM-Dateien und -Festplatten vom Speichersystem aus zu verwalten. Stattdessen werden LUNs bereitgestellt, und VMFS verwaltet die einzelnen Dateien. Dies erschwert es dem Speichersystem, die Speicherleistung, das Klonen und den Schutz einzelner VMs direkt zu verwalten. vVols bieten die Speichergranularität, die Kunden mit NFS-Speicher bereits nutzen, kombiniert mit den robusten und leistungsstarken SAN-Funktionen von ONTAP.

Mit vSphere 8 und den ONTAP tools for VMware vSphere 9.12 und höher stehen nun dieselben detaillierten Steuerungsmöglichkeiten, die von vVols für ältere SCSI-basierte Protokolle verwendet wurden, auch im modernen Fibre Channel SAN mit NVMe over Fabrics zur Verfügung, um eine noch höhere Leistung im großen Maßstab zu erzielen. Mit vSphere 8.0 Update 1 ist es nun möglich, eine vollständige End-to-End-NVMe-Lösung mit vVols ohne jegliche E/A-Übersetzung im Hypervisor-Speicherstack bereitzustellen.

Bessere Auslagerungsmöglichkeiten

Während VAAI eine Vielzahl von Operationen anbietet, die auf den Speicher ausgelagert werden, gibt es einige Lücken, die vom VASA Provider geschlossen werden. SAN VAAI ist nicht in der Lage, von VMware verwaltete Snapshots auf das Speichersystem auszulagern. NFS VAAI kann VM-verwaltete Snapshots auslagern, allerdings gibt es Einschränkungen für VMs mit speichernativen Snapshots. Da vVols einzelne LUNs, Namespaces oder Dateien für virtuelle Maschinenfestplatten verwenden, kann ONTAP die Dateien oder LUNs schnell und effizient klonen, um VM-granulare Snapshots zu erstellen, die keine Delta-Dateien mehr benötigen. NFS VAAI unterstützt auch keine Auslagerung von Klonvorgängen bei Hot-vMotion-Migrationen (bei eingeschaltetem System). Die VM muss ausgeschaltet werden, um die Migration bei Verwendung von VAAI mit

herkömmlichen NFS-Datenspeichern auszulagern. Der VASA Provider in ONTAP Tools ermöglicht nahezu sofortige, speichereffiziente Klone für Hot- und Cold-Migrationen und unterstützt außerdem nahezu sofortige Kopien für Cross-Volume-Migrationen von vVols. Aufgrund dieser signifikanten Vorteile hinsichtlich der Speichereffizienz können Sie die Vorteile von vVols Workloads unter den folgenden Bedingungen voll ausschöpfen: "Effizienz-Garantie" Programm. Sollten Cross-Volume-Klone mit VAAI Ihre Anforderungen nicht erfüllen, können Sie Ihre geschäftliche Herausforderung wahrscheinlich dank der Verbesserungen beim Kopiervorgang mit vVols lösen.

Häufige Anwendungsfälle für VVols

Neben diesen Vorteilen sehen wir auch folgende häufige Anwendungsfälle für vVol Storage:

- **Bedarfsgesteuerte Bereitstellung von VMs**
  - Private Cloud oder Service-Provider-IaaS.
  - Automatisierung und Orchestrierung über die Aria (ehemals vRealize) Suite, OpenStack usw.
- **First Class Disks (FCDs)**
  - Persistente Volumes des VMware vSphere Kubernetes Service (VKS).
  - Bereitstellung von Amazon EBS-ähnlichen Diensten durch unabhängiges VMDK-Lebenszyklusmanagement.
- **On-Demand Bereitstellung temporärer VMs**
  - Labore für Test und Entwicklung
  - Schulungsumgebungen

Gemeinsame Vorteile mit VVols

Wenn VVols so eingesetzt werden, wie in den oben genannten Anwendungsfällen, bieten sie folgende spezifische Verbesserungen:

- Klone können schnell innerhalb eines einzelnen Volumes oder über mehrere Volumes in einem ONTAP Cluster erstellt werden, was im Vergleich zu herkömmlichen VAAI-fähigen Klonen ein Vorteil ist. Sie sind außerdem speichereffizient. Klone innerhalb eines Volumes verwenden ONTAP -Dateiklone, die wie FlexClone -Volumes funktionieren und nur Änderungen gegenüber der Quell-vVol-Datei/LUN/Namensraum speichern. So lassen sich langfristige VMs für den Produktiveinsatz oder andere Anwendungszwecke schnell erstellen, benötigen nur minimalen Speicherplatz und profitieren von VM-Schutz (mittels NetApp SnapCenter Plugin für VMware vSphere, VMware-verwalteten Snapshots oder VADP-Backup) und Leistungsmanagement (mit ONTAP QoS). Volumeübergreifende Klone sind mit vVols wesentlich schneller als mit VAAI, da wir mit VASA den Klon erstellen und den Zugriff darauf am Zielort ermöglichen können, bevor der Kopiervorgang abgeschlossen ist. Die Datenblöcke werden als Hintergrundprozess kopiert, um das Ziel-vVol zu füllen. Dies ist vergleichbar mit der Funktionsweise des ONTAP -Verfahrens zur unterbrechungsfreien LUN-Verschiebung bei herkömmlichen LUNs.
- VVols stellen die ideale Storage-Technologie dar, wenn ein TKG mit vSphere CSI verwendet wird und separate Storage-Klassen und Kapazitäten bereitstellt, die vom vCenter Administrator gemanagt werden.
- Amazon EBS-ähnliche Dienste können über FCDs bereitgestellt werden, da eine FCD VMDK, wie der Name schon sagt, ein erstklassiges Element in vSphere ist und einen Lebenszyklus besitzt, der unabhängig von den VMs, an die sie angehängt sein könnte, verwaltet werden kann.

Checkliste

Verwenden Sie diese Installationscheckliste, um eine erfolgreiche Implementierung sicherzustellen (aktualisiert für 10.3 und höher).

1 Anfangsplanung

- Bevor Sie mit der Installation beginnen, sollten Sie die überprüfen "Interoperabilitäts-Matrix-Tool (IMT)", um sicherzustellen, dass Ihre Bereitstellung zertifiziert wurde.
- Bestimmen Sie, welche Größe und Art von ONTAP Tools in Ihrer Umgebung konfiguriert werden müssen. Weitere Informationen finden Sie im "Konfigurationsbeschränkungen für die Implementierung von ONTAP Tools für VMware vSphere".
- Ermitteln Sie, ob mandantenfähige SVMs verwendet oder vollständigen Cluster-Zugriff gewährt werden sollen. Wenn Sie mandantenfähige SVMs verwenden, benötigen Sie auf jeder zu verwendenden SVM eine SVM-Management-LIF. Dieses LIF muss mit ONTAP-Tools über Port 443 erreichbar sein.
- Stellen Sie fest, ob Sie Fibre Channel (FC) für die Storage-Konnektivität verwenden werden. Ist dies der Fall, müssen "Konfigurieren Sie das Zoning" Sie auf Ihren FC-Switches die Konnektivität zwischen den ESXi Hosts und den FC-LIFs des SVM aktivieren.
- Stellen Sie fest, ob Sie den ONTAP Tools Storage Replication Adapter (SRA) für VMware Site Recovery Manager (SRM) oder die Live Site Recovery (VLSR) verwenden werden. In diesem Fall müssen Sie auf die SRM/VLSR-Serververwaltungsschnittstelle zugreifen, um SRA zu installieren.
- Wenn Sie SnapMirror-Replizierung verwenden, die über ONTAP-Tools gemanagt wird (einschließlich, aber nicht beschränkt auf SnapMirror Active Sync), müssen "Cluster-übergreifende SVM-Peer-Beziehung in ONTAP erstellen" Sie von Ihrem ONTAP-Administrator "Cluster-Peer-Beziehung in ONTAP erstellen" zunächst die ONTAP-Tools mit SnapMirror verwenden.
- "Download" Die ONTAP-Tools OVA und ggf. die SRA tar.gz-Datei.

2 Stellen Sie IP-Adressen und DNS-Einträge bereit

- Fordern Sie die folgenden IP-Informationen von Ihrem Netzwerkteam an. Die ersten drei IP-Adressen sind erforderlich. Node 2 und Node 3 werden für Implementierungen mit horizontal skalierbarer Hochverfügbarkeit (High Availability, HA) verwendet. DNS-Hosteinträge sind erforderlich, und alle Knotennamen und alle Adressen sollten sich in demselben VLAN und Subnetz befinden.
- ONTAP Tools-Anwendungsadresse _____ . ____\ . _\ . ___
- Adresse der internen Dienste _____ . ____\ . _\ . ___
- Der DNS-Hostname des Knotens 1 _______________
- Die IP-Adresse des Knotens ____ . _____ . ____\ . __
- Subnetzmaske ___\ . _\ . _\ . __
- Standard-Gateway ___\ . _\ . _\ . __
- DNS-Server 1 _____ . ____\ . _\ . ___
- DNS-Server 2 _____ . ____\ . _\ . ___
- DNS-Suchdomäne ______________\
- Der DNS-Hostname des zweiten Knotens (optional) _______________
- IP-Adresse des zweiten Knotens (optional) ____ . _____ . ____\ . __
- Der DNS-Hostname des dritten Knotens (optional) _____________
- IP-Adresse des dritten Knotens (optional) _____ . _____ . ____\ . __
- Erstellen Sie DNS-Einträge für alle oben genannten IP-Adressen.

3 Konfiguration der Netzwerk-Firewall

- Öffnen Sie die erforderlichen Ports für die oben genannten IP-Adressen in Ihrer Netzwerk-Firewall. Das neueste Update finden Sie unter "Port-Anforderungen".

4 Storage

- Ein Datastore auf einem gemeinsam genutzten Speichergerät ist erforderlich. Optional können Sie eine Content Library auf demselben Datastore wie Knoten 1 verwenden, um das schnelle Klonen der Vorlage mit VAAI zu erleichtern.
- Inhaltsbibliothek (nur für HA erforderlich) __________
- Node 1 Datastore ________________
- Zwei Nodes Datastore (optional, aber für HA empfohlen) __________
- Knoten drei (optional, aber für HA empfohlen) _________________

5 Implementieren Sie die OVA

- Beachten Sie, dass dieser Schritt bis zu 45 Minuten dauern kann
- "Implementieren Sie die OVA" Verwenden des vSphere-Clients.
- Wählen Sie in Schritt 3 der OVA-Bereitstellung die Option „Anpassung der Hardware dieser virtuellen Maschine“ aus, und legen Sie Folgendes auf Schritt 10 fest:
- „CPU-Hot-Add aktivieren“
- „Hot-Plug-Speicher“

6 Fügen Sie vCenter zu ONTAP-Tools hinzu

- "Fügen Sie vCenter Server-Instanzen hinzu" Im ONTAP Tools Manager.

7 Fügen Sie Storage Back-Ends zu ONTAP Tools hinzu

- "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen" Verwenden der enthaltenen JSON-Datei, wenn nicht admin verwendet wird.
- Wenn Sie bestimmte SVMs mithilfe von Storage Multitenancy vCentern zuweisen möchten, anstatt ONTAP Cluster-Anmeldeinformationen in vCenter zu verwenden, führen Sie die folgenden Schritte aus:
- "Onboard Cluster" Im ONTAP Tools Manager und verknüpfen Sie sie mit vCenters.
- "Onboard SVMs" In den ONTAP Tools vCenter UI.
- Wenn Sie **keine** Multitenant-SVMs innerhalb von vCenter verwenden:
- "Onboard Cluster" Direkt in der vCenter UI der ONTAP Tools Alternativ ist es in diesem Szenario möglich, SVMs direkt hinzuzufügen, wenn keine VVols verwendet werden.

8 Konfigurieren von Appliance-Services (optional)

- Um VVols zu verwenden, müssen Sie zunächst "Bearbeiten Sie die Appliance-Einstellungen, und

aktivieren Sie den VASA-Service". Überprüfen Sie gleichzeitig die folgenden beiden Punkte.

- Wenn Sie VVols in der Produktion verwenden möchten, "Hochverfügbarkeit" geben Sie die beiden optionalen IP-Adressen oben ein.
- Wenn Sie die ONTAP Tools Storage Replication Adapter (SRA) für VMware Site Recovery Manager oder Live Site Recovery verwenden möchten, "SRA-Services werden aktiviert"

9 **Zertifikate (optional)**

- Pro VMware sind durch eine Zertifizierungsstelle signierte Zertifikate erforderlich, wenn VVols mit mehreren vCenter verwendet werden.
- VASA Services ________________
- Verwaltungsdienste _____________

10 **Andere Aufgaben nach der Bereitstellung**

- Erstellen von Affinitätsregeln für VMs in einer HA-Implementierung
- Bei Verwendung von HA werden die Storage vMotion Nodes zwei und drei auf separate Datastores verschoben (optional, aber empfohlen).
- "Verwenden Sie Zertifikate verwalten" Im ONTAP-Tools-Manager, um alle erforderlichen CA-signierten Zertifikate zu installieren.
- Wenn Sie SRA für SRM/VLSR zum Schutz herkömmlicher Datastores aktiviert haben, "Konfigurieren Sie SRA auf der VMware Live Site Recovery-Appliance".
- Konfigurieren Sie native Backups für "RPO nahezu Null"Die
- Konfigurieren Sie regelmäßige Backups auf anderen Speichermedien.

Verwendung von VVols mit ONTAP

Der Schlüssel für die Nutzung von VVols mit NetApp sind ONTAP Tools für VMware vSphere, die als VASA (vSphere API for Storage Awareness) Provider-Schnittstelle für NetApp ONTAP 9 Systeme genutzt werden.

ONTAP-Tools umfassen auch vCenter-UI-Erweiterungen, REST-API-Services, Storage Replication Adapter für VMware Site Recovery Manager / Live Site Recovery, Monitoring und Host-Konfigurations-Tools sowie eine Reihe von Berichten, die Sie beim besseren Management Ihrer VMware-Umgebung unterstützen.

Produkte und Dokumentation

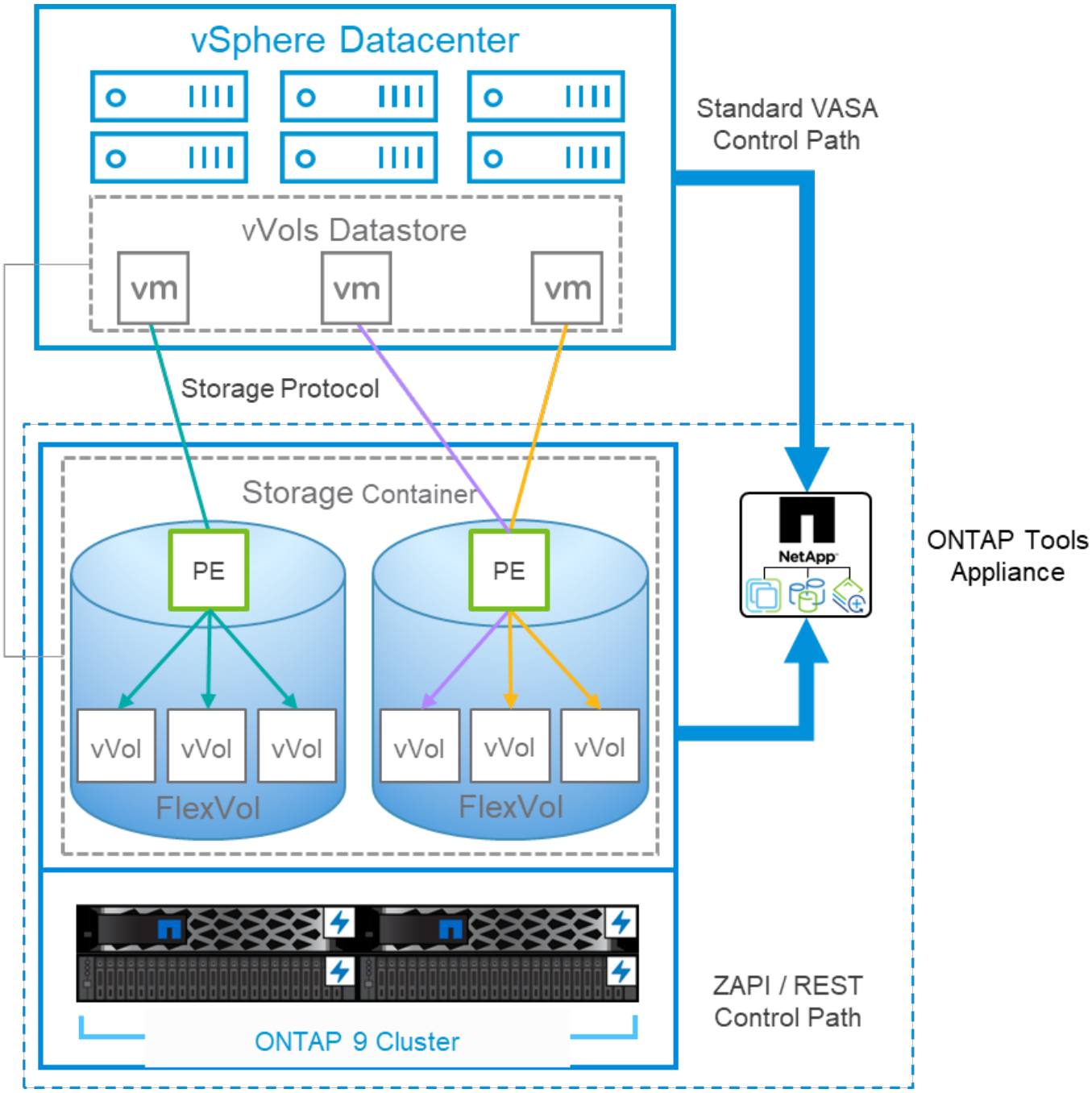
Die ONTAP One Lizenz umfasst alle erforderlichen Lizenzen zur Nutzung von VVols auf ONTAP Systemen. Die einzige zusätzliche Anforderung ist die kostenlose ONTAP-Tools OVA, die als VASA Provider fungiert. In einer VVols Umgebung übersetzt die VASA Provider Software die Array-Funktionen in richtlinienbasierte Attribute, die über die VASA APIs genutzt werden können. Der vSphere Administrator muss sich nicht im Hintergrund mit dem Management der Funktionen auskennen. Dadurch wird eine dynamische Nutzung der zugewiesenen Storage-Kapazität basierend auf Richtlinien ermöglicht, sodass keine herkömmlichen Datenspeicher manuell erstellt und individuelle Storage-Verbrauchsraten gemanagt werden müssen. Kurz gesagt: VVols vereinfachen das Management von Enterprise Storage ganz und reduzieren es nicht mehr vom vSphere Administrator, sodass sie sich auf die Virtualisierungsebene konzentrieren können.

Bei Kunden, die VMware Cloud Foundation mit vSAN verwenden, können VVols zu jeder Management- oder

Workload-Domäne als zusätzlichen Storage hinzugefügt werden. VVols können über ein gemeinsames Storage-richtlinienbasiertes Management-Framework nahtlos in vSAN integriert werden.

Die Versionsfamilie der nächsten Generation der ONTAP Tools 10 modernisiert vorhandene Funktionen mit einer skalierbaren, containerbasierten Microservice-Architektur, die über eine einfache Appliance im OVA-Format auf ESXi implementiert werden kann. ONTAP Tools 10 vereint alle Funktionen dreier früherer Appliances und Produkte in einer einzigen Implementierung. Zum VVols Management verwenden Sie die intuitiven vCenter UI-Erweiterungen oder REST-APIs für die ONTAP Tools VASA Provider. Die SRA Komponente gilt für herkömmliche Datastores. VMware Site Recovery Manager verwendet für VVols jedoch keine SRA.

ONTAP nutzt die VASA Provider Architektur beim Einsatz von iSCSI oder FCP mit einheitlichen Systemen



Produktinstallation

Bei Neuinstallationen implementieren Sie die virtuelle Appliance in Ihrer vSphere Umgebung. Sobald die Implementierung abgeschlossen ist, können Sie sich in der Manager-UI einloggen oder die REST-APIs verwenden, um Ihre Implementierung vertikal oder horizontal zu skalieren. Zudem können Sie vCenters (registriert das Plug-in im vCenter) integrieren, integrierte Storage-Systeme integrieren und Storage-Systeme den vCenter zuweisen. Aufnahme von Storage-Systemen in die Benutzeroberfläche des ONTAP Tools Manager und Zuordnung von Clustern mit vCenter sind nur erforderlich, wenn Sie die sichere Mandantenfähigkeit mit dedizierten SVMs verwenden möchten. Andernfalls können Sie die gewünschten Storage-Cluster einfach in die vCenter UI-Erweiterungen der ONTAP Tools integrieren oder die REST-APIs verwenden.

Siehe "Implementierung von VVols Storage" in diesem Dokument oder "Dokumentation zu ONTAP Tools für VMware vSphere".

Als Best Practice empfiehlt es sich, Ihre ONTAP Tools und vCenter Appliances auf herkömmlichen NFS- oder VMFS-Datenspeichern zu speichern, um Konflikte zwischen wechselseitigen Abhängigkeiten zu vermeiden. Da sowohl vCenter als auch ONTAP Tools während des VVols Betriebs miteinander kommunizieren müssen, dürfen die ONTAP Tools Appliances oder vCenter Server Appliances (VCSA) nicht auf den von ihnen gemanagten VVols Storage installiert oder verschoben werden. In diesem Fall kann ein Neustart der vCenter oder ONTAP Tools Appliances zu einer Unterbrechung des Zugriffs auf die Kontrollebene führen und die Appliance nicht gebootet werden kann.

In-Place-Upgrades von ONTAP-Tools werden durch die Upgrade-ISO-Datei unterstützt, die auf der NetApp Support-Website zum Download zur Verfügung steht "ONTAP Tools for VMware vSphere 10 - Downloads" (Anmeldung erforderlich). Befolgen Sie die "Upgrade von ONTAP Tools für VMware vSphere 10.x auf 10.3" Anweisungen in der Anleitung, um das Gerät zu aktualisieren. Es ist auch möglich, ein Side-by-side-Upgrade von ONTAP Tools 9.13 auf 10.3 zu tun. Weitere Informationen zu diesem Thema finden Sie unter "Migrieren Sie von ONTAP-Tools für VMware vSphere 9.x zu 10.3".

Informationen zur Dimensionierung Ihrer virtuellen Appliance und Informationen über die Konfigurationsgrenzen finden Sie unter "Konfigurationsbeschränkungen für die Implementierung von ONTAP Tools für VMware vSphere"

Produktdokumentation

Die folgende Dokumentation ist verfügbar, um Sie bei der Implementierung von ONTAP Tools zu unterstützen.

"Dokumentation zu ONTAP Tools für VMware vSphere"

Los geht's

- "Versionshinweise"
- "Überblick über die ONTAP Tools für VMware vSphere"
- "Implementierung von ONTAP Tools"
- "Upgrade von ONTAP-Tools"

Verwenden Sie ONTAP-Tools

- "Bereitstellung von Datenspeichern"
- "Konfigurieren Sie die rollenbasierte Zugriffssteuerung"

- "Konfigurieren Sie Hochverfügbarkeit"
- "Ändern der ESXi-Hosteinstellungen"

Sicherung und Management von Datenspeichern

- "Konfigurieren Sie vSphere Metro Storage-Cluster (vMSC) mit ONTAP Tools und SnapMirror Active Sync"
- "Sicherung von Virtual Machines" Mit SRM
- "Überwachung von Clustern, Datastores und Virtual Machines"

VASA Provider Dashboard

Vasa Provider umfasst ein Dashboard mit Performance- und Kapazitätsinformationen für einzelne VVols VMs. Diese Informationen beziehen sich direkt von ONTAP für die vVol Dateien und LUNs, einschließlich Latenz, IOPS, Durchsatz und mehr. Es ist standardmäßig aktiviert, wenn alle derzeit unterstützten Versionen von ONTAP 9 verwendet werden. Nach der Erstkonfiguration kann es bis zu 30 Minuten dauern, bis die Daten im Dashboard geladen sind.

Weitere Best Practices

Die Verwendung von ONTAP VVols mit vSphere ist einfach und folgt den veröffentlichten vSphere-Methoden (siehe Arbeiten mit virtuellen Volumes unter vSphere-Speicher in der VMware-Dokumentation für Ihre Version von ESXi). Nachfolgend finden Sie einige weitere Vorgehensweisen, die Sie in Verbindung mit ONTAP in Betracht ziehen sollten.

Grenzen

ONTAP unterstützt im Allgemeinen VVols-Limits gemäß der Definition von VMware (siehe veröffentlicht "Konfigurationsmaxima"). Prüfen Sie immer, ob die "NetApp Hardware Universe" Limits für die Anzahl und Größen von LUNs, Namespaces und Dateien aktualisiert sind.

Verwenden Sie ONTAP-Tools für VMware vSphere UI-Erweiterungen oder REST-APIs zur Bereitstellung von VVols-Datastores und Protokollendpunkten.

VVols Datastores können über die allgemeine vSphere Schnittstelle erstellt werden, aber mithilfe von ONTAP Tools werden automatisch bei Bedarf Protokollendpunkte erstellt und FlexVol Volumes (nicht erforderlich bei ASA r2) anhand der Best Practices von ONTAP erstellt. Klicken Sie einfach mit der rechten Maustaste auf den Host/Cluster/Datacenter und wählen Sie dann „*ONTAP Tools*“ und „*Provision Datastore*“ aus. Wählen Sie dann im Assistenten einfach die gewünschten VVols Optionen aus.

Speichern Sie die ONTAP Tools Appliance oder vCenter Server Appliance (VCSA) niemals auf einem VVols Datastore, den sie verwalten.

Dies kann zu einer „Hühnerei-Situation“ führen, wenn Sie die Appliances neu starten müssen, da sie während des Neustarts nicht ihre eigenen VVols ablösen können. Sie können sie auf einem VVols Datastore speichern, der von verschiedenen ONTAP Tools und einer vCenter Implementierung gemanagt wird.

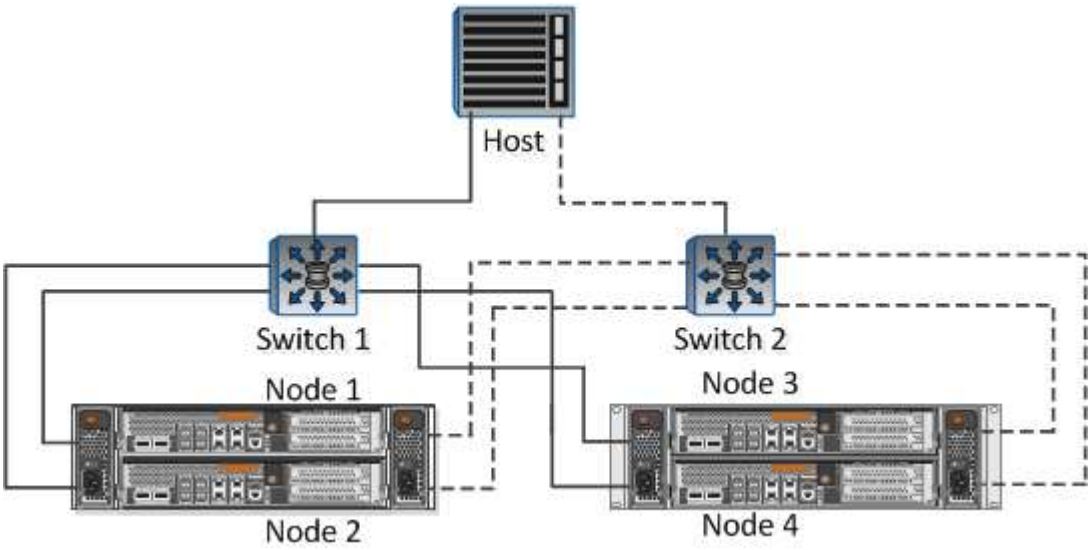
Vermeiden Sie VVols-Vorgänge über verschiedene ONTAP-Versionen hinweg.

Unterstützte Storage-Funktionen wie QoS, Personality und mehr haben sich in verschiedenen Versionen des VASA Providers verändert, einige sind von der ONTAP Version abhängig. Die Verwendung verschiedener Versionen in einem ONTAP-Cluster oder das Verschieben von VVols zwischen Clustern mit unterschiedlichen Versionen können zu unerwartetem Verhalten oder Compliance-Alarmen führen.

Zonen Sie Ihre Fibre Channel Fabric vor der Verwendung von FCP für VVols.

Der ONTAP-Tools VASA Provider managt FCP- und iSCSI-Initiatorgruppen sowie NVMe-Subsysteme in ONTAP, die auf erkannten Initiatoren von gemanagten ESXi-Hosts basieren. Es ist jedoch nicht in Fibre-Channel-Switches integriert, um das Zoning zu managen. Bevor eine Bereitstellung stattfinden kann, muss das Zoning nach Best Practices erfolgen. Nachfolgend ein Beispiel für das Einzel-Initiator-Zoning für vier ONTAP-Systeme:

Einzel-Initiator-Zoning:



Weitere Best Practices finden Sie in folgenden Dokumenten:

"*TR-4080 Best Practices for Modern SAN ONTAP 9*"

"*TR-4684 Implementierung und Konfiguration moderner SANs mit NVMe-of*"

- Planen Sie Ihre Backing-FlexVol-Volumes nach Ihren Bedürfnissen.*

Bei Systemen ohne ASA r2 ist es wünschenswert, mehrere Backup-Volumes zum VVols Datastore hinzuzufügen, um den Workload über das ONTAP Cluster zu verteilen, verschiedene Richtlinienoptionen zu unterstützen oder die Anzahl der zulässigen LUNs oder Dateien zu erhöhen. Wenn jedoch eine maximale Storage-Effizienz erforderlich ist, platzieren Sie alle Ihre Backup Volumes auf einem einzigen Aggregat. Wenn eine maximale Klon-Performance erforderlich ist, ziehen Sie die Verwendung eines einzelnen FlexVol Volumes in Erwägung und halten Ihre Vorlagen- oder Content Library im selben Volume. Der VASA Provider verlagert viele VVols Storage-Vorgänge auf ONTAP, einschließlich Migration, Klonen und Snapshots. Wenn dies in einem einzelnen FlexVol Volume geschieht, werden platzsparende Klone von Dateien verwendet und stehen so gut wie sofort zur Verfügung. Wenn dies über FlexVol Volumes hinweg durchgeführt wird, sind die Kopien schnell verfügbar und verwenden Inline-Deduplizierung und -Komprimierung. Allerdings kann eine maximale Storage-Effizienz erst dann wiederhergestellt werden, wenn Hintergrundjobs auf Volumes mithilfe von Deduplizierung und Komprimierung im Hintergrund ausgeführt werden. Je nach Quelle und Ziel kann die Effizienz beeinträchtigt werden.

Bei ASA r2 Systemen entfällt diese Komplexität, da das Konzept eines Volumes oder Aggregats vom Benutzer abstrahiert wird. Die dynamische Platzierung wird automatisch übernommen und Protokollendpunkte werden nach Bedarf erstellt. Zusätzliche Protokollendpunkte können automatisch im laufenden Betrieb erstellt werden, wenn zusätzliche Skalierung erforderlich ist.

Erwägen Sie die Verwendung von max IOPS zur Steuerung unbekannter VMs oder zum Testen von VMs.

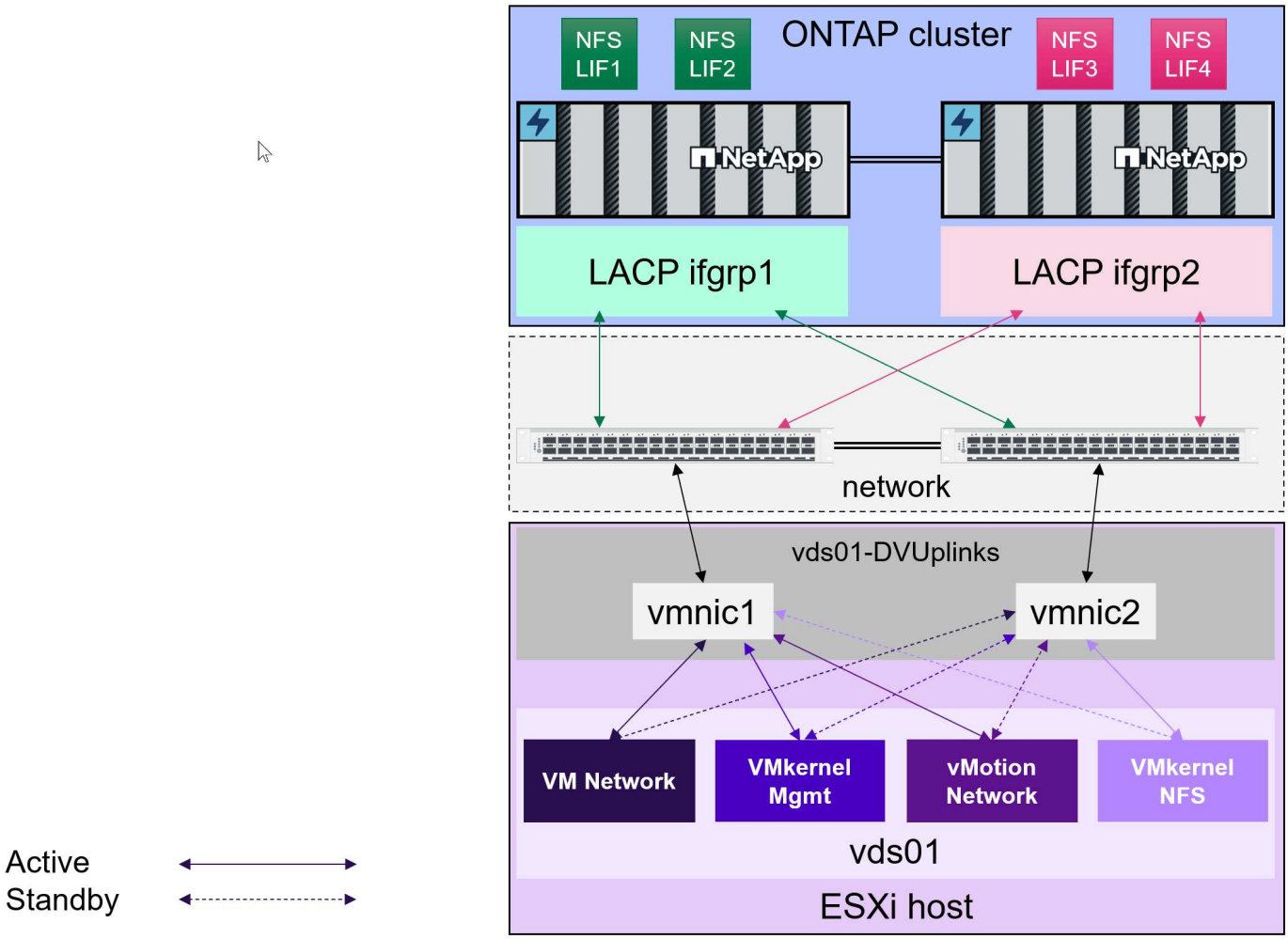
Erstmals in VASA Provider 7.1 verfügbar, können maximale IOPS verwendet werden, um IOPS bei einem unbekannten Workload auf ein bestimmtes vVol zu beschränken und so Auswirkungen auf andere, kritischere Workloads zu vermeiden. Tabelle 4 enthält weitere Informationen zum Performance-Management.

Stellen Sie sicher, dass Sie ausreichend Daten-LIFs haben. Siehe "Implementierung von VVols Storage".

Befolgen Sie alle Best Practices für Protokolle.

Weitere Best Practice-Leitfäden zu dem von Ihnen gewählten Protokoll finden Sie in den Leitfäden von NetApp und VMware. Im Allgemeinen gibt es keine anderen Änderungen als die bereits erwähnten.

Beispiel einer Netzwerkkonfiguration mit VVols über NFS v3



Die Implementierung von VVols auf AFF, ASA, ASA r2 und FAS Systemen

Folgen Sie diesen Best Practices zur Erstellung von VVols Storage für Ihre Virtual Machines.

Die Bereitstellung von VVols Datastores umfasst mehrere Schritte. Die ASA r2-Systeme von NetApp wurden für VMware-Workloads entwickelt und bieten eine andere Benutzererfahrung als herkömmliche ONTAP-Systeme. Beim Einsatz von ASA r2 Systemen erfordern ONTAP Tools ab Version 10.3 weniger Schritte zur Einrichtung und beinhalten UI-Erweiterungen sowie für die neue Storage-Architektur optimierte REST-API-Unterstützung.

Vorbereiten der Erstellung von VVols-Datenspeichern mit ONTAP Tools

Sie können die ersten beiden Schritte des Implementierungsprozesses überspringen, wenn Sie bereits ONTAP Tools zum Managen, Automatisieren und Berichten über Ihren vorhandenen VMFS- oder herkömmlichen NFS-basierten Storage nutzen. Darüber hinaus können Sie sich bei der Bereitstellung und Konfiguration von ONTAP-Tools mit diesem vollständigen "Checkliste"Bericht informieren.

1. Erstellen Sie die Storage Virtual Machine (SVM) und deren Protokollkonfiguration. Beachten Sie, dass dies für ASA r2-Systeme möglicherweise nicht erforderlich ist, da diese in der Regel bereits über eine einzelne SVM für Datendienste verfügen. Sie wählen NVMe/FC (nur ONTAP Tools 9.13), NFSv3, NFSv4.1, iSCSI, FCP oder eine Kombination dieser Optionen. NVMe/TCP und NVMe/FC können auch für traditionelle VMFS-Datenspeicher mit ONTAP Tools ab Version 10.3 verwendet werden. Sie können entweder die ONTAP System Manager-Assistenten oder die Cluster-Shell-Befehlszeile verwenden.
   - "Zuweisung lokaler Tiers (Aggregate) zu SVMs" Für alle nicht-ASA r2-Systeme.
   - Mindestens eine LIF pro Node für jede Switch-/Fabric-Verbindung. Als Best Practice sollten Sie mindestens zwei pro Node für FCP-, iSCSI- oder NVMe-basierte Protokolle erstellen. Für NFS-basierte VVols ist eine LIF pro Node ausreichend, allerdings sollte diese LIF durch eine LACP-ifgroup geschützt werden. Weitere Informationen finden Sie unter "Konfiguration der LIFs – Übersicht" und "Kombinieren Sie physische Ports zum Erstellen von Schnittstellengruppen".
   - Mindestens eine Management-LIF pro SVM, wenn Sie SVM-bezogene Anmeldeinformationen für Ihre Mandanten-vCenters verwenden möchten.
   - Wenn Sie planen, SnapMirror zu verwenden, stellen Sie Ihre Quelle und Ziel "ONTAP Cluster und SVMs sind auf Peering angewiesen".
   - Bei Systemen, die nicht dem ASA r2-Standard entsprechen, können Volumes zwar zu diesem Zeitpunkt erstellt werden, es empfiehlt sich jedoch, dies dem Assistenten „Provision Datastore“ in den ONTAP -Tools zu überlassen. Die einzige Ausnahme von dieser Regel besteht, wenn Sie die vVols Replikation mit VMware Site Recovery Manager und ONTAP Tools 9.13 verwenden möchten. Dies lässt sich einfacher mit bereits vorhandenen FlexVol Volumes und bestehenden SnapMirror Beziehungen einrichten. Achten Sie darauf, QoS nicht für Volumes zu aktivieren, die für vVols verwendet werden sollen, da dies von SPBM- und ONTAP Tools verwaltet werden soll.
2. "Implementieren Sie ONTAP-Tools für VMware vSphere" Verwenden der von der NetApp Support-Website heruntergeladenen OVA.
   - ONTAP tools 10.0 und höher unterstützen mehrere vCenter Server pro Appliance; Sie müssen nicht mehr für jeden vCenter Server eine ONTAP tools Appliance bereitstellen.
     - Wenn Sie mehrere vCenter-Server mit einer einzigen ONTAP -Tools-Instanz verbinden möchten, müssen Sie CA-signierte Zertifikate erstellen und installieren. Siehe "Verwalten von Zertifikaten" für Schritte.
   - Ab Version 10.3 werden die ONTAP -Tools nun als kleine Einzelknoten-Appliance bereitgestellt, die für die meisten Nicht-vVols-Workloads geeignet ist.

- Die empfohlene Vorgehensweise ist folgende: "Tools für die horizontale Skalierung von ONTAP" 10.3 und später auf die 3-Knoten-Hochverfügbarkeitskonfiguration (HA) für alle Produktionsworkloads umzustellen. Für Labor- oder Testzwecke ist eine Einzelknoten-Bereitstellung möglich.
- Die empfohlene Best Practice für den produktiven Einsatz von vVols besteht darin, jegliche Single Points of Failure zu eliminieren. Erstellen Sie Anti-Affinitätsregeln, um zu verhindern, dass die ONTAP -Tools-VMs gleichzeitig auf demselben Host ausgeführt werden. Nach der ersten Bereitstellung wird außerdem empfohlen, Storage vMotion zu verwenden, um die ONTAP -Tools-VMs in verschiedene Datenspeicher zu verschieben. Lesen Sie mehr über "Verwendung von Affinitätsregeln ohne vSphere DRS" oder "VM-VM-Affinitätsregel erstellen"Die Sie sollten außerdem regelmäßige Datensicherungen einplanen und/oder "Verwenden Sie das integrierte Konfigurationsdienstprogramm"Die

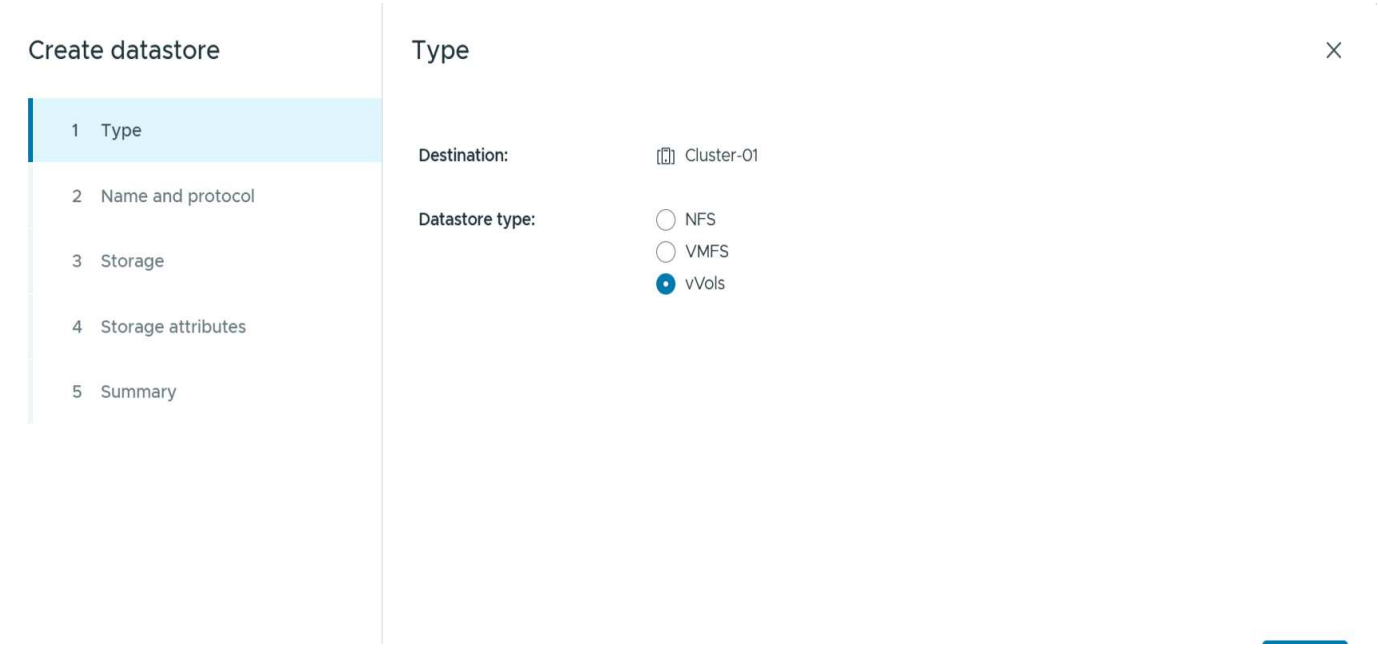
1. Konfigurieren Sie ONTAP Tools 10.3 für Ihre Umgebung.
   - "Fügen Sie vCenter Server-Instanzen hinzu" In der ONTAP Tools Manager-UI.
   - Die ONTAP Tools 10.3 unterstützen die sichere Mandantenfähigkeit. Wenn Sie keine sichere Mandantenfähigkeit benötigen, wechseln Sie einfach "Fügen Sie Ihre ONTAP-Cluster hinzu" zum Menü „ONTAP Tools“ in vCenter und klicken auf „*Storage Backends*“ und anschließend auf die Schaltfläche „*add*“.
   - In einer sicheren mandantenfähigen Umgebung, in der bestimmte Storage Virtual Machines (SVMs) an bestimmte vCenter delegiert werden sollen, müssen Sie Folgendes tun.
     - Melden Sie sich bei der UI für den ONTAP-Tools-Manager an
     - "Onboard des Storage-Clusters"
     - "Ordnen Sie ein Storage-Back-End einer vCenter Server-Instanz zu"
     - Geben Sie dem vCenter-Administrator die spezifischen SVM-Zugangsdaten, der die SVM dann im Menü „ONTAP Tools Storage Backends“ in vCenter als Storage-Backend hinzufügt.

- In der Best Practice wird empfohlen, RBAC-Rollen für Ihre Storage-Konten zu erstellen.
- ONTAP tools beinhaltet eine JSON-Datei, die die für die ONTAP tools-Speicherkonten erforderlichen Rollenberechtigungen enthält. Sie können die JSON-Datei in den ONTAP System Manager hochladen, um die Erstellung von RBAC-Rollen und Benutzern zu vereinfachen.
- Weitere Informationen zu den Rollen für rollenbasierte Zugriffssteuerung von ONTAP finden Sie unter "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen".

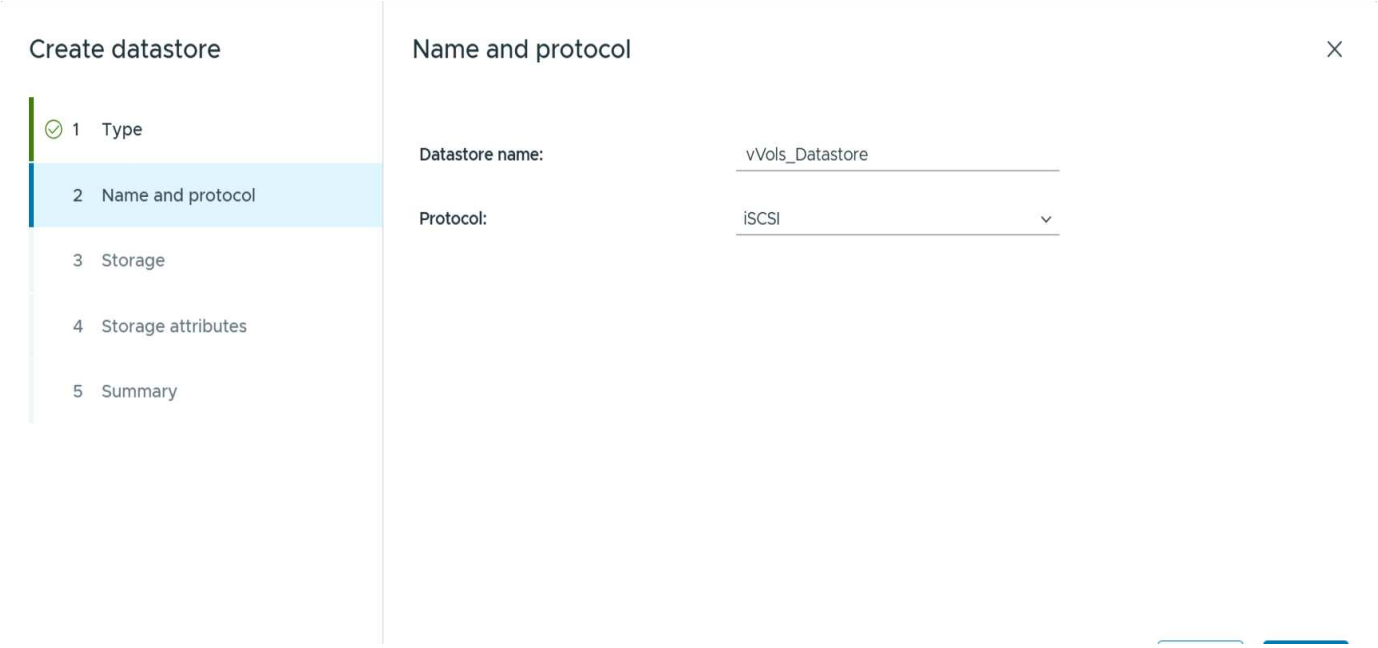
Der Grund dafür, dass der gesamte Cluster in der ONTAP Tools Manager-Benutzeroberfläche eingebunden werden muss, liegt darin, dass viele der für vVols verwendeten APIs nur auf Clusterebene verfügbar sind.

Erstellen von VVols Datastores mit ONTAP Tools

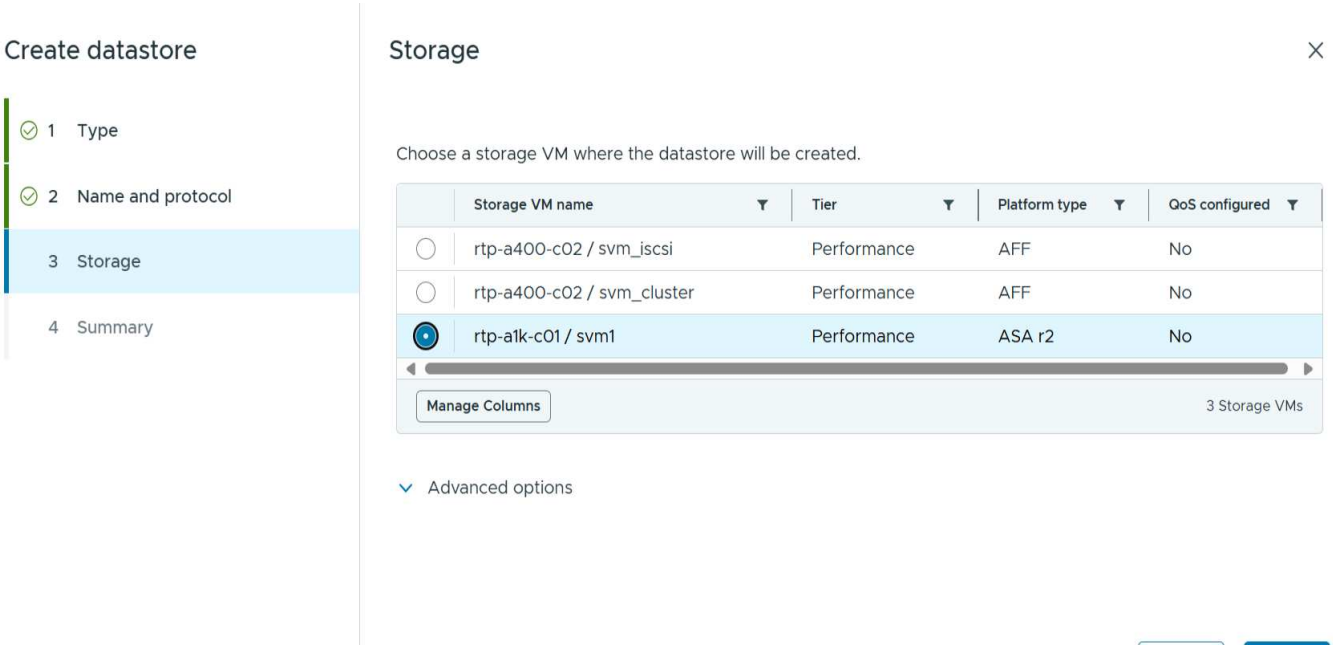
Klicken Sie mit der rechten Maustaste auf den Host, das Cluster oder das Datacenter, auf dem Sie den VVols-Datastore erstellen möchten, und wählen Sie dann *ONTAP Tools* > *Provisioning Datastore* aus.



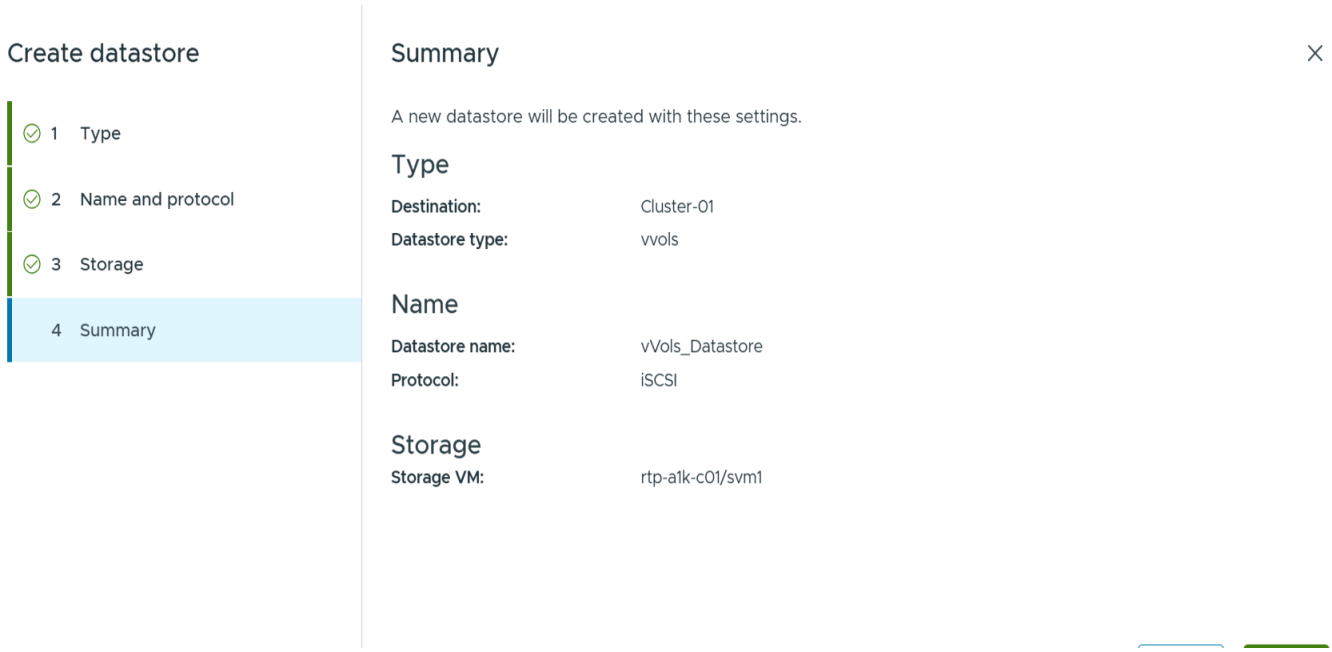
- Wählen Sie VVols, einen aussagekräftigen Namen aus und wählen Sie das gewünschte Protokoll aus. Sie können auch eine Beschreibung des Datastore angeben.
  - ONTAP Tools 10.3 mit ASA r2.



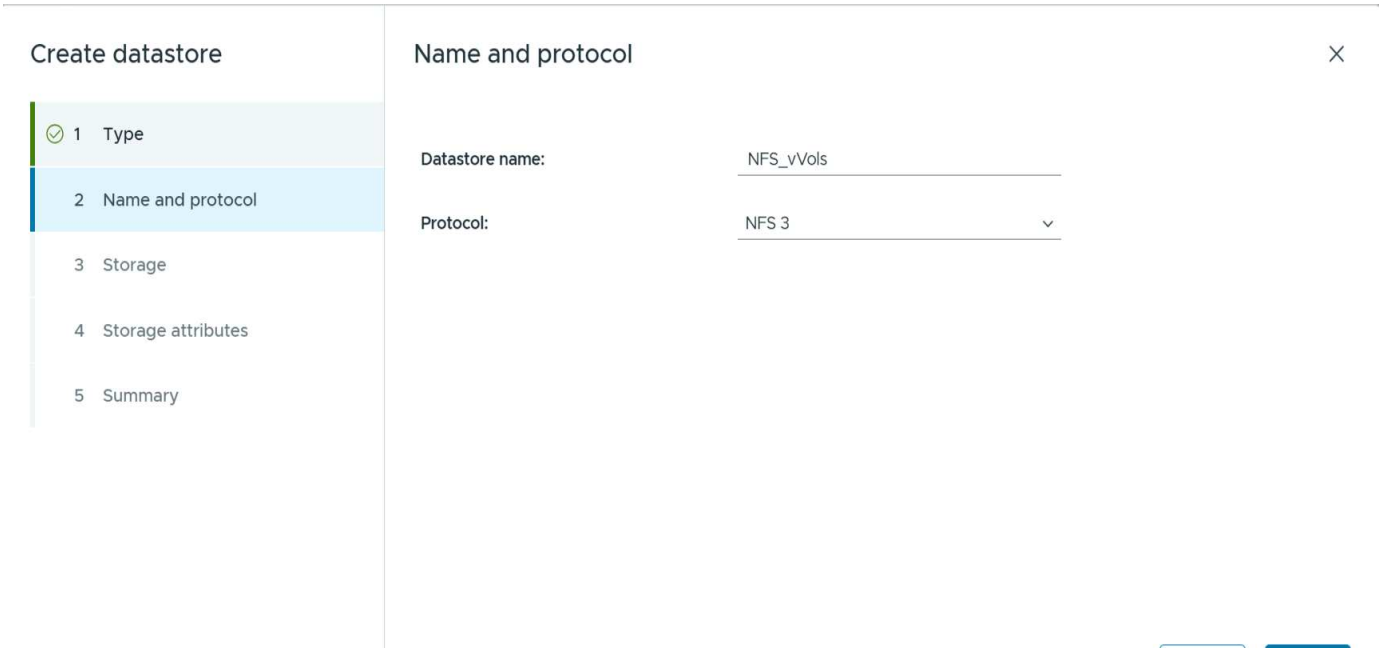
- Wählen Sie die SVM des ASA r2-Systems aus und klicken Sie auf *Next*.



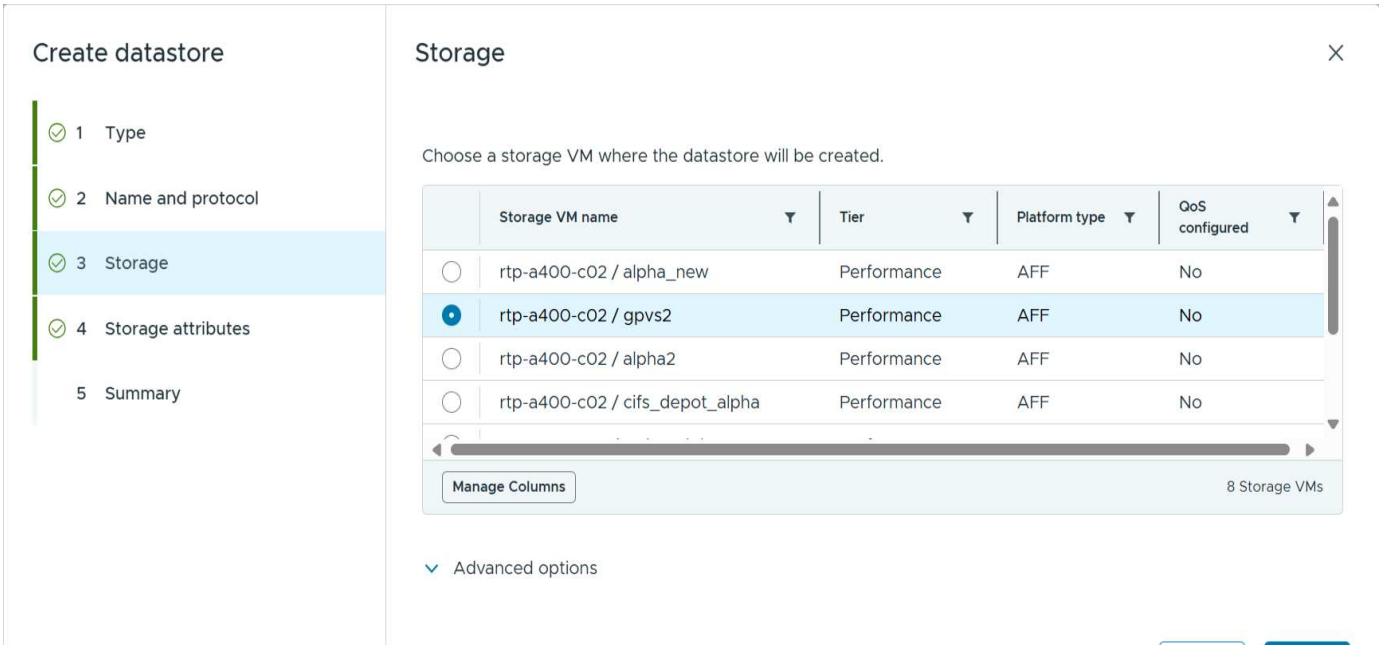
- Klicken Sie auf „*Finish*“



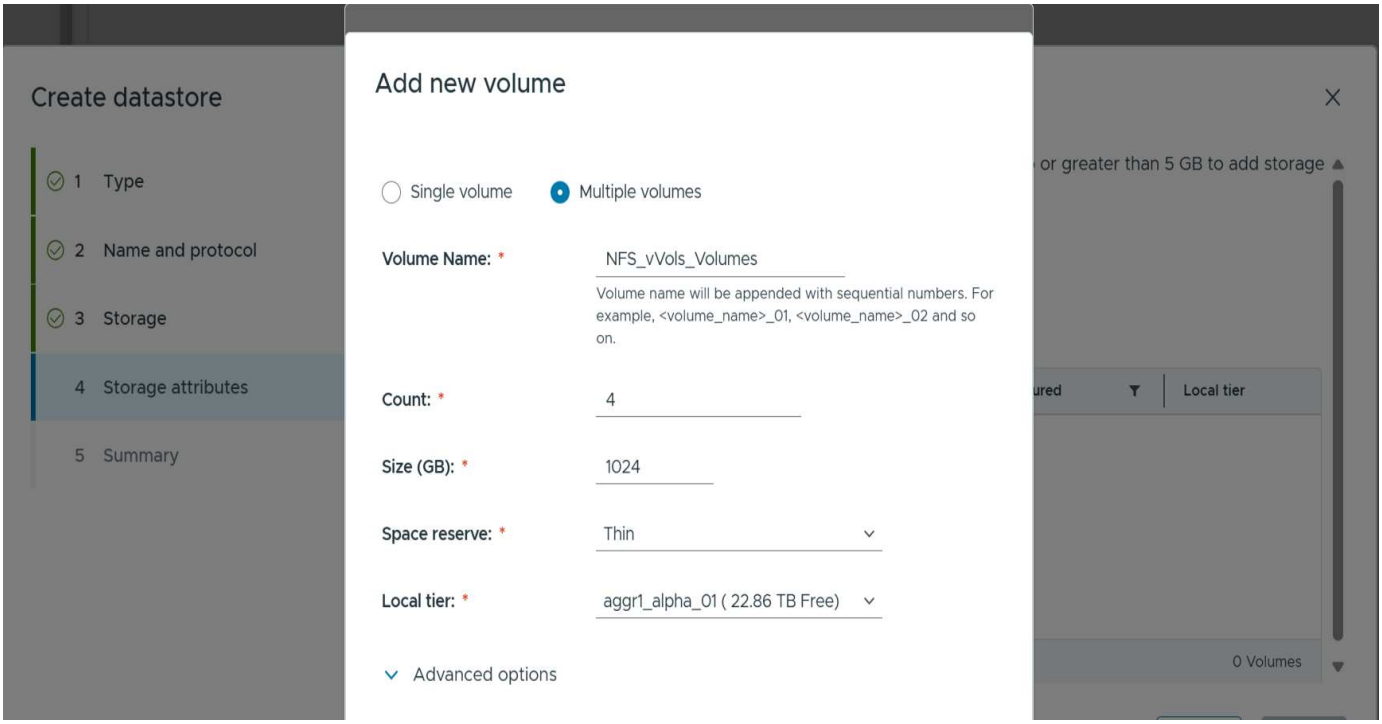
- So einfach ist das!
  - ONTAP Tools 10.3 mit ONTAP FAS, AFF und ASA vor ASA r2.
- Wählen Sie das Protokoll aus

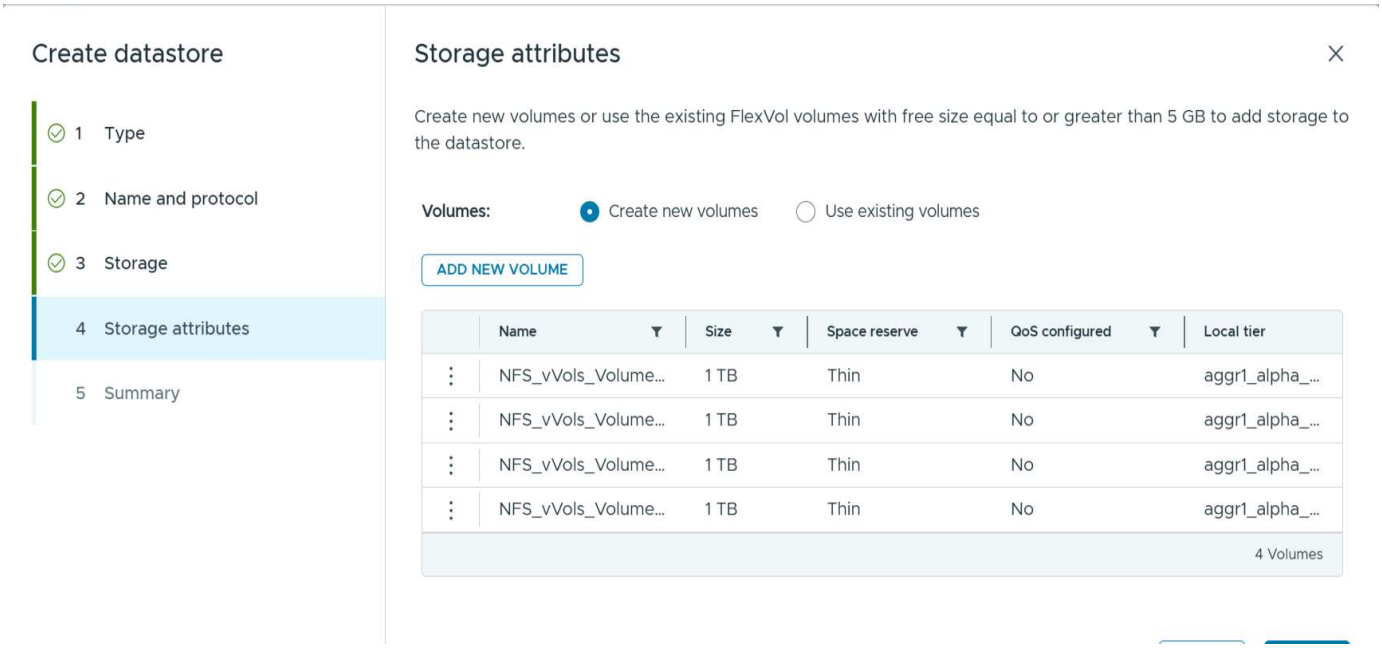


- Wählen Sie die SVM aus und klicken Sie auf *Next*.

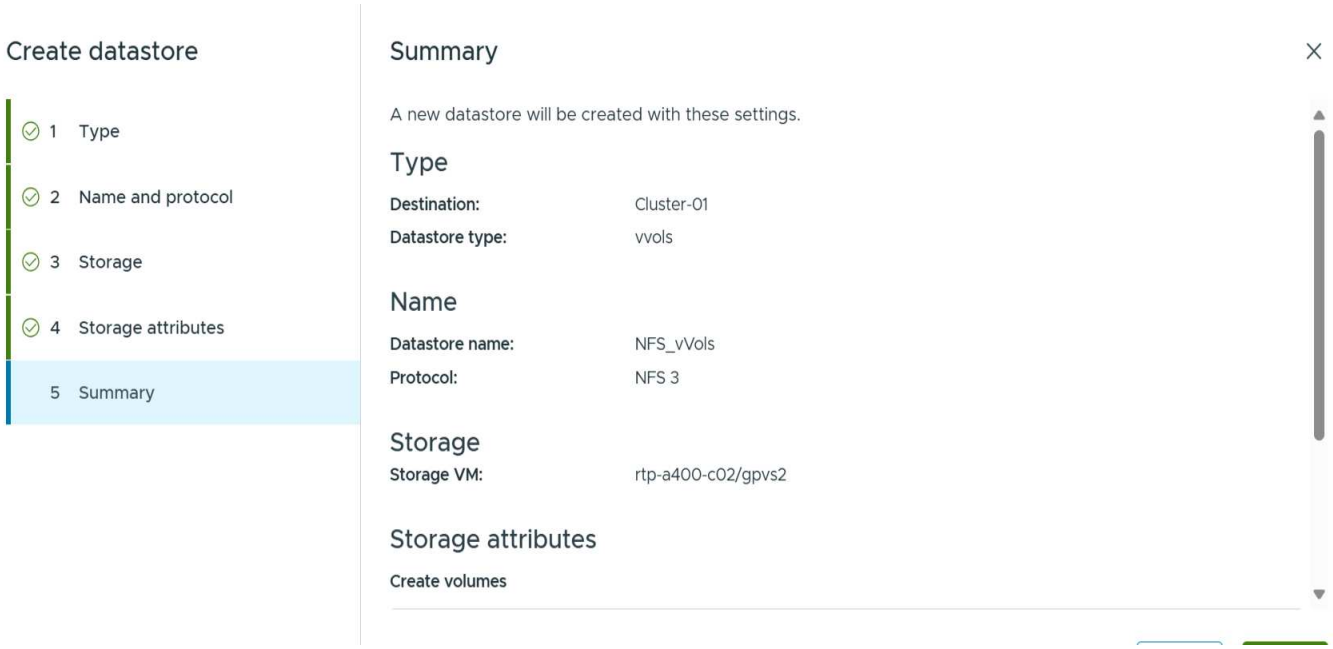


- Klicken Sie auf *neue Volumes hinzufügen* oder *vorhandenes Volume verwenden* und geben Sie die Attribute an. Beachten Sie, dass Sie in ONTAP tools 10.3 die gleichzeitige Erstellung mehrerer Volumes anfordern können. Sie können auch manuell mehrere Volumes hinzufügen, um diese gleichmäßig über den ONTAP Cluster zu verteilen. Klicken Sie auf *weiter*

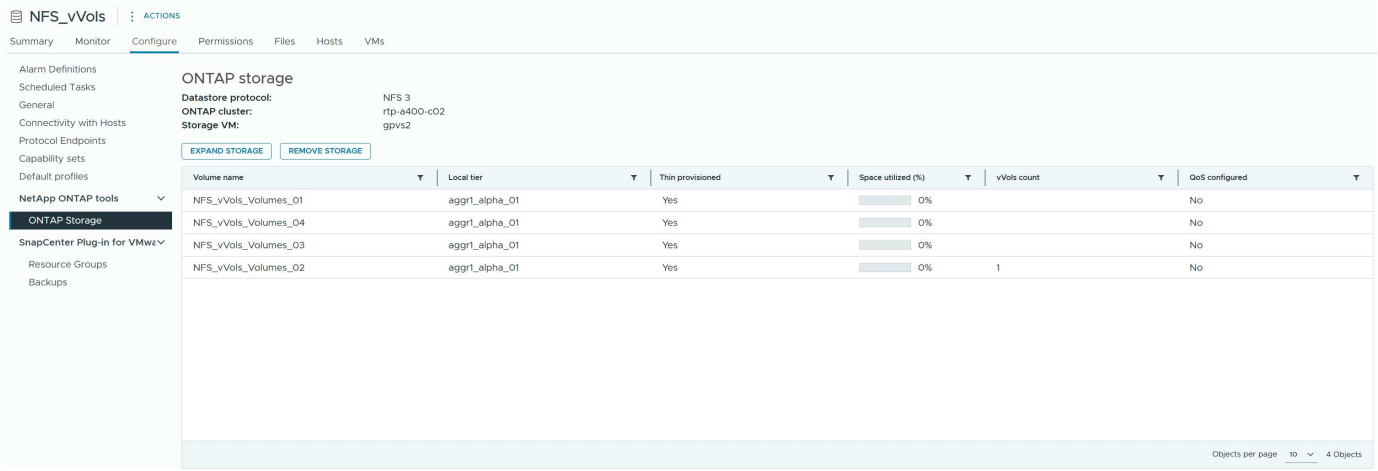




- Klicken Sie auf „*Finish*“



- Sie können die zugewiesenen Volumes im Menü „ONTAP-Tools“ der Registerkarte „Configure“ für den Datastore anzeigen.



- Sie können jetzt VM-Storage-Richtlinien über das Menü „*Policies and Profiles*“ in der vCenter UI erstellen.

Migration von VMs von herkömmlichen Datastores auf VVols

Die Migration von VMs von herkömmlichen Datastores in einen VVols Datastore ist nicht komplizierter als das Verschieben von VMs zwischen herkömmlichen Datastores. Wählen Sie einfach die VM(s) aus, dann Migrate aus der Liste der Aktionen und dann einen Migrationstyp von *change Storage only* aus. Wählen Sie bei der entsprechenden Aufforderung eine VM-Storage-Richtlinie aus, die Ihrem VVols-Datastore entspricht. Vorgänge für Migrationskopien können für SAN VMFS zu VVols Migrationen mit vSphere 6.0 und höher verlagert werden, jedoch nicht von NAS VMDKs zu VVols.

Verwalten von VMs mithilfe von Richtlinien

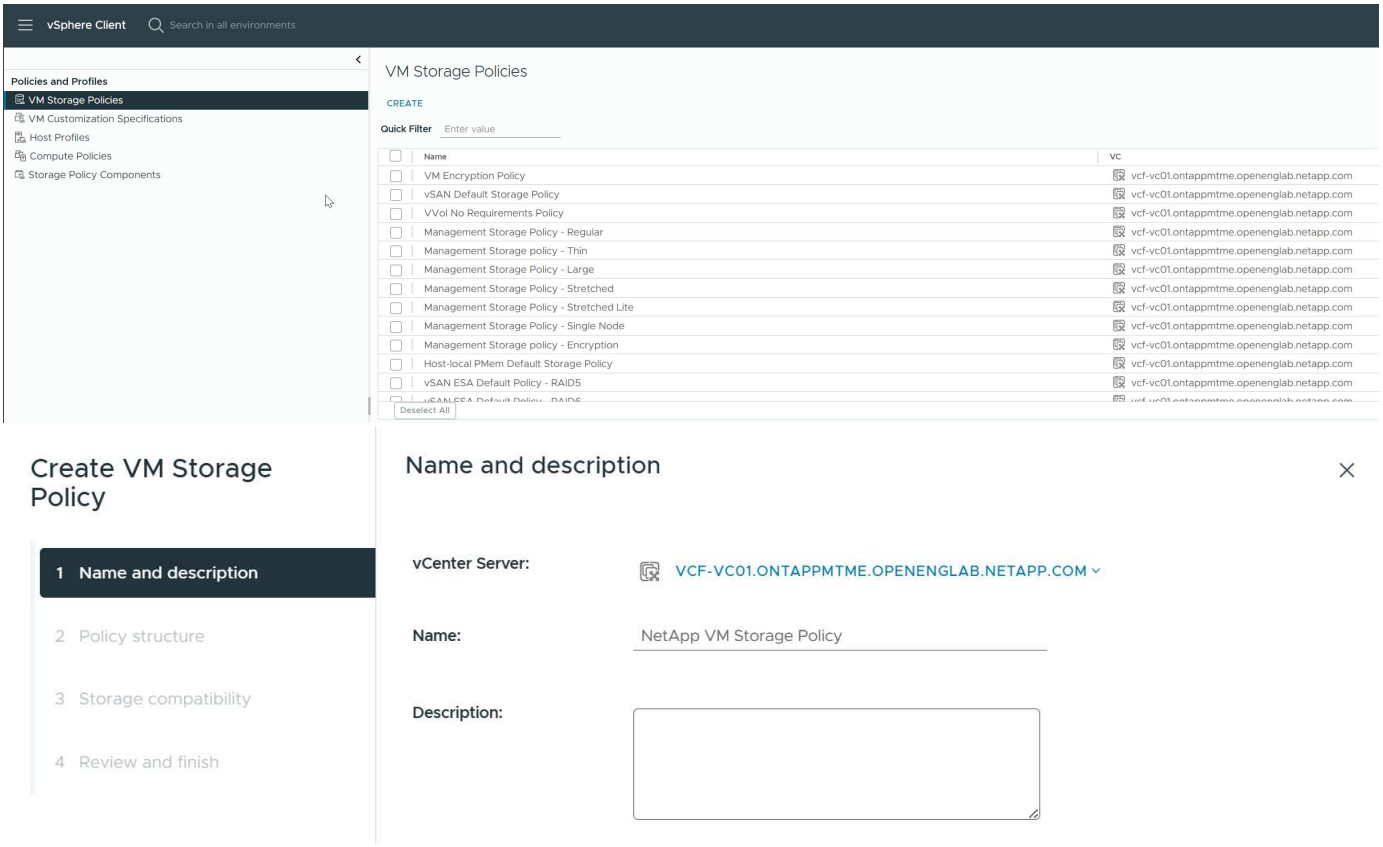
Um die Speicherbereitstellung mit richtlinienbasierter Verwaltung zu automatisieren, müssen Sie VM-Speicherrichtlinien erstellen, die den gewünschten Speicherkapazitäten zugeordnet sind.

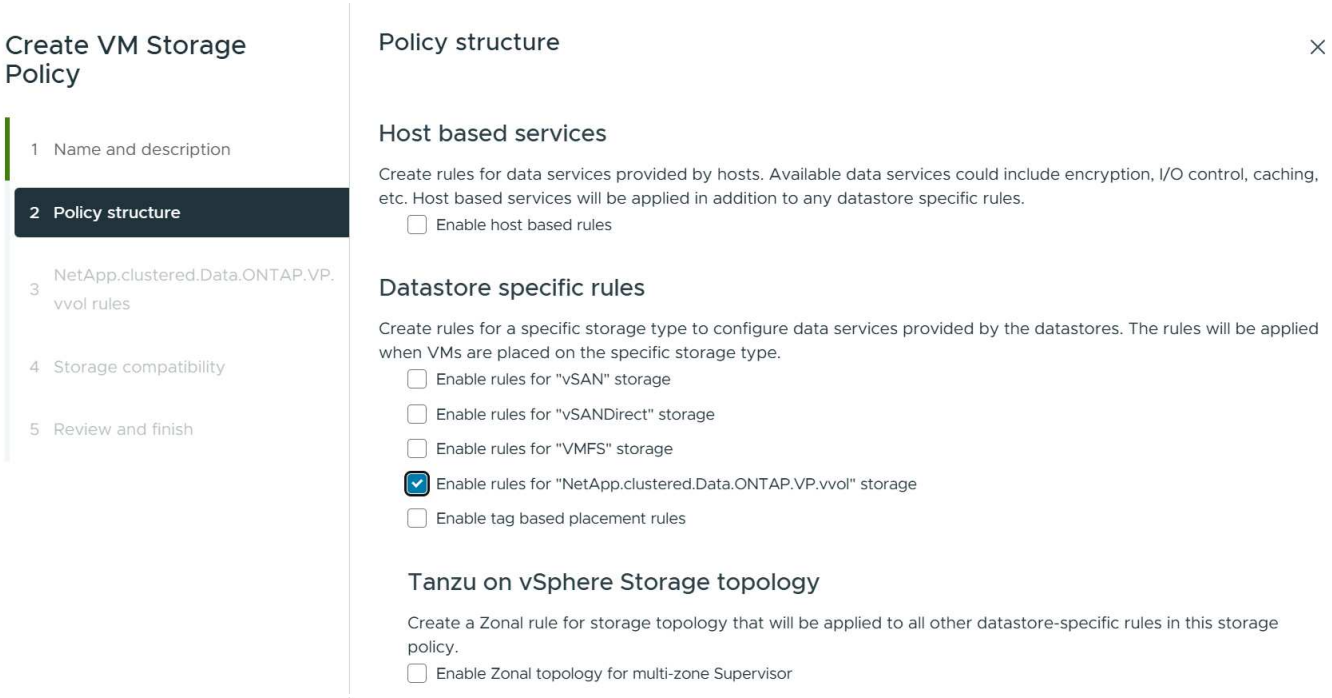
ONTAP-Tools ab Version 10.0 verwenden keine Speicherfähigkeitsprofile mehr wie frühere Versionen. Stattdessen sind die Storage-Funktionen direkt in der Richtlinie für den VM-Storage selbst definiert.

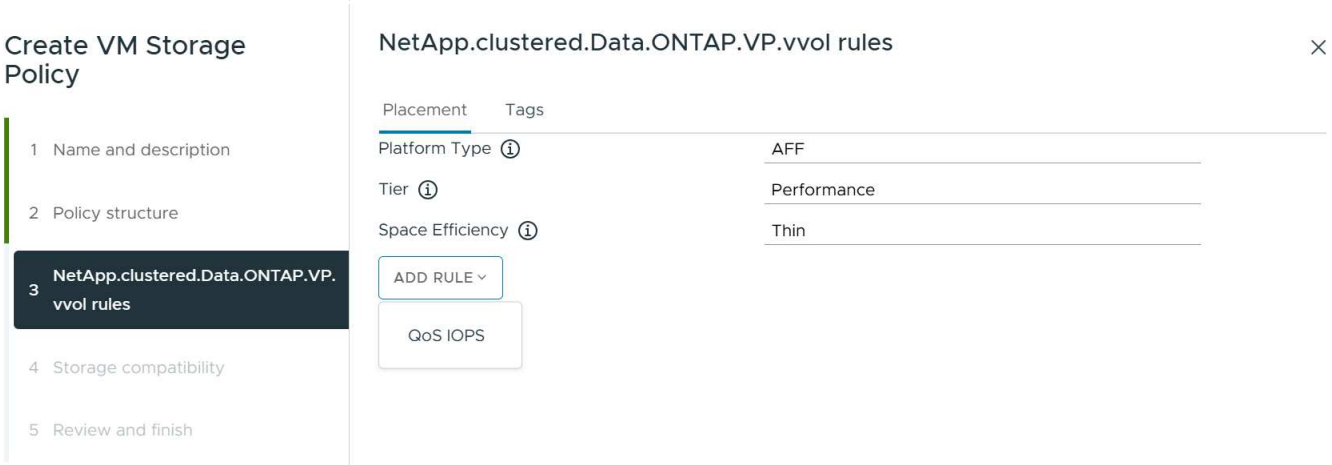
Erstellen von VM-Storage-Richtlinien

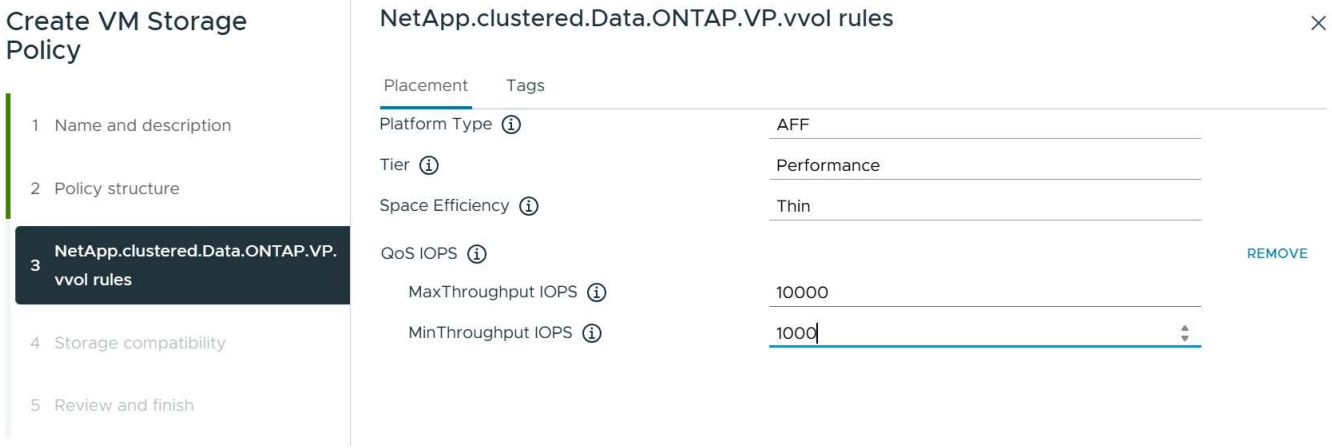
VM-Speicherrichtlinien werden in vSphere verwendet, um optionale Funktionen wie Storage I/O Control oder vSphere Encryption zu verwalten. Sie werden auch zusammen mit vVols verwendet, um der VM bestimmte Speicherfunktionen zuzuweisen. Verwenden Sie den Speichertyp "NetApp.clustered.Data.ONTAP ONTAP". Unter example network configuration using vVols over NFS v3 finden Sie ein Beispiel hierfür mit dem ONTAP Tools VASA Provider. Regeln für den Speicher „NetApp.clustered.Data. ONTAP.VP.VASA10“ sind mit Datenspeichern zu verwenden, die nicht auf vVols basieren.

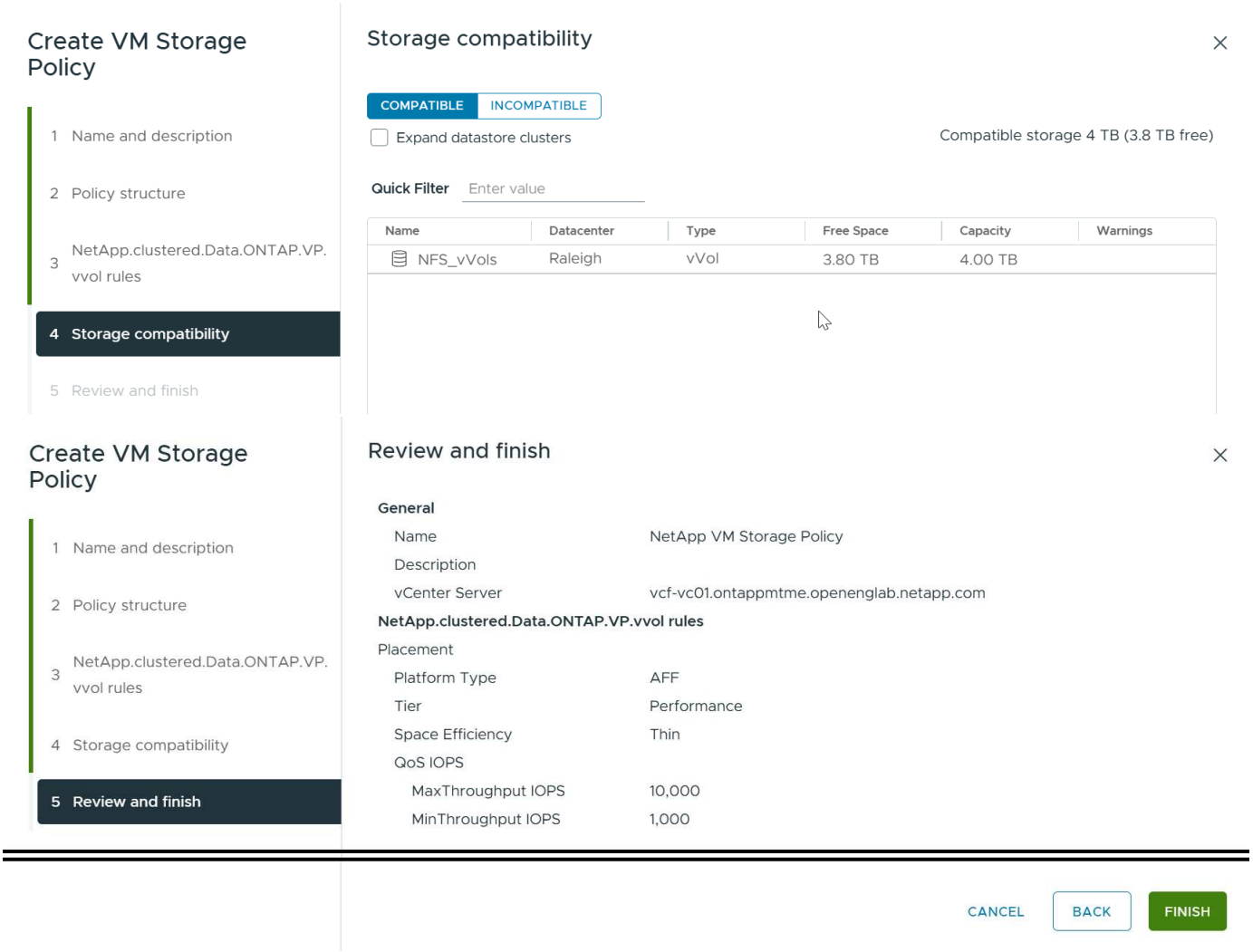
Sobald die Storage-Richtlinie erstellt wurde, kann sie bei der Bereitstellung neuer VMs verwendet werden.




Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP. vvol rules
4 Storage compatibility
5 Review and finish
Policy structure
Host based services
Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.
Enable host based rules
Datastore specific rules
Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.
Enable rules for "vSAN" storage
Enable rules for "vSANDirect" storage
Enable rules for "VMFS" storage
Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
Enable tag based placement rules
Tanzu on vSphere Storage topology
Create a Zonal rule for storage topology that will be applied to all other datastore-specific rules in this storage policy.
Enable Zonal topology for multi-zone Supervisor


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP. vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
ADD RULE
QoS IOPS


Create VM Storage Policy
1 Name and description
2 Policy structure
3 NetApp.clustered.Data.ONTAP.VP. vvol rules
4 Storage compatibility
5 Review and finish
NetApp.clustered.Data.ONTAP.VP.vvol rules
Placement
Tags
Platform Type
AFF
Tier
Performance
Space Efficiency
Thin
QoS IOPS
REMOVE
MaxThroughput IOPS
10000
MinThroughput IOPS
1000



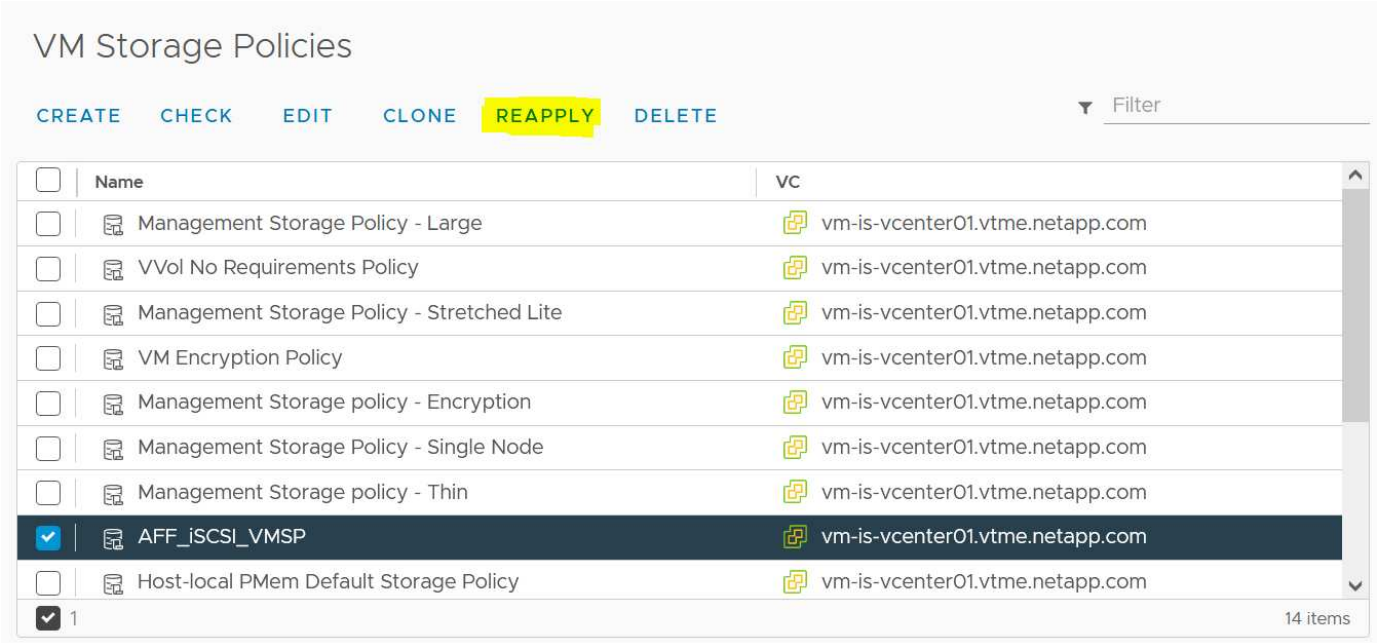
Performance-Management mit ONTAP Tools

ONTAP Tools verwenden einen eigenen Algorithmus für optimierte Platzierung, um ein neues vVol in den besten FlexVol volume zu platzieren – mit einheitlichen oder klassischen ASA Systemen oder einer Storage Availability Zone (SAZ) mit ASA r2 Systemen innerhalb eines VVols Datastore. Die Platzierung muss dem zugrunde liegende Storage mit der VM-Storage-Richtlinie übereinstimmen. Dadurch wird sichergestellt, dass der Datastore und der zugrunde liegende Storage die angegebenen Performance-Anforderungen erfüllen können.

Änderungen an den Leistungsfunktionen, wie z. B. Min und Max IOPS, erfordern eine genaue Konfiguration.

- **Min. Und Max. IOPS** können in einer VM Policy angegeben werden.
  - Eine Änderung der IOPS in der Richtlinie ändert die QoS auf den vVols erst dann, wenn die VM-Richtlinie erneut auf die VMs angewendet wird, die sie verwenden. Alternativ können Sie eine neue Richtlinie mit den gewünschten IOPS erstellen und diese auf die Ziel-VMs anwenden. Im Allgemeinen empfiehlt es sich, für verschiedene Serviceebenen separate VM-Speicherrichtlinien zu definieren und die VM-Speicherrichtlinie einfach auf der VM zu ändern.
  - Die Persönlichkeitstypen ASA, ASA r2, AFF und FAS haben unterschiedliche IOP-Einstellungen. Sowohl Min als auch Max sind auf allen Blitzsystemen verfügbar; allerdings können Nicht AFF -Systeme nur die Max-IOPS-Einstellungen verwenden.
- ONTAP-Tools erstellen individuelle QoS-Richtlinien ohne gemeinsame Nutzung mit derzeit unterstützten Versionen von ONTAP. Daher erhält jede einzelne VMDK eine eigene IOPS-Zuweisung.

Erneutes Anwenden der VM-Speicherrichtlinie



Sicherung von VVols

In den folgenden Abschnitten werden die Verfahren und Best Practices für die Verwendung von VMware VVols mit ONTAP Storage beschrieben.

VASA Provider High Availability

NetApp VASA Provider wird als Teil der virtuellen Appliance zusammen mit dem vCenter Plug-in und REST API-Server (ehemals Virtual Storage Console [VSC]) und Storage Replication Adapter ausgeführt. Wenn der VASA Provider nicht verfügbar ist, werden VMs mit VVols weiterhin ausgeführt. Es können jedoch keine neuen VVols-Datastores erstellt werden. VVols können nicht über vSphere erstellt oder gebunden werden. Das bedeutet, dass VMs mit VVols nicht eingeschaltet werden können, da vCenter die Erstellung des Swap-vVol nicht anfordern kann. Außerdem können ausgeführte VMs vMotion nicht für die Migration zu einem anderen Host verwenden, da die VVols nicht an den neuen Host gebunden werden können.

VASA Provider 7.1 und höher unterstützen neue Funktionen, damit die Services bei Bedarf verfügbar sind. Sie umfasst neue Watchdog-Prozesse zur Überwachung von VASA Provider und integrierten Datenbankdiensten. Wenn ein Fehler erkannt wird, werden die Protokolldateien aktualisiert und die Dienste dann automatisch neu gestartet.

Der weitere Schutz muss vom vSphere-Administrator mithilfe derselben Verfügbarkeitsfunktionen konfiguriert werden, die auch zum Schutz anderer geschäftskritischer VMs vor Fehlern in Software, Host-Hardware und Netzwerk verwendet werden. Es ist keine zusätzliche Konfiguration für die virtuelle Appliance erforderlich, um diese Funktionen nutzen zu können. Konfigurieren Sie sie einfach mit dem Standard-vSphere-Ansatz. Sie wurden getestet und werden von NetApp unterstützt.

VSphere High Availability lässt sich leicht konfigurieren, um eine VM auf einem anderen Host im Host-Cluster bei einem Ausfall neu zu starten. VSphere Fault Tolerance bietet eine höhere Verfügbarkeit, indem eine sekundäre VM erstellt wird, die kontinuierlich repliziert wird und an jedem beliebigen Punkt übernommen werden kann. Weitere Informationen zu diesen Funktionen finden Sie im "Dokumentation zu ONTAP Tools für VMware vSphere (Konfiguration von Hochverfügbarkeit für ONTAP Tools)", Sowie VMware vSphere Dokumentation (suchen Sie nach vSphere Verfügbarkeit unter ESXi und vCenter Server).

ONTAP Tools VASA Provider sichert die VVols Konfiguration automatisch in Echtzeit auf gemanagten ONTAP Systemen, auf denen die VVols Informationen innerhalb der FlexVol Volume-Metadaten gespeichert sind. Sollte die ONTAP Tools Appliance aus irgendeinem Grund nicht mehr verfügbar sein, können Sie schnell und einfach eine neue Appliance implementieren und die Konfiguration importieren. Weitere Informationen zu den Schritten zur Wiederherstellung von VASA Provider finden Sie in diesem KB-Artikel:

"So führen Sie eine VASA Provider Disaster Recovery - Resolution Guide durch"

VVols Replizierung

Viele ONTAP Kunden replizieren ihre herkömmlichen Datastores auf sekundäre Storage-Systeme mithilfe von NetApp SnapMirror. Bei einem Ausfall stellen sie dann mithilfe des Sekundärsystems individuelle VMs oder einen kompletten Standort wieder her. In den meisten Fällen verwenden Kunden hierfür ein Software Tool, z. B. ein Backup Software-Produkt wie das NetApp SnapCenter Plug-in für VMware vSphere oder eine Disaster Recovery-Lösung wie Site Recovery Manager von VMware (zusammen mit dem Storage Replication Adapter in ONTAP Tools).

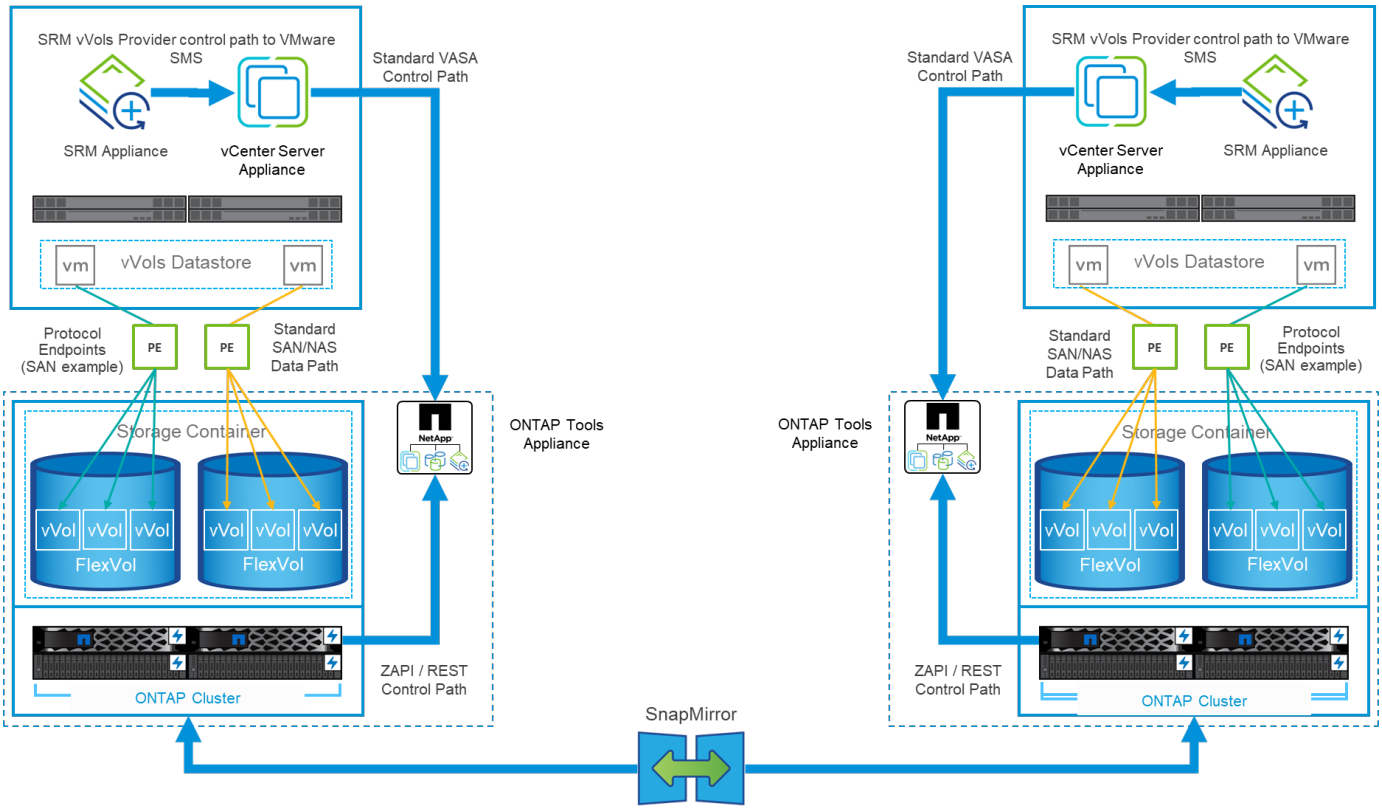
Diese Anforderung an ein Software-Tool ist für das Management der VVols Replizierung noch wichtiger. Einige Aspekte können durch native Funktionen gemanagt werden (beispielsweise werden durch VMware gemanagte Snapshots von VVols auf ONTAP verlagert, bei denen schnelle, effiziente Datei- oder LUN-Klone verwendet werden), doch ist allgemeine Orchestrierung für das Management der Replizierung und Recovery erforderlich. Metadaten zu VVols werden sowohl durch ONTAP als auch durch den VASA Provider geschützt, für die Nutzung an einem sekundären Standort ist jedoch eine zusätzliche Verarbeitung erforderlich.

Die ONTAP Tools 9.7.1 unterstützen in Verbindung mit der VMware Site Recovery Manager (SRM) Version 8.3 zusätzlich die Orchestrierung von Disaster Recovery und Migrations-Workflows mithilfe der NetApp SnapMirror Technologie.

In der ersten Version der SRM-Unterstützung mit ONTAP Tools 9.7.1 war es erforderlich, FlexVol Volumes vorab zu erstellen und die SnapMirror-Sicherung zu aktivieren, bevor sie als Backup-Volumes für einen VVols-Datastore verwendet werden konnten. Ab ONTAP Tools 9.10 wird dieser Prozess nicht mehr benötigt. Sie können jetzt vorhandene Backup Volumes um SnapMirror Schutz erweitern und Ihre VM-Storage-Richtlinien aktualisieren, um von richtlinienbasiertem Management mit Disaster Recovery, Migrationorchestrierung und Automatisierung, integriert in SRM, zu profitieren.

Derzeit ist VMware SRM die einzige von NetApp unterstützte Lösung für Disaster Recovery und Migrationsautomatisierung für VVols. ONTAP Tools überprüfen die Existenz eines SRM 8.3 oder eines höheren Servers, der bei vCenter registriert ist, bevor Sie die VVols Replizierung aktivieren können. Es ist zwar möglich, die REST-APIs der ONTAP Tools zur Erstellung eigener Services zu nutzen.

VVols Replizierung mit SRM



MetroCluster-Unterstützung

ONTAP Tools können zwar keine MetroCluster-Umschaltung auslösen, doch es unterstützt NetApp MetroCluster Systeme für VVols, die Volumes in einer einheitlichen vSphere Metro Storage Cluster (vMSC) Konfiguration sichern. Die Umschaltung eines MetroCluster-Systems erfolgt auf normale Weise.

NetApp SnapMirror Business Continuity (SM-BC) kann zwar auch als Basis für eine vMSC Konfiguration verwendet werden, wird jedoch derzeit nicht mit VVols unterstützt.

In diesen Leitfäden finden Sie weitere Informationen über NetApp MetroCluster:

"*TR-4689 MetroCluster IP Lösungsarchitektur und Design*"

"TR-4705 NetApp MetroCluster Lösungsarchitektur und Design_"

"*VMware KB 2031038 VMware vSphere Unterstützung mit NetApp MetroCluster*"

VVols Backup-Übersicht

Für die Sicherung von VMs gibt es verschiedene Ansätze, beispielsweise die Verwendung von Backup-Agenten in Gastbetrieben, das Anhängen von VM-Datendateien an einen Backup-Proxy oder die Verwendung definierter APIs wie VMware VADP. VVols können über dieselben Mechanismen geschützt werden, und viele NetApp Partner unterstützen VM-Backups, einschließlich VVols.

Wie bereits erwähnt, werden von VMware vCenter gemanagte Snapshots in platzsparende und schnelle ONTAP Datei-/LUN-Klone ausgelagert. Diese können für schnelle, manuelle Backups verwendet werden, sind aber von vCenter auf maximal 32 Snapshots beschränkt. Sie können vCenter verwenden, um Snapshots zu erstellen und bei Bedarf zurückzusetzen.

Ab dem SnapCenter Plug-in für VMware vSphere (SCV) 4.6 wird in Verbindung mit den ONTAP Tools 9.10 und höher die Unterstützung für absturzkonsistentes Backup und Recovery von VVols-basierten VMs unterstützt.

Dabei werden ONTAP FlexVol Volume Snapshots mit Unterstützung für SnapMirror und SnapVault-Replizierung verwendet. Pro Volume werden bis zu 1023 Snapshots unterstützt. SCV kann mithilfe von SnapMirror mit einer Mirror-Vault-Richtlinie auch mehr Snapshots mit längerer Aufbewahrung auf sekundären Laufwerken speichern.

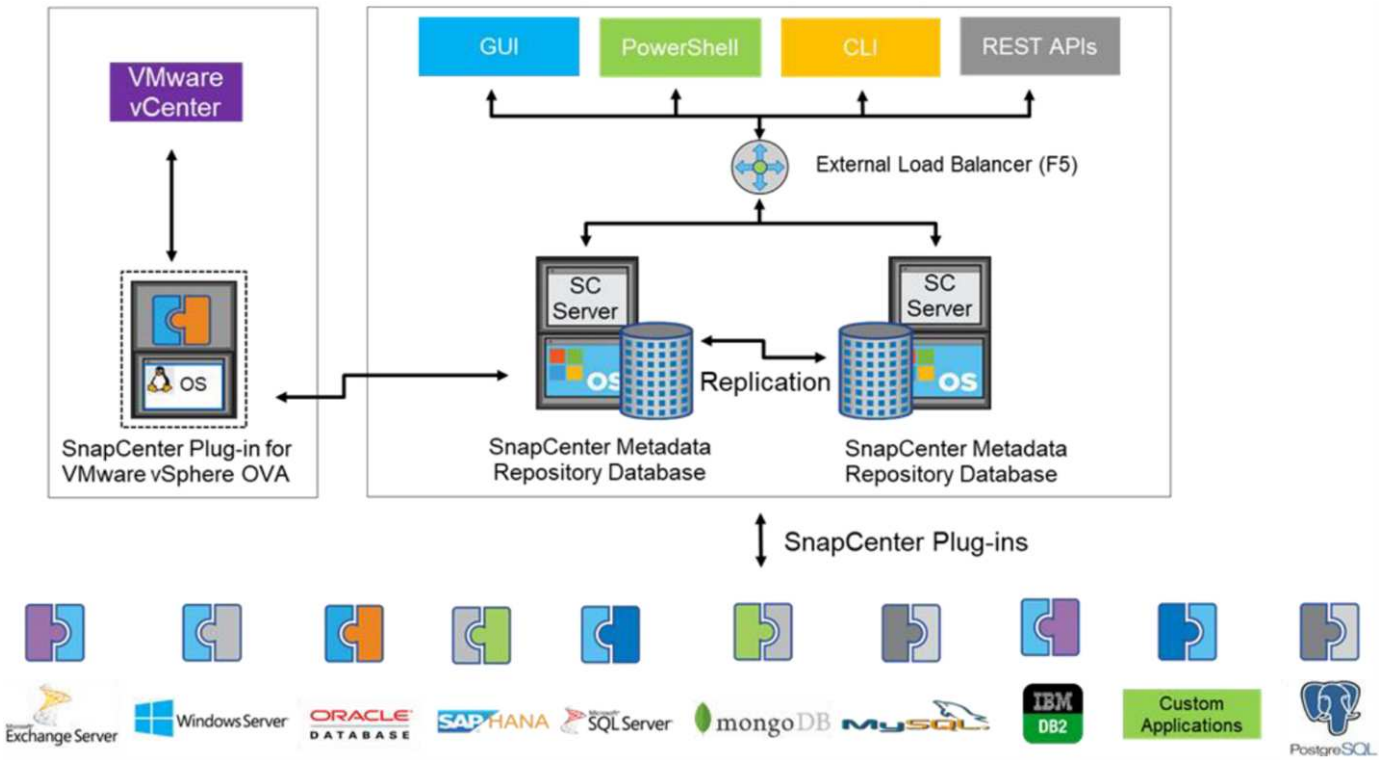
Die Unterstützung für vSphere 8.0 wurde mit SCV 4.7 eingeführt, wobei eine isolierte lokale Plug-in-Architektur verwendet wurde. Die Unterstützung für vSphere 8.0U1 wurde zu SCV 4.8 hinzugefügt, wodurch die neue Remote-Plug-in-Architektur vollständig umgestellt wurde.

VVols Backup mit SnapCenter Plug-in für VMware vSphere

Mit NetApp SnapCenter können Sie nun auf Tags und/oder Ordnern basierende Ressourcengruppen für VVols erstellen und so automatisch die Vorteile der auf ONTAP FlexVol basierenden Snapshots für VVols basierte VMs nutzen. So können Sie Backup- und Recovery-Services definieren, die VMs automatisch bei der dynamischen Bereitstellung in Ihrer Umgebung sichern.

Das SnapCenter Plug-in für VMware vSphere wird als Standalone-Appliance implementiert, die als vCenter-Erweiterung registriert und über die vCenter UI oder ÜBER REST-APIs zur Automatisierung von Backup- und Recovery-Services gemanagt wird.

Architektur von SnapCenter



Da zum Zeitpunkt dieses Schreibens die anderen SnapCenter-Plug-ins VVols noch nicht unterstützen, konzentrieren wir uns in diesem Dokument auf das eigenständige Implementierungsmodell.

Da SnapCenter ONTAP FlexVol Snapshots verwendet, wird kein Overhead auf vSphere platziert. Es gibt auch keine Performance-Einbußen, wie man bei herkömmlichen VMs mit von vCenter gemanagten Snapshots sehen könnte. Da die SCV-Funktionalität über REST-APIs zugänglich ist, wird die Erstellung automatisierter Workflows mit Tools wie VMware Aria Automation, Ansible, Terraform und nahezu jedem anderen Automatisierungs-Tool, das standardmäßige REST-APIs verwenden kann, erleichtert.

Informationen zu SnapCenter-REST-APIs finden Sie unter "Übersicht ÜBER REST-APIs"

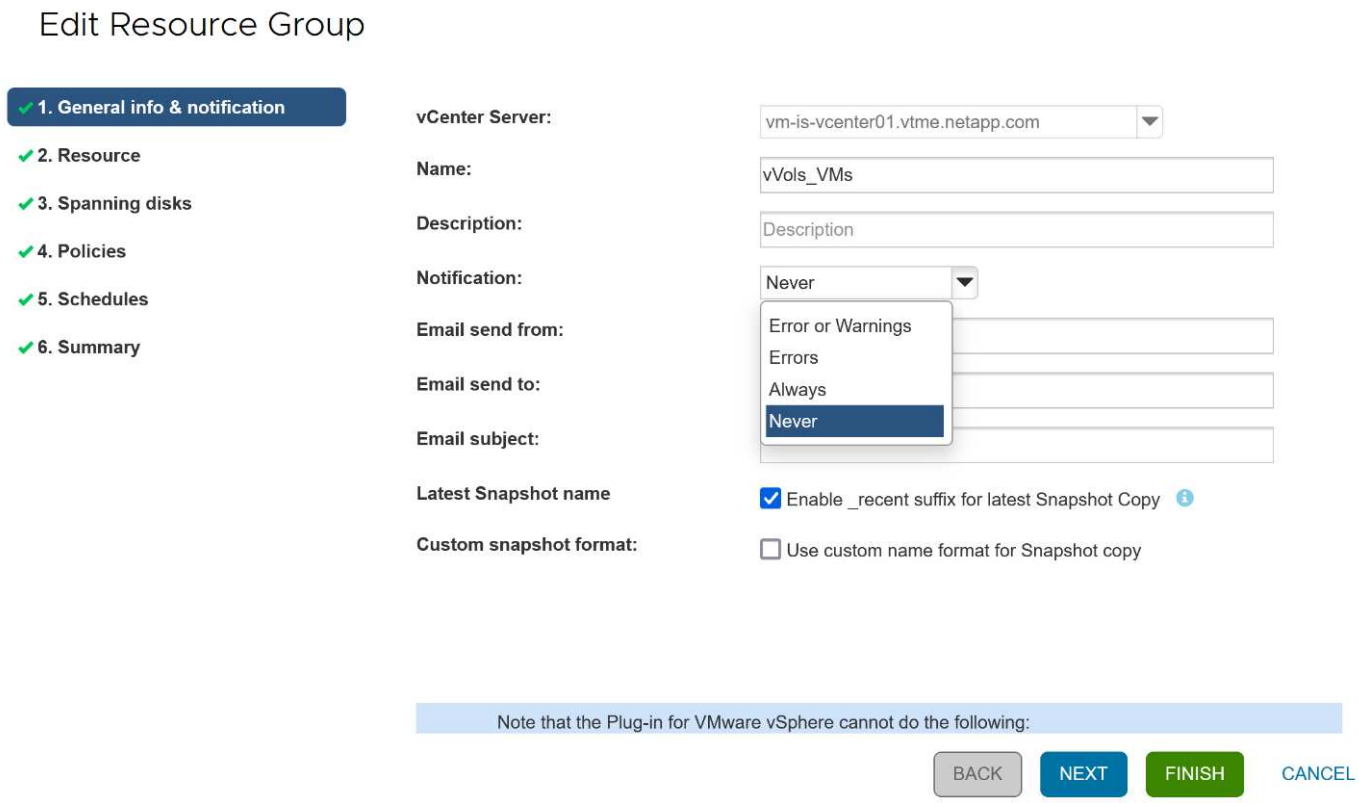
Informationen zum SnapCenter Plug-in für VMware vSphere REST-APIs finden Sie unter "SnapCenter Plug-in für VMware vSphere REST-APIs"

Best Practices In Sich Vereint

Die folgenden Best Practices unterstützen Sie dabei, die Vorteile Ihrer SnapCenter Implementierung optimal zu nutzen.

- SCV unterstützt sowohl vCenter Server RBAC als auch ONTAP RBAC und umfasst vordefinierte vCenter Rollen, die automatisch für Sie erstellt werden, wenn das Plug-in registriert ist. Sie finden weitere Informationen zu den unterstützten Typen von RBAC "Hier."
  - Verwenden Sie die vCenter-Benutzeroberfläche, um den Zugriff auf das Konto mit den geringsten Berechtigungen mithilfe der beschriebenen vordefinierten Rollen zuzuweisen "Hier".
  - Wenn Sie SCV mit SnapCenter-Server verwenden, müssen Sie die Rolle *SnapCenterAdmin* zuweisen.
  - ONTAP RBAC bezieht sich auf das Benutzerkonto, das zum Hinzufügen und Managen der vom SCV verwendeten Speichersysteme verwendet wird. Die rollenbasierte Zugriffssteuerung von ONTAP gilt nicht für VVols-basierte Backups. Erfahren Sie mehr über ONTAP RBAC und SCV "Hier".
- Replizieren Sie Backup-Datensätze auf ein zweites System und verwenden Sie SnapMirror für vollständige Replikate der Quell-Volumes. Wie bereits erwähnt, können Sie auch Mirror-Vault Richtlinien für die längerfristige Aufbewahrung von Backup-Daten unabhängig von den Quell-Volume Snapshot Aufbewahrungseinstellungen verwenden. Beide Mechanismen werden durch VVols unterstützt.
- Da SCV außerdem ONTAP-Tools für VMware vSphere für VVols Funktionen erfordert, prüfen Sie immer das NetApp Interoperabilitäts-Matrix-Tool (IMT), ob die jeweilige Version kompatibel ist
- Wenn Sie eine VVols-Replizierung mit VMware SRM verwenden, sollten Sie Ihre Richtlinien-RPO und Backup-Zeitplan beachten
- Backup-Richtlinien auf Aufbewahrungseinstellungen erstellen, die die in Ihrem Unternehmen definierten Recovery Point Objectives (RPOs) erfüllen
- Konfigurieren Sie Benachrichtigungseinstellungen für Ihre Ressourcengruppen, um über den Status der Backups informiert zu werden (siehe Abbildung 10 unten).

Benachrichtigungsoptionen für Ressourcengruppen



Erste Schritte mit SCV mit diesen Dokumenten

"Erfahren Sie mehr über das SnapCenter Plug-in für VMware vSphere"

"Implementieren Sie das SnapCenter Plug-in für VMware vSphere"

Fehlerbehebung

Es stehen mehrere Ressourcen zur Fehlerbehebung mit zusätzlichen Informationen zur Verfügung.

NetApp Support Website

Zusätzlich zu einer Vielzahl von Knowledgebase-Artikeln für NetApp Virtualisierungsprodukte bietet die NetApp Support-Website auch eine praktische Landing Page für das "ONTAP Tools für VMware vSphere" Produkt. Dieses Portal bietet Links zu Artikeln, Downloads, technischen Berichten und Diskussionen zu VMware Lösungen in der NetApp Community. Sie ist verfügbar unter:

"NetApp Support Site_"

Weitere Dokumentation zur Lösung finden Sie hier:

"*NetApp-Lösungen für die Virtualisierung mit VMware von Broadcom*"

Fehlerbehebung Für Produkte

Die verschiedenen Komponenten von ONTAP Tools wie vCenter Plug-in, VASA Provider und Storage Replication Adapter sind im NetApp Dokumenten-Repository zusammengefasst. Jedes hat jedoch einen separaten Unterabschnitt der Wissensdatenbank und kann spezifische Fehlerbehebungsverfahren haben.

Diese betreffen die häufigsten Probleme, die mit dem VASA Provider auftreten können.

Probleme BEI DER VASA Provider-UI

Gelegentlich stößt der vCenter vSphere Web Client auf Probleme mit den Serenity-Komponenten, wodurch die Menüelemente VASA Provider for ONTAP nicht angezeigt werden. Weitere Informationen finden Sie unter Beheben von Problemen bei der Registrierung von VASA Provider im Implementierungsleitfaden oder in dieser Knowledgebase "Artikel".

VVols Datastore-Bereitstellung schlägt fehl

Gelegentlich treten bei der Erstellung des VVols-Datastores bei vCenter-Services möglicherweise eine Zeitlang aus. Um sie zu korrigieren, starten Sie den vmware-sps-Service neu und mounten Sie den VVols-Datastore über die vCenter-Menüs (Storage > New Datastore) neu. Dies wird durch die fehlgeschlagenen VVols Datastore-Bereitstellung mit vCenter Server 6.5 im Administrationshandbuch abgedeckt.

Das Aktualisieren von Unified Appliance schlägt fehl, um ISO zu mounten

Aufgrund eines Fehlers in vCenter kann das zur Aktualisierung der Unified Appliance von einem Release auf das nächste verwendete ISO möglicherweise nicht mounten. Wenn das ISO mit der Appliance in vCenter verbunden werden kann, befolgen Sie den Prozess in dieser Knowledgebase "Artikel" Zu beseitigen.

VMware Site Recovery Manager mit ONTAP

VMware Live-Site Recovery mit ONTAP

ONTAP ist seit der Einführung von ESX in modernen Rechenzentren vor mehr als zwei Jahrzehnten eine führende Speicherlösung für VMware vSphere und in jüngerer Zeit für Cloud Foundation. NetApp führt weiterhin innovative Systeme ein, beispielsweise die neueste Generation der ASA A-Serie zusammen mit Funktionen wie SnapMirror Active Sync. Diese Fortschritte vereinfachen die Verwaltung, verbessern die Ausfallsicherheit und senken die Gesamtbetriebskosten (TCO) Ihrer IT-Infrastruktur.

Dieses Dokument stellt die ONTAP -Lösung für VMware Live Site Recovery (VLSR), früher bekannt als Site Recovery Manager (SRM), die branchenführende Disaster Recovery (DR)-Software von VMware, vor, einschließlich der neuesten Produktinformationen und Best Practices zur Optimierung der Bereitstellung, Risikominderung und Vereinfachung der laufenden Verwaltung.

Diese Dokumentation ersetzt den zuvor veröffentlichten technischen Bericht *TR-4900: VMware Site Recovery Manager mit ONTAP*

Andere Dokumente wie Leitfäden und Kompatibilitäts-Tools werden durch Best Practices ergänzt. Sie werden basierend auf Labortests und umfassenden praktischen Erfahrungen der NetApp Ingenieure und Kunden entwickelt. In einigen Fällen passen empfohlene Best Practices möglicherweise nicht zu Ihrer Umgebung. Sie sind jedoch im Allgemeinen die einfachsten Lösungen, die die Anforderungen der meisten Kunden erfüllen.

Der Schwerpunkt dieses Dokuments liegt auf den Funktionen der neuesten Versionen von ONTAP 9, die in Verbindung mit ONTAP-Tools für VMware vSphere 10.4 (einschließlich NetApp Storage Replication Adapter [SRA] und VASA Provider [VP]) sowie VMware Live Site Recovery 9 verwendet werden.

Vorteile von ONTAP mit VLSR oder SRM

NetApp Datenverwaltungsplattformen auf Basis von ONTAP gehören zu den am weitesten verbreiteten Speicherlösungen für VLSR. Die Gründe dafür sind vielfältig: Eine sichere, leistungsstarke Datenverwaltungsplattform mit einheitlichem Protokoll (NAS und SAN zusammen), die branchenführende Speichereffizienz, Mandantenfähigkeit, Qualitätskontrollen, Datenschutz mit platzsparenden Snapshots und Replikation mit SnapMirror bietet. Alle nutzen die native Hybrid-Multi-Cloud-Integration zum Schutz von VMware-Workloads und eine Vielzahl von Automatisierungs- und Orchestrierungstools, die Ihnen jederzeit zur Verfügung stehen.

Wenn Sie SnapMirror für die Array-basierte Replikation verwenden, profitieren Sie von einer der bewährtesten und ausgereiftesten Technologien von ONTAP. SnapMirror bietet Ihnen den Vorteil sicherer und hocheffizienter Datenübertragungen, da nur geänderte Dateisystemblöcke kopiert werden, nicht ganze VMs oder Datenspeicher. Sogar diese Blöcke profitieren von Platzeinsparungen wie Deduplizierung, Komprimierung und Verdichtung. Moderne ONTAP -Systeme verwenden jetzt das versionsunabhängige SnapMirror, sodass Sie Ihre Quell- und Zielcluster flexibel auswählen können. SnapMirror hat sich tatsächlich zu einem der leistungsstärksten verfügbaren Tools für die Notfallwiederherstellung entwickelt.

Unabhängig davon, ob Sie herkömmliche NFS-, iSCSI- oder Fibre Channel-Datenspeicher verwenden (jetzt mit Unterstützung für vVols Datenspeicher), bietet VLSR ein robustes First-Party-Angebot, das die besten ONTAP Funktionen für die Notfallwiederherstellung oder die Planung und Orchestrierung der Datencenter-Migration nutzt.

Wie VLSR ONTAP 9 nutzt

VLSR nutzt die erweiterten Datenmanagement-Technologien von ONTAP Systemen. Die Integration mit ONTAP Tools für VMware vSphere, einer virtuellen Appliance mit drei Hauptkomponenten:

- Das vCenter Plug-in der ONTAP Tools, früher als Virtual Storage Console (VSC) bekannt, vereinfacht das Storage Management und die Effizienzfunktionen, erhöht die Verfügbarkeit und senkt die Storage-Kosten und den Betriebsaufwand, sowohl bei SAN als auch bei NAS. Dieses Plug-in nutzt Best Practices für die Bereitstellung von Datastores und optimiert ESXi Hosteinstellungen für NFS- und Block-Storage-Umgebungen. Wegen all dieser Vorteile empfiehlt NetApp bei der Nutzung von vSphere bei Systemen mit ONTAP dieses Plug-in.
- Die ONTAP Tools VASA Provider unterstützen das VMware vStorage APIs for Storage Awareness (VASA) Framework. VASA Provider verbindet vCenter Server mit ONTAP und erleichtert so die Bereitstellung und das Monitoring von VM-Storage. Auf diese Weise wurden VMware Virtual Volumes (VVols) unterstützt und das Management von VM-Storage-Richtlinien sowie die VVols-Performance für einzelne VMs wurde ermöglicht. Außerdem gibt es Alarme zur Überwachung der Kapazität und der Konformität mit den Profilen.
- SRA wird zusammen mit VLSR eingesetzt, um die Replizierung von VM-Daten zwischen Produktions- und Disaster-Recovery-Standorten bei herkömmlichen VMFS- und NFS-Datenspeichern sowie zum unterbrechungsfreien Testen von DR-Replikaten zu managen. Diese Software hilft bei der Automatisierung der Erkennungs-, Recovery- und Sicherungsaufgaben. Es enthält sowohl eine SRA-Server-Appliance als auch SRA-Adapter für den Windows SRM-Server und die VLSR-Appliance.

Nachdem Sie die SRA-Adapter auf dem VLSR-Server zum Schutz von Nicht-vVols-Datenspeichern installiert und konfiguriert haben, können Sie mit der Konfiguration Ihrer vSphere-Umgebung für die Notfallwiederherstellung beginnen.

SRA bietet eine Befehls- und Kontrollschnittstelle für den VLSR-Server zur Verwaltung der ONTAP FlexVol-Volumes, die Ihre virtuellen VMware-Maschinen (VMs) enthalten, sowie zur Sicherung der SnapMirror-Replikation.

VLSR kann Ihren DR-Plan unterbrechungsfrei testen, indem es die proprietäre FlexClone -Technologie von

NetApp verwendet, um nahezu sofortige Klone Ihrer geschützten Datenspeicher an Ihrem DR-Standort zu erstellen. VLSR erstellt eine Sandbox zum sicheren Testen, sodass Ihr Unternehmen und Ihre Kunden im Falle einer echten Katastrophe geschützt sind. So können Sie darauf vertrauen, dass Ihr Unternehmen im Katastrophenfall ein Failover durchführen kann.

Bei einem echten Ausfall oder sogar einer geplanten Migration können Sie mit VLSR alle Last-Minute-Änderungen am Datensatz über ein letztes SnapMirror Update senden (sofern Sie dies tun). Dann wird die Spiegelung unterbrochen und der Datenspeicher wird Ihren DR-Hosts gemountet. An diesem Punkt können Ihre VMs automatisch in beliebiger Reihenfolge gemäß Ihrer vorab geplanten Strategie hochgefahren werden.

Mit ONTAP Systemen können Sie SVMs zwecks SnapMirror Replizierung im selben Cluster kombinieren, jedoch wurde dieses Szenario nicht mit VLSR getestet und zertifiziert. Daher wird empfohlen, bei Verwendung von VLSR nur SVMs aus unterschiedlichen Clustern zu verwenden.

VLSR mit ONTAP und anderen Anwendungsfällen: Hybrid Cloud und Migration

Durch die Integration Ihrer VLSR-Bereitstellung mit den erweiterten Datenverwaltungsfunktionen von ONTAP können Sie im Vergleich zu lokalen Speicheroptionen eine deutlich verbesserte Skalierbarkeit und Leistung erzielen. Darüber hinaus bietet es die Flexibilität der Hybrid Cloud. Mit der Hybrid Cloud können Sie Geld sparen, indem Sie ungenutzte Datenblöcke von Ihrem Hochleistungs-Array mithilfe von FabricPool auf Ihren bevorzugten Hyperscaler auslagern. Dabei kann es sich um einen lokalen S3-Speicher wie NetApp StorageGRID handeln. Sie können SnapMirror auch für Edge-basierte Systeme mit softwaredefiniertem ONTAP Select oder Cloud-basierter DR verwenden, indem Sie "NetApp Storage auf Equinix Metal"oder andere gehostete ONTAP -Dienste.

Anschließend könnten Sie dank FlexClone ein Test-Failover innerhalb des Datacenters eines Cloud-Service-Providers durchführen, bei einem Storage-Platzbedarf von nahezu null. Der Schutz Ihres Unternehmens ist jetzt günstiger als je zuvor.

Mit VLSR können auch geplante Migrationen durchgeführt werden, indem VMs mit SnapMirror effizient von einem Datacenter in ein anderes oder sogar innerhalb desselben Datacenters übertragen werden, unabhängig davon, ob es sich um Ihr eigenes Datacenter oder über eine beliebige Anzahl an Service Providern von NetApp Partnern handelt.

Best Practices für die Implementierung

In den folgenden Abschnitten werden die Best Practices für die Implementierung mit ONTAP und VMware SRM beschrieben.

Verwenden Sie die neueste Version von ONTAP Tools 10

Die ONTAP Tools 10 bieten im Vergleich zu den Vorgängerversionen erhebliche Verbesserungen, darunter:

- 8-mal schnelleres Test-Failover*
- 2x schnellere Bereinigung und erneuer Schutz*
- 32 % schnellerer Failover*
- Besser skalieren
- Native Unterstützung für gemeinsam genutzte Site-Layouts

*Diese Verbesserungen basieren auf internen Tests und können je nach Umgebung variieren.

SVM-Layout und Segmentierung für SMT

Mit ONTAP sorgt das Konzept der Storage Virtual Machine (SVM) für eine strenge Segmentierung in sicheren mandantenfähigen Umgebungen. SVM-Benutzer auf einer SVM können nicht auf Ressourcen einer anderen SVM zugreifen bzw. diese managen. Auf diese Weise können Sie die ONTAP Technologie nutzen, indem Sie separate SVMs für verschiedene Geschäftseinheiten erstellen, die ihre eigenen SRM Workflows im selben Cluster managen, um eine größere Storage-Effizienz zu erzielen.

Erwägen Sie die Verwaltung von ONTAP mit SVM-Scoped-Konten und SVM-Management-LIFs, um nicht nur die Sicherheitskontrolle zu verbessern, sondern auch die Performance zu verbessern. Die Performance ist bei der Nutzung von Verbindungen mit SVM-Umfang höher, da der SRA nicht erforderlich ist, alle Ressourcen eines gesamten Clusters – einschließlich physischer Ressourcen – zu verarbeiten. Stattdessen müssen sie nur die logischen Ressourcen verstehen, die zu der jeweiligen SVM abstrahiert sind.

Best Practices für das Management von ONTAP 9 Systemen

Wie bereits erwähnt, können Sie ONTAP Cluster mit Anmeldedaten im Cluster oder SVM-Umfang und Management-LIFs managen. Um die optimale Performance zu erzielen, sollten Sie immer dann die Verwendung von VVols in Betracht ziehen, wenn Sie über den SVM-Umfang verfügen. Dabei sollten Sie sich jedoch einigen Anforderungen bewusst sein und dass einige Funktionen verloren gehen.

- Das Standard-vsadmin SVM-Konto verfügt nicht über die erforderliche Zugriffsebene, um ONTAP-Tools-Aufgaben durchzuführen. Daher müssen Sie ein neues SVM-Konto erstellen. "Konfigurieren Sie ONTAP-Benutzerrollen und -Berechtigungen" Verwenden der enthaltenen JSON-Datei. Diese Option kann für SVM oder Konten mit Cluster-Umfang verwendet werden.
- Da es sich bei dem vCenter UI Plug-in, VASA Provider und SRA Server um vollständig integrierte Microservices handelt, müssen Sie ebenso wie beim Hinzufügen von Storage in der vCenter UI für ONTAP-Tools Storage zum SRA-Adapter in SRM hinzufügen. Andernfalls erkennt der SRA-Server möglicherweise nicht die Anfragen, die von SRM über den SRA-Adapter gesendet werden.
- Die NFS-Pfadprüfung wird bei Verwendung der im SVM-Umfang enthaltenen Anmeldedaten nicht durchgeführt, es sei denn, Sie befinden sich zuerst "Onboard Cluster" im ONTAP Tools Manager und verknüpfen sie mit den vCenter. Der Grund dafür ist, dass der physische Standort logisch von der SVM abstrahiert ist. Dies stellt jedoch keine Sorge mehr dar, da bei der Verwendung von indirekten Pfaden nicht mehr deutliche Performance-Einbußen bei modernen ONTAP Systemen auftreten.
- Es werden möglicherweise keine Aggregat-Platzeinsparungen aufgrund von Storage-Effizienz gemeldet.
- Wenn unterstützt, können Spiegelungen zur Lastverteilung nicht aktualisiert werden.
- Die EMS-Protokollierung wird möglicherweise nicht auf ONTAP Systemen durchgeführt, die mit den Anmeldedaten im Umfang des SVM-Service gemanagt werden.

Best Practices für betriebliche Prozesse

In den folgenden Abschnitten werden die betrieblichen Best Practices für VMware SRM und ONTAP Storage beschrieben.

Datenspeicher und Protokolle

- Wenn möglich, verwenden Sie immer ONTAP Tools, um Datenspeicher und Volumes bereitzustellen. Damit stellen wir sicher, dass Volumes, Verbindungspfade, LUNs, Initiatorgruppen, Exportrichtlinien Und andere Einstellungen sind kompatibel konfiguriert.
- SRM unterstützt iSCSI, Fibre Channel und NFS Version 3 mit ONTAP 9 bei Nutzung der Array-basierten Replizierung über SRA. SRM unterstützt nicht die Array-basierte Replizierung für NFS Version 4.1 mit

herkömmlichen oder VVols-Datastores.

- Zur Bestätigung der Konnektivität überprüfen Sie immer, ob Sie einen neuen Testdatenspeicher am DR-Standort vom Ziel-ONTAP-Cluster aus mounten und wieder mounten können. Testen Sie jedes Protokoll, das Sie für die Datastore-Konnektivität verwenden möchten. Eine Best Practice besteht darin, mit ONTAP-Tools Ihren Testdatenspeicher zu erstellen, da dies die gesamte Datastore-Automatisierung gemäß den Anweisungen von SRM erfolgt.
- SAN-Protokolle sollten für jeden Standort homogen sein. Sie können NFS und SAN mixen, aber die SAN-Protokolle sollten nicht innerhalb eines Standorts gemischt werden. Sie können beispielsweise FCP in Standort A und iSCSI in Standort B verwenden. Sie sollten nicht sowohl FCP als auch iSCSI an Standort A verwenden
- In den vorherigen Leitfäden wurde das Erstellen von LIF zur Datenlokalität empfohlen. Das heißt, mounten Sie immer einen Datenspeicher mit einer LIF auf dem Node, der physisch Eigentümer des Volume ist. Das ist zwar immer noch die Best Practice, ist aber in modernen Versionen von ONTAP 9 nicht mehr vorgeschrieben. Wenn möglich und im Cluster-Umfang Zugangsdaten angegeben, entscheiden sich ONTAP Tools weiterhin für den Lastausgleich über lokale LIFs hinweg für die Daten, allerdings sind dies keine Voraussetzungen für Hochverfügbarkeit oder Performance.
- ONTAP 9 kann so konfiguriert werden, dass Snapshots automatisch entfernt werden, um die Uptime aufrechtzuerhalten, falls ein Speicherplatz nicht ausreicht, wenn Autosize nicht in der Lage ist, eine ausreichende Notfallkapazität zur Verfügung zu stellen. In der Standardeinstellung für diese Funktion werden die von SnapMirror erstellten Snapshots nicht automatisch gelöscht. Wenn SnapMirror Snapshots gelöscht werden, kann NetApp SRA die Replizierung für das betroffene Volume nicht rückgängig machen und erneut synchronisieren. Um zu verhindern, dass ONTAP SnapMirror Snapshots löscht, konfigurieren Sie die Funktion für automatisches Löschen von Snapshots und wählen Sie „versuchen“.

```
snap autodelete modify -volume -commitment try
```

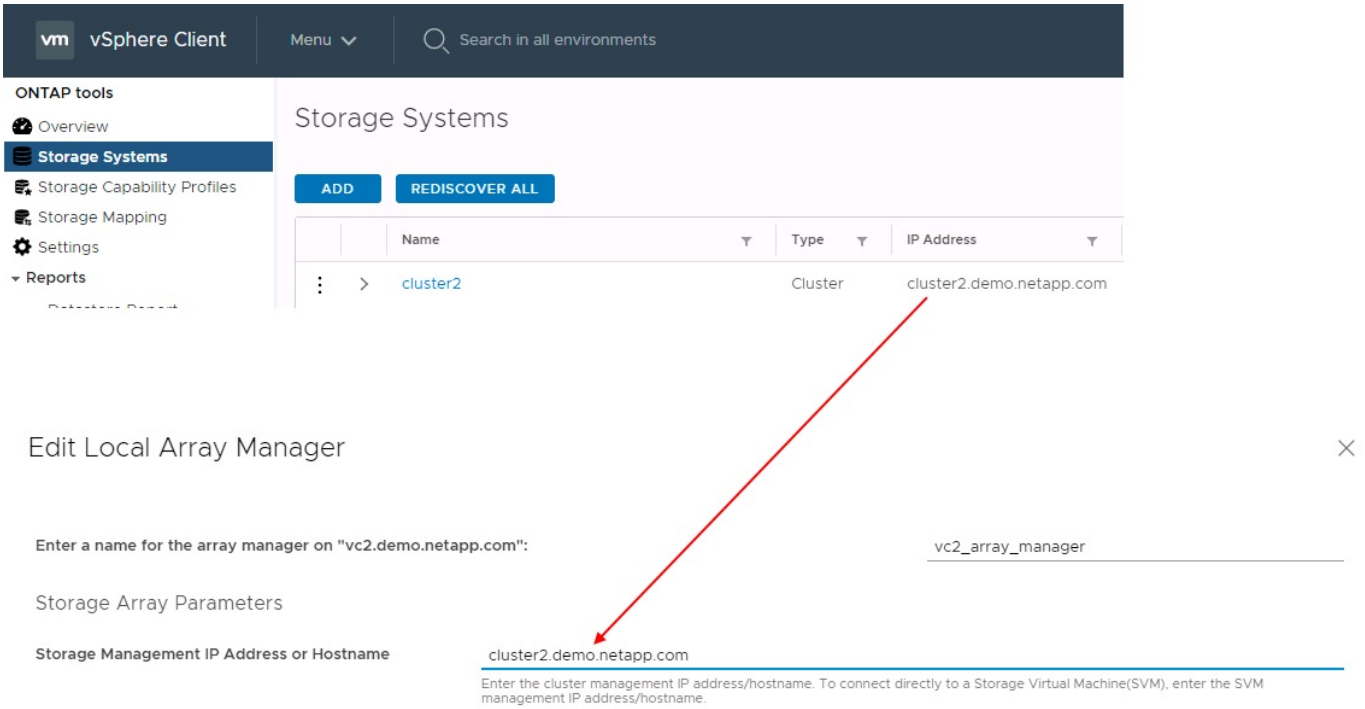
- Die automatische Größenanpassung von Volumes sollte für Volumes, die SAN-Datastores enthalten, und `grow_shrink` für NFS-Datastores auf festgelegt werden `grow`. Erfahren Sie mehr über dieses Thema unter "Konfigurieren Sie Volumes für die automatische Vergrößerung und Verkleinerung ihrer Größe".
- SRM führt am besten aus, wenn die Anzahl der Datastores und damit die Schutzgruppen in Ihren Recovery-Plänen minimiert wird. Daher sollten Sie die Optimierung für die VM-Dichte in SRM-geschützten Umgebungen in Betracht ziehen, in denen RTO eine zentrale Bedeutung hat.
- Nutzen Sie den Distributed Resource Scheduler (DRS), um die Last auf den geschützten und Recovery ESXi Clustern auszugleichen. Wenn Sie ein Failback planen, werden die zuvor geschützten Cluster beim Ausführen eines Reprotect zu den neuen Recovery-Clustern. DRS hilft dabei, die Platzierung in beide Richtungen auszugleichen.
- Wenn möglich, vermeiden Sie die Verwendung von IP-Anpassung mit SRM, da dies Ihre RTO erhöhen kann.

Allgemeines zu Array-Paaren

Für jedes Array-Paar wird ein Array-Manager erstellt. Zusammen mit SRM und ONTAP Tools erfolgt die Kopplung jedes Arrays mit dem Umfang einer SVM, auch wenn Cluster-Anmeldedaten verwendet werden. So können Sie DR-Workflows zwischen Mandanten segmentieren, basierend auf den ihnen zugewiesenen SVMs. Sie können mehrere Array-Manager für ein bestimmtes Cluster erstellen und diese asymmetrisch sein. Sie können Fan-out oder Fan-in zwischen verschiedenen ONTAP 9 Clustern. So können beispielsweise SVM-A und SVM-B auf Cluster-1 und damit auf SVM-C auf Cluster-2, SVM-D auf Cluster-3 oder umgekehrt genutzt werden.

Wenn Sie Array-Paare in SRM konfigurieren, sollten Sie sie immer in SRM auf die gleiche Weise hinzufügen,

wie Sie sie den ONTAP Tools hinzugefügt haben. Das bedeutet, dass sie denselben Benutzernamen, dasselbe Passwort und dieselbe Management-LIF verwenden müssen. Diese Anforderung stellt sicher, dass SRA ordnungsgemäß mit dem Array kommuniziert. Der folgende Screenshot veranschaulicht, wie ein Cluster in ONTAP-Tools angezeigt wird und wie es zu einem Array Manager hinzugefügt werden kann.



Allgemeines zu Replikationsgruppen

Replikationsgruppen enthalten logische Sammlungen von virtuellen Maschinen, die zusammen wiederhergestellt werden. Da die ONTAP SnapMirror Replizierung auf Volume-Ebene stattfindet, befinden sich alle VMs in einem Volume in derselben Replizierungsgruppe.

Es gibt mehrere Faktoren, die bei Replizierungsgruppen berücksichtigt werden müssen und die Art und Weise, wie VMs über FlexVol Volumes verteilt werden. Das Gruppieren ähnlicher VMs im selben Volume kann die Storage-Effizienz in älteren ONTAP Systemen steigern, bei denen Deduplizierung auf Aggregatebene fehlt. Beim Gruppieren wird jedoch die Größe des Volumes vergrößert und die Volume-I/O-Parallelität verringert. Moderne ONTAP Systeme bieten ein optimales Verhältnis zwischen Performance und Storage-Effizienz, indem VMs über FlexVol Volumes im selben Aggregat verteilt werden. Dadurch wird die Deduplizierung auf Aggregatebene genutzt und die I/O-Parallelisierung über mehrere Volumes hinweg wird gesteigert. Sie können VMs in den Volumes zusammen wiederherstellen, da eine (nachfolgend erläutert) Sicherungsgruppe mehrere Replizierungsgruppen enthalten kann. Der Nachteil dieses Layouts besteht darin, dass Blöcke mehrmals über das Netzwerk übertragen werden können, da bei SnapMirror die Aggregatdeduplizierung nicht berücksichtigt wird.

Eine letzte Überlegung für Replikationsgruppen besteht darin, dass jede von Natur aus eine logische Konsistenzgruppe ist (nicht zu verwechseln mit SRM-Konsistenzgruppen). Das liegt daran, dass alle VMs im Volume mithilfe desselben Snapshots zusammen übertragen werden. Wenn Sie also VMs haben, die stets konsistent sein müssen, sollten Sie sie in der gleichen FlexVol speichern.

Allgemeines zu Schutzgruppen

Sicherungsgruppen definieren VMs und Datastores in Gruppen, die am geschützten Standort zusammen wiederhergestellt werden. Am geschützten Standort befinden sich die VMs, die in einer Schutzgruppe konfiguriert sind, im normalen Steady-State-Betrieb. Es ist wichtig zu beachten, dass eine Schutzgruppe nicht

mehrere Array-Manager umfassen kann, obwohl SRM möglicherweise mehrere Array-Manager für eine Schutzgruppe anzeigt. Aus diesem Grund sollten Sie VM-Dateien nicht über Datastores auf unterschiedlichen SVMs verteilen.

Recovery-Pläne sprechen

Recovery-Pläne legen fest, welche Schutzgruppen im gleichen Prozess wiederhergestellt werden. Mehrere Sicherungsgruppen können im selben Recovery-Plan konfiguriert werden. Um darüber hinaus mehr Optionen für die Ausführung von Recovery-Plänen zu aktivieren, kann eine einzige Sicherungsgruppe in mehreren Recovery-Plänen enthalten sein.

Durch Recovery-Pläne können SRM-Administratoren Recovery-Workflows definieren, indem VMs einer Prioritätsgruppe von 1 (hoch) bis 5 (niedrig) zugewiesen werden, wobei 3 (mittel) standardmäßig verwendet wird. Innerhalb einer Prioritätsgruppe können VMs für Abhängigkeiten konfiguriert werden.

So könnte Ihr Unternehmen beispielsweise eine geschäftskritische Tier-1-Applikation nutzen, die für seine Datenbank auf einen Microsoft SQL Server aufbaut. Sie entscheiden also, Ihre VMs in Prioritätsgruppe 1 einzufügen. Innerhalb der Prioritätsgruppe 1 beginnen Sie mit der Planung des Auftrages der Dienste. Wahrscheinlich möchten Sie, dass Ihr Microsoft Windows Domänencontroller vor Ihrem Microsoft SQL Server gebootet wird, der vor Ihrem Anwendungsserver online sein müsste usw. Sie würden alle diese VMs der Prioritätsgruppe hinzufügen und dann die Abhängigkeiten festlegen, da Abhängigkeiten nur innerhalb einer bestimmten Prioritätsgruppe gelten.

NetApp empfiehlt besonders, mit Ihren Applikationsteams zusammenarbeiten zu müssen, um die Reihenfolge der für ein Failover-Szenario erforderlichen Operationen zu ermitteln und die Recovery-Pläne entsprechend zu erstellen.

Testen Sie den Failover

Als Best Practice empfiehlt es sich, immer dann ein Test-Failover durchzuführen, wenn an der Konfiguration des geschützten VM-Storage Änderungen vorgenommen werden. Dadurch wird sichergestellt, dass Sie bei einem Notfall darauf vertrauen können, dass Site Recovery Manager Services innerhalb des erwarteten RTO-Ziels wiederherstellen kann.

NetApp empfiehlt zudem, die Funktion der in Gast-Applikationen gelegentlich zu bestätigen, insbesondere nach der Neukonfiguration von VM-Storage.

Wenn ein Test-Recovery-Vorgang ausgeführt wird, wird auf dem ESXi Host für die VMs ein privates Test-Bubble-Netzwerk erstellt. Dieses Netzwerk wird jedoch nicht automatisch mit physischen Netzwerkadaptern verbunden und bietet daher keine Verbindung zwischen den ESXi Hosts. Um die Kommunikation zwischen VMs zu ermöglichen, die während des DR-Tests auf verschiedenen ESXi Hosts ausgeführt werden, wird ein physisches privates Netzwerk zwischen den ESXi Hosts am DR-Standort erstellt. Um zu überprüfen, ob das Testnetzwerk privat ist, kann das Testblasennetzwerk physisch oder mittels VLANs oder VLAN-Tagging getrennt werden. Dieses Netzwerk muss von dem Produktionsnetzwerk getrennt werden, da die VMs wiederhergestellt werden und nicht mit IP-Adressen im Produktionsnetzwerk platziert werden können, die mit den tatsächlichen Produktionssystemen kollidieren können. Nach dem Erstellen eines Recovery-Plans in SRM kann das erstellte Testnetzwerk als privates Netzwerk ausgewählt werden, um die VMs mit während des Tests zu verbinden.

Nachdem der Test validiert und nicht mehr erforderlich ist, führen Sie eine Bereinigung durch. Bei der Durchführung der Bereinigung werden die geschützten VMs in ihren Ausgangszustand zurückversetzt und der Recovery-Plan wird auf den Status „bereit“ zurückgesetzt.

Überlegungen zum Failover

Wenn es um Failover an einem Standort zusätzlich zur in diesem Leitfaden beschriebenen Reihenfolge geht, müssen noch einige weitere Aspekte berücksichtigt werden.

Ein Problem, mit dem Sie möglicherweise zu kämpfen haben, ist die Netzwerkunterschiede zwischen den Standorten. In einigen Umgebungen können am primären Standort und am DR-Standort dieselben Netzwerk-IP-Adressen verwendet werden. Diese Fähigkeit wird als Stretched Virtual LAN (VLAN) oder Stretched Network Setup bezeichnet. Andere Umgebungen müssen möglicherweise unterschiedliche Netzwerk-IP-Adressen (z. B. in unterschiedlichen VLANs) am primären Standort relativ zum DR-Standort verwenden.

VMware bietet verschiedene Möglichkeiten zur Lösung dieses Problems. Netzwerkvirtualisierungstechnologien wie VMware NSX-T Data Center abstrahieren den gesamten Netzwerk-Stack von Ebene 2 bis 7 von der Betriebsumgebung und ermöglichen so portablere Lösungen. Weitere Informationen zu "NSX-T-Optionen mit SRM".

SRM ermöglicht es Ihnen auch, die Netzwerkkonfiguration einer VM wie das Recovery zu ändern. Diese Neukonfiguration umfasst Einstellungen wie IP-Adressen, Gateway-Adressen und DNS-Servereinstellungen. Verschiedene Netzwerkeinstellungen, die bei der Wiederherstellung auf einzelne VMs angewendet werden, können in den Einstellungen einer VM der Eigenschaft im Recovery-Plan angegeben werden.

Um SRM so zu konfigurieren, dass verschiedene Netzwerkeinstellungen auf mehrere VMs angewendet werden können, ohne die Eigenschaften der einzelnen im Recovery-Plan bearbeiten zu müssen, stellt VMware ein Tool namens dr-ip-Customizer bereit. Informationen zur Verwendung dieses Dienstprogramms finden Sie unter "VMware Dokumentation".

Schützen

Nach einem Recovery wird der Recovery-Standort zum neuen Produktionsstandort. Da der Recovery-Vorgang die SnapMirror Replizierung ausbrach, ist der neue Produktionsstandort nicht vor zukünftigen Ausfällen geschützt. Als Best Practice wird empfohlen, den neuen Produktionsstandort unmittelbar nach dem Recovery auf einen anderen Standort zu schützen. Wenn der ursprüngliche Produktionsstandort betriebsbereit ist, kann der VMware Administrator den ursprünglichen Produktionsstandort als neuen Recovery-Standort zum Schutz des neuen Produktionsstandorts verwenden und damit die Richtung des Schutzes umkehren. Repschutz ist nur bei nicht-katastrophalen Ausfällen verfügbar. Daher müssen die ursprünglichen vCenter Server, ESXi Server, SRM Server und entsprechenden Datenbanken irgendwann wiederhergestellt werden können. Falls diese nicht verfügbar sind, müssen eine neue Schutzgruppe und ein neuer Recovery-Plan erstellt werden.

Failback

Ein Failback-Vorgang ist im Grunde ein Failover in eine andere Richtung als zuvor. Als Best Practice überprüfen Sie, ob der ursprüngliche Standort wieder zu akzeptablen Funktionsstufen zurückkehrt, bevor Sie ein Failback durchführen, oder, anders ausgedrückt, ein Failover zum ursprünglichen Standort durchführen. Falls der ursprüngliche Standort weiterhin kompromittiert wird, sollten Sie ein Failback verzögern, bis der Ausfall ausreichend behoben ist.

Eine weitere Failback Best Practice besteht darin, immer einen Test-Failover auszuführen, nachdem der erneute Schutz abgeschlossen und bevor das endgültige Failback durchgeführt wurde. Dadurch wird sichergestellt, dass die vorhandenen Systeme am ursprünglichen Standort den Betrieb abschließen können.

Wiederherstellung der Originalseite

Nach dem Failback sollten Sie mit allen Stakeholdern bestätigen, dass ihre Dienste wieder in den Normalzustand gebracht wurden, bevor Sie erneut den Schutz erneut ausführen,

Wenn eine erneute Sicherung nach dem Failback ausgeführt wird, befindet sich die Umgebung im Wesentlichen in dem Zustand, in dem sie sich zu Beginn befand. Die SnapMirror Replizierung wird erneut vom Produktionsstandort zum Recovery-Standort ausgeführt.

Replizierungstopologien

In ONTAP 9 sind die physischen Komponenten eines Clusters für Cluster-Administratoren sichtbar, sind aber für die Applikationen und Hosts, die das Cluster nutzen, nicht direkt sichtbar. Die physischen Komponenten stellen einen Pool mit gemeinsam genutzten Ressourcen bereit, anhand dessen die logischen Clusterressourcen erstellt werden. Applikationen und Hosts greifen ausschließlich über SVMs auf Daten zu, die Volumes und LIFs enthalten.

Jede NetApp SVM wird in Site Recovery Manager als eindeutiges Array behandelt. VLSR unterstützt bestimmte Array-zu-Array- (oder SVM-zu-SVM-) Replikationslayouts.

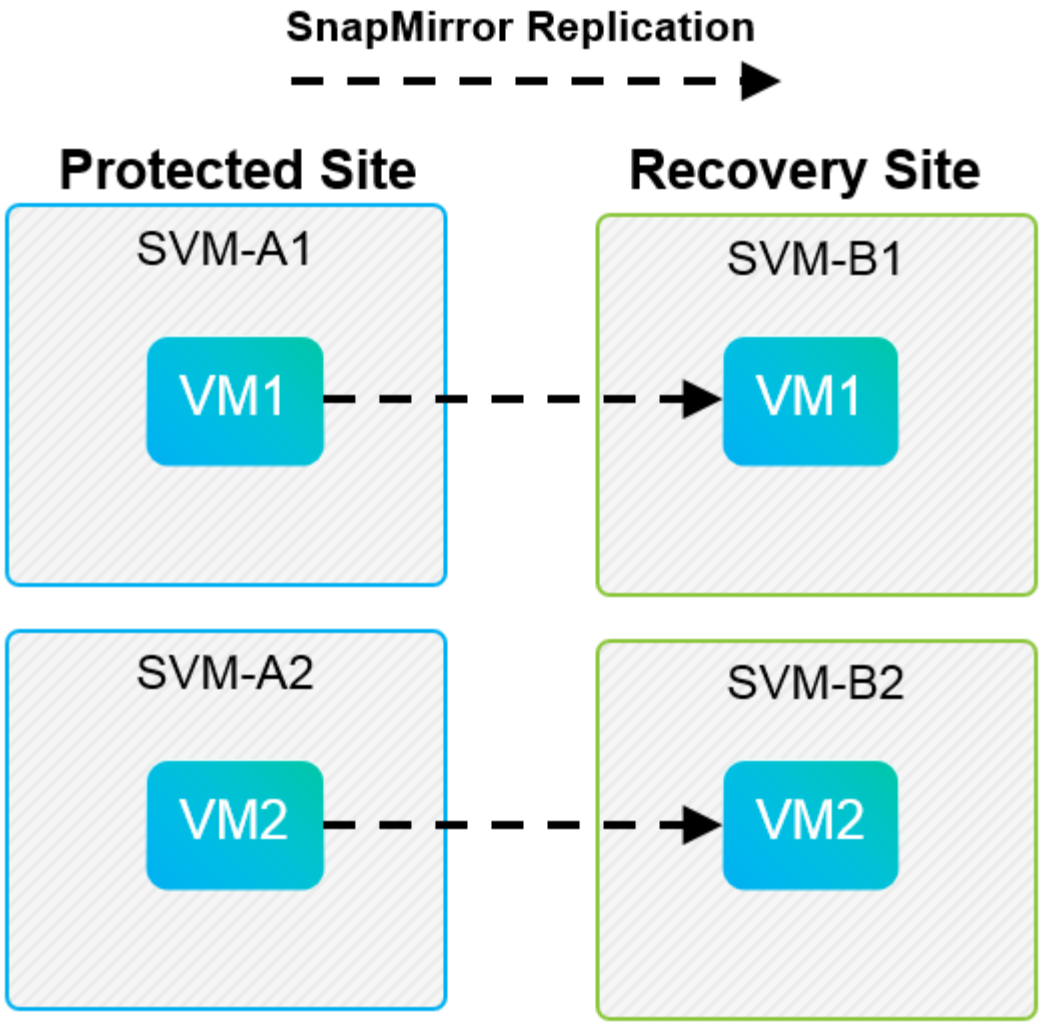
Eine einzelne VM kann aus den folgenden Gründen keine Daten besitzen – Virtual Machine Disk (VMDK) oder RDM – auf mehr als einem VLSR Array:

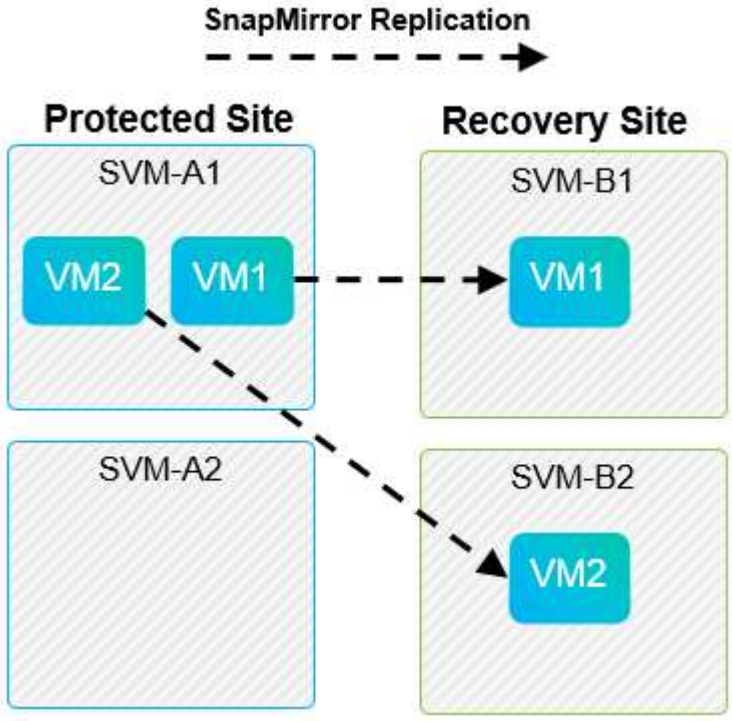
- VLSR sieht nur die SVM, nicht einen individuellen physischen Controller.
- Eine SVM kann LUNs und Volumes steuern, die mehrere Nodes in einem Cluster umfassen.

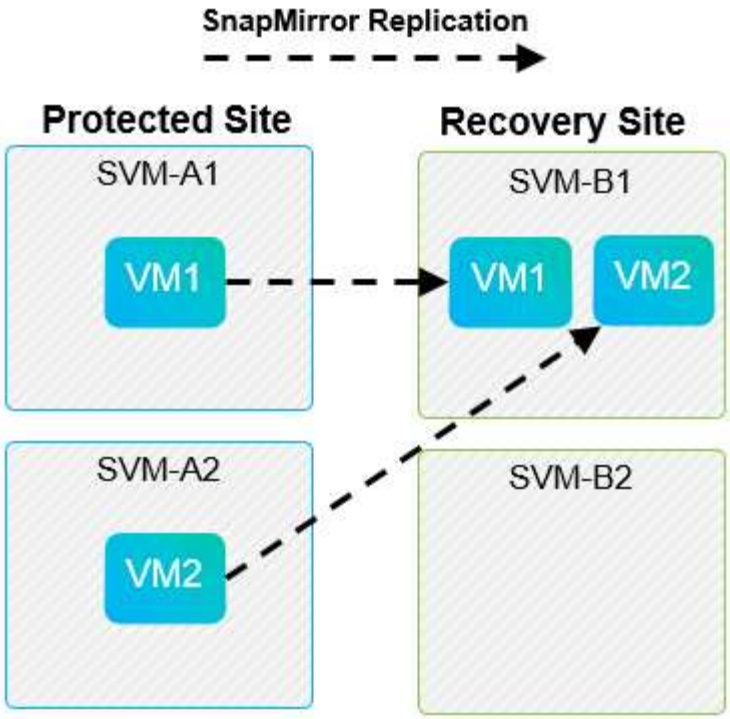
Best Practices In Sich
Bedenken Sie bei der Ermittlung von Supportmöglichkeiten diese Regel: Um eine VM mithilfe von VLSR und der NetApp SRA zu schützen, müssen alle Bestandteile der VM nur auf einer SVM vorhanden sein. Diese Regel gilt sowohl für den geschützten Standort als auch für den Recovery-Standort.

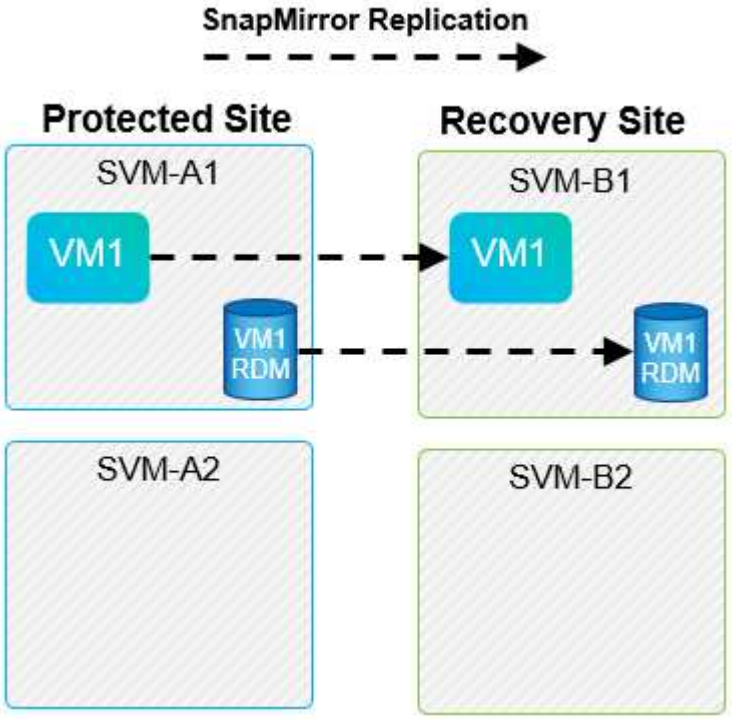
Unterstützte SnapMirror Layouts

Die folgenden Abbildungen zeigen die Szenarien des SnapMirror Beziehungs-Layouts, die von VLSR und SRA unterstützt werden. Jede VM in den replizierten Volumes besitzt die Daten auf nur einem VLSR Array (SVM) an jedem Standort.


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM1
SVM-B1
VM1
SVM-A2
VM2
SVM-B2
VM2


SnapMirror Replication
Protected Site
Recovery Site
SVM-A1
VM2
VM1
SVM-B1
VM1
SVM-A2
SVM-B2
VM2





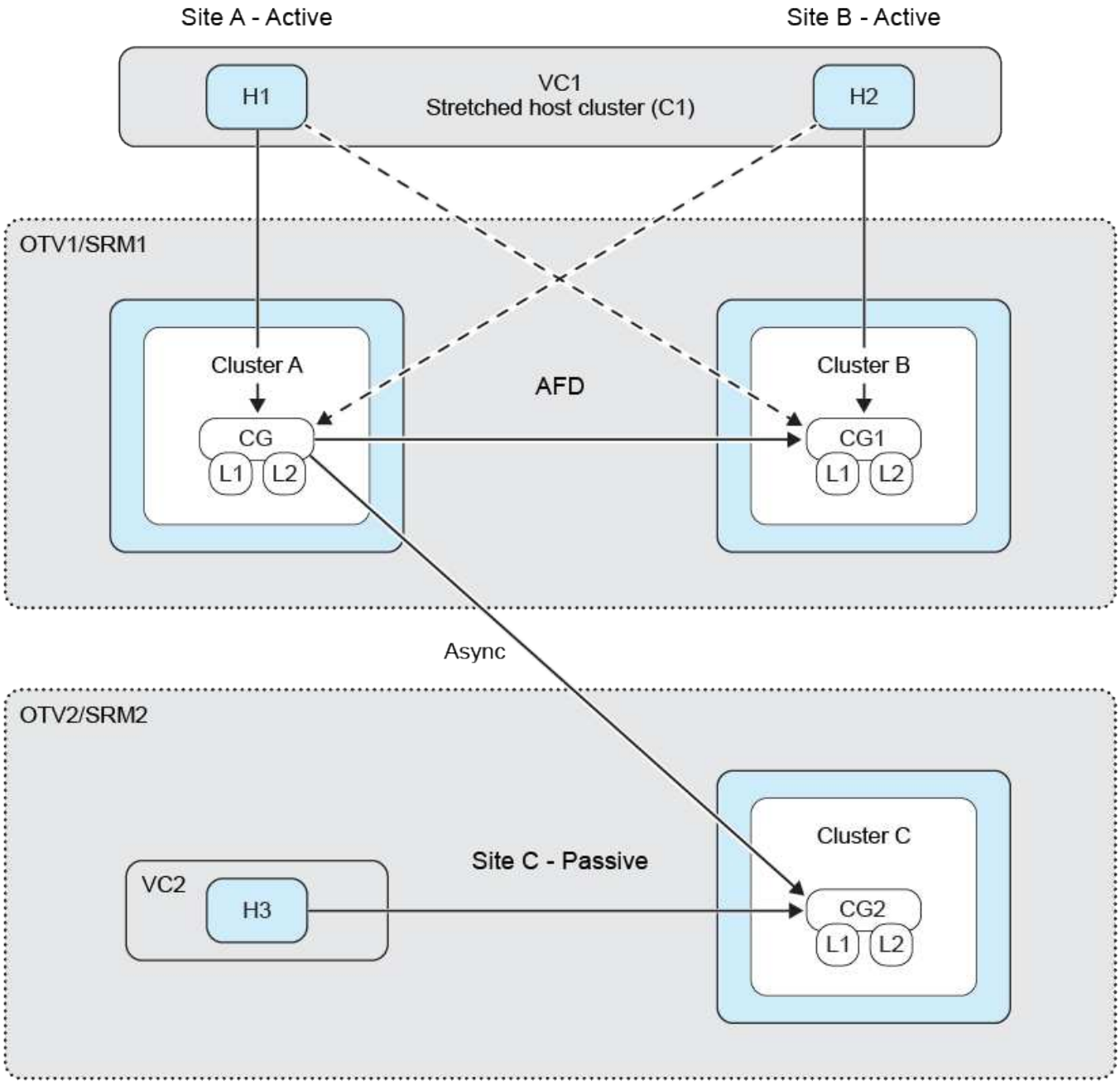
VMFS-Unterstützung mit SnapMirror Active Sync

ONTAP Tools 10.3 und höher unterstützen auch den Schutz Ihrer VMFS-Datenspeicher mit SnapMirror Active Sync (SMas). Dies ermöglicht ein transparentes Failover zur Gewährleistung der Geschäftskontinuität zwischen zwei Rechenzentren (als Fehlerdomänen bezeichnet), die relativ nahe beieinander liegen. Die Notfallwiederherstellung über große Entfernungen kann dann mithilfe von SnapMirror asynchron über die ONTAP -Tools SRA mit VLSR orchestriert werden.

"Erfahren Sie mehr über ONTAP SnapMirror Active Sync"

Datenspeicher werden in einer Konsistenzgruppe (CG) zusammengefasst und die VMs aller Datenspeicher bleiben als Mitglieder derselben CG hinsichtlich der Schreibreihenfolge konsistent.

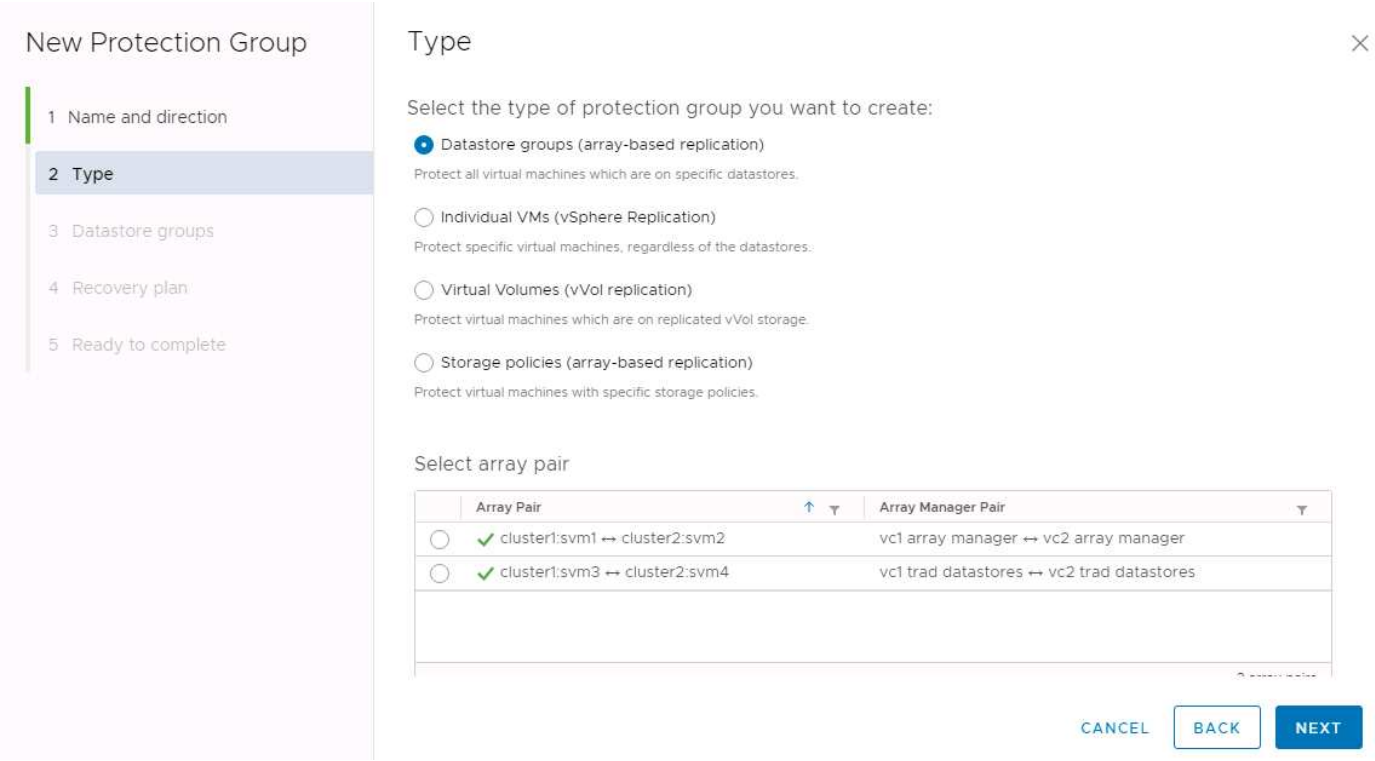
Einige Beispiele könnten sein, dass Standorte in Berlin und Hamburg durch SMas geschützt sind und dass eine dritte Standortreplik SnapMirror asynchron verwendet und durch VLSR geschützt ist. Ein weiteres Beispiel wäre der Schutz von Standorten in New York und New Jersey durch SMas sowie eines dritten Standorts in Chicago.



Unterstützte Array Manager-Layouts

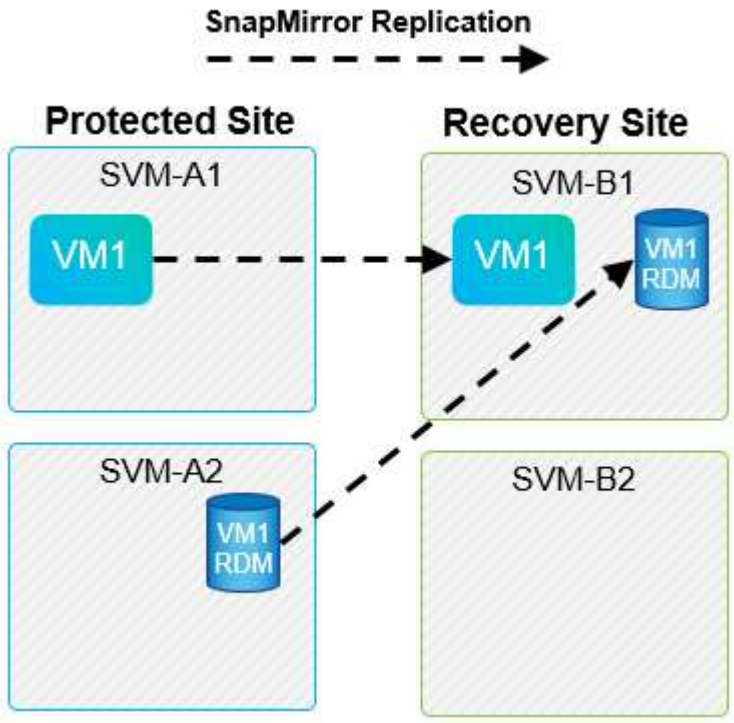
Wenn Sie in VLSR Array-basierte Replizierung (ABR) verwenden, werden Schutzgruppen auf ein einzelnes Array-Paar isoliert, wie im folgenden Screenshot dargestellt. In diesem Szenario `SVM1` und `SVM2` werden mit und `SVM4` am Recovery-Standort gesteuert `SVM3`. Sie können jedoch nur eines der beiden Array-Paare

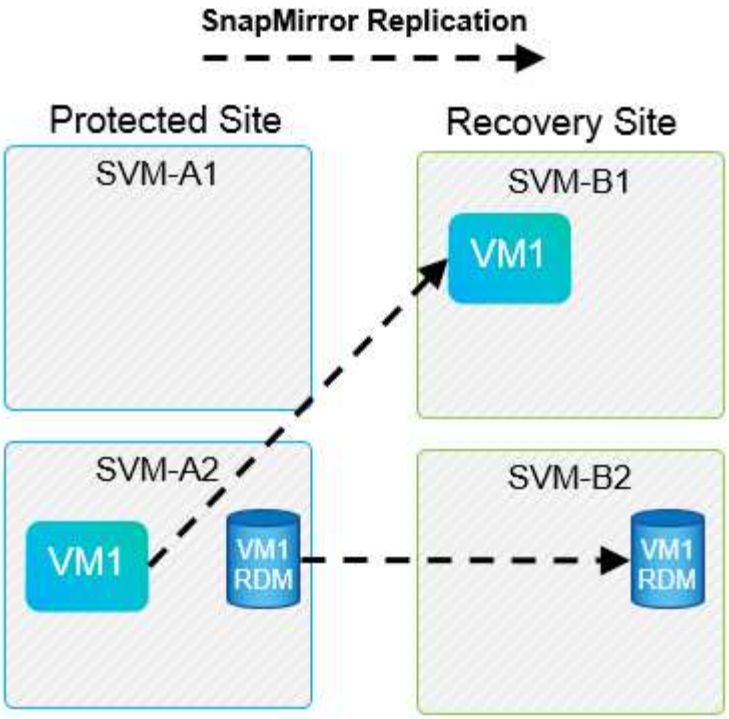
auswählen, wenn Sie eine Schutzgruppe erstellen.



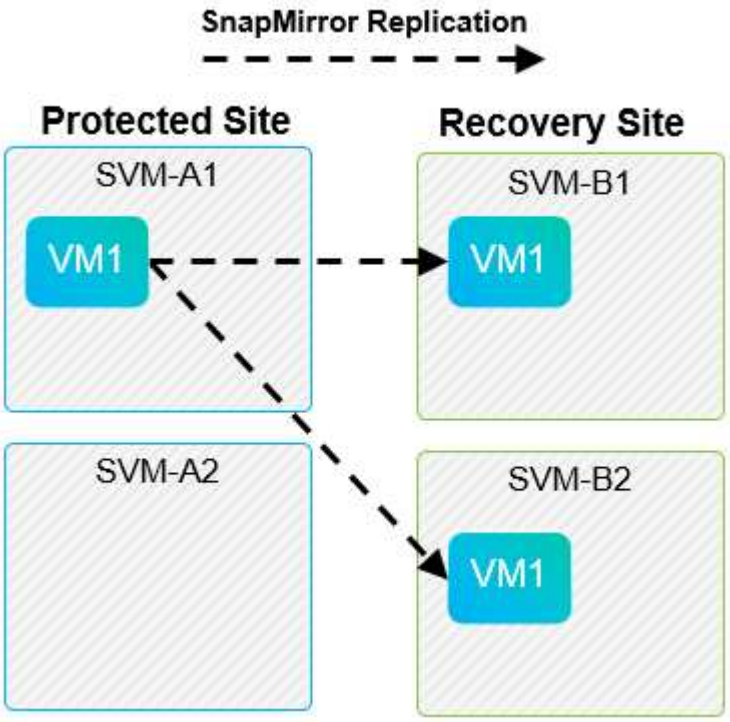
Nicht unterstützte Layouts

Nicht unterstützte Konfigurationen beinhalten Daten (VMDK oder RDM) auf mehreren SVMs, die sich im Besitz einer individuellen VM befinden. In den Beispielen in den folgenden Abbildungen `VM1` kann nicht für den Schutz mit VLSR konfiguriert werden, da `VM1` Daten auf zwei SVMs vorhanden sind.





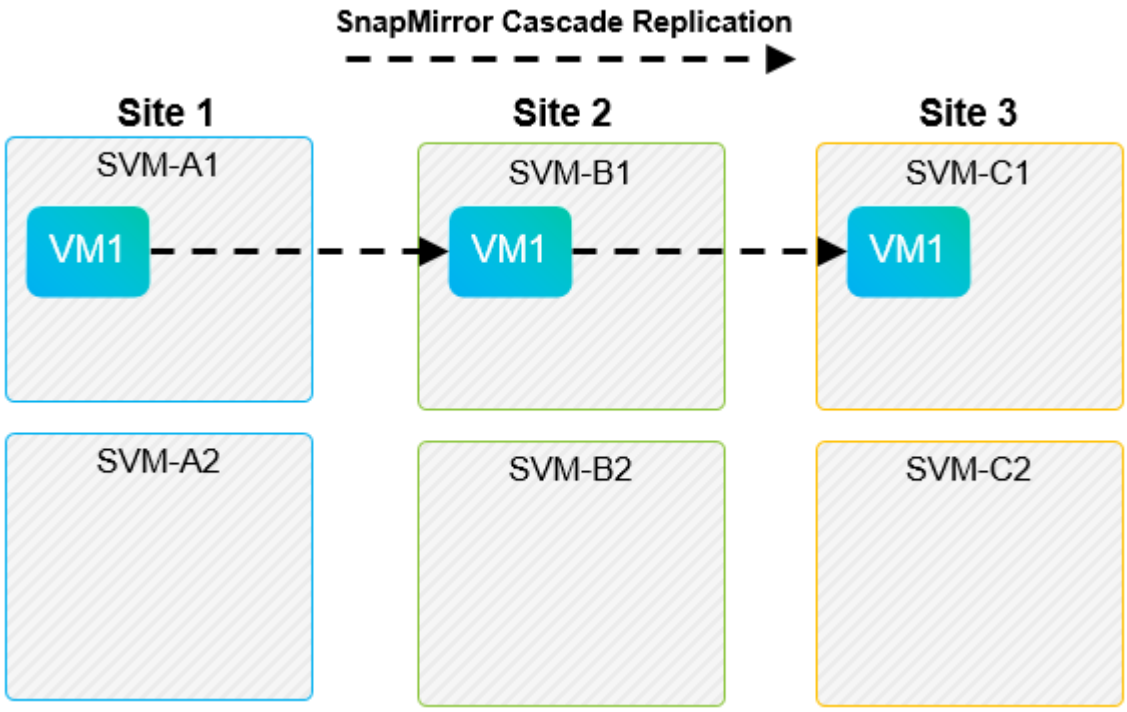
Jegliche Replizierungsbeziehungen, bei denen ein einzelnes NetApp Volume von einer Quell-SVM auf mehrere Ziele in derselben SVM oder in verschiedenen SVMs repliziert wird, werden als SnapMirror Fan-out bezeichnet. Fan-out wird mit VLSR nicht unterstützt. In dem in der folgenden Abbildung gezeigten Beispiel `VM1` kann nicht für den Schutz in VLSR konfiguriert werden, da es mit SnapMirror an zwei verschiedenen Standorten repliziert wird.



SnapMirror Kaskadierung

VLSR unterstützt keine Kaskadierung von SnapMirror Beziehungen, bei denen ein Quell-Volume auf einem Ziel-Volume repliziert wird und das Ziel-Volume ebenfalls mit SnapMirror auf einem anderen Ziel-Volume

repliziert wird. In dem in der folgenden Abbildung gezeigten Szenario kann VLSR nicht für das Failover zwischen mehreren Standorten verwendet werden.



SnapMirror und SnapVault

Die NetApp SnapVault Software ermöglicht festplattenbasierte Backups von Unternehmensdaten zwischen NetApp Storage-Systemen. SnapVault und SnapMirror können in derselben Umgebung nebeneinander bestehen. VLSR unterstützt jedoch nur das Failover der SnapMirror Beziehungen.

Die NetApp SRA unterstützt das `mirror-vault` Richtlinientyp.

SnapVault wurde für ONTAP 8.2 von Grund auf neu aufgebaut. Obwohl frühere Benutzer von Data ONTAP 7-Mode Ähnlichkeiten finden sollten, wurden in dieser Version von SnapVault wesentliche Verbesserungen vorgenommen. Eine wichtige Verbesserung ist die Möglichkeit zur Wahrung der Storage-Effizienz von Primärdaten während der SnapVault Transfers.

Eine wichtige Architekturänderung ist, dass SnapVault in ONTAP 9 wie bei 7-Mode SnapVault auf Volume-Ebene repliziert, nicht auf qtree-Ebene. Bei diesem Setup muss die Quelle einer SnapVault Beziehung ein Volume sein, und das Volume muss auf sein eigenes Volume auf dem sekundären SnapVault System repliziert werden.

In einer Umgebung, in der SnapVault verwendet wird, werden auf dem primären Storage-System speziell benannte Snapshots erstellt. Je nach implementierter Konfiguration können die benannten Snapshots auf dem Primärsystem nach einem SnapVault-Zeitplan oder durch eine Anwendung wie NetApp Active IQ Unified Manager erstellt werden. Die benannten Snapshots, die auf dem Primärsystem erstellt werden, werden dann auf das SnapMirror Ziel repliziert und von dort auf das SnapVault Ziel archiviert.

Ein Quell-Volume kann in einer Kaskadenkonfiguration erstellt werden, bei der ein Volume auf ein SnapMirror Ziel am DR-Standort repliziert wird und von dort aus auf ein SnapVault Ziel verlagert wird. Ein Quell-Volume kann auch in einer Fan-out-Beziehung erstellt werden, wobei ein Ziel ein SnapMirror Ziel ist und das andere Ziel eine SnapVault Ziel ist. SRA rekonfiguriert jedoch nicht automatisch die SnapVault-Beziehung neu, um das SnapMirror Ziel-Volume als Quelle für den Vault zu verwenden, wenn das VLSR Failover oder eine Umkehrung

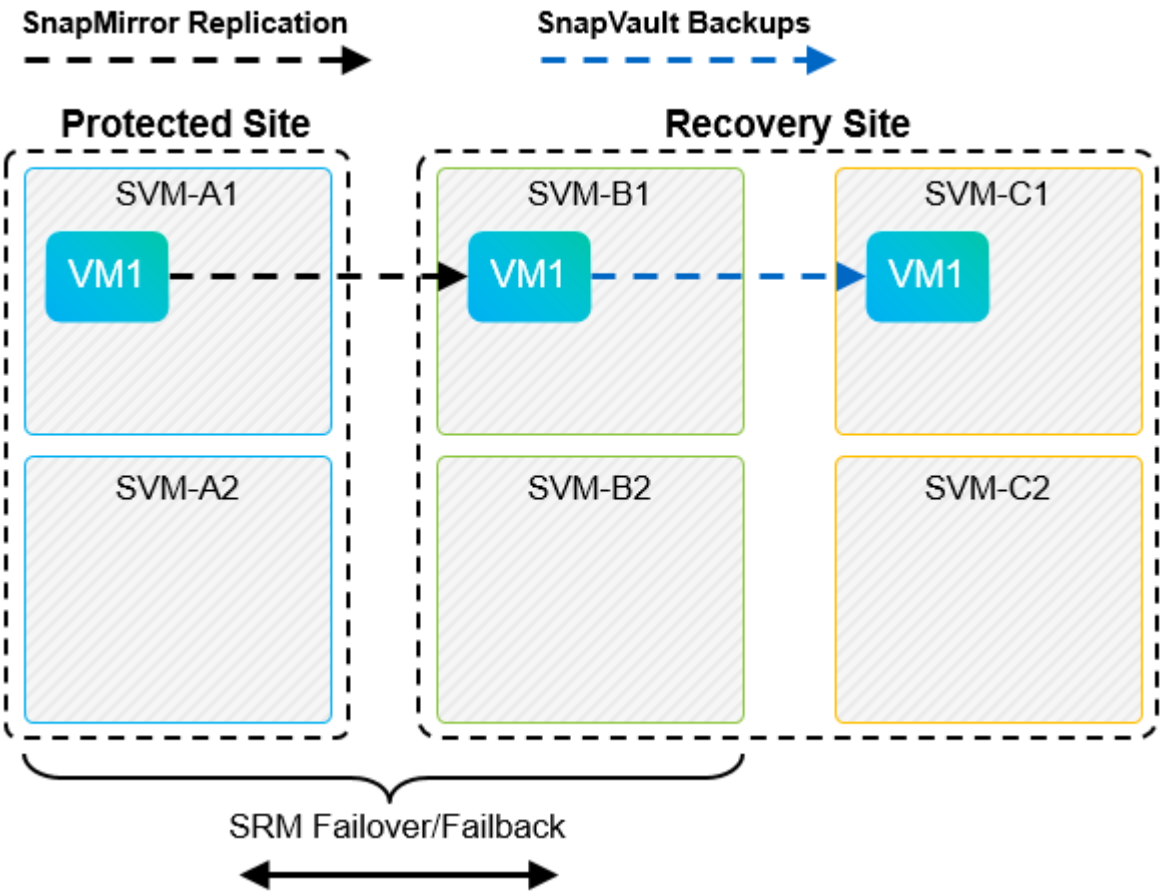
der Replizierung stattfindet.

Die neuesten Informationen zu SnapMirror und SnapVault für ONTAP 9 finden Sie hier: "TR-4015 SnapMirror Configuration Best Practice Guide für ONTAP 9."

Best Practices In Sich
Wenn in derselben Umgebung SnapVault und VLSR eingesetzt werden, empfiehlt NetApp, eine Kaskadenkonfiguration von SnapMirror auf SnapVault zu verwenden, bei der SnapVault Backups normalerweise über das SnapMirror Ziel am DR-Standort ausgeführt werden. Bei einem Notfall kann der primäre Standort durch diese Konfiguration nicht mehr zugänglich sein. Indem das SnapVault Ziel am Recovery-Standort gehalten wird, können SnapVault Backups nach dem Failover neu konfiguriert werden, sodass SnapVault Backups weiterhin am Recovery-Standort ausgeführt werden können.

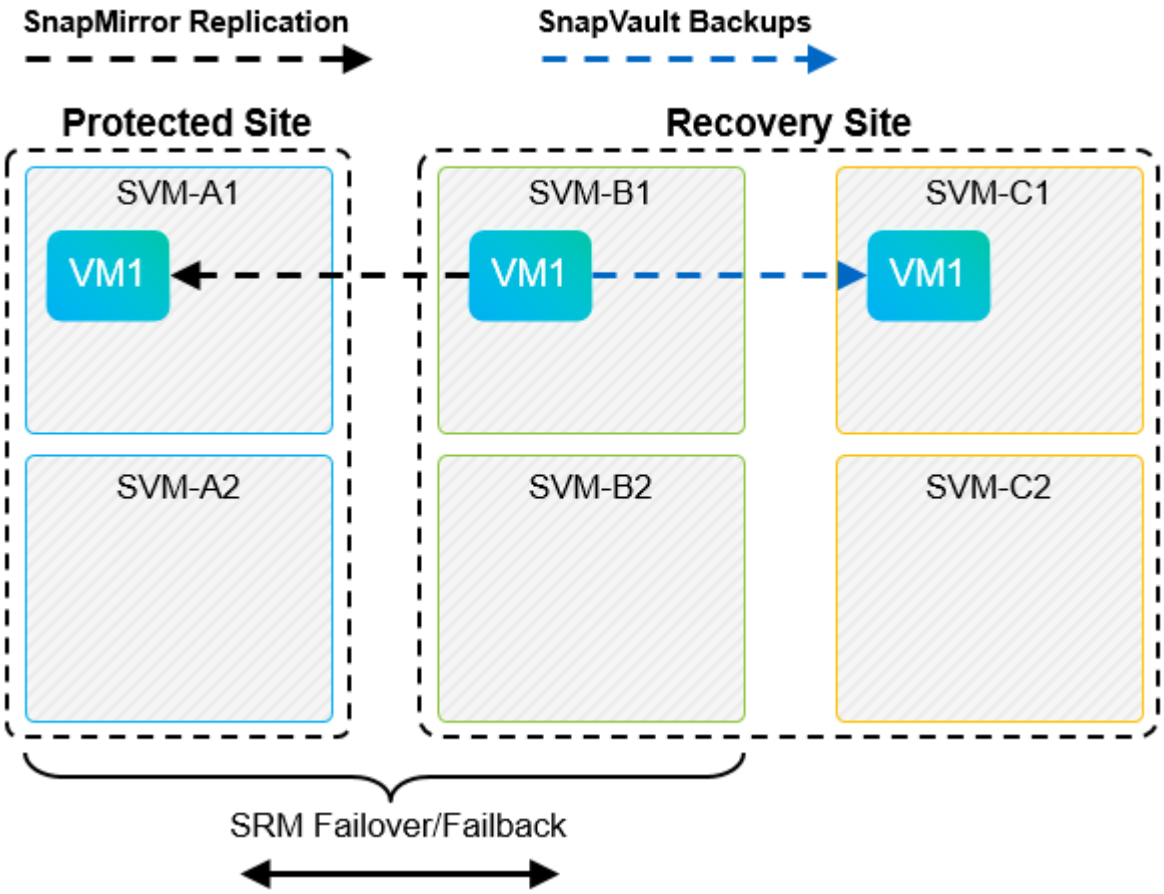
In einer VMware Umgebung verfügt jeder Datenspeicher über eine universelle eindeutige Kennung (Universal Unique Identifier, UUID) und jede VM über eine eindeutige Managed Object ID (MOID). Diese IDs werden während Failover oder Failback durch VLSR nicht gepflegt. Da Datastore-UIDs und VM-MOIDs beim Failover durch VLSR nicht gepflegt werden, müssen nach dem VLSR Failover alle Applikationen, die von diesen IDs abhängen, neu konfiguriert werden. Eine Beispielapplikation ist NetApp Active IQ Unified Manager, wo die SnapVault Replizierung mit der vSphere Umgebung koordiniert wird.

Die folgende Abbildung zeigt die Kaskadenkonfiguration von SnapMirror auf SnapVault. Wenn sich das SnapVault Ziel am DR-Standort oder an einem tertiären Standort befindet, der nicht von einem Ausfall am primären Standort betroffen ist, kann die Umgebung neu konfiguriert werden, sodass Backups nach dem Failover fortgesetzt werden können.



In der folgenden Abbildung wird die Konfiguration dargestellt, nachdem VLSR die SnapMirror Replizierung zurück auf den primären Standort umgekehrt hat. Die Umgebung wurde außerdem neu konfiguriert, sodass

SnapVault Backups von der jetzt SnapMirror Quelle durchgeführt werden. Bei dieser Einrichtung handelt es sich um eine Fan-out-Konfiguration für SnapMirror SnapVault.



Nachdem vsrm ein Failback und eine zweite Umkehr der SnapMirror Beziehungen durchführt, sind die Produktionsdaten am primären Standort zurück. Die Daten werden jetzt auf dieselbe Weise gesichert wie vor dem Failover zum DR-Standort – über SnapMirror und SnapVault Backups.

Verwendung von Qtrees in Site Recovery Manager-Umgebungen

Qtrees sind spezielle Verzeichnisse, die die Anwendung von Filesystem-Kontingenten für NAS ermöglichen. ONTAP 9 ermöglicht die Erstellung von qtrees und qtrees in Volumes, die mit SnapMirror repliziert werden. SnapMirror ermöglicht jedoch nicht die Replizierung einzelner qtrees oder Qtree-Level-Replikationen. Alle SnapMirror Replikation befindet sich nur auf Volume-Ebene. Aus diesem Grund empfiehlt NetApp die Verwendung von qtrees mit VLSR nicht.

Gemischte FC- und iSCSI-Umgebungen

Mit den unterstützten SAN-Protokollen (FC, FCoE und iSCSI) bietet ONTAP 9 LUN-Services an, d. h. die Möglichkeit, LUNs zu erstellen und angebundenen Hosts zuzuweisen. Da das Cluster aus mehreren Controllern besteht, gibt es mehrere logische Pfade, die von Multipath I/O zu einer beliebigen einzelnen LUN gemanagt werden. Auf den Hosts wird mithilfe des Asymmetric Logical Unit Access (ALUA) der optimale Pfad zu einer LUN ausgewählt und für den Datentransfer aktiviert. Wenn sich der optimierte Pfad zu einer LUN ändert (z. B. weil das zugehörige Volume verschoben wird), erkennt ONTAP 9 diese Änderung automatisch und passt sich unterbrechungsfrei an. Wenn der optimierte Pfad nicht mehr verfügbar ist, kann ONTAP ohne Unterbrechungen zu einem anderen verfügbaren Pfad wechseln.

VMware VLSR und NetApp SRA unterstützen die Nutzung des FC-Protokolls an einem Standort und das

iSCSI-Protokoll am anderen Standort. Eine Kombination aus FC-Attached Datastores und iSCSI-Attached Datastores wird jedoch auf demselben ESXi Host oder auf verschiedenen Hosts im selben Cluster nicht unterstützt. Diese Konfiguration wird mit VLSR nicht unterstützt, da VLSR während des VLSR Failover oder des Test-Failovers alle FC- und iSCSI-Initiatoren in den ESXi-Hosts in der Anforderung enthält.

Best Practices In Sich
VLSR und SRA unterstützen gemischte FC- und iSCSI-Protokolle zwischen den geschützten und den Recovery-Standorten. Allerdings sollte jeder Standort nur mit einem Protokoll, entweder FC oder iSCSI, konfiguriert werden, nicht mit beiden Protokollen am selben Standort. Wenn FC- und iSCSI-Protokolle am selben Standort konfiguriert werden müssen, empfiehlt NetApp, dass einige Hosts iSCSI verwenden und andere Hosts FC verwenden. NetApp empfiehlt in diesem Fall außerdem die VLSR-Ressourcenzuordnung, damit die VMs für das Failover in eine Gruppe von Hosts oder die andere konfiguriert werden.

Fehlerbehebung bei VLSRM/SRM bei Verwendung der VVols-Replikation

Bei Verwendung der ONTAP Tools 9.13P2 unterscheidet sich der Workflow innerhalb von VLSR und SRM bei der VVols-Replizierung erheblich von dem, was mit SRA und herkömmlichen Datastores verwendet wird. Zum Beispiel gibt es kein Konzept für Array-Manager. So `discoverarrays` und `discoverdevices` Befehle werden nie gesehen.

Bei der Fehlerbehebung sind die neuen Workflows zu verstehen, die im Folgenden aufgeführt sind:

1. QueryReplicationPeer: Ermittelt die Replikationsvereinbarungen zwischen zwei Fehlerdomänen.
2. QueryFaultDomain: Ermittelt die Fehlerdomäne-Hierarchie.
3. QueryReplicationGroup: Ermittelt die in den Quell- oder Zieldomänen vorhandenen Replikationsgruppen.
4. SyncReplicationGroup: Synchronisiert die Daten zwischen Quelle und Ziel.
5. QueryPointInTimeReplica: Ermittelt die Point-in-Time-Replikate auf einem Ziel.
6. TestFailoverReplicationGroupStart: Startet Test Failover.
7. TestFailoverReplicationGroupStop: Beendet das Test-Failover.
8. PromoteReplicationGroup: Fördert eine Gruppe, die sich derzeit in der Produktion befindet.
9. PreparreFailoverReplicationGroup: Bereitet sich auf eine Notfallwiederherstellung vor.
10. Failover ReplicationGroup: Durchführung einer Disaster Recovery
11. ReverseReplicateGroup: Initiiert Reverse-Replikation.
12. QueryMatchingContainer: Sucht Container (zusammen mit Hosts oder Replikationsgruppen), die eine Bereitstellungsanfrage mit einer bestimmten Richtlinie erfüllen können.
13. QueryResourceMetadaten: Ermittelt die Metadaten aller Ressourcen des VASA Providers, kann die Ressourcenauslastung als Antwort auf die queryMatchingContainer-Funktion zurückgegeben werden.

Der häufigste Fehler bei der Konfiguration der VVols-Replizierung ist das Erkennen der SnapMirror Beziehungen. Dies geschieht, weil die Volumes und SnapMirror Beziehungen außerhalb der ONTAP Tools-Ansicht erstellt werden. Daher empfiehlt es sich, immer sicherzustellen, dass die SnapMirror Beziehung vollständig initialisiert ist und dass Sie an beiden Standorten eine erneute Bestandsaufnahme in ONTAP Tools ausführen, bevor Sie versuchen, einen replizierten VVols Datastore zu erstellen.

Weitere Informationen

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

- ONTAP-Tools für VMware vSphere 10.x-Ressourcen
  "https://mysupport.netapp.com/site/products/all/details/otv10/docs-tab"
- ONTAP-Tools für VMware vSphere 9.x-Ressourcen
  "https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"
- TR-4597: VMware vSphere für ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"
- TR-4400: VMware vSphere Virtual Volumes with ONTAP
  "https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html"
- TR-4015 SnapMirror -Konfigurationsleitfaden – Best Practices für ONTAP 9
  https://www.netapp.com/pdf.html?item=/media/17229-tr-4015-snapmirror-configuration-ontap.pdf
- VMware Live Site Recovery-Dokumentation "https://techdocs.broadcom.com/us/en/vmware-cis/live-recovery/live-site-recovery/9-0.html"

"Interoperabilitäts-Matrix-Tool (IMT)"Überprüfen Sie auf der NetApp-Support-Website, ob die in diesem Dokument angegebenen Produktversionen und Funktionen in Ihrer IT-Umgebung unterstützt werden. Das NetApp IMT definiert die Produktkomponenten und -Versionen, die für von NetApp unterstützte Konfigurationen verwendet werden können. Die dort angezeigten Ergebnisse basieren auf der spezifischen Infrastruktur des jeweiligen Kunden bzw. auf den technischen Daten der in dieser Infrastruktur enthaltenen Komponenten.

VSphere Metro Storage-Cluster mit ONTAP

VSphere Metro Storage-Cluster mit ONTAP

Der branchenführende vSphere-Hypervisor von VMware kann als erweiterbares Cluster, auch als vSphere Metro Storage-Cluster (vMSC) bezeichnet, implementiert werden.

VMSC Lösungen werden sowohl mit NetApp® MetroCluster™ als auch mit SnapMirror Active Sync (früher als SnapMirror Business Continuity oder SMBC bekannt) unterstützt und bieten erweiterte Business Continuity, wenn eine oder mehrere Ausfall-Domains ausfallen. Die Widerstandsfähigkeit gegenüber verschiedenen Fehlermodi hängt davon ab, welche Konfigurationsoptionen Sie wählen.

Diese Dokumentation ersetzt bereits veröffentlichte technische Berichte *TR-4128: VSphere on NetApp MetroCluster*

Lösungen für kontinuierliche Verfügbarkeit für vSphere Umgebungen

Die ONTAP Architektur ist eine flexible und skalierbare Speicherplattform, die SAN- (FCP, iSCSI und NVMe-oF) und NAS-Dienste (NFS v3 und v4.1) für Datenspeicher bereitstellt. Die NetApp AFF, ASA und FAS -Speichersysteme verwenden das ONTAP -Betriebssystem, um zusätzliche Protokolle für den Speicherzugriff von Gästen anzubieten, beispielsweise S3 und SMB/CIFS.

NetApp MetroCluster nutzt die NetApp HA-Funktion (Controller Failover oder CFO) zum Schutz vor Controller-Ausfällen. Außerdem beinhaltet es lokale SyncMirror Technologie, Cluster Failover bei Disaster (Cluster Failover bei Disaster Recovery oder CFOD), Hardwareredundanz und geografische Trennung, um ein hohes

Maß an Verfügbarkeit zu erzielen. SyncMirror spiegelt Daten synchron auf die beiden Hälften der MetroCluster Konfiguration und schreibt sie in zwei Plexe: Der lokale Plex (auf dem lokalen Shelf), der aktiv Daten bereitstellt, und der Remote-Plex (auf dem Remote-Shelf), der normalerweise keine Daten bereitstellt. Für alle MetroCluster Komponenten wie Controller, Storage, Kabel, Switches (zur Verwendung mit Fabric MetroCluster) und Adapter besteht Hardwareredundanz.

NetApp SnapMirror Active Sync ist auf Systemen anderer Anbieter als MetroCluster und ASA r2 Systemen verfügbar und bietet granulare Datastore-Sicherung mit FCP- und iSCSI-SAN-Protokollen. Mit dieser Technologie können Sie entweder das gesamte vMSC schützen oder Workloads mit hoher Priorität selektiv schützen. Es bietet aktiv/aktiv-Zugriff auf lokale und Remote-Standorte, im Gegensatz zu NetApp MetroCluster, die eine aktiv/Standby-Lösung ist. Ab ONTAP 9.15.1 unterstützt SnapMirror Active Sync eine symmetrische aktiv/aktiv-Funktion, sodass I/O-Vorgänge für Lese- und Schreibvorgänge von beiden Kopien einer geschützten LUN mit bidirektionaler synchroner Replizierung möglich sind. Dadurch können beide LUN-Kopien lokal für I/O-Vorgänge genutzt werden. Vor ONTAP 9.15.1 unterstützt SnapMirror Active Sync nur asymmetrische aktiv/aktiv-Konfigurationen, bei denen die Daten am sekundären Standort per Proxy auf die primäre Kopie einer LUN übertragen werden.

Um einen VMware HA/DRS Cluster über zwei Standorte zu erstellen, werden ESXi-Hosts von einer vCenter Server Appliance (VCSA) verwendet und gemanagt. Die vSphere-Management-, vMotion®- und Virtual Machine-Netzwerke sind über ein redundantes Netzwerk zwischen den beiden Standorten verbunden. Der vCenter Server, der den HA/DRS Cluster verwaltet, kann eine Verbindung zu den ESXi-Hosts an beiden Standorten herstellen und sollte über vCenter HA konfiguriert werden.

Siehe "Wie erstellen und konfigurieren Sie Cluster im vSphere Client" Um vCenter HA zu konfigurieren.

Sie sollten sich auch auf "Empfohlene Practices für VMware vSphere Metro Storage-Cluster".

Was ist vSphere Metro Storage-Cluster?

vSphere Metro Storage Cluster (vMSC) ist eine zertifizierte Konfiguration, die virtuelle Maschinen (VMs) und Container vor Ausfällen schützt. Dies wird durch die Verwendung von Stretched-Storage-Konzepten zusammen mit Clustern von ESXi-Hosts erreicht, die über verschiedene Fehlerdomänen wie Racks, Gebäude, Campusse oder sogar Städte verteilt sind. Die Active-Sync-Speichertechnologien NetApp MetroCluster und SnapMirror werden verwendet, um den Host-Clustern einen Schutz mit Null-Recovery-Point-Objective (RPO=0) zu bieten. Die vMSC-Konfiguration soll sicherstellen, dass die Daten auch dann immer verfügbar sind, wenn ein kompletter physischer oder logischer „Standort“ ausfällt. Ein Speichergerät, das Teil der vMSC-Konfiguration ist, muss nach erfolgreichem Durchlaufen eines vMSC-Zertifizierungsprozesses zertifiziert werden. Alle unterstützten Speichergeräte finden Sie im "VMware Storage Compatibility Guide".

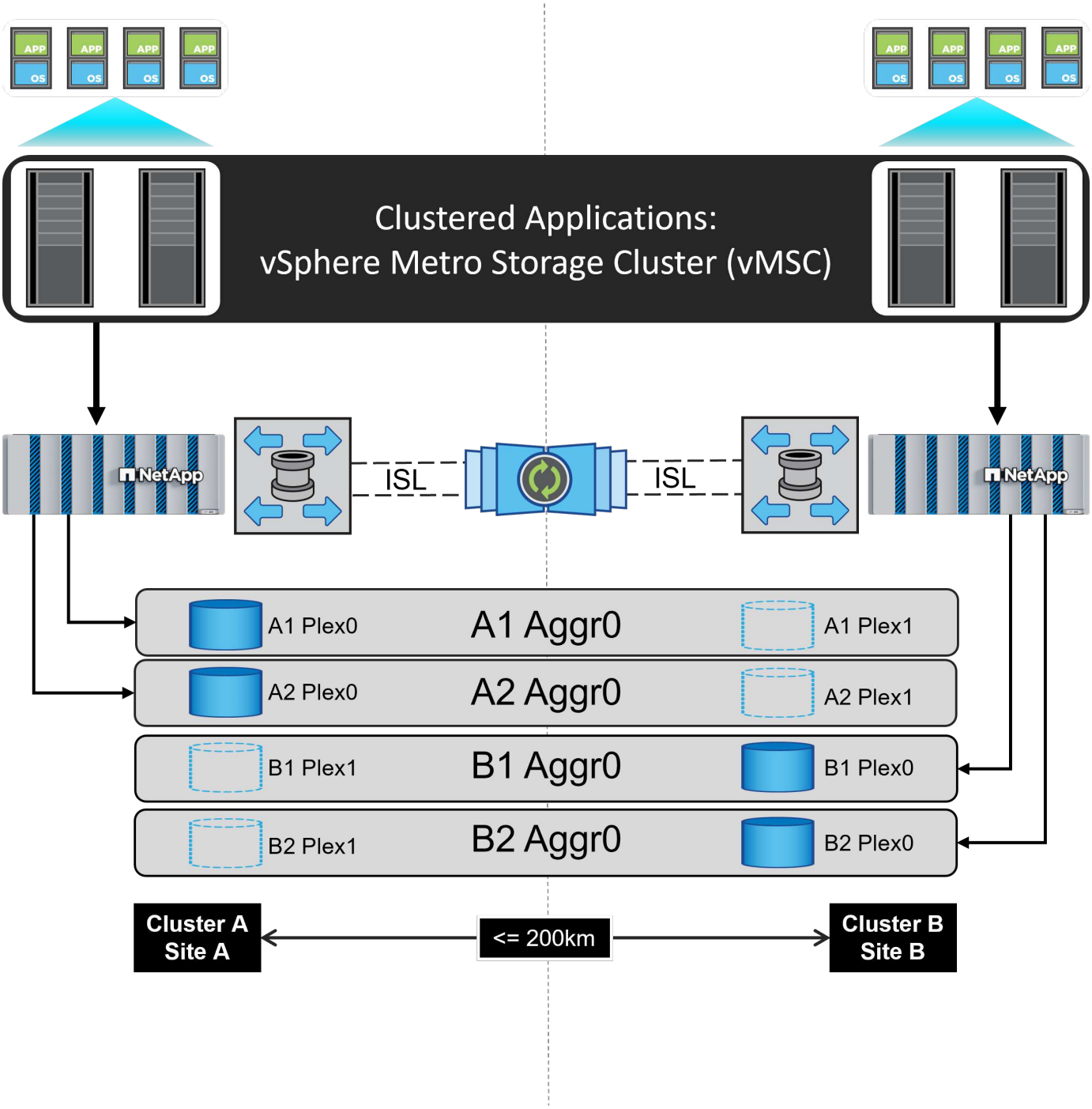
Weitere Informationen zu den Designrichtlinien für vSphere Metro Storage Cluster finden Sie in der folgenden Dokumentation:

- "Unterstützung von VMware vSphere für NetApp MetroCluster"
- "Unterstützung von VMware vSphere mit NetApp SnapMirror Business Continuity" (Jetzt bekannt als SnapMirror Active Sync)

NetApp MetroCluster kann für vSphere in zwei unterschiedlichen Konfigurationen implementiert werden:

- Stretch-MetroCluster
- Fabric MetroCluster

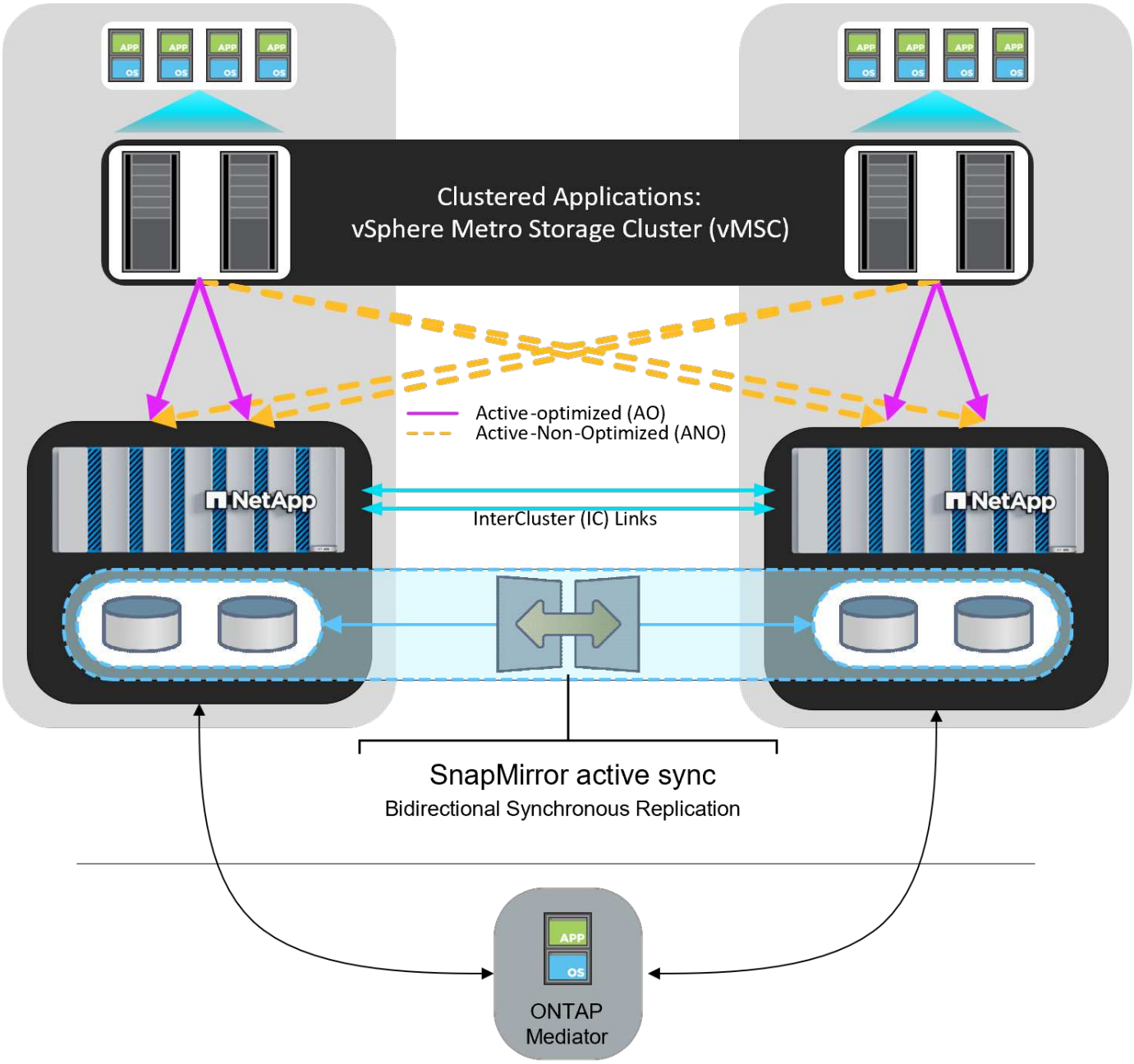
Im Folgenden finden Sie ein High-Level-Topologiediagramm von Stretch MetroCluster.



Siehe "MetroCluster-Dokumentation" Finden Sie spezifische Design- und Implementierungsinformationen für MetroCluster.

SnapMirror Active Sync kann darüber hinaus auf zwei verschiedene Arten implementiert werden.

- Asymmetrisch
- Symmetrische aktive Synchronisierung (ONTAP 9.15.1)



Spezifische Design- und Bereitstellungsinformationen für SnapMirror Active Sync finden Sie unter "NetApp Dokumente".

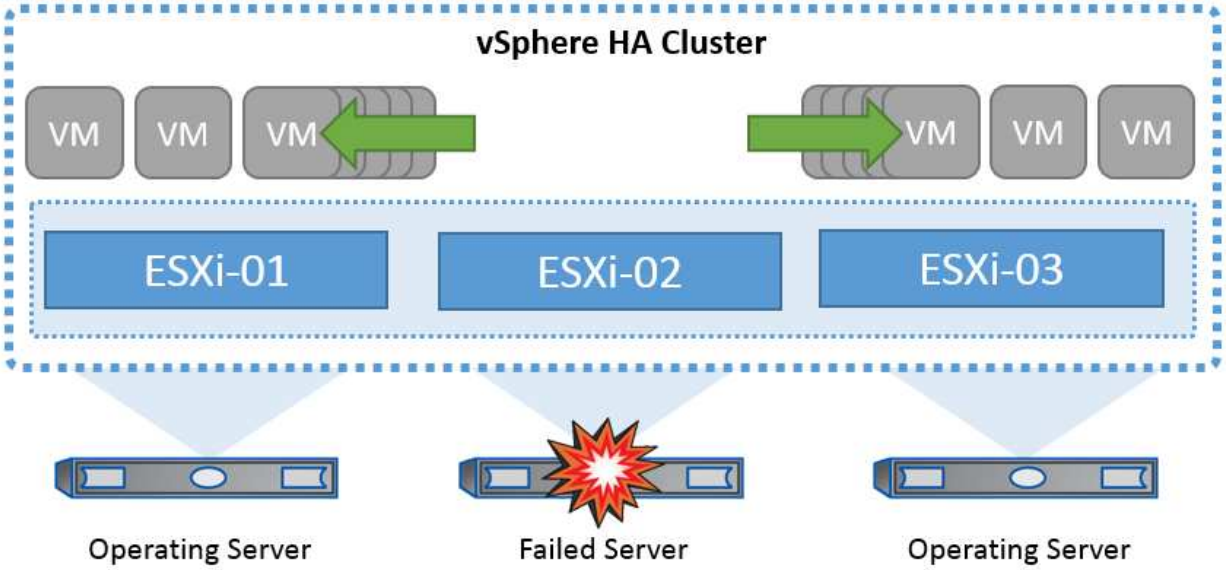
VMware vSphere Lösungsübersicht

Die vCenter Server Appliance (VCSA) ist ein leistungsstarkes, zentralisiertes Managementsystem und eine zentrale Benutzeroberfläche für vSphere, die es Administratoren ermöglicht, ESXi-Cluster effektiv zu betreiben. Es ermöglicht wichtige Funktionen wie die Bereitstellung virtueller Maschinen, vMotion-Operationen, Hochverfügbarkeit (HA), Distributed Resource Scheduler (DRS), VMware vSphere Kubernetes Service (VKS) und mehr. Es handelt sich um eine wesentliche Komponente in VMware-Cloud-Umgebungen, bei deren Entwicklung die Verfügbarkeit der Dienste im Vordergrund stand.

VSphere High Availability

Die Cluster-Technologie von VMware gruppiert ESXi Server zu Pools gemeinsam genutzter Ressourcen für virtuelle Maschinen und bietet vSphere High Availability (HA). VSphere HA bietet benutzerfreundliche Hochverfügbarkeit für Anwendungen, die in virtuellen Maschinen ausgeführt werden. Wenn die HA-Funktion auf dem Cluster aktiviert ist, hält jeder ESXi-Server die Kommunikation mit anderen Hosts aufrecht, sodass ein ESXi-Host nicht mehr reagiert oder isoliert wird. der HA-Cluster kann die Wiederherstellung der Virtual Machines, die auf diesem ESXi-Host ausgeführt wurden, zwischen den noch intakten Hosts im Cluster aushandeln. Im Falle eines Ausfalls eines Gastbetriebssystems kann vSphere HA die betroffene Virtual Machine auf demselben physischen Server neu starten. VSphere HA ermöglicht es, geplante Ausfallzeiten zu reduzieren, ungeplante Ausfallzeiten zu vermeiden und ein schnelles Recovery nach Ausfällen zu ermöglichen.

vSphere HA-Cluster stellt VMs von einem ausgefallenen Server wieder her.



Es ist wichtig zu wissen, dass VMware vSphere weder über NetApp MetroCluster noch über SnapMirror Active Sync verfügt und alle ESXi Hosts im vSphere Cluster als berechtigte Hosts für HA-Clustervorgänge erkennt, je nach Host- und VM-Gruppenaffinitätskonfigurationen.

Erkennung Von Host-Ausfällen

Sobald der HA-Cluster erstellt ist, nehmen alle Hosts im Cluster an der Wahl teil, und einer der Hosts wird zum Master. Jeder Slave sendet einen Netzwerk-Heartbeat an den Master, und der Master sendet seinerseits einen Netzwerk-Heartbeat an alle Slave-Hosts. Der Master-Host eines vSphere HA-Clusters ist für die Erkennung des Ausfalls von Slave-Hosts zuständig.

Je nach Art des erkannten Fehlers müssen die auf den Hosts ausgeführten virtuellen Maschinen möglicherweise ein Failover durchführen.

In einem vSphere HA-Cluster werden drei Arten von Host-Ausfällen erkannt:

- Fehler: Ein Host funktioniert nicht mehr.
- Isolierung: Ein Host wird zu einem isolierten Netzwerk.
- Partition: Ein Host verliert die Netzwerkverbindung mit dem Master-Host.

Der Master-Host überwacht die Slave-Hosts im Cluster. Diese Kommunikation erfolgt durch den Austausch

von Netzwerk-Heartbeats jede Sekunde. Wenn der Master-Host diese Heartbeats nicht mehr von einem Slave-Host empfängt, prüft er die Host-Lebendigkeit, bevor er den Host für fehlgeschlagen erklärt. Die Liveness-Prüfung, die der Master-Host durchführt, besteht darin festzustellen, ob der Slave-Host Heartbeats mit einem der Datastores austauscht. Außerdem prüft der Master-Host, ob der Host auf ICMP-Pings reagiert, die an seine Management-IP-Adressen gesendet werden, um festzustellen, ob er lediglich von seinem Master-Knoten isoliert oder vollständig vom Netzwerk isoliert ist. Dies erfolgt durch Ping an das Standard-Gateway. Eine oder mehrere Isolationsadressen können manuell angegeben werden, um die Zuverlässigkeit der Isolationsvalidierung zu erhöhen.

NetApp empfiehlt, mindestens zwei zusätzliche Isolationsadressen anzugeben, und jede dieser Adressen sollte standortlokal sein. Dies erhöht die Zuverlässigkeit der Isolationsvalidierung.

Antwort Der Hostisolation

Die Isolationsreaktion ist eine Einstellung in vSphere HA, die festlegt, welche Aktion auf virtuellen Maschinen ausgelöst wird, wenn ein Host in einem vSphere HA-Cluster seine Management-Netzwerkverbindungen verliert, aber weiterhin ausgeführt wird. Für diese Einstellung gibt es drei Optionen: „Deaktiviert“, „VMs herunterfahren und neu starten“ und „VMs ausschalten und neu starten“.

„Herunterfahren“ ist besser als „Ausschalten“, da bei letzterem die zuletzt vorgenommenen Änderungen nicht auf die Festplatte geschrieben und Transaktionen nicht gespeichert werden. Wenn virtuelle Maschinen nicht innerhalb von 300 Sekunden heruntergefahren werden, werden sie ausgeschaltet. Um die Wartezeit zu ändern, verwenden Sie die erweiterte Option das.isolationshutdowntimeout.

Bevor HA die Isolationsantwort initiiert, prüft es zunächst, ob der vSphere HA-Master-Agent den Datenspeicher besitzt, der die VM-Konfigurationsdateien enthält. Wenn dies nicht der Fall ist, löst der Host die Isolationsantwort nicht aus, da kein Master zum Neustart der VMs vorhanden ist. Der Host überprüft regelmäßig den Datastore-Status, um festzustellen, ob er von einem vSphere HA-Agent beansprucht wird, der die Master-Rolle besitzt.

NetApp empfiehlt, die „Host-Isolationsantwort“ auf deaktiviert zu setzen.

Ein Split-Brain-Zustand kann auftreten, wenn ein Host vom vSphere HA-Master-Host isoliert oder partitioniert wird und der Master nicht über Heartbeat Datastores oder Ping kommunizieren kann. Der Master erklärt den isolierten Host für tot und startet die VMs auf anderen Hosts im Cluster neu. Eine Split-Brain-Bedingung besteht jetzt, weil zwei Instanzen der virtuellen Maschine ausgeführt werden, von denen nur eine die virtuellen Laufwerke lesen oder schreiben kann. Split-Brain-Bedingungen können jetzt durch die Konfiguration von VM Component Protection (VMCP) vermieden werden.

Schutz von VM-Komponenten (VMCP)

Eine der Funktionsverbesserungen bei vSphere 6, relevant für HA, ist VMCP. VMCP bietet erweiterten Schutz vor All Paths Down (APD) und Permanent Device Loss (PDL) für Block (FC, iSCSI, FCoE) und File Storage (NFS).

Permanenter Geräteverlust (PDL)

PDL ist ein Zustand, der eintritt, wenn ein Speichermedium dauerhaft ausfällt oder administrativ entfernt wird und voraussichtlich nicht wiederhergestellt werden kann. Das NetApp -Speicherarray sendet einen SCSI-Sense-Code an ESXi, der signalisiert, dass das Gerät dauerhaft ausgefallen ist. Im Abschnitt „Fehlerbedingungen und VM-Reaktion“ von vSphere HA können Sie konfigurieren, wie die Reaktion nach dem Erkennen einer PDL-Bedingung aussehen soll.

NetApp empfiehlt, die "Reaktion für Datenspeicher mit PDL" auf "**VMs ausschalten und neu starten**" einzustellen. Wird dieser Zustand erkannt, wird eine VM sofort auf einem fehlerfreien Host innerhalb des vSphere HA-Clusters neu gestartet.

Alle Pfade nach unten (APD)

APD ist ein Zustand, der auftritt, wenn ein Speichermedium für den Host nicht mehr zugänglich ist und keine Pfade zum Array mehr verfügbar sind. ESXi betrachtet dies als ein vorübergehendes Problem mit dem Gerät und geht davon aus, dass es bald wieder verfügbar sein wird.

Wenn eine APD-Bedingung erkannt wird, wird ein Timer gestartet. Nach 140 Sekunden wird der APD-Zustand offiziell deklariert und das Gerät als APD-Zeitabmeldung markiert. Nach Ablauf der 140 Sekunden zählt HA die Anzahl der Minuten, die in der Verzögerung für VM-Failover-APD angegeben sind. Wenn die angegebene Zeit verstrichen ist, startet HA die betroffenen virtuellen Maschinen neu. Sie können VMCP so konfigurieren, dass es bei Bedarf anders reagiert (deaktiviert, Ereignisse ausstellen oder VMs aus- und neu starten).

- NetApp empfiehlt, die „Antwort für Datastore mit APD“ auf „**Ausschalten und Neustart von VMs (konservativ)**“ zu konfigurieren.
- „Konservativ“ bezieht sich auf die Wahrscheinlichkeit, dass HA VMs neu starten kann. Bei der Einstellung „Konservativ“ startet HA die von der APD betroffene VM nur dann neu, wenn bekannt ist, dass ein anderer Host sie neu starten kann. Im Modus „Aggressiv“ versucht HA, die VM neu zu starten, selbst wenn der Status der anderen Hosts unbekannt ist. Dies kann dazu führen, dass VMs nicht neu gestartet werden, wenn kein Host Zugriff auf den Datenspeicher hat, in dem sie sich befinden.
- Wenn der APD-Status aufgelöst wird und der Zugriff auf den Speicher wiederhergestellt wird, bevor das Timeout abgelaufen ist, startet HA die virtuelle Maschine nicht unnötig neu, es sei denn, Sie konfigurieren sie explizit dafür. Wenn eine Antwort gewünscht wird, selbst wenn sich die Umgebung von der APD-Bedingung erholt hat, sollte die Antwort für APD-Wiederherstellung nach APD-Timeout so konfiguriert werden, dass die VMs zurückgesetzt werden.
- NetApp empfiehlt, die Antwort für die APD-Wiederherstellung nach der APD-Zeitüberschreitung auf deaktiviert zu konfigurieren.

VMware DRS Implementierung für NetApp SnapMirror Active Sync

VMware DRS ist eine Funktion, die die Host-Ressourcen in einem Cluster aggregiert und hauptsächlich zum Lastausgleich innerhalb eines Clusters in einer virtuellen Infrastruktur verwendet wird. VMware DRS berechnet in erster Linie die CPU- und Arbeitsspeicherressourcen für den Lastausgleich in einem Cluster. Da vSphere das erweiterte Clustering nicht kennt, werden beim Lastausgleich alle Hosts an beiden Standorten berücksichtigt.

VMware DRS Implementierung für NetApp MetroCluster

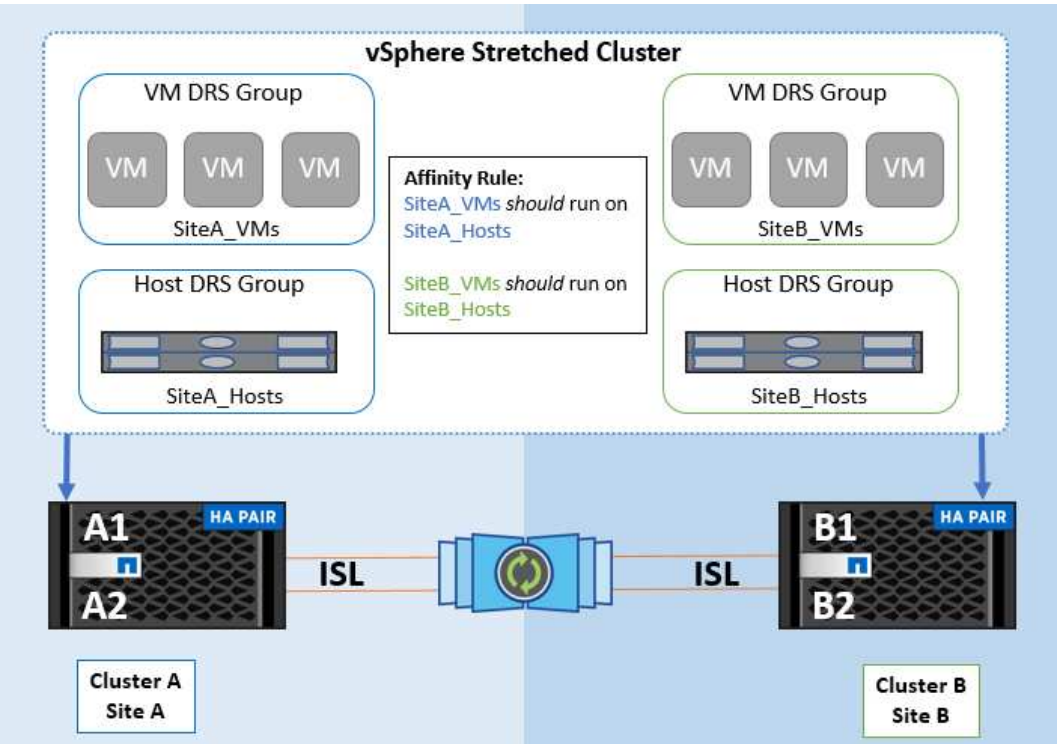
```
 To avoid cross-site traffic, NetApp recommends configuring DRS affinity
rules to manage a logical separation of VMs. This will ensure that, unless
there is a complete site failure, HA and DRS will only use local hosts.
Wenn Sie eine DRS-Affinitätsregel für Ihr Cluster erstellen, können Sie
festlegen, wie vSphere diese Regel während eines Failover einer virtuellen
Maschine anwendet.
```

Es gibt zwei Arten von Regeln, die Sie für das Failover-Verhalten von vSphere HA festlegen können:

- VM-Anti-Affinitätsregeln zwingen bestimmte Virtual Machines dazu, bei Failover-Aktionen getrennt zu bleiben.
- VM-Host-Affinitätsregeln platzieren angegebene Virtual Machines während Failover-Aktionen auf einem bestimmten Host oder einem Mitglied einer definierten Gruppe von Hosts.

Mithilfe der VM Host-Affinitätsregeln in VMware DRS lässt sich eine logische Trennung zwischen Standort A und Standort B erreichen, sodass die VM auf dem Host am selben Standort ausgeführt wird wie das Array, das als primärer Lese-/Schreib-Controller für einen bestimmten Datenspeicher konfiguriert ist. Zudem bleiben Virtual Machines gemäß den Regeln zur VM Host-Affinität lokal im Storage, wodurch wiederum die Virtual Machine-Verbindung im Falle von Netzwerkausfällen zwischen den Standorten hergestellt wird.

Nachfolgend finden Sie ein Beispiel für VM-Hostgruppen und Affinitätsregeln.



Best Practice

NetApp empfiehlt die Implementierung der „sollte“-Regeln statt der „müssen“-Regeln, da im Falle eines Ausfalls von vSphere HA gegen diese verstoßen wird. Die Verwendung von „Must“-Regeln kann zu Serviceausfällen führen.

Die Verfügbarkeit von Dienstleistungen sollte stets Vorrang vor der Leistung haben. Im Falle eines vollständigen Ausfalls des Rechenzentrums müssen die "Muss"-Regeln Hosts aus der VM-Hostaffinitätsgruppe auswählen, und wenn das Rechenzentrum nicht verfügbar ist, werden die virtuellen Maschinen nicht neu gestartet.

VMware Storage DRS Implementierung mit NetApp MetroCluster

Die VMware Storage DRS-Funktion ermöglicht die Aggregation von Datastores in eine einzige Einheit und gleicht Festplatten der virtuellen Maschine aus, wenn die SIOC-Schwellenwerte (Storage I/O Control) überschritten werden.

Die Storage-I/O-Steuerung ist bei DRS-Clustern mit Storage DRS standardmäßig aktiviert. Mit der Storage-I/O-Kontrolle kann ein Administrator die Menge an Storage-I/O steuern, die Virtual Machines bei I/O-Engpässen zugewiesen wird. Dadurch können wichtigeren Virtual Machines bei der I/O-Ressourcenzuweisung Vorrang vor weniger wichtigen Virtual Machines geben.

Storage DRS verwendet Storage vMotion, um die virtuellen Maschinen auf verschiedene Datastores innerhalb eines Datastore-Clusters zu migrieren. In einer NetApp MetroCluster Umgebung muss eine Migration von Virtual Machines innerhalb der Datenspeicher dieses Standorts gesteuert werden. Eine Virtual Machine A, die auf einem Host an Standort A ausgeführt wird, sollte idealerweise innerhalb der Datenspeicher der SVM an Standort A migriert werden Wenn dies nicht der Fall ist, wird die virtuelle Maschine weiterhin betrieben, jedoch mit verminderter Leistung, da das Lesen/Schreiben der virtuellen Festplatte von Standort B über standortübergreifende Links erfolgt.

*Bei Verwendung von ONTAP-Speicher wird empfohlen, Storage DRS zu deaktivieren.

- Storage DRS wird in der Regel nicht für die Verwendung mit ONTAP Storage-Systemen benötigt oder empfohlen.
- ONTAP bietet seine eigenen Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung und Data-Compaction, die von Storage DRS beeinflusst werden können.
- Wenn Sie ONTAP Snapshots verwenden, würde Storage vMotion die Kopie der VM im Snapshot zurücklassen, was möglicherweise die Speicherauslastung erhöht und sich auf Backup-Anwendungen wie NetApp SnapCenter auswirken kann, die VMs und ihre ONTAP Snapshots verfolgen.

VMSC Design- und Implementierungsrichtlinien

Dieses Dokument enthält Design- und Implementierungsrichtlinien für vMSC mit ONTAP Storage-Systemen.

NetApp-Speicherkonfiguration

Setup-Anweisungen für NetApp MetroCluster finden Sie unter "MetroCluster-Dokumentation". Anweisungen für SnapMirror Active Sync (SMAS) finden Sie auch unter "Überblick über die Business Continuity in SnapMirror".

Sobald Sie MetroCluster konfiguriert haben, ist die Verwaltung wie das Management einer herkömmlichen ONTAP-Umgebung. Sie können Storage Virtual Machines (SVMs) mithilfe verschiedener Tools wie Command Line Interface (CLI), System Manager oder Ansible einrichten. Sobald die SVMs konfiguriert sind, erstellen Sie logische Schnittstellen (LIFs), Volumes und LUNs (Logical Unit Numbers) auf dem Cluster, die für den normalen Betrieb verwendet werden. Diese Objekte werden automatisch über das Cluster-Peering-Netzwerk auf den anderen Cluster repliziert.

Wenn Sie nicht MetroCluster nutzen oder ONTAP Systeme haben, die nicht von MetroCluster unterstützt werden, beispielsweise ASA r2-Systeme, können Sie SnapMirror Active Sync verwenden. Dies bietet granularen Datastore-Schutz und aktiv/aktiv-Zugriff über mehrere ONTAP-Cluster in verschiedenen Ausfall-Domains hinweg. SMAS verwendet Konsistenzgruppen (CGS), um die Konsistenz der Schreibreihenfolge zwischen einem oder mehreren Datastores sicherzustellen. Je nach Applikations- und Datastore-Anforderungen können Sie mehrere CGS erstellen. Konsistenzgruppen sind insbesondere für Applikationen nützlich, die eine Datensynchronisierung zwischen mehreren Datastores erfordern. Beispielsweise Gast-LVMs, die zwischen Datastores verteilt sind. SMAS unterstützt auch Raw Device Mapping (RDMs) und über das Gastsystem verbundenen Storage mit in-Guest-iSCSI-Initiatoren. Weitere Informationen zu Konsistenzgruppen finden Sie unter "Übersicht über Konsistenzgruppen".

Es gibt einen Unterschied beim Management einer vMSC Konfiguration mit aktiver SnapMirror

Synchronisierung im Vergleich zu einer MetroCluster. Zunächst einmal ist SMAS eine reine SAN-Konfiguration. Es können keine NFS-Datastores mit aktiver SnapMirror-Synchronisierung gesichert werden. Als zweites müssen Sie Ihren ESXi-Hosts beide Kopien der LUNs zuordnen, damit sie auf die replizierten Datastores in beiden Ausfall-Domains zugreifen können. Als drittes müssen Sie eine oder mehrere Konsistenzgruppen für die Datastores erstellen, die Sie mit aktiver SnapMirror-Synchronisierung schützen möchten. Schließlich müssen Sie eine SnapMirror-Richtlinie für die von Ihnen erstellten Konsistenzgruppen erstellen. All dies ist ganz einfach mit dem „Protect Cluster“-Assistenten im vCenter Plug-in der ONTAP Tools oder durch manuelle Verwendung der ONTAP CLI oder des System Managers möglich.

Verwenden des ONTAP Tools vCenter Plug-ins für SnapMirror Active Sync

Das vCenter Plug-in der ONTAP Tools bietet eine einfache und intuitive Möglichkeit zur Konfiguration der SnapMirror Active Sync für vMSC. Mit dem ONTAP Tools vCenter Plug-in können Sie aktive SnapMirror Synchronisierungsbeziehungen zwischen zwei ONTAP Clustern erstellen und managen. Dieses Plug-in bietet eine benutzerfreundliche Oberfläche, über die diese Beziehungen effizient aufgebaut und verwaltet werden können. Sie können mehr über die ONTAP Tools vCenter Plugin unter erfahren "ONTAP Tools für VMware vSphere", oder direkt in springen "Schützen mit Host-Cluster-Schutz".

VMware vSphere Konfiguration

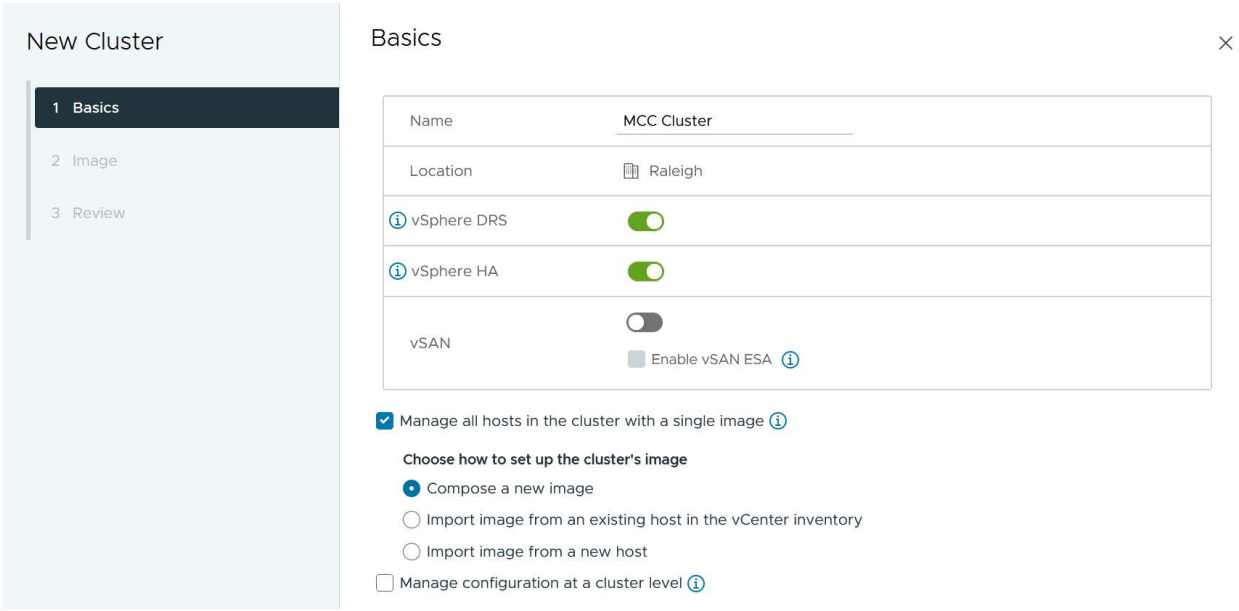
Erstellen Sie einen vSphere HA-Cluster

Die Erstellung eines vSphere HA-Clusters ist ein mehrstufiger Prozess, der in vollständig dokumentiert ist "Wie erstellen und konfigurieren Sie Cluster im vSphere Client auf docs.vmware.com". Kurz gesagt: Sie müssen zuerst einen leeren Cluster erstellen, dann mit vCenter Hosts hinzufügen und vSphere HA und andere Einstellungen des Clusters angeben.

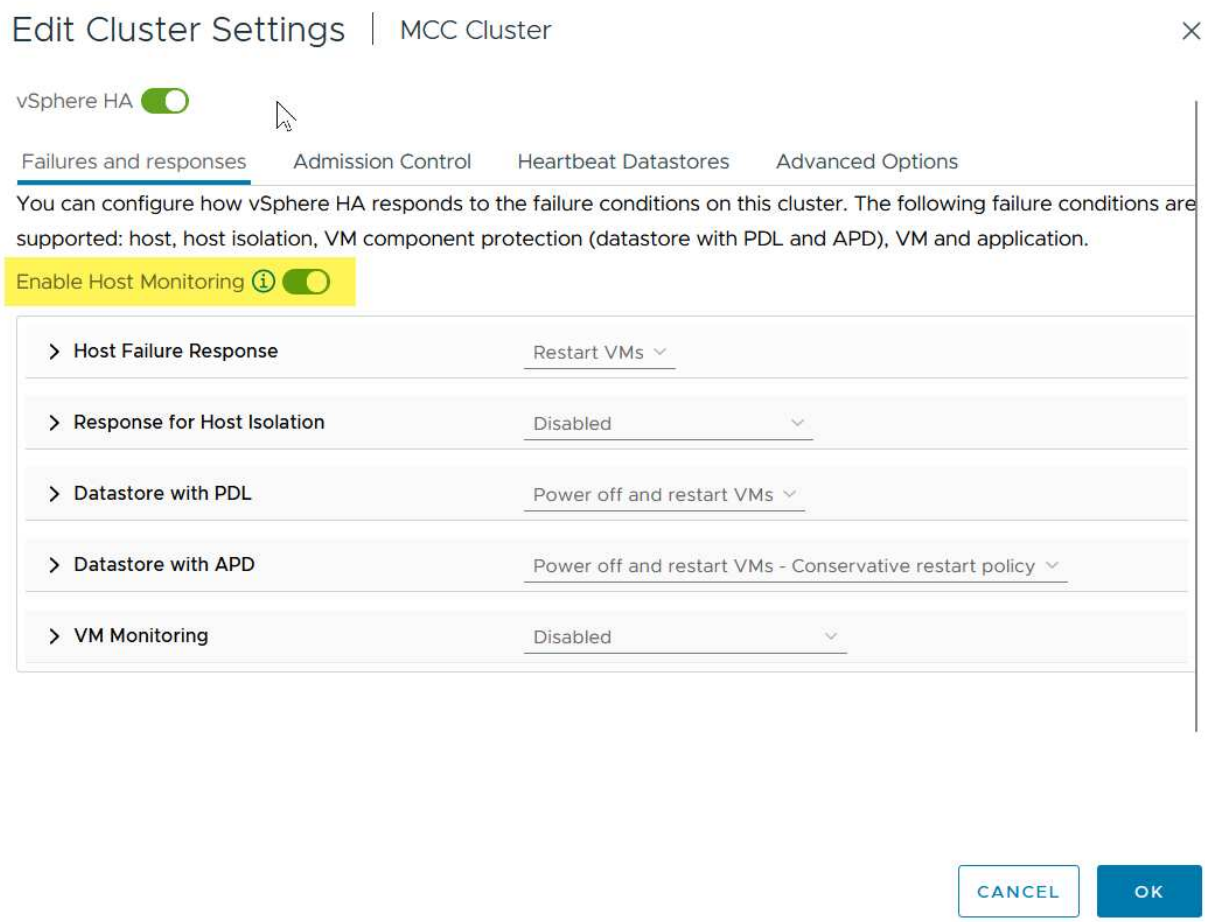
> ⓘ Nichts in diesem Dokument ersetzt "Empfohlene Practices für VMware vSphere Metro Storage-Cluster". Dieser Inhalt dient zur einfachen Referenz und stellt keinen Ersatz für die offizielle VMware Dokumentation dar.

Führen Sie zum Konfigurieren eines HA-Clusters die folgenden Schritte aus:

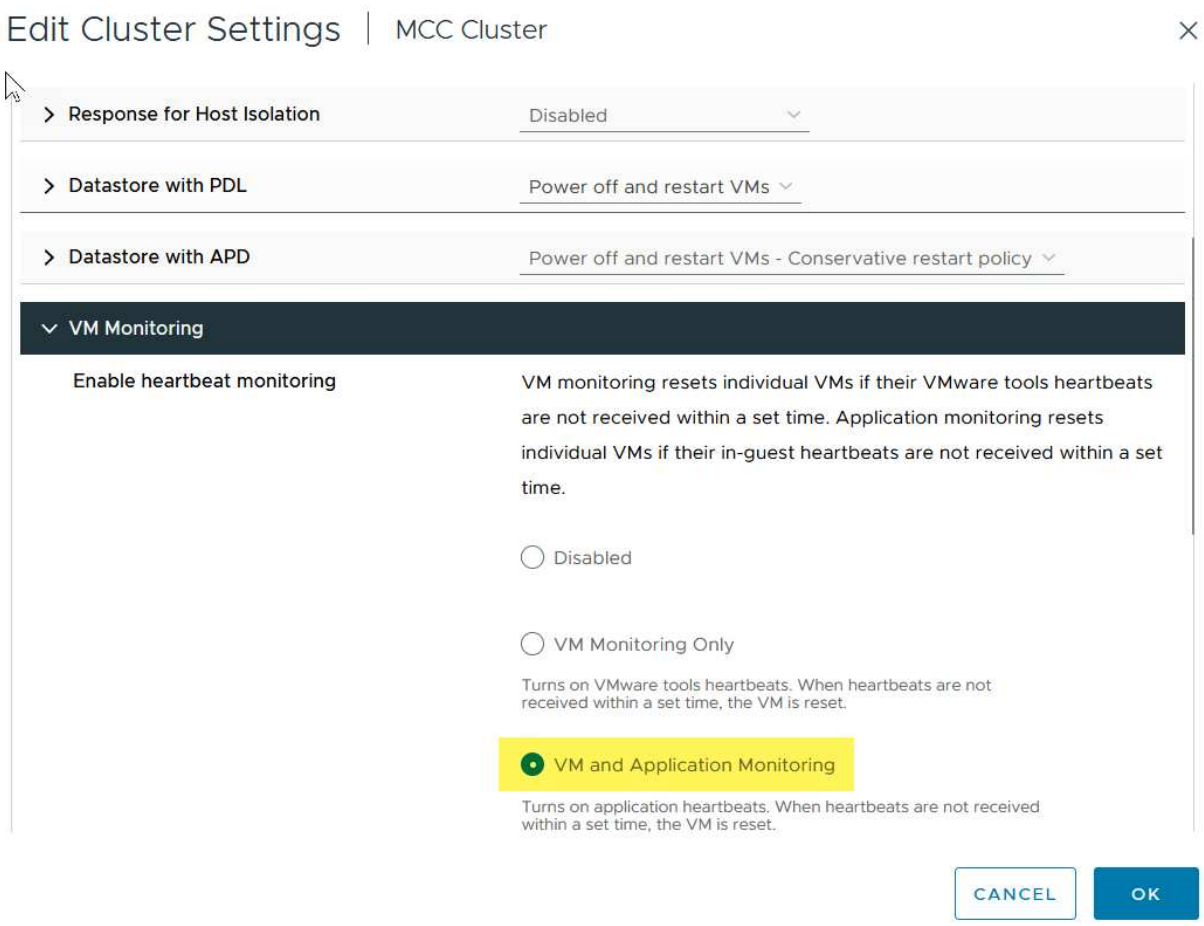
1. Stellen Sie eine Verbindung zur vCenter-Benutzeroberfläche her.
2. Navigieren Sie unter Hosts und Cluster zum Rechenzentrum, in dem Sie Ihr HA-Cluster erstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf das Datacenter-Objekt, und wählen Sie Neuer Cluster aus. Unter Grundlagen stellen Sie sicher, dass Sie vSphere DRS und vSphere HA aktiviert haben. Schließen Sie den Assistenten ab.



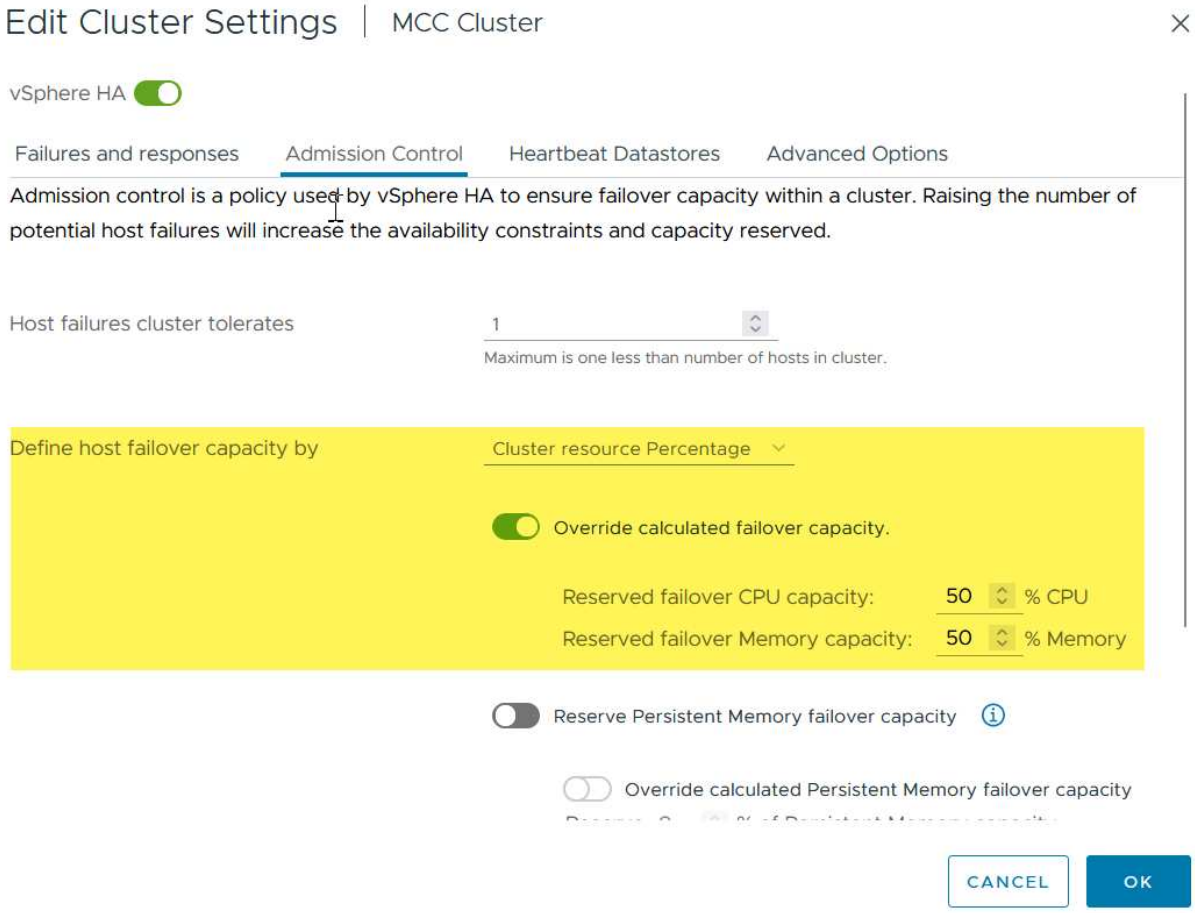
1. Wählen Sie den Cluster aus, und wechseln Sie zur Registerkarte Konfigurieren. Wählen Sie vSphere HA aus, und klicken Sie auf Bearbeiten.
2. Wählen Sie unter Host-Überwachung die Option Host-Überwachung aktivieren aus.



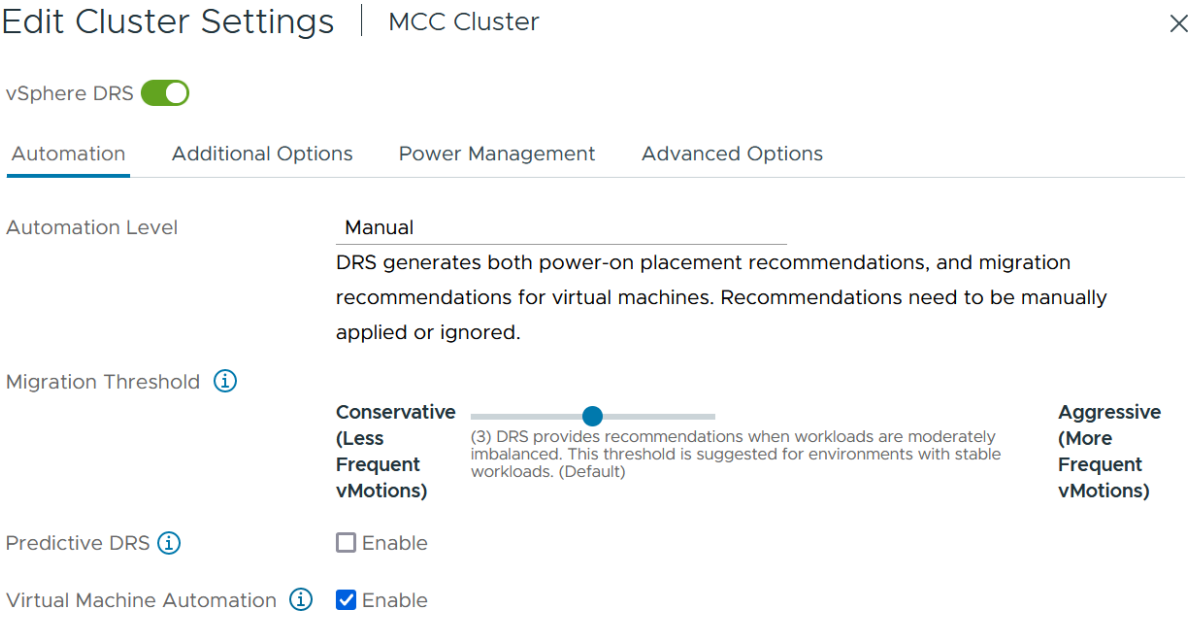
1. Wählen Sie auf der Registerkarte „Fehler und Antworten“ unter „VM-Überwachung“ die Option „nur VM-Überwachung“ oder „VM- und Anwendungsüberwachung“ aus.



1. Legen Sie unter Admission Control die Option HA-Eintrittskontrolle auf Cluster-Ressourcenreserve fest. Verwenden Sie 50 % CPU/MEM.



1. Klicken Sie auf „OK“.
2. Wählen Sie DRS und klicken Sie auf BEARBEITEN.
3. Setzen Sie den Automatisierungsgrad auf manuell, sofern dies nicht von Ihren Anwendungen erforderlich ist.



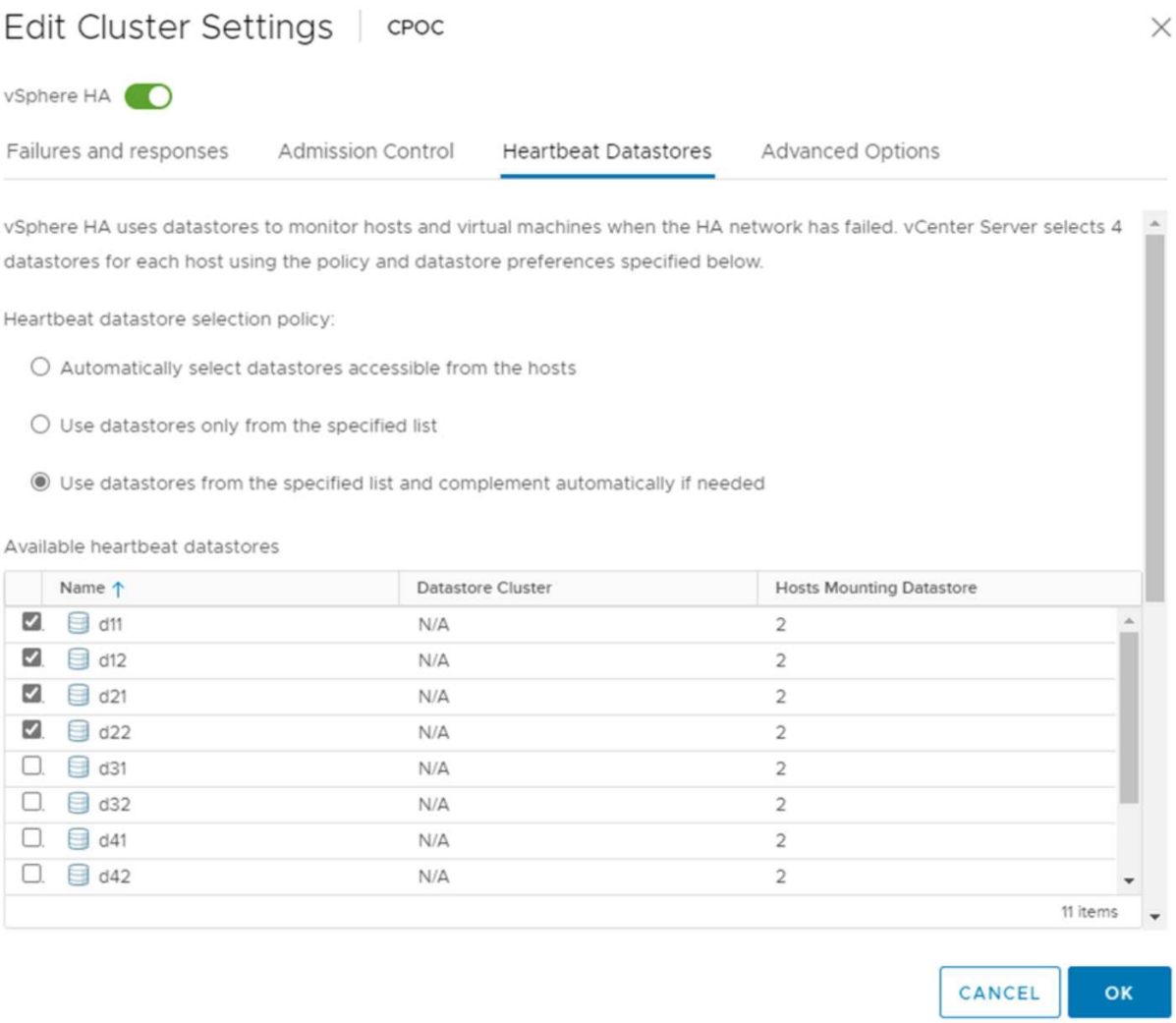
1. Aktivieren Sie den Schutz von VM-Komponenten, siehe "docs.vmware.com".
2. Die folgenden zusätzlichen vSphere HA-Einstellungen werden für vMSC mit MetroCluster empfohlen:

Ausfall	Antwort
Host-Ausfall	Starten Sie die VMs neu
Host-Isolierung	Deaktiviert
Datenspeicher mit Permanent Device Loss (PDL)	Schalten Sie die VMs aus und starten Sie sie neu
Datastore mit All Paths Down (APD)	Schalten Sie die VMs aus und starten Sie sie neu
Der Gast ist nicht herzschlagend	Setzt die VMs zurück
Richtlinie für den Neustart der VM	Bestimmt durch die Bedeutung der VM
Antwort für Host-Isolation	Fahren Sie die VMs herunter, und starten Sie sie neu
Antwort für Datastore mit PDL	Schalten Sie die VMs aus und starten Sie sie neu
Antwort für Datenspeicher mit APD	VMs ausschalten und neu starten (konservativ)
Verzögerung bei VM-Failover für APD	3 Minuten
Antwort für APD-Wiederherstellung mit APD-Timeout	Deaktiviert
Sensitivität für VM-Monitoring	Voreinstellung hoch

Konfigurieren Sie Datastores für Heartbeating

VSphere HA verwendet Datastores, um Hosts und virtuelle Maschinen zu überwachen, wenn das Managementnetzwerk ausgefallen ist. Sie können konfigurieren, wie vCenter Heartbeat-Datenspeicher auswählt. Gehen Sie wie folgt vor, um Datastores für Heartbeating zu konfigurieren:

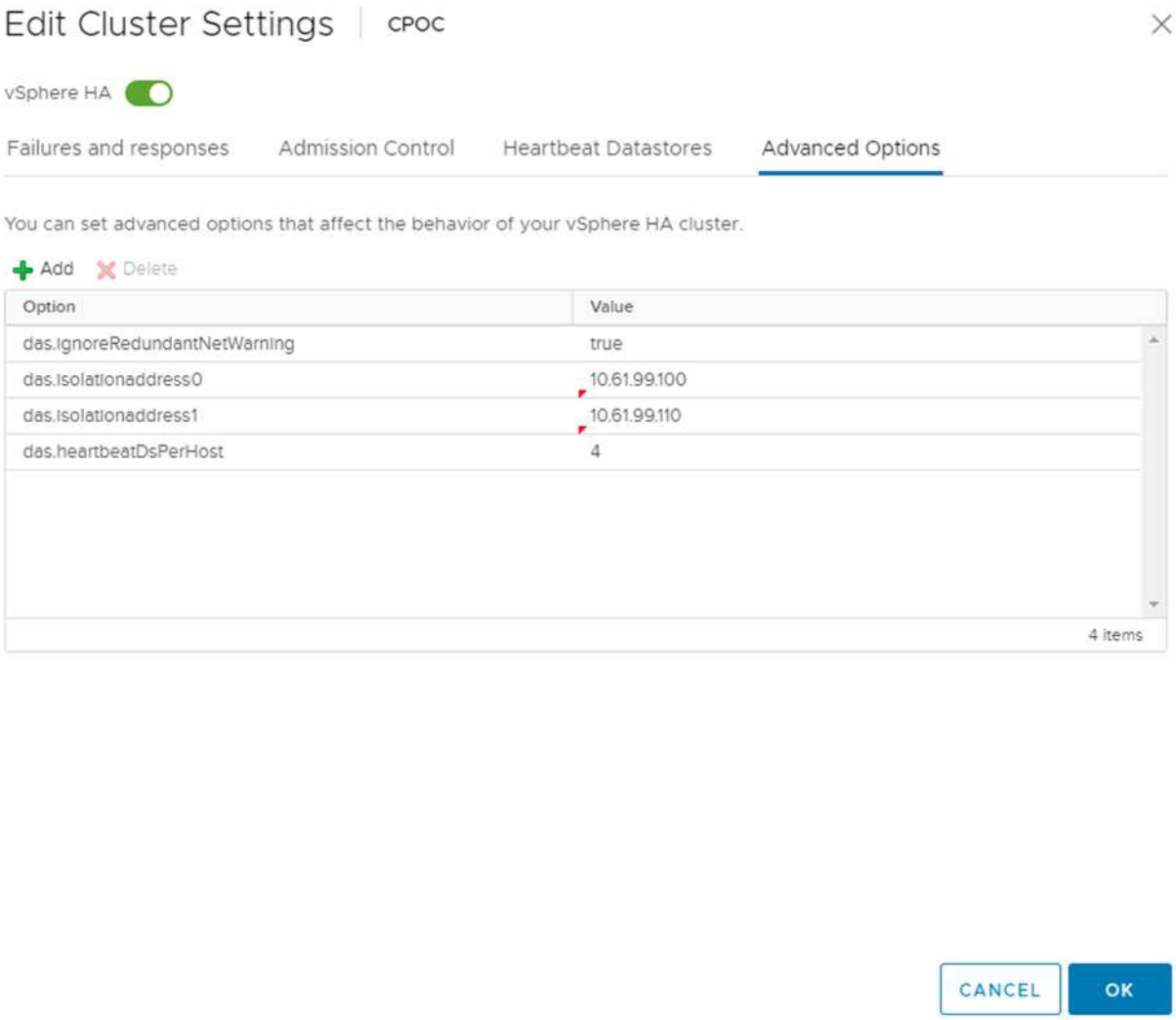
1. Wählen Sie im Abschnitt Datastore Heartbeating die Option Datastores aus der angegebenen Liste verwenden aus und ergänzen Sie bei Bedarf automatisch.
2. Wählen Sie die Datastores aus, die vCenter von beiden Standorten verwenden soll, und drücken Sie OK.



Konfigurieren Sie Die Erweiterten Optionen

Isolierungsereignisse treten auf, wenn Hosts innerhalb eines HA-Clusters die Verbindung zum Netzwerk oder zu anderen Hosts im Cluster verlieren. Standardmäßig verwendet vSphere HA das Standard-Gateway für sein Managementnetzwerk als Standard-Isolationsadresse. Sie können jedoch zusätzliche Isolationsadressen für den Host angeben, um zu bestimmen, ob eine Isolationsantwort ausgelöst werden soll. Fügen Sie zwei isolierte IPs hinzu, die Ping-Daten senden können, eine pro Standort. Verwenden Sie nicht die Gateway-IP. Die erweiterte vSphere HA-Einstellung ist das.isolationaddress. Dazu können Sie ONTAP- oder Mediator-IP-Adressen verwenden.

Weitere Informationen finden Sie unter "Empfohlene Practices für VMware vSphere Metro Storage-Cluster"._



Das Hinzufügen einer erweiterten Einstellung namens das.heartbeatDsPerHost kann die Anzahl der Heartbeat-Datenspeicher erhöhen. Verwenden Sie vier Heartbeat Datastores (HB DSS) – zwei pro Standort. Verwenden Sie die Option „aus Liste auswählen, aber Kompliment“. Dies wird benötigt, da Sie bei Ausfall eines Standorts immer noch zwei HB DSS benötigen. Diese müssen jedoch nicht durch MetroCluster oder SnapMirror Active Sync geschützt werden.

Weitere Informationen finden Sie unter "Empfohlene Practices für VMware vSphere Metro Storage-Cluster"._

VMware DRS Affinity zu NetApp MetroCluster

In diesem Abschnitt erstellen wir DRS Gruppen für VMs und Hosts für jeden Standort\Cluster in der MetroCluster Umgebung. Anschließend konfigurieren wir VM\Host-Regeln, um die VM Host-Affinität mit lokalen Storage-Ressourcen auszurichten. Beispielsweise gehören Standort A VMs zur VM-Gruppe sitea_vms und Standort A Hosts zur Host-Gruppe sitea_Hosts. Als nächstes geben wir in VM\Host Rules an, dass sitea_vms auf Hosts in sitea_Hosts ausgeführt werden sollen.

- NetApp empfiehlt dringend die Spezifikation **sollte auf Hosts in Gruppe** laufen anstatt der Spezifikation **muss auf Hosts in Gruppe** ausgeführt werden. Im Falle eines Host-Ausfalls von Standort A müssen die VMs von Standort A über vSphere HA auf Hosts an Standort B neu gestartet werden. Bei der letzteren Spezifikation ist jedoch nicht möglich, dass HA die VMs auf Standort B neu starten, da es die harte Regel ist. Die frühere Spezifikation ist eine weiche Regel und wird im Falle von HA verletzt, wodurch die Verfügbarkeit anstatt die Leistung ermöglicht wird.
- Sie können einen ereignisbasierten Alarm erstellen, der ausgelöst wird, wenn eine virtuelle Maschine gegen eine VM-Host-Affinitätsregel verstößt. Fügen Sie im vSphere Client einen neuen Alarm für die virtuelle Maschine hinzu und wählen Sie als Ereignisauslöser „VM verletzt VM-Host Affinity Rule“ aus. Weitere Informationen zum Erstellen und Bearbeiten von Alarmen finden Sie in "VSphere Monitoring und Performance"der Dokumentation.

DRS-Host-Gruppen erstellen

So erstellen Sie DRS Host-Gruppen speziell für Standort A und Standort B:

1. Klicken Sie im vSphere-Webclient mit der rechten Maustaste auf den Cluster in der Bestandsaufnahme, und wählen Sie Einstellungen aus.
2. Klicken Sie auf VM\Host Groups.
3. Klicken Sie Auf Hinzufügen.
4. Geben Sie den Namen der Gruppe ein (z. B. sitea_Hosts).
5. Wählen Sie im Menü Typ die Option Host-Gruppe aus.
6. Klicken Sie auf Hinzufügen, wählen Sie die gewünschten Hosts von Standort A aus, und klicken Sie auf OK.
7. Wiederholen Sie diese Schritte, um eine weitere Host-Gruppe für Standort B hinzuzufügen
8. Klicken Sie auf OK.

DRS VM-Gruppen erstellen

So erstellen Sie DRS VM-Gruppen speziell für Standort A und Standort B:

1. Klicken Sie im vSphere-Webclient mit der rechten Maustaste auf den Cluster in der Bestandsaufnahme, und wählen Sie Einstellungen aus.
2. Klicken Sie auf VM\Host Groups.
3. Klicken Sie Auf Hinzufügen.
4. Geben Sie den Namen der Gruppe ein (z. B. sitea_vms).
5. Wählen Sie im Menü Typ die Option VM-Gruppe aus.
6. Klicken Sie auf Hinzufügen, wählen Sie die gewünschten VMs von Standort A aus, und klicken Sie auf OK.
7. Wiederholen Sie diese Schritte, um eine weitere Host-Gruppe für Standort B hinzuzufügen
8. Klicken Sie auf OK.

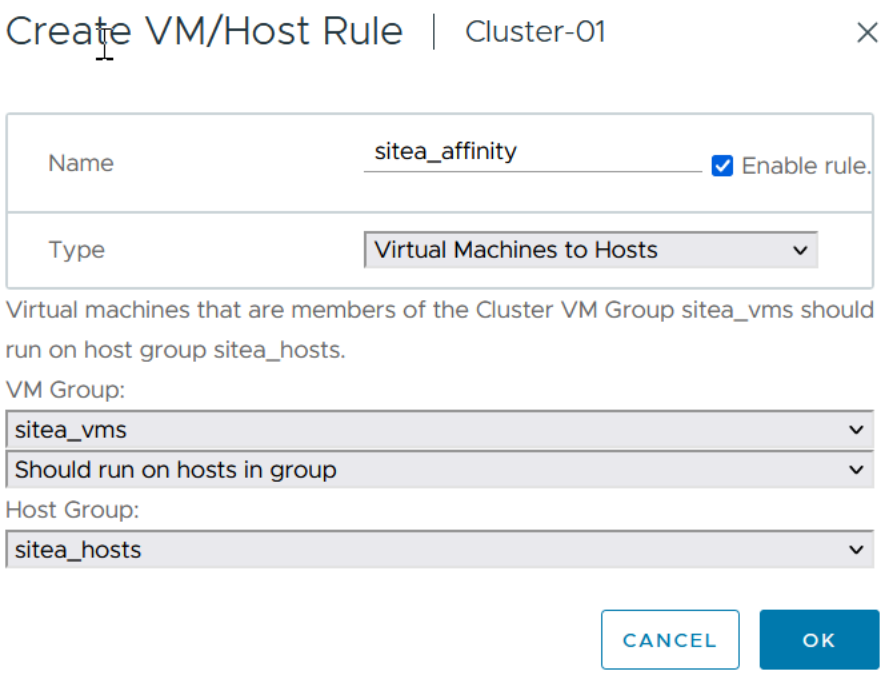
Erstellen Sie VM-Hostregeln

Gehen Sie wie folgt vor, um DRS-Affinitätsregeln für Standort A und Standort B zu erstellen:

1. Klicken Sie im vSphere-Webclient mit der rechten Maustaste auf den Cluster in der Bestandsaufnahme,

und wählen Sie Einstellungen aus.

2. Klicken Sie auf VM\Hostregeln.
3. Klicken Sie Auf Hinzufügen.
4. Geben Sie den Namen der Regel ein (z. B. sitea_Affinity).
5. Überprüfen Sie, ob die Option Regel aktivieren aktiviert ist.
6. Wählen Sie im Menü Typ die Option Virtuelle Maschinen zu Hosts aus.
7. Wählen Sie die VM-Gruppe aus (z.B. sitea_vms).
8. Wählen Sie die Host-Gruppe aus (z. B. sitea_Hosts).
9. Wiederholen Sie diese Schritte, um eine weitere VM\Host-Regel für Standort B hinzuzufügen
10. Klicken Sie auf OK.



Datastore-Cluster bei Bedarf erstellen

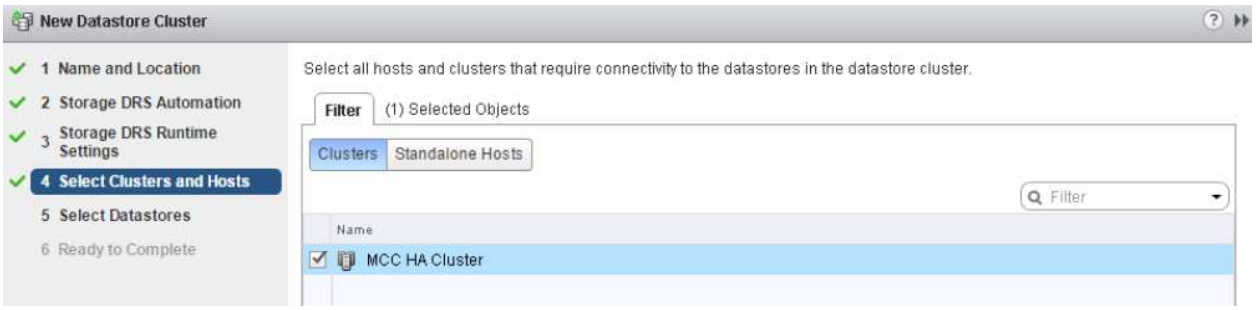
Führen Sie die folgenden Schritte aus, um ein Datastore-Cluster für jeden Standort zu konfigurieren:

1. Navigieren Sie mithilfe des vSphere-Webclients zum Rechenzentrum, in dem sich der HA-Cluster unter Speicher befindet.
2. Klicken Sie mit der rechten Maustaste auf das Datacenter-Objekt, und wählen Sie Storage > New Datastore Cluster aus.

*Bei Verwendung von ONTAP-Speicher wird empfohlen, Storage DRS zu deaktivieren.

- Storage DRS wird in der Regel nicht für die Verwendung mit ONTAP Storage-Systemen benötigt oder empfohlen.
- ONTAP bietet seine eigenen Storage-Effizienzfunktionen wie Deduplizierung, Komprimierung und Data-Compaction, die von Storage DRS beeinflusst werden können.
- Wenn Sie ONTAP-Snapshots verwenden, würde Storage vMotion die VM-Kopie im Snapshot zurücklassen, wodurch möglicherweise die Speicherauslastung erhöht wird und sich auf Backup-Anwendungen wie NetApp SnapCenter auswirken könnte, die VMs und ihre ONTAP-Snapshots nachverfolgen.

1. Wählen Sie das HA-Cluster aus, und klicken Sie auf Weiter.



1. Wählen Sie die Datastores aus, die zu Standort A gehören, und klicken Sie auf Weiter.

1. Überprüfen Sie die Optionen, und klicken Sie auf Fertig stellen.
2. Wiederholen Sie diese Schritte, um das Datastore-Cluster an Standort B zu erstellen und sicherzustellen, dass nur Datastores von Standort B ausgewählt sind.

VCenter Server-Verfügbarkeit

Ihre vCenter Server Appliances (VCSAs) sollten durch vCenter HA geschützt werden. Mit vCenter HA können Sie zwei VCSAs in einem aktiv/Passiv-HA-Paar implementieren. Einer in jeder Ausfall-Domäne. Weitere Informationen zu vCenter HA finden Sie im "docs.vmware.com".

Ausfallsicherheit bei geplanten und ungeplanten Ereignissen

NetApp MetroCluster und SnapMirror Active Sync sind leistungsstarke Tools, die die Hochverfügbarkeit und den unterbrechungsfreien Betrieb von NetApp Hardware und ONTAP Software verbessern.

Diese Tools bieten standortweiten Schutz für die gesamte Storage-Umgebung und stellen sicher, dass Ihre Daten immer verfügbar sind. Ob Sie Standalone-Server, Hochverfügbarkeits-Server-Cluster, Container oder virtualisierte Server verwenden – die NetApp Technologie sorgt nahtlos für die Storage-Verfügbarkeit im Falle eines totalen Ausfalls aufgrund von Strom-, Kühlungs- oder Netzwerkfehlern, Storage Array Shutdown oder Bedienungsfehlern.

MetroCluster und SnapMirror Active Sync bieten drei grundlegende Methoden für die Datenverfügbarkeit bei geplanten und ungeplanten Ereignissen:

- Redundante Komponenten zum Schutz vor dem Ausfall einer einzelnen Komponente
- Lokaler HA-Takeover für Ereignisse, die sich auf einen einzelnen Controller auswirken
- Vollständiger Standortschutz: Schnelle Wiederaufnahme des Service durch Verschieben des Speicher- und Client-Zugriffs vom Quell-Cluster auf den Ziel-Cluster

Das bedeutet, dass die Abläufe bei Ausfall einer einzelnen Komponente reibungslos fortgesetzt werden und beim Austausch der ausgefallenen Komponente automatisch in den redundanten Betrieb zurückkehren.

Alle ONTAP Cluster außer Cluster mit einem Node (in der Regel softwaredefinierte Versionen, wie beispielsweise ONTAP Select) verfügen über integrierte HA-Funktionen für Takeover und Giveback. Jeder Controller im Cluster wird mit einem anderen Controller gepaart, wodurch ein HA-Paar entsteht. Diese Paare stellen sicher, dass jeder Node lokal mit dem Speicher verbunden ist.

Die Übernahme ist ein automatisierter Prozess, bei dem ein Node den Storage des anderen zur Aufrechterhaltung der Datenservices übernimmt. GiveBack bedeutet umgekehrter Prozess, der den normalen Betrieb wiederherstellt. Takeover können geplant werden, beispielsweise bei Hardware-Wartungsarbeiten oder ONTAP Upgrades oder aufgrund von Node-Panic- oder Hardware-Ausfällen.

Während einer Übernahme führen NAS LIFs in MetroCluster Konfigurationen automatisch ein Failover durch. SAN LIFs führen jedoch keinen Failover durch, sondern verwenden weiterhin den direkten Pfad zu den Logical Unit Numbers (LUNs).

Weitere Informationen zu HA-Takeover und Giveback finden Sie im "HA-Paar-Management – Übersicht". Erwähnenswert ist, dass diese Funktion nicht spezifisch für MetroCluster oder SnapMirror für die aktive Synchronisierung ist.

Eine Standortumschaltung mit MetroCluster erfolgt, wenn ein Standort offline ist oder als geplante Aktivität für die standortweite Wartung vorgesehen ist. Der verbleibende Standort übernimmt die Eigentümerschaft der Storage-Ressourcen (Festplatten und Aggregate) des Offline-Clusters, und die SVMs am ausgefallenen Standort werden online geschaltet und am Disaster-Standort neugestartet. Dabei bleibt die volle Identität für den Client- und Host-Zugriff erhalten.

Da beide Kopien gleichzeitig aktiv verwendet werden, arbeiten Ihre vorhandenen Hosts mit der aktiven SnapMirror Synchronisierung weiter. Der ONTAP-Mediator ist erforderlich, um sicherzustellen, dass ein Standort-Failover korrekt ausgeführt wird.

Ausfallszenarien für vMSC mit MetroCluster

In den folgenden Abschnitten werden die erwarteten Ergebnisse verschiedener Ausfallszenarien mit vMSC- und NetApp MetroCluster-Systemen beschrieben.

Ausfall Eines Einzelnen Storage-Pfads

Wenn in diesem Szenario Komponenten wie der HBA-Port, der Netzwerkport, der Front-End-Datenschalterport oder ein FC- oder Ethernet-Kabel ausfallen, wird dieser bestimmte Pfad zum Speichergerät vom ESXi-Host als „tot“ markiert. Wenn mehrere Pfade durch Ausfallsicherheit am HBA/Netzwerk/Switch Port für das Storage-Gerät konfiguriert sind, führt ESXi idealerweise eine Pfadumschaltung durch. Während dieser Zeit bleiben Virtual Machines ohne Beeinträchtigungen verfügbar, da für die Storage-Verfügbarkeit mehrere Pfade zum Storage-Gerät bereitgestellt werden.

Es gibt keine Änderung im MetroCluster Verhalten in diesem Szenario, und alle Datenspeicher sind weiterhin von ihren jeweiligen Seiten intakt.

Best Practice

In Umgebungen mit NFS/iSCSI-Volumes empfiehlt NetApp, mindestens zwei Netzwerk-Uplinks für den NFS-VMkernel-Port im Standard-vSwitch und dieselbe Port-Gruppe zu konfigurieren, bei der die NFS-VMkernel-Schnittstelle für den verteilten vSwitch zugeordnet ist. NIC-Teaming kann entweder aktiv-aktiv oder aktiv-Standby konfiguriert werden.

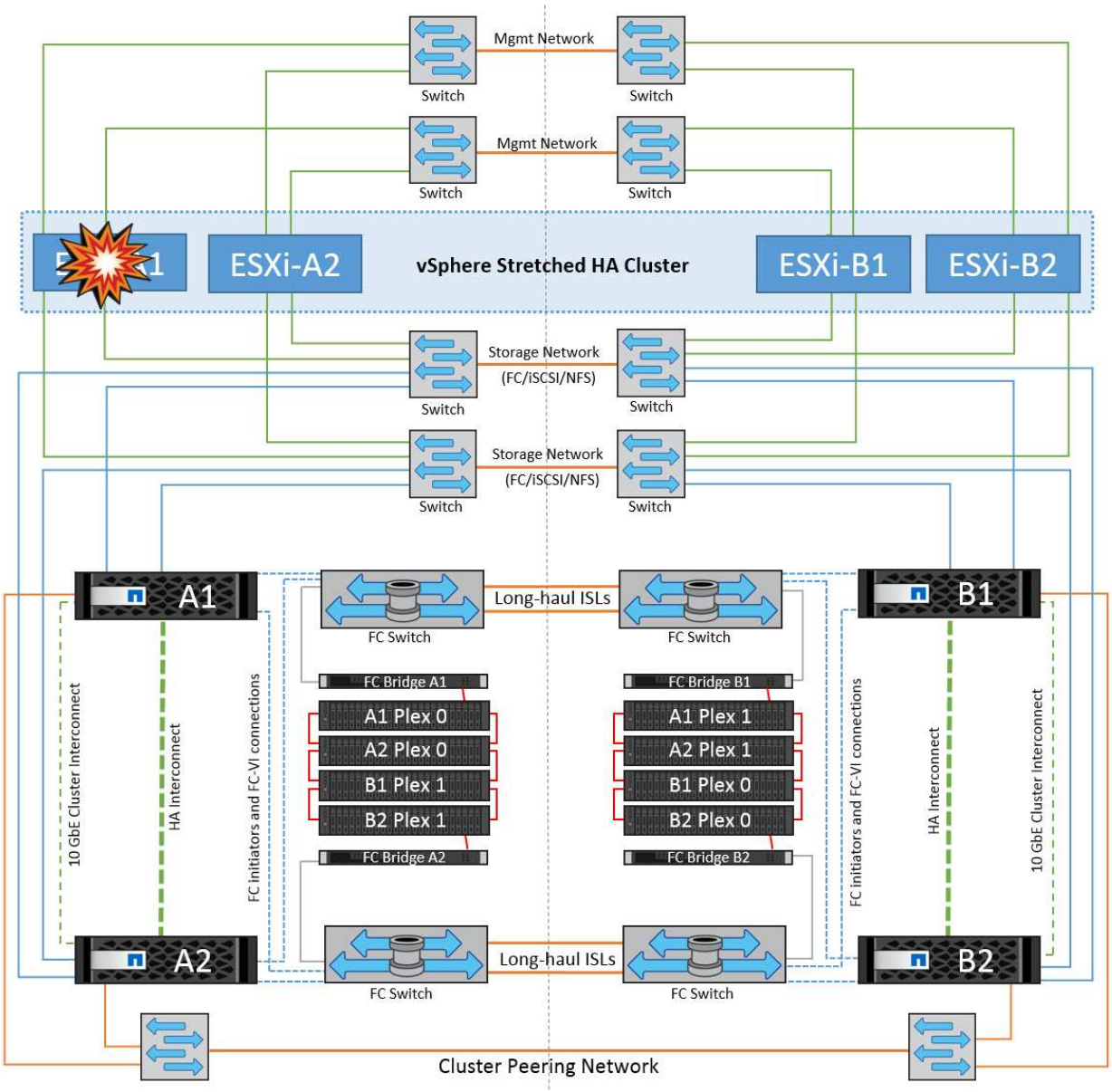
Außerdem muss bei iSCSI LUNs Multipathing konfiguriert werden, indem die VMkernel-Schnittstellen an die iSCSI-Netzwerkadapter gebunden werden. Weitere Informationen finden Sie in der vSphere-Speicherdokumentation.

Best Practice

In Umgebungen mit Fibre-Channel-LUNs empfiehlt NetApp die Verwendung von mindestens zwei HBAs, wodurch Ausfallsicherheit auf HBA-/Port-Ebene garantiert wird. NetApp empfiehlt für das Zoning von einem einzelnen Initiator außerdem als Best Practice zum Konfigurieren des Zoning.

Sie sollten mithilfe der Virtual Storage Console (VSC) Multipathing-Richtlinien festlegen, da sie Richtlinien für alle neuen und vorhandenen NetApp Storage-Geräte definiert.

Ausfall eines einzelnen ESXi-Hosts



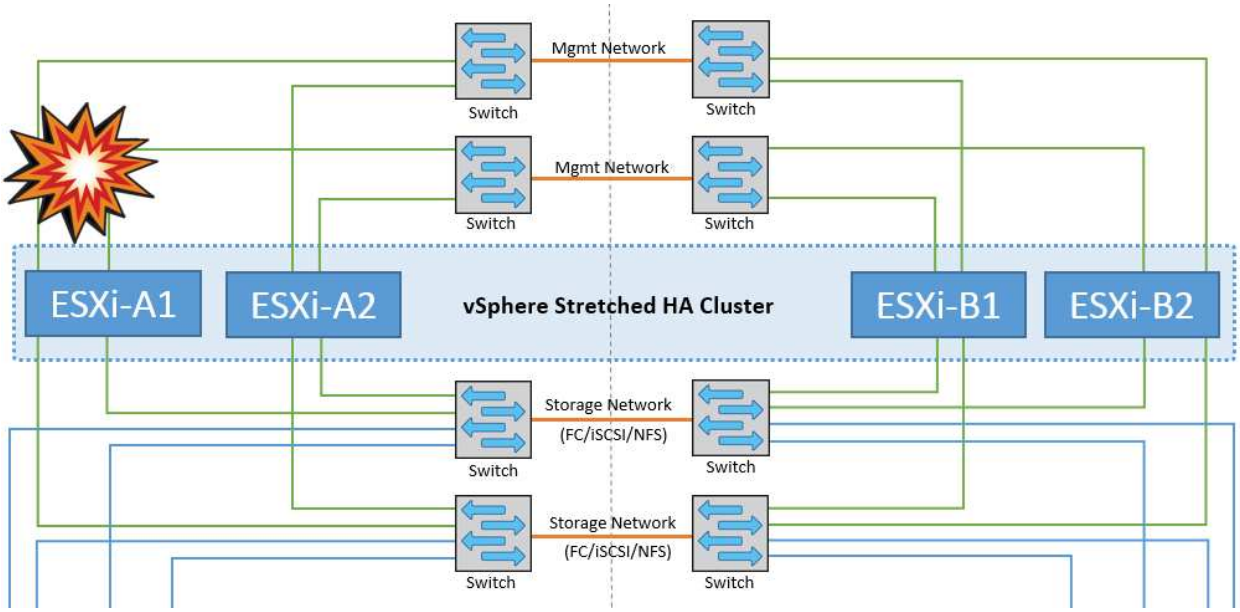
Wenn in diesem Szenario ein ESXi-Host ausfällt, erkennt der Master-Node im VMware HA-Cluster den Host-Ausfall, da er keine Netzwerk-Heartbeats mehr empfängt. Um festzustellen, ob der Host wirklich ausgefallen ist oder nur eine Netzwerkpartition ist, überwacht der Master-Knoten die Datastore-Heartbeats und führt, falls sie nicht vorhanden sind, eine abschließende Prüfung durch, indem er die Management-IP-Adressen des ausgefallenen Hosts anpingt. Wenn alle Prüfungen negativ sind, erklärt der Master-Node diesen Host als ausgefallenen Host, und alle virtuellen Maschinen, die auf diesem ausgefallenen Host ausgeführt wurden, werden auf dem noch verbleibenden Host im Cluster neu gestartet.

Wenn DRS VM und Host Affinity Regeln konfiguriert wurden (VMs in VM Gruppe sitea_vms sollten Hosts in Host Gruppe sitea_Hosts laufen lassen), dann prüft der HA Master zunächst auf verfügbare Ressourcen an Standort A. Wenn an Standort A keine verfügbaren Hosts vorhanden sind, versucht der Master, die VMs auf den Hosts an Standort B neu zu starten

Es ist möglich, dass die virtuellen Maschinen auf den ESXi-Hosts am anderen Standort gestartet werden, wenn am lokalen Standort eine Ressourcenbeschränkung vorhanden ist. Die definierten Regeln für die DRS-VM und Host-Affinität werden jedoch korrigiert, wenn Regeln verletzt werden, indem die virtuellen Maschinen zurück zu den noch verbleibenden ESXi-Hosts am lokalen Standort migriert werden. In Fällen, in denen DRS auf manuell festgelegt ist, empfiehlt NetApp, DRS zu aktivieren und die Empfehlungen anzuwenden, um die Platzierung der Virtual Machines zu korrigieren.

Es gibt keine Änderung im MetroCluster Verhalten in diesem Szenario und alle Datenspeicher bleiben von ihren jeweiligen Seiten intakt.

ESXi-Host-Isolierung

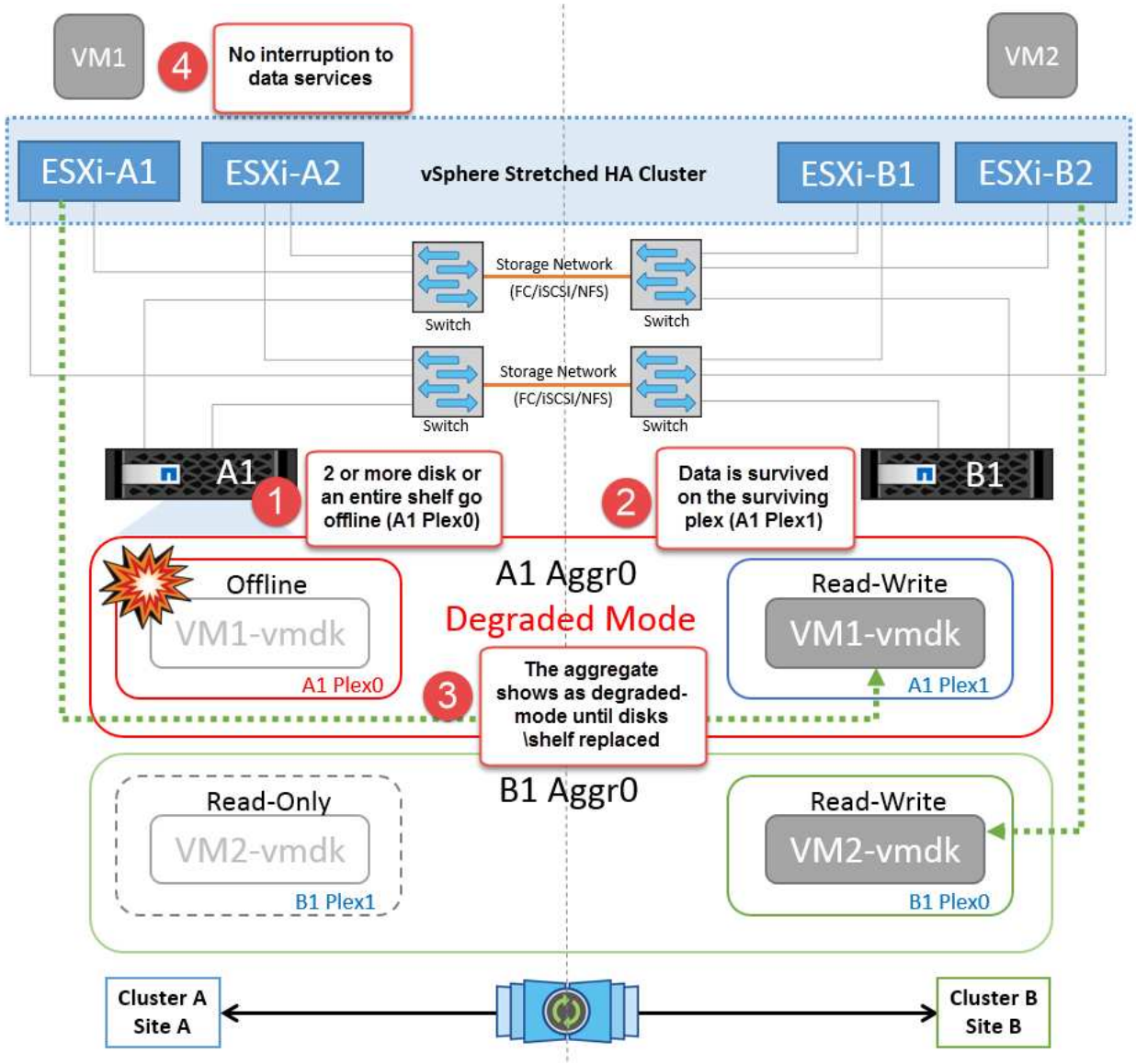


Wenn in diesem Szenario das Managementnetzwerk des ESXi-Hosts ausgefallen ist, erhält der Master-Node im HA-Cluster keine Heartbeats, wodurch dieser Host im Netzwerk isoliert wird. Um festzustellen, ob es ausgefallen ist oder nur isoliert ist, beginnt der Master-Node mit der Überwachung des Datastore-Herzschlags. Wenn er vorhanden ist, wird der Host vom Master-Knoten isoliert deklariert. Je nach konfigurierter Isolationsantwort kann der Host sich entscheiden, die virtuellen Maschinen auszuschalten, herunterzufahren oder die virtuellen Maschinen sogar eingeschaltet zu lassen. Das Standardintervall für die Isolationsantwort beträgt 30 Sekunden.

Es gibt keine Änderung im MetroCluster Verhalten in diesem Szenario und alle Datenspeicher bleiben von ihren jeweiligen Seiten intakt.

Platten-Shelf-Fehler

In diesem Szenario kommt es zu einem Ausfall von mehr als zwei Festplatten oder eines gesamten Shelf. Daten werden vom verbleibenden Plex ohne Unterbrechung der Datenservices bereitgestellt. Der Festplattenausfall kann sich auf einen lokalen oder einen Remote-Plex auswirken. Die Aggregate werden als degradierter Modus angezeigt, da nur ein Plex aktiv ist. Sobald die ausgefallenen Festplatten ersetzt wurden, werden die betroffenen Aggregate automatisch neu synchronisiert, um die Daten neu aufzubauen. Nach der Neusynchronisierung kehren die Aggregate automatisch in den normalen gespiegelten Modus zurück. Wenn mehr als zwei Laufwerke innerhalb einer einzelnen RAID-Gruppe ausgefallen sind, muss der Plex neu aufgebaut werden.

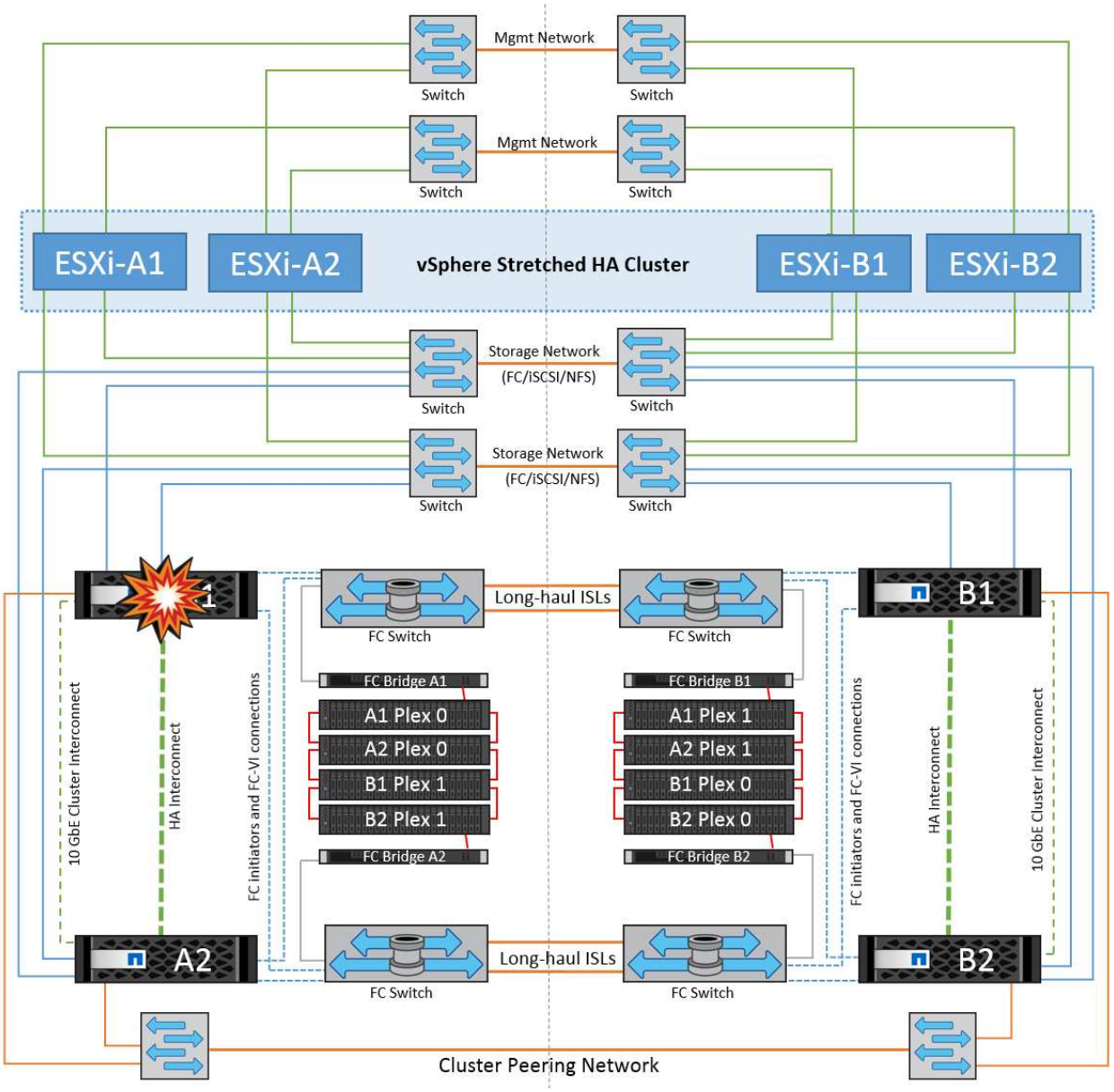


*[HINWEIS]

- Während dieses Zeitraums gibt es keine Auswirkungen auf die I/O-Vorgänge der virtuellen Maschine, aber die Performance ist beeinträchtigt, da über ISL-Links auf die Daten vom Remote-Festplatten-Shelf aus zugegriffen wird.

Ausfall Eines Einzelnen Storage Controllers

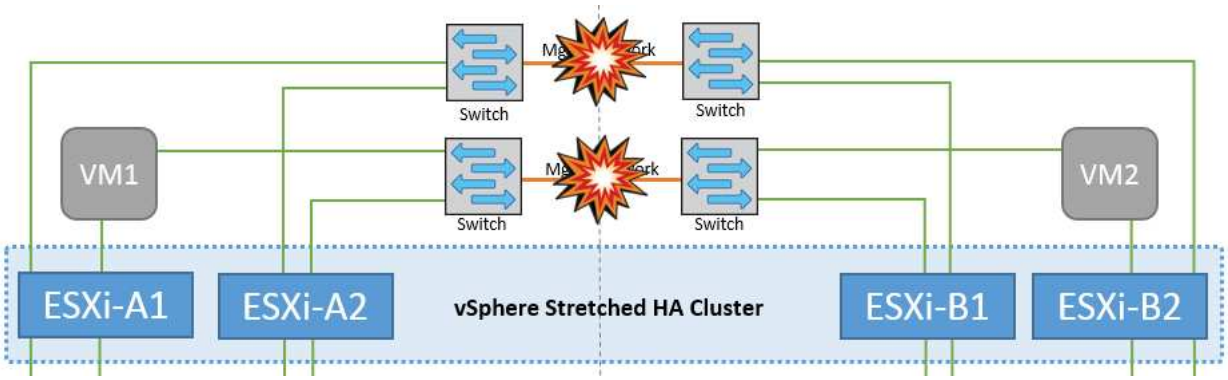
In diesem Szenario fällt einer der beiden Storage Controller an einem Standort aus. Da an jedem Standort ein HA-Paar vorhanden ist, wird bei einem Ausfall eines Node automatisch ein Failover auf den anderen Node ausgelöst. Wenn beispielsweise Node A1 ausfällt, werden dessen Storage und Workloads automatisch auf Node A2 übertragen. Virtuelle Maschinen sind nicht betroffen, da alle Plexe verfügbar bleiben. Die Knoten des zweiten Standorts (B1 und B2) sind davon nicht betroffen. Außerdem führt vSphere HA keine Aktion durch, da der Master-Node im Cluster weiterhin Netzwerk-Heartbeats empfängt.



Wenn der Failover Teil eines rollierenden Disaster ist (Node A1 führt ein Failover auf A2 durch) und ein nachfolgender Ausfall von A2 oder ein vollständiger Ausfall von Standort A auftritt, kann an Standort B das Umschalten nach einem Ausfall stattfinden

Verbindungsfehler Zwischen Switches

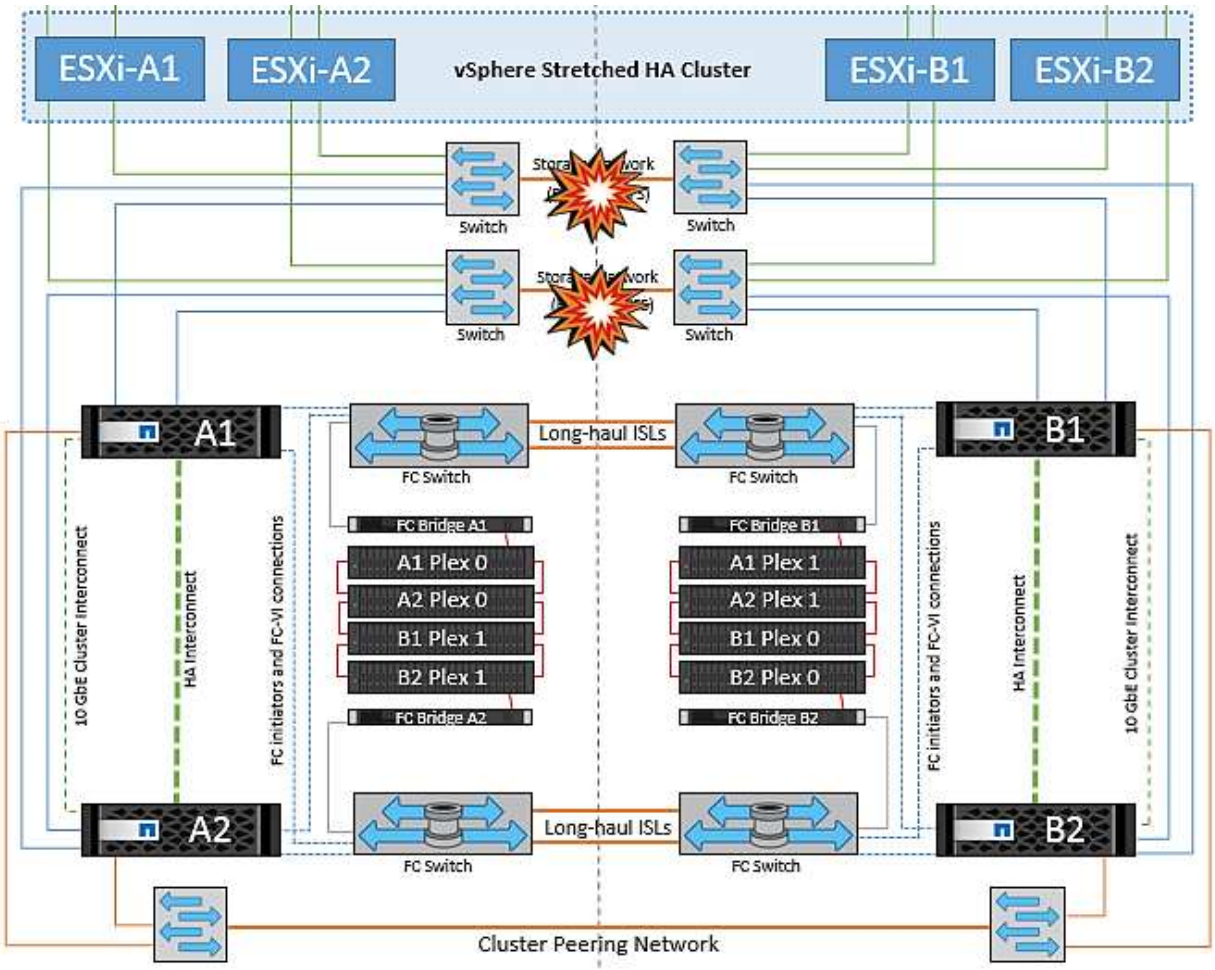
Verbindungsfehler zwischen Switches im Managementnetzwerk



In diesem Szenario können die ESXi-Hosts an Standort A nicht mit ESXi-Hosts an Standort B kommunizieren, wenn die ISL-Links am Front-End-Hostverwaltungsnetzwerk fehlschlagen Dies führt zu einer Netzwerkpartition, da ESXi-Hosts an einem bestimmten Standort die Netzwerk-Heartbeats nicht an den Master-Node im HA-Cluster senden können. Daher gibt es aufgrund der Partition zwei Netzwerksegmente, und in jedem Segment gibt es einen Master-Knoten, der die VMs vor Host-Ausfällen innerhalb des jeweiligen Standorts schützt.

Während dieses Zeitraums bleiben die virtuellen Maschinen aktiv, und es gibt keine Änderung im MetroCluster-Verhalten in diesem Szenario. Alle Datenspeicher bleiben von ihren jeweiligen Seiten intakt.

Verbindungsfehler zwischen Switches im Speichernetzwerk



Wenn in diesem Szenario die ISL-Verbindungen im Back-End-Speichernetzwerk ausfallen, verlieren die Hosts an Standort A den Zugriff auf die Speicher-Volumes oder LUNs von Cluster B an Standort B und umgekehrt. Die VMware DRS Regeln sind so definiert, dass die Host-Storage-Standortaffinität die Ausführung der Virtual Machines ohne Auswirkungen auf den Standort erleichtert.

Während dieses Zeitraums bleiben die virtuellen Maschinen an ihren jeweiligen Standorten in Betrieb und es gibt keine Änderung im MetroCluster-Verhalten in diesem Szenario. Alle Datenspeicher bleiben von ihren jeweiligen Seiten intakt.

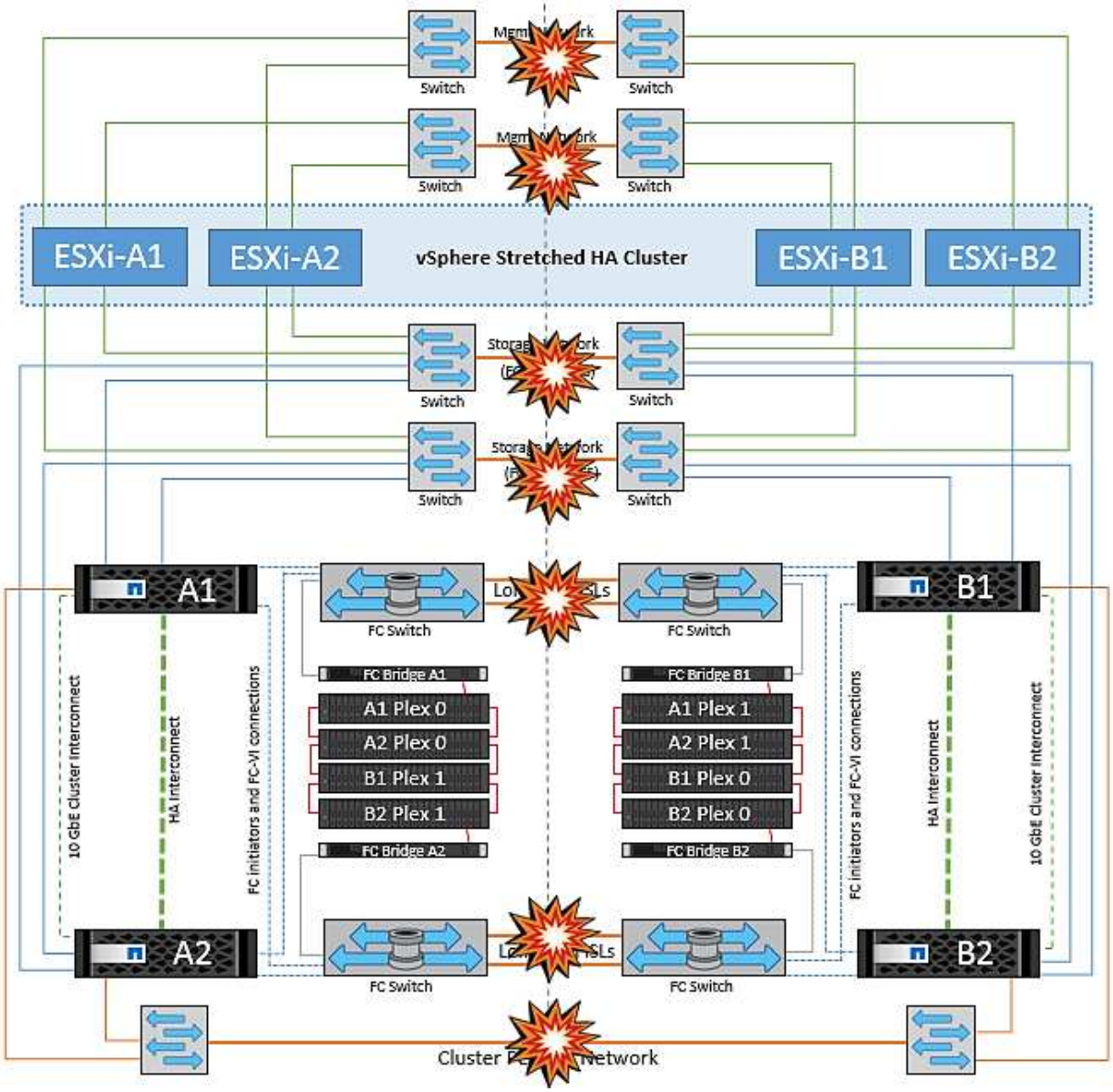
Wenn aus irgendeinem Grund die Affinitätsregel verletzt wurde (z. B. VM1, das von Standort A ausgeführt werden sollte, wo sich seine Festplatten auf lokalen Cluster A-Knoten befinden, auf einem Host an Standort B ausgeführt wird), wird der Remote-Zugriff auf das Laufwerk der virtuellen Maschine über ISL-Links erfolgen.

Aufgrund eines ISL-Verbindungsfehlers kann VM1, der an Standort B ausgeführt wird, nicht auf seine Festplatten schreiben, da die Pfade zum Storage-Volume ausgefallen sind und die jeweilige Virtual Machine nicht verfügbar ist. In diesen Situationen nimmt VMware HA keine Aktion vor, da die Hosts aktiv Heartbeats senden. Diese Virtual Machines müssen an den jeweiligen Standorten manuell ausgeschaltet und eingeschaltet werden. Die folgende Abbildung zeigt eine VM, die gegen eine DRS Affinitätsregel verstößt.

Alle Interswitch-Fehler oder komplette Rechenzentrumspartition

In diesem Szenario sind alle ISL-Verbindungen zwischen den Standorten ausgefallen und beide Standorte voneinander isoliert. Wie bereits in früheren Szenarien erläutert, wie z. B. ISL-Fehler im Managementnetzwerk und im Speichernetzwerk, werden die virtuellen Maschinen bei einem vollständigen ISL-Ausfall nicht beeinträchtigt.

Nachdem ESXi-Hosts zwischen Standorten partitioniert wurden, prüft der vSphere HA-Agent auf Datastore-Heartbeats. An jedem Standort sind die lokalen ESXi-Hosts in der Lage, die Datastore-Heartbeats auf ihr jeweiliges Lese-/Schreibvolumen/LUN zu aktualisieren. Hosts an Standort A gehen davon aus, dass die anderen ESXi-Hosts an Standort B ausgefallen sind, da keine Netzwerk-/Datastore-Heartbeats vorhanden sind. VSphere HA an Standort A versucht, die virtuellen Maschinen von Standort B neu zu starten, was schließlich fehlschlägt, da die Datastores von Standort B aufgrund eines Storage-ISL-Fehlers nicht verfügbar sind. Eine ähnliche Situation wiederholt sich in Standort B.



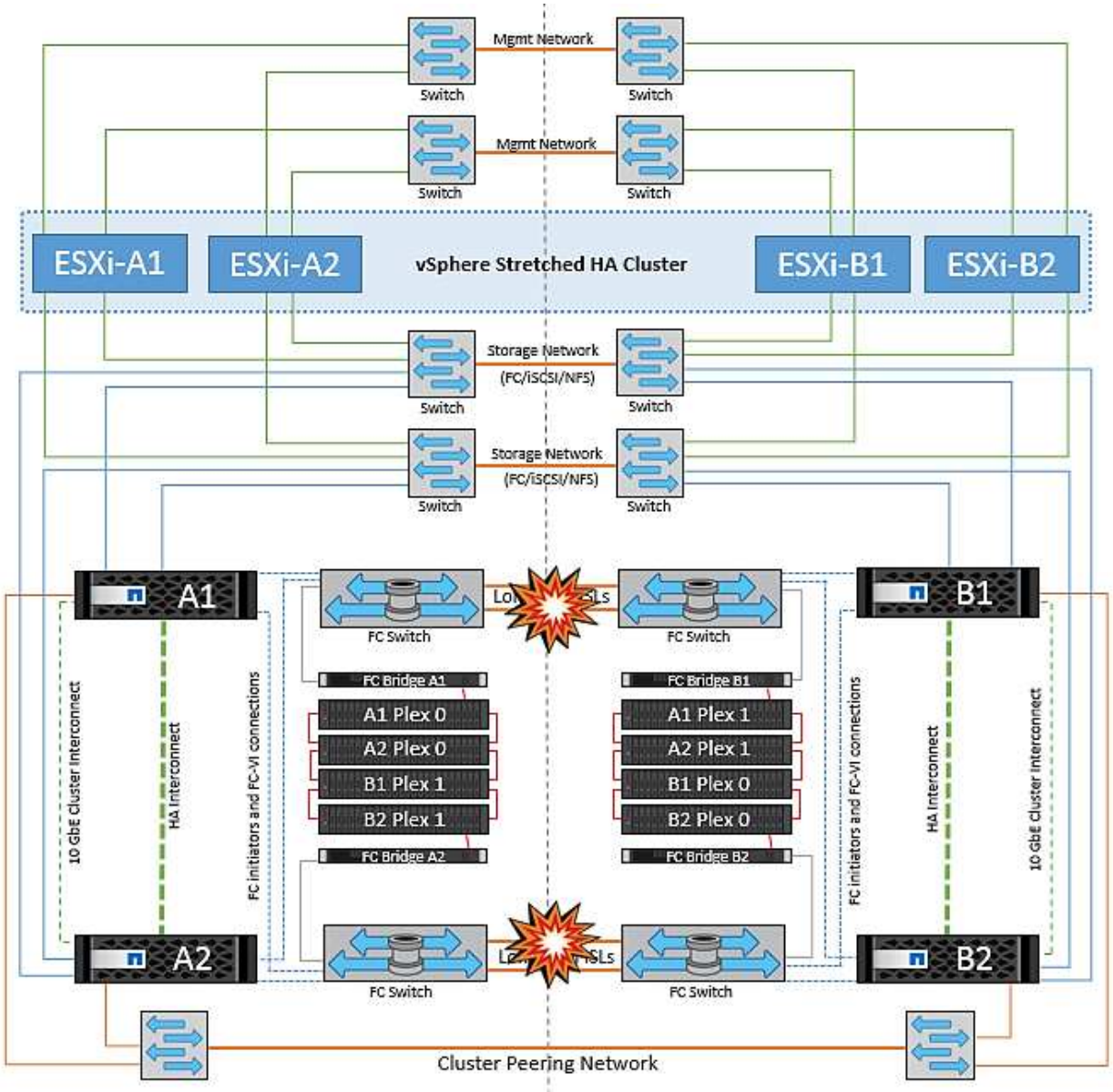
NetApp empfiehlt, festzustellen, ob eine Virtual Machine gegen die DRS Regeln verstoßen hat. Alle virtuellen Maschinen, die von einem Remote-Standort aus ausgeführt werden, sind ausgefallen, da sie nicht auf den Datastore zugreifen können, und vSphere HA startet diese virtuelle Maschine am lokalen Standort neu. Nachdem die ISL-Links wieder online sind, wird die virtuelle Maschine, die am Remote-Standort ausgeführt wurde, abgebrochen, da es nicht zwei Instanzen virtueller Maschinen geben kann, die mit denselben MAC-Adressen ausgeführt werden.

Verbindungsfehler zwischen Switches auf beiden Fabrics in NetApp MetroCluster

In einem Szenario, in dem ein oder mehrere ISLs ausfallen, wird der Datenverkehr über die verbleibenden Links fortgesetzt. Wenn alle ISLs auf beiden Fabrics ausfallen, sodass kein Link zwischen den Standorten für die Storage- und NVRAM-Replizierung vorhanden ist, stellt jeder Controller weiterhin seine lokalen Daten bereit. Bei mindestens einer ISL wird die Neusynchronisierung aller Plexe automatisch durchgeführt.

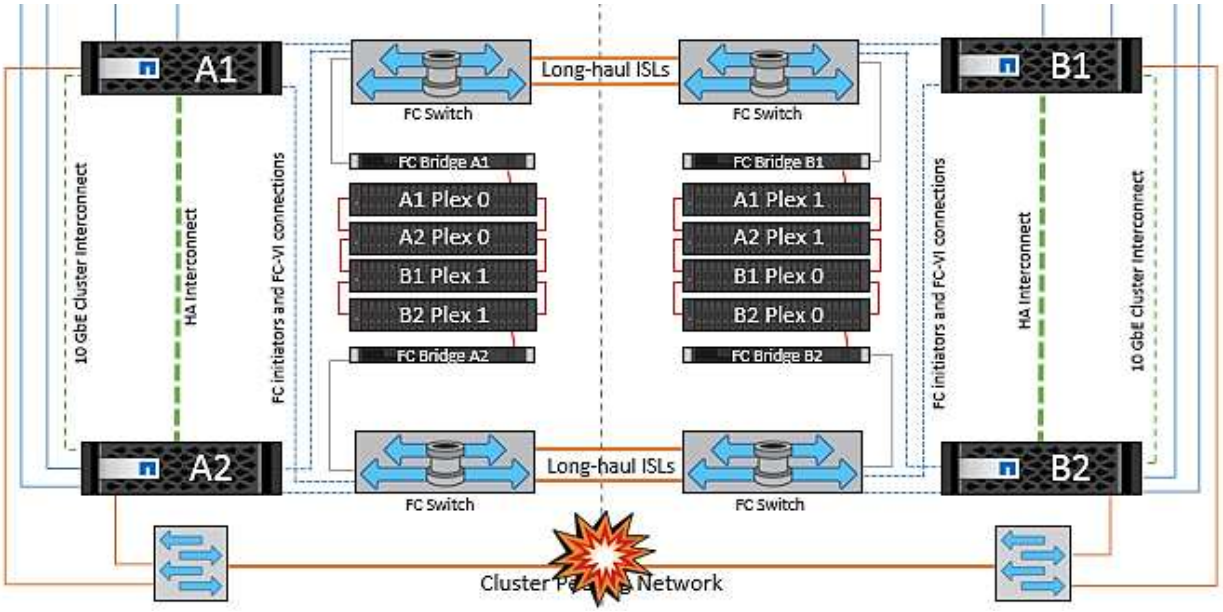
Alle Schreibvorgänge, die nach einem Ausfall aller ISLs stattfinden, werden nicht auf den anderen Standort gespiegelt. Bei einem Disaster-Switchover käme es, während sich die Konfiguration in diesem Zustand befindet, zu einem Verlust der nicht synchronisierten Daten. In diesem Fall ist ein manueller Eingriff für die Wiederherstellung nach der Umschaltung erforderlich. Wenn es wahrscheinlich ist, dass über einen längeren

Zeitraum keine ISLs verfügbar sind, kann ein Administrator alle Datenservices herunterfahren, um bei Bedarf ein Switchover im Notfall zu verhindern, dass Daten verloren gehen. Die Durchführung dieser Maßnahme sollte mit der Wahrscheinlichkeit einer Katastrophe abgewogen werden, die eine Umschaltung erfordert, bevor mindestens eine ISL verfügbar wird. Wenn ISLs in einem kaskadierenden Szenario ausfallen, könnte ein Administrator alternativ eine geplante Umschaltung zu einem der Standorte auslösen, bevor alle Links fehlgeschlagen sind.



Verbindungsfehler Bei Peered Cluster

In einem Peering-Cluster-Link-Ausfallszenario, da die Fabric-ISLs noch aktiv sind, werden die Datenservices (Lese- und Schreibvorgänge) an beiden Standorten auf beiden Plexen fortgesetzt. Jegliche Änderungen an der Cluster-Konfiguration (beispielsweise das Hinzufügen einer neuen SVM, die Bereitstellung eines Volumes oder einer LUN in einer vorhandenen SVM) können nicht an den anderen Standort weitergegeben werden. Diese werden in den lokalen CRS-Metadaten-Volumes aufbewahrt und bei der Wiederherstellung der Peering-Cluster-Verbindung automatisch an das andere Cluster weitergegeben. Wenn eine erzwungene Umschaltung erforderlich ist, bevor der Peered Cluster-Link wiederhergestellt werden kann, werden ausstehende Cluster-Konfigurationsänderungen automatisch von der replizierten Remote-Kopie der Metadaten-Volumes am noch verbleibenden Standort im Rahmen der Umschaltung eingespielt.



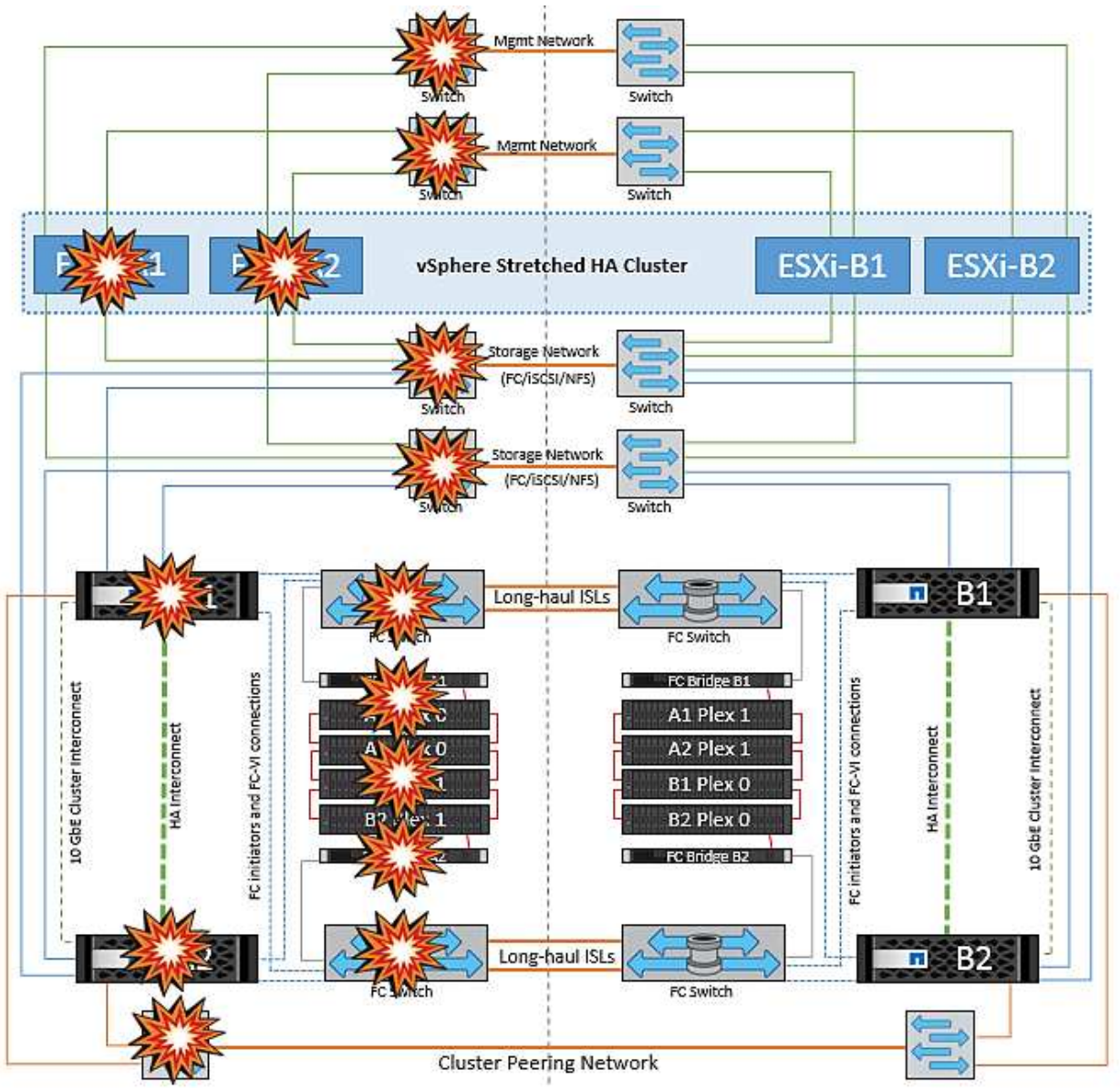
Kompletter Standortausfall

In einem kompletten Standort-A-Fehlerszenario erhalten die ESXi-Hosts an Standort B keinen Netzwerk-Heartbeat von den ESXi-Hosts an Standort A, weil sie ausgefallen sind. Der HA-Master an Standort B überprüft, ob die Datastore-Heartbeats nicht vorhanden sind, deklariert die Hosts an Standort A als fehlgeschlagen und versucht, die virtuellen Maschinen an Standort A an Standort B neu zu starten In diesem Zeitraum führt der Speicheradministrator eine Umschaltung durch, um die Dienste der ausgefallenen Nodes am noch intakten Standort wiederaufzunehmen. Dadurch werden alle Speicherservices von Standort A an Standort B wiederhergestellt Nachdem die Volumes oder LUNs an Standort A an Standort B verfügbar sind, versucht der HA-Master-Agent, die virtuellen Maschinen am Standort A an Standort B neu zu starten

Wenn der Versuch des vSphere HA Master-Agenten, eine VM neu zu starten, fehlschlägt (d. h. sie wird registriert und eingeschaltet), wird der Neustart nach einer Verzögerung erneut durchgeführt. Die Verzögerung zwischen den Neustarts kann auf maximal 30 Minuten konfiguriert werden. VSphere HA versucht diese Neustarts für eine maximale Anzahl von Versuchen (standardmäßig sechs Versuche).

Der HA-Master startet die Neustartversuche nicht, bis der Platzierungsmanager den geeigneten Storage findet. Im Falle eines vollständigen Standortausfalls steht dies also nach der Umschaltung zur Verfügung.

Wenn Standort A umgeschaltet wurde, kann ein nachträglicher Ausfall eines der noch intakten Knoten Standort B nahtlos durch einen Failover auf den noch intakten Knoten bewältigt werden. In diesem Fall wird die Arbeit von vier Nodes jetzt nur von einem Node ausgeführt. Die Wiederherstellung würde in diesem Fall eine Rückgabe an den lokalen Knoten bedeuten. Wenn Standort A wiederhergestellt wird, wird ein Switchback-Vorgang durchgeführt, um den stabilen Konfigurationsbetrieb wiederherzustellen.



Produktsicherheit

ONTAP Tools für VMware vSphere

Das Software Engineering mit ONTAP Tools für VMware vSphere nutzt die folgenden sicheren Entwicklungsaktivitäten:

- **Threat Modeling.** der Zweck der Bedrohungsmodellierung ist es, Sicherheitslücken in einem Feature, einer Komponente oder einem Produkt frühzeitig im Lebenszyklus der Softwareentwicklung zu entdecken. Ein Bedrohungsmodell ist eine strukturierte Darstellung aller Informationen, die die Sicherheit einer Anwendung beeinflussen. Im Wesentlichen ist es ein Blick auf die Anwendung und ihre Umgebung durch die Linsen der Sicherheit.
- **Dynamic Application Security Testing (DAST).** Diese Technologie wurde entwickelt, um gefährdete Bedingungen für Anwendungen im laufenden Zustand zu erkennen. DAST testet die freigesetzten HTTP- und HTML-Schnittstellen von Web-enable-Anwendungen.
- **Codewährung von Drittanbietern.** im Rahmen der Softwareentwicklung mit Open-Source-Software (OSS) müssen Sie Sicherheitslücken schließen, die mit jedem OSS in Ihr Produkt integriert werden

könnten. Dies ist ein fortdauernde Bemühung, da bei einer neuen OSS-Version möglicherweise jederzeit eine neu entdeckte Sicherheitsanfälligkeit gemeldet wird.

- **Schwachstellenscans.** Zweck der Schwachstellenanalyse ist es, häufige und bekannte Sicherheitslücken in NetApp Produkten zu erkennen, bevor diese bei den Kunden freigegeben werden.
- **Penetrationstest.** Penetrationstest ist der Prozess, um ein System, eine Web-Anwendung oder ein Netzwerk zu bewerten, um Sicherheitslücken zu finden, die von einem Angreifer ausgenutzt werden könnten. Penetrationstests (Penetrationstests) bei NetApp werden von einer Gruppe genehmigter und vertrauenswürdiger Drittanbieter durchgeführt. Ihr Testumfang umfasst die Einleitung von Angriffen gegen eine Anwendung oder Software ähnlich wie feindliche Eindringlinge oder Hacker mit ausgereiften Methoden oder Tools zur Ausbeutung.

Produktsicherheitsfunktionen

Die ONTAP Tools für VMware vSphere beinhalten in jeder Version die folgenden Sicherheitsfunktionen.

- **Anmeldebanner** SSH ist standardmäßig deaktiviert und erlaubt nur einmalige Anmeldungen, wenn sie über die VM-Konsole aktiviert sind. Das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen Benutzernamen in die Anmeldeaufforderung eingegeben hat:

  WARNUNG: der unerlaubte Zugriff auf dieses System ist verboten und wird gesetzlich verfolgt. Durch den Zugriff auf dieses System erklären Sie sich damit einverstanden, dass Ihre Maßnahmen überwacht werden können, wenn eine unbefugte Nutzung vermutet wird.

  Nachdem der Benutzer die Anmeldung über den SSH-Kanal abgeschlossen hat, wird der folgende Text angezeigt:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC).** ONTAP Tools verfügen über zwei Arten von RBAC-Steuerungsoptionen:
  - Native vCenter Server-Berechtigungen
  - Spezifische Berechtigungen für vCenter Plug-in Weitere Informationen finden Sie unter "Dieser Link".
- **Verschlüsselte Kommunikationskanäle.** Alle externen Kommunikation erfolgt über HTTPS mit Version 1.2 von TLS.
- **Minimal Port Exposure.** nur die benötigten Ports sind an der Firewall geöffnet.

  In der folgenden Tabelle werden die Details zum offenen Anschluss beschrieben.

TCP v4/v6-Port #	Richtung	Funktion
8143	Eingehend	HTTPS-Verbindungen für REST-API
8043	Eingehend	HTTPS-Verbindungen

TCP v4/v6-Port #	Richtung	Funktion
9060	Eingehend	HTTPS-Verbindungen Wird für SOAP-über-https-Verbindungen verwendet Dieser Port muss geöffnet werden, damit ein Client eine Verbindung zum ONTAP Tools API-Server herstellen kann.
22	Eingehend	SSH (standardmäßig deaktiviert)
9080	Eingehend	HTTPS-Verbindungen - VP und SRA - nur interne Verbindungen von Loopback
9083	Eingehend	HTTPS-Verbindungen – VP und SRA Wird für SOAP-über-https-Verbindungen verwendet
1162	Eingehend	VP SNMP-Trap-Pakete
1527	Nur zur internen Nutzung	Derby-Datenbank-Port, nur zwischen diesem Computer und sich selbst, externe Verbindungen nicht akzeptiert — nur interne Verbindungen
443	Bidirektional	Wird für Verbindungen zu ONTAP-Clustern verwendet

- **Unterstützung für Zertifizierungsstelle (CA) signierte Zertifikate.** ONTAP Tools für VMware vSphere unterstützt CA signierte Zertifikate. Siehe das "kb-Artikel" Finden Sie weitere Informationen.
- **Audit Logging.** Supportpakete können heruntergeladen werden und sind äußerst detailliert. Die ONTAP Tools protokollieren alle Benutzer-Login- und -Abmeldeaktivitäten in einer separaten Protokolldatei. VASA API-Aufrufe werden in einem dedizierten VASA Audit Log (Local cxf.log) protokolliert.
- **Passwortrichtlinien.** folgende Kennwortrichtlinien werden befolgt:
  - Passwörter werden nicht in Protokolldateien protokolliert.
  - Passwörter werden nicht im Klartext kommuniziert.
  - Während des Installationsvorgangs selbst werden Passwörter konfiguriert.
  - Der Passwortverlauf ist ein konfigurierbarer Parameter.
  - Das Mindestalter des Kennworts ist auf 24 Stunden festgelegt.
  - Die Felder für das Kennwort werden automatisch ausgefüllt.
  - ONTAP-Tools verschlüsselt alle gespeicherten Anmeldeinformationen mithilfe von SHA256 Hashing.

SnapCenter Plug-in VMware vSphere

Das NetApp SnapCenter Plug-in für VMware vSphere nutzt folgende sichere Entwicklungsaktivitäten:

- **Threat Modeling.** der Zweck der Bedrohungsmodellierung ist es, Sicherheitslücken in einem Feature,

einer Komponente oder einem Produkt frühzeitig im Lebenszyklus der Softwareentwicklung zu entdecken. Ein Bedrohungsmodell ist eine strukturierte Darstellung aller Informationen, die die Sicherheit einer Anwendung beeinflussen. Im Wesentlichen ist es ein Blick auf die Anwendung und ihre Umgebung durch die Linsen der Sicherheit.

- **Dynamic Application Security Testing (DAST).** Technologien, die entwickelt wurden, um gefährdete Bedingungen für Anwendungen in ihrem laufenden Zustand zu erkennen. DAST testet die freigesetzten HTTP- und HTML-Schnittstellen von Web-enable-Anwendungen.
- **Codewährung von Drittanbietern.** im Rahmen der Entwicklung von Software und der Verwendung von Open-Source-Software (OSS) ist es wichtig, Sicherheitslücken zu beheben, die mit OSS verbunden sein könnten, die in Ihr Produkt integriert wurden. Dies ist ein kontinuierlicher Aufwand, da bei der Version der OSS-Komponente eine neu entdeckte Sicherheitsanfälligkeit jederzeit gemeldet wird.
- **Schwachstellenscans.** Zweck der Schwachstellenanalyse ist es, häufige und bekannte Sicherheitslücken in NetApp Produkten zu erkennen, bevor diese bei den Kunden freigegeben werden.
- **Penetrationstest.** Penetrationstest ist der Prozess, um ein System, eine Web-Anwendung oder ein Netzwerk zu evaluieren, um Sicherheitslücken zu finden, die von einem Angreifer ausgenutzt werden könnten. Penetrationstests (Penetrationstests) bei NetApp werden von einer Gruppe genehmigter und vertrauenswürdiger Drittanbieter durchgeführt. Ihr Testumfang umfasst die Einleitung von Angriffen gegen eine Anwendung oder Software wie feindliche Eindringlinge oder Hacker mit ausgereiften Exploitationsmethoden oder -Tools.
- **Aktion zur Reaktion auf Produktsicherheitsvorfälle.** Sicherheitsschwachstellen werden sowohl intern als auch extern im Unternehmen entdeckt und können ein ernsthaftes Risiko für den Ruf von NetApp darstellen, wenn sie nicht rechtzeitig behoben werden. Zur Erleichterung dieses Prozesses meldet ein PSIRT (Product Security Incident Response Team) die Sicherheitsanfälligkeiten und verfolgt diese.

Produktsicherheitsfunktionen

Das NetApp SnapCenter Plug-in für VMware vSphere umfasst die folgenden Sicherheitsfunktionen in jeder Version:

- **Eingeschränkter Shell-Zugriff.** SSH ist standardmäßig deaktiviert, und einmalige Anmeldungen sind nur erlaubt, wenn sie über die VM-Konsole aktiviert sind.
- **Zugangswarnung im Anmeldebanner.** das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen Benutzernamen in die Anmeldeaufforderung eingegeben hat:

  WARNUNG: der unerlaubte Zugriff auf dieses System ist verboten und wird gesetzlich verfolgt. Durch den Zugriff auf dieses System erklären Sie sich damit einverstanden, dass Ihre Maßnahmen überwacht werden können, wenn eine unbefugte Nutzung vermutet wird.

  Nachdem der Benutzer die Anmeldung über den SSH-Kanal abgeschlossen hat, wird die folgende Ausgabe angezeigt:

```
Linux vsc1 4.19.0-12-amd64 #1 SMP Debian 4.19.152-1 (2020-10-18) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

- **Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC).** ONTAP Tools verfügen über

zwei Arten von RBAC-Steuerungsoptionen:

  - Native vCenter Server-Berechtigungen.
  - Spezifische Berechtigungen für VMware vCenter Plug-in Weitere Informationen finden Sie unter "Rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC)".

- **Verschlüsselte Kommunikationskanäle.** Alle externen Kommunikation erfolgt über HTTPS mit TLS.
- **Minimal Port Exposure.** nur die benötigten Ports sind an der Firewall geöffnet.

Die folgende Tabelle enthält die Details zum offenen Anschluss.

TCP v4/v6-Portnummer	Funktion
8144	HTTPS-Verbindungen für REST-API
8080	HTTPS-Verbindungen für OVA GUI
22	SSH (standardmäßig deaktiviert)
3306	MySQL (nur interne Verbindungen; externe Verbindungen standardmäßig deaktiviert)
443	Nginx (Datensicherungsservices)

- **Unterstützung für Zertifizierungsstelle (CA) signierte Zertifikate.** SnapCenter Plug-in für VMware vSphere unterstützt die Funktion von CA signierten Zertifikaten. Siehe "Erstellen und/oder Importieren eines SSL-Zertifikats in das SnapCenter Plug-in für VMware vSphere (SCV)".
- **Passwortrichtlinien.** die folgenden Kennwortrichtlinien sind in Kraft:
  - Passwörter werden nicht in Protokolldateien protokolliert.
  - Passwörter werden nicht im Klartext kommuniziert.
  - Während des Installationsvorgangs selbst werden Passwörter konfiguriert.
  - Alle Anmeldeinformationen werden mit SHA256 Hashing gespeichert.
- **Basis Betriebssystem-Image.** das Produkt wird mit Debian Base OS für OVA ausgeliefert, mit eingeschränktem Zugriff und Shell-Zugriff. So wird die Angriffsfläche reduziert. Jedes Betriebssystem der SnapCenter Version wird mit den neuesten Sicherheits-Patches aktualisiert, die für maximale Sicherheit verfügbar sind.

NetApp entwickelt Softwarefunktionen und Sicherheits-Patches zu den SnapCenter Plug-ins für die VMware vSphere Appliance und gibt sie anschließend dem Kunden als gebündelte Software-Plattform frei. Da diese Appliances bestimmte Linux Unterbetriebssystem-Abhängigkeiten sowie unsere proprietäre Software umfassen, empfiehlt NetApp, am Unterbetriebssystem keine Änderungen vorzunehmen, da dies ein hohes Potenzial hat, die NetApp Appliance zu beeinträchtigen. Dies könnte sich darauf auswirken, inwieweit NetApp die Appliance unterstützt. NetApp empfiehlt, unsere neueste Code-Version für Appliances zu testen und zu implementieren, da sie veröffentlicht werden, um sicherheitsbezogene Probleme zu patchen.

Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere

Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere 9.13

Der Security Hardening Guide für ONTAP-Tools für VMware vSphere enthält umfassende Anweisungen zur Konfiguration der sichersten Einstellungen.

Diese Anleitungen gelten sowohl für die Anwendungen als auch für das Gastbetriebssystem des Geräts selbst.

Überprüfen der Integrität der ONTAP-Tools für VMware vSphere 9.13-Installationspakete

Es gibt zwei Methoden, mit denen Kunden die Integrität ihrer Installationspakete für ONTAP-Tools überprüfen können.

1. Überprüfen der Prüfsummen
2. Überprüfen der Signatur

Prüfsummen werden auf den Download-Seiten der OTV-Installationspakete zur Verfügung gestellt. Benutzer müssen die Prüfsummen der heruntergeladenen Pakete anhand der auf der Download-Seite angegebenen Prüfsumme überprüfen.

Überprüfen der Signatur der ONTAP-Tools OVA

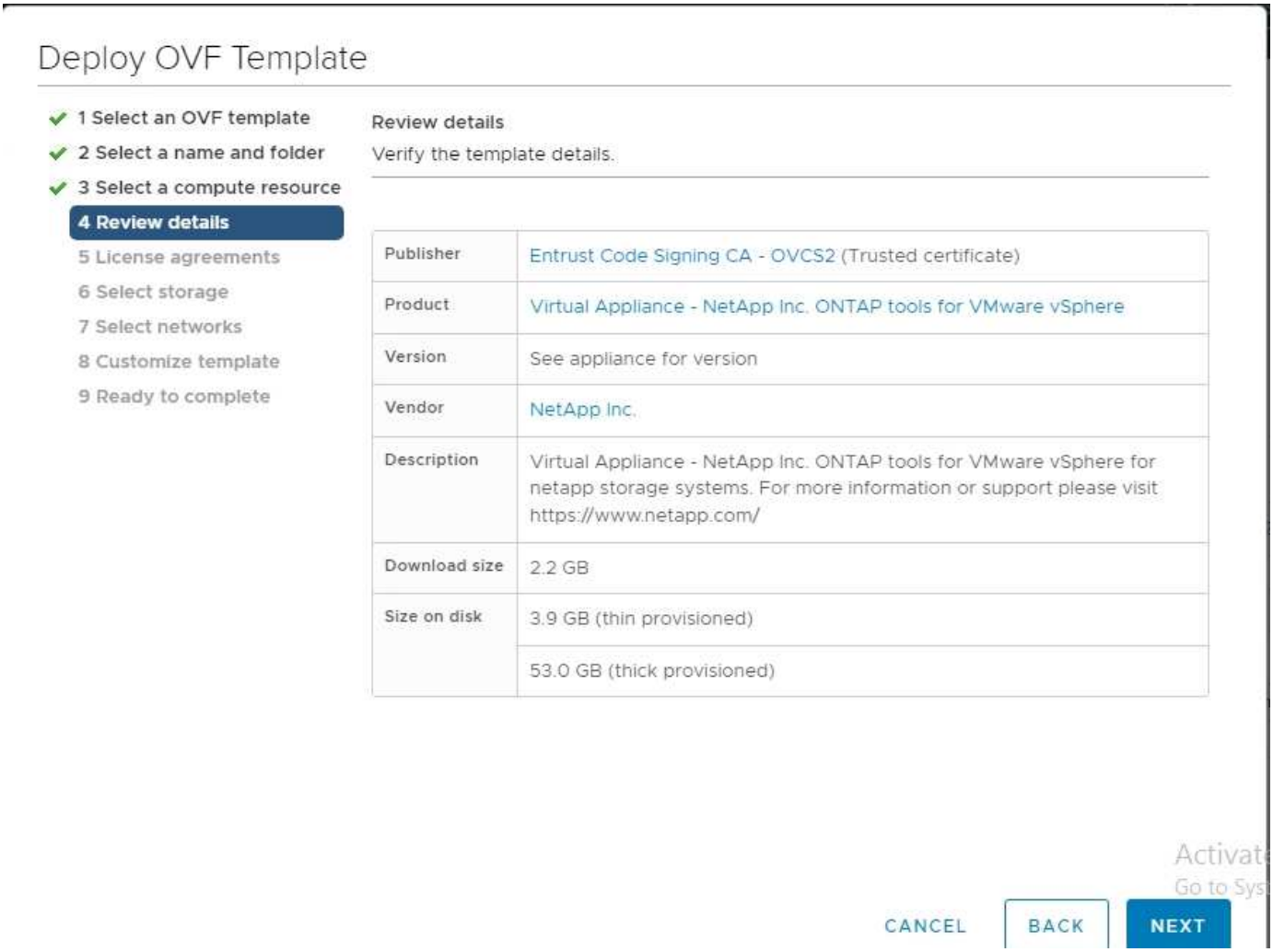
Das vApp-Installationspaket wird in Form eines Tarballs geliefert. Dieser Tarball enthält Zwischen- und Root-Zertifikate für das virtuelle Gerät sowie eine README-Datei und ein OVA-Paket. Die README-Datei führt Benutzer dazu, wie die Integrität des vApp OVA-Pakets überprüft wird.

Kunden müssen auch das bereitgestellte Root- und Intermediate-Zertifikat auf vCenter Version 7.0U3E und höher hochladen. Bei vCenter-Versionen zwischen 7.0.1 und 7.0.U3E wird die Funktion zur Überprüfung des Zertifikats von VMware nicht unterstützt. Kunden müssen kein Zertifikat für vCenter Version 6.x hochladen

Hochladen des vertrauenswürdigen Stammzertifikats in vCenter

1. Melden Sie sich mit dem VMware vSphere Client beim vCenter Server an.
2. Geben Sie den Benutzernamen und das Kennwort für administrator@vsphere.local oder ein anderes Mitglied der vCenter Single Sign-On-Administratorgruppe an. Wenn Sie während der Installation eine andere Domäne angegeben haben, melden Sie sich als Administrator@mydomain an.
3. Navigieren Sie zur Benutzeroberfläche Zertifikatverwaltung: a. Wählen Sie im Home-Menü Administration aus. b. Klicken Sie unter Zertifikate auf Zertifikatverwaltung.
4. Wenn Sie vom System aufgefordert werden, geben Sie die Anmeldedaten Ihres vCenter-Servers ein.
5. Klicken Sie unter Vertrauenswürdige Stammzertifikate auf Hinzufügen.
6. Klicken Sie auf Durchsuchen, und wählen Sie den Speicherort der .pem-Zertifikatdatei (OTV_OVA_INTER_ROOT_CERT_CHAIN.pem) aus.
7. Klicken Sie Auf Hinzufügen. Das Zertifikat wird dem Store hinzugefügt.

Siehe "Fügen Sie dem Zertifikatspeicher ein vertrauenswürdiges Stammzertifikat hinzu" Finden Sie weitere Informationen. Während der Bereitstellung einer vApp (mithilfe der OVA-Datei) kann die digitale Signatur für das vApp-Paket auf der Seite „Details überprüfen“ überprüft werden. Wenn es sich bei dem heruntergeladenen vApp-Paket um ein Originalprodukt handelt, wird in der Spalte „Publisher“ (Herausgeber) die Option „Vertrauenswürdiges Zertifikat“ angezeigt (wie im folgenden Screenshot).



Überprüfen der Signatur der ONTAP-Tools ISO und SRA tar.gz

NetApp teilt sein Code Signing-Zertifikat mit Kunden auf der Produkt-Download-Seite, zusammen mit den Produkt-Zip-Dateien für OTV-ISO und SRA.tgz.

Aus dem Code-Signing-Zertifikat können Benutzer den öffentlichen Schlüssel wie folgt extrahieren:

```
 #> openssl x509 -in <code-sign-cert, pem file> -pubkey -noout > <public-
key name>
Dann sollte der öffentliche Schlüssel verwendet werden, um die Signatur
für iso und tgz Produkt zip wie unten zu überprüfen:
```

```
 #> openssl dgst -sha256 -verify <public-key> -signature <signature-file>
<binary-name>
Beispiel:
```

```
#> openssl x509 -in OTV_ISO_CERT.pem -pubkey -noout > OTV_ISO.pub
#> openssl dgst -sha256 -verify OTV_ISO.pub -signature netapp-ontap-tools-
for-vmware-vsphere-9.12-upgrade-iso.sig netapp-ontap-tools-for-vmware-
vsphere-9.12-upgrade.iso
Verified OK  => response
```

Ports und Protokolle für ONTAP-Tools 9.13

In dieser Liste sind die erforderlichen Ports und Protokolle aufgeführt, die die Kommunikation zwischen ONTAP Tools für VMware vSphere Server und anderen Einheiten wie gemanagten Storage-Systeme, Servern und anderen Komponenten ermöglichen.

Für OTV erforderliche ein- und ausgehende Ports

Beachten Sie die folgende Tabelle, in der die ein- und ausgehenden Ports aufgeführt sind, die für das ordnungsgemäße Funktionieren der ONTAP-Tools erforderlich sind. Es ist wichtig sicherzustellen, dass nur die in der Tabelle genannten Ports für Verbindungen von Remotecomputern geöffnet sind, während alle anderen Ports für Verbindungen von Remotecomputern gesperrt werden sollten. Dadurch wird die Sicherheit und Sicherheit Ihres Systems gewährleistet.

In der folgenden Tabelle werden die Details zum offenen Anschluss beschrieben.

TCP v4/v6-Port #	Richtung	Funktion
8143	Eingehend	HTTPS-Verbindungen für REST-API
8043	Eingehend	HTTPS-Verbindungen
9060	Eingehend	HTTPS-Verbindungen Wird für SOAP über HTTPS-Verbindungen verwendet Dieser Port muss geöffnet werden, damit ein Client eine Verbindung zum ONTAP Tools API-Server herstellen kann.
22	Eingehend	SSH (standardmäßig deaktiviert)
9080	Eingehend	HTTPS-Verbindungen - VP und SRA - nur interne Verbindungen von Loopback
9083	Eingehend	HTTPS-Verbindungen - VP und SRA Wird für SOAP-Verbindungen über HTTPS verwendet
1162	Eingehend	VP SNMP-Trap-Pakete
8443	Eingehend	Remote-Plug-In
1527	Nur zur internen Nutzung	Derby-Datenbank-Port, nur zwischen diesem Computer und sich selbst, externe Verbindungen nicht akzeptiert - nur interne Verbindungen
8150	Nur zur internen Nutzung	Der Protokollintegritätsservice wird auf dem Port ausgeführt
443	Bidirektional	Wird für Verbindungen zu ONTAP-Clustern verwendet

Steuern des Remote-Zugriffs auf die Derby-Datenbank

Administratoren können mit den folgenden Befehlen auf die derby-Datenbank zugreifen. Der Zugriff ist über die lokale VM der ONTAP-Tools sowie über einen Remote-Server mit den folgenden Schritten möglich:

```
java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
connect 'jdbc:derby://<OTV-
IP>:1527//opt/netapp/vpserver/vvoldb;user=<user>;password=<password>';
```

Beispiel:

```
root@UnifiedVSC:~# java -classpath "/opt/netapp/vpserver/lib/*" org.apache.derby.tools.ij;
ij version 10.15
ij> connect 'jdbc:derby://localhost:1527//opt/netapp/vpserver/vvoldb;user=app;password=[redacted]';
ij> show tables;
TABLE_SCHEM         |TABLE_NAME                    |REMARKS
------------------------------------------------------------------------
SYS                 |SYSALIASES                    |
SYS                 |SYSCHECKS                     |
SYS                 |SYSCOLPERMS                   |
SYS                 |SYSCOLUMNS                    |
SYS                 |SYSCONGLOMERATES              |
SYS                 |SYSCONSTRAINTS                |
SYS                 |SYSDEPENDS                    |
SYS                 |SYSFILES                      |
SYS                 |SYSFOREIGNKEYS                |
SYS                 |SYSKEYS                       |
SYS                 |SYSPERMS                      |
```

ONTAP Tools für VMware vSphere 9.13 Zugriffspunkte (Benutzer)

Mit der Installation der ONTAP Tools für VMware vSphere werden drei Benutzertypen erstellt und verwendet:

1. Systembenutzer: Das root-Benutzerkonto
2. Anwendungsbenutzer: Administratorbenutzer, Benutzerkonten und db-Benutzerkonten
3. Support-Benutzer: Das diag-Benutzerkonto

1. Systembenutzer

System(root) Benutzer wird von ONTAP-Tools-Installation auf dem zugrunde liegenden Betriebssystem (Debian) erstellt.

- Ein Standardsystembenutzer "root" wird auf Debian von der Installation der ONTAP-Tools erstellt. Der Standardwert ist deaktiviert und kann per Ad-hoc-Funktion über die „Wartung“-Konsole aktiviert werden.

2. Anwendungsbenutzer

Der Anwendungsbenutzer wird in ONTAP-Tools als lokaler Benutzer benannt. Diese Benutzer wurden in der Anwendung ONTAP Tools erstellt. In der folgenden Tabelle sind die Typen von Anwendungsbenutzern aufgeführt:

* Benutzer*	Beschreibung
Administratorbenutzer	Es wird während der Installation von ONTAP Tools erstellt, und Benutzer bietet die Anmeldeinformationen während der Bereitstellung der ONTAP Tools. Benutzer haben die Möglichkeit, das 'Passwort' in der 'Wartung'-Konsole zu ändern. Das Passwort läuft in 90 Tagen ab, und Benutzer werden davon ausgehen, dass es sich um dasselbe Passwort handelt.
Wartungsbenutzer	Es wird während der Installation von ONTAP Tools erstellt, und Benutzer bietet die Anmeldeinformationen während der Bereitstellung der ONTAP Tools. Benutzer haben die Möglichkeit, das 'Passwort' in der 'Wartung'-Konsole zu ändern. Dies ist ein Wartungsbenutzer und wird zur Ausführung der Wartungskonsolenoperationen erstellt.
Datenbankbenutzer	Es wird während der Installation von ONTAP Tools erstellt, und Benutzer bietet die Anmeldeinformationen während der Bereitstellung der ONTAP Tools. Benutzer haben die Möglichkeit, das 'Passwort' in der 'Wartung'-Konsole zu ändern. Das Passwort läuft in 90 Tagen ab, und Benutzer werden davon ausgehen, dass es sich um dasselbe Passwort handelt.

3. Support user(diag user)

Während der Installation der ONTAP-Tools wird ein Support-Benutzer erstellt. Dieser Benutzer kann für den Zugriff auf ONTAP-Tools bei Problemen oder Ausfällen im Server und zum Sammeln von Protokollen verwendet werden. Standardmäßig ist dieser Benutzer deaktiviert, kann aber per Ad-hoc-Funktion über die „Wartung“-Konsole aktiviert werden. Beachten Sie, dass dieser Benutzer nach einem bestimmten Zeitraum automatisch deaktiviert wird.

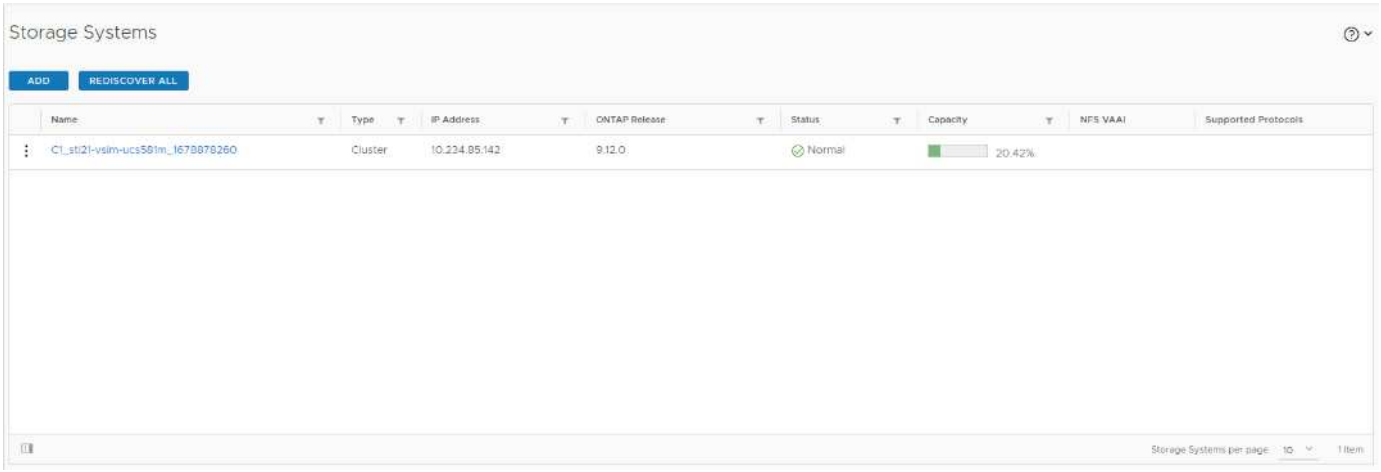
ONTAP Tools 9.13 gegenseitige TLS (zertifikatbasierte Authentifizierung)

ONTAP Version 9.7 und höher unterstützen die gegenseitige TLS-Kommunikation. Ab ONTAP Tools für VMware und vSphere 9.12 wird wechselseitiges TLS für die Kommunikation mit neu hinzugefügten Clustern verwendet (je nach ONTAP Version).

ONTAP

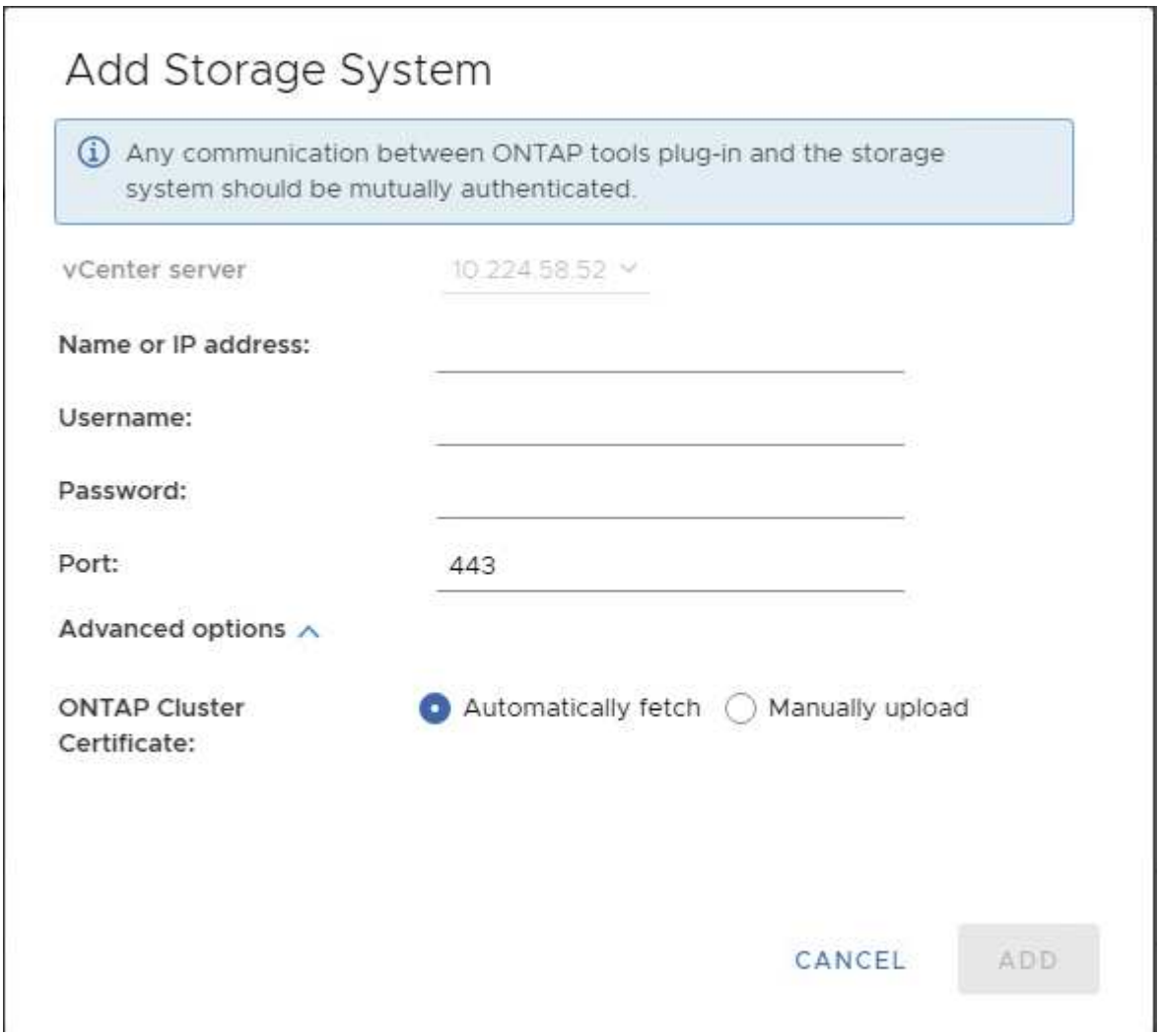
Für alle zuvor hinzugefügten Speichersysteme: Während eines Upgrades werden alle hinzugefügten Speichersysteme automatisch vertrauenswürdig und die zertifikatbasierten Authentifizierungsmechanismen werden konfiguriert.

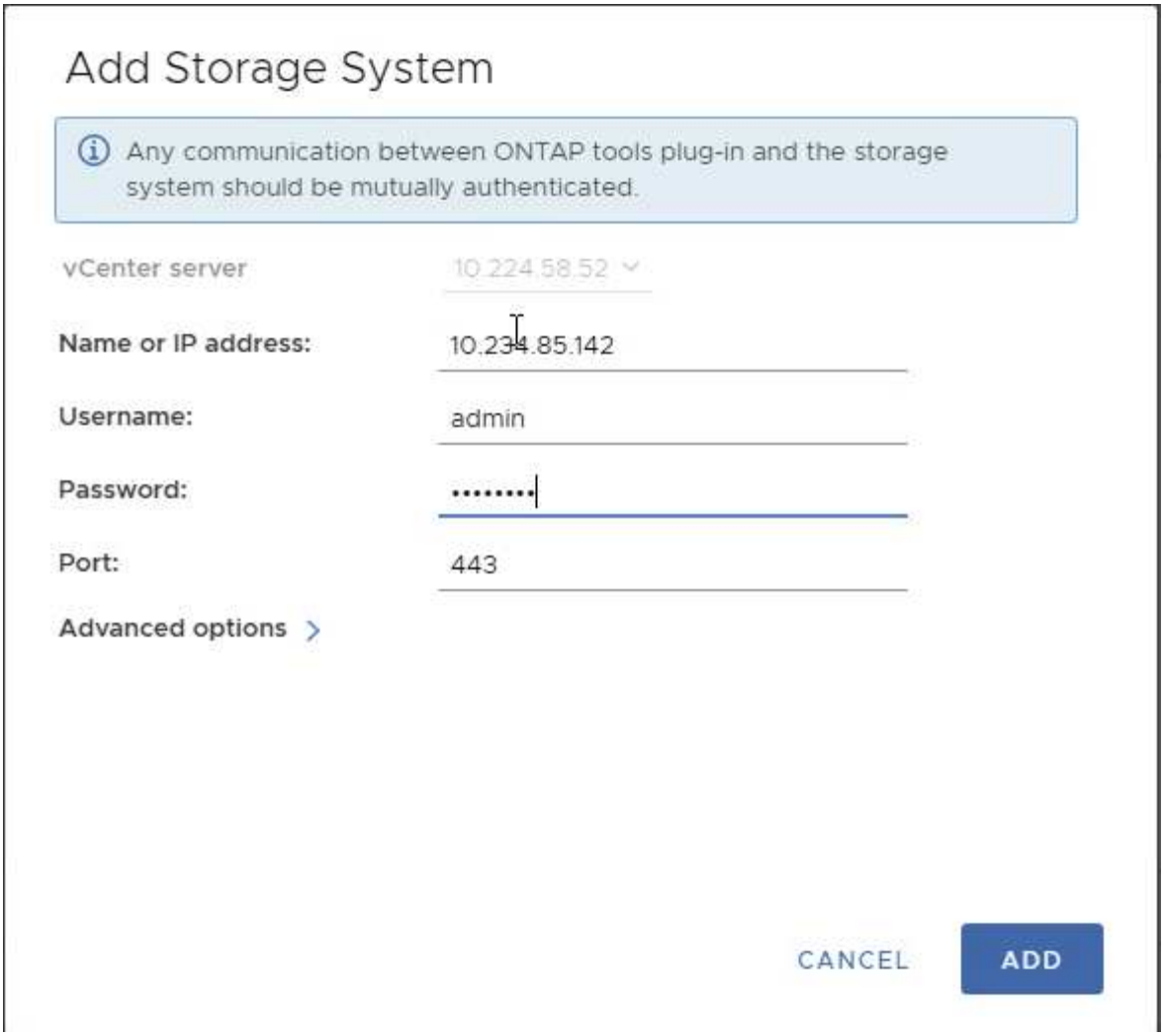
Wie im Screenshot unten gezeigt, zeigt die Cluster-Setup-Seite den Status von Mutual TLS (Certificate-Based Authentication) an, die für jeden Cluster konfiguriert wurden.

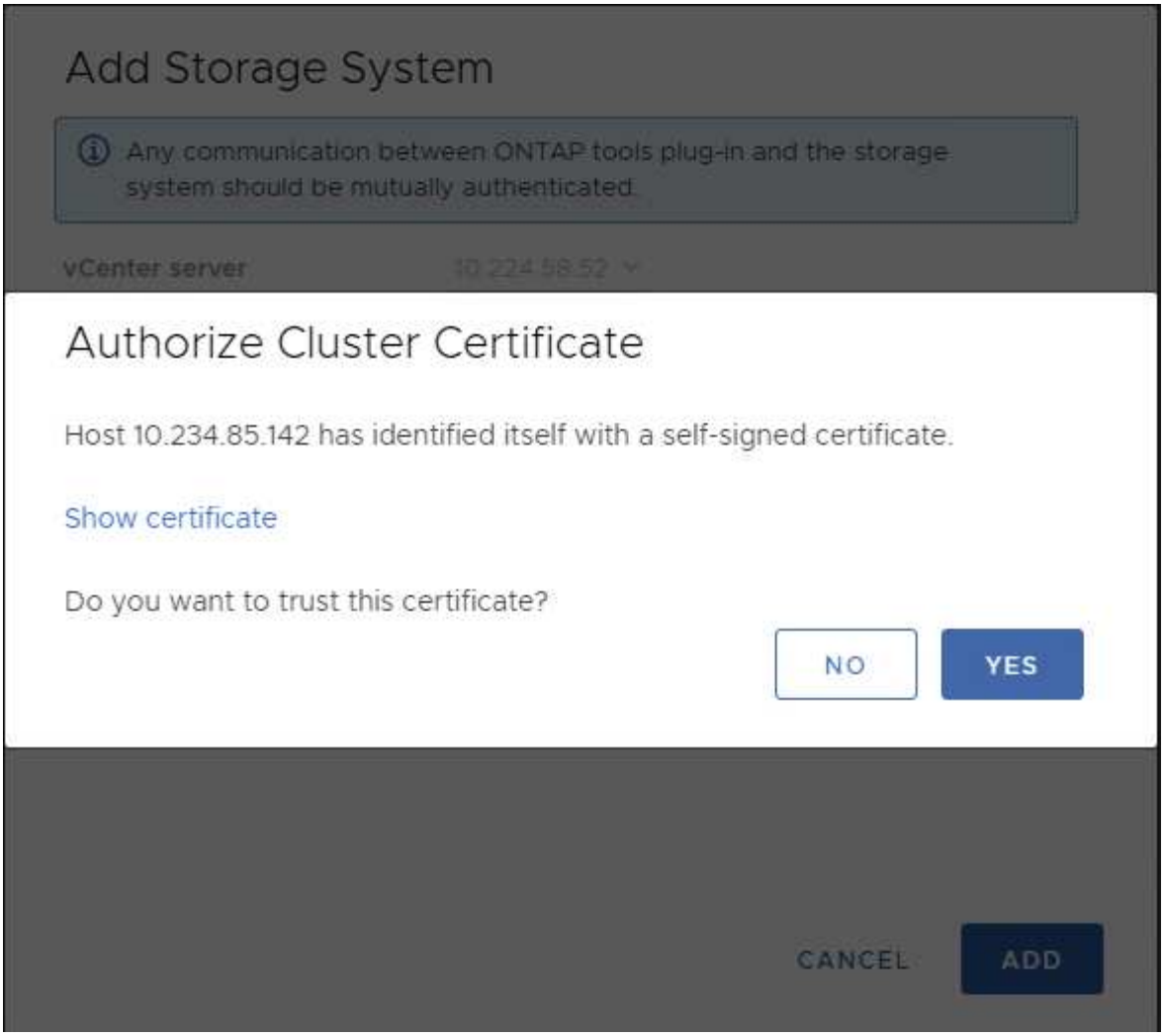


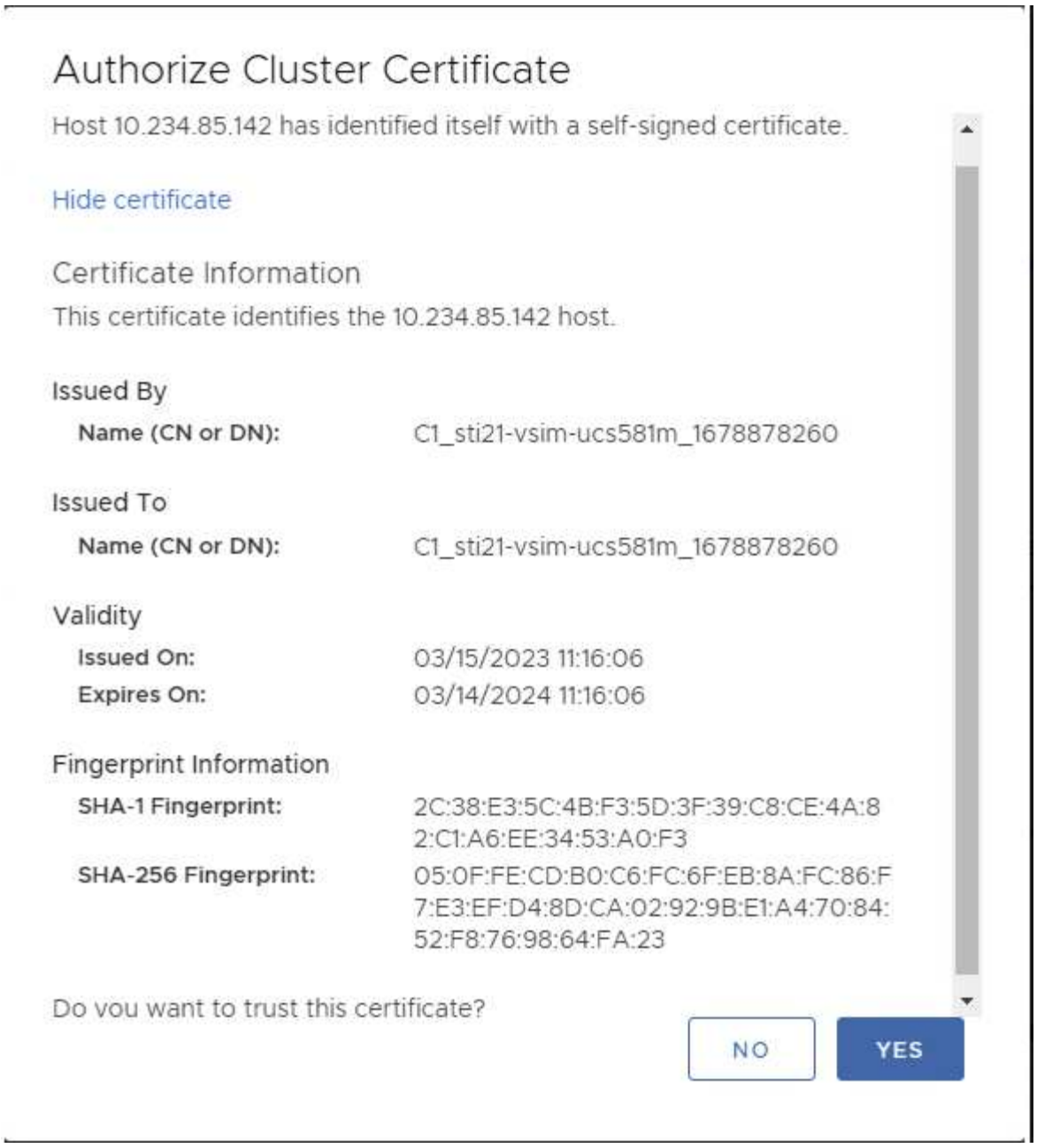
Cluster Hinzufügen

Wenn das hinzugefügte Cluster MTLS unterstützt, wird MTLS während des Cluster-Add-Workflows standardmäßig konfiguriert. Der Benutzer muss hierfür keine Konfiguration vornehmen. Im Screenshot unten wird der Bildschirm angezeigt, der dem Benutzer beim Hinzufügen von Cluster angezeigt wird.




Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
10.224.58.52
Name or IP address:
10.234.85.142
Username:
admin
Password:
Port:
443
Advanced options
CANCEL
ADD

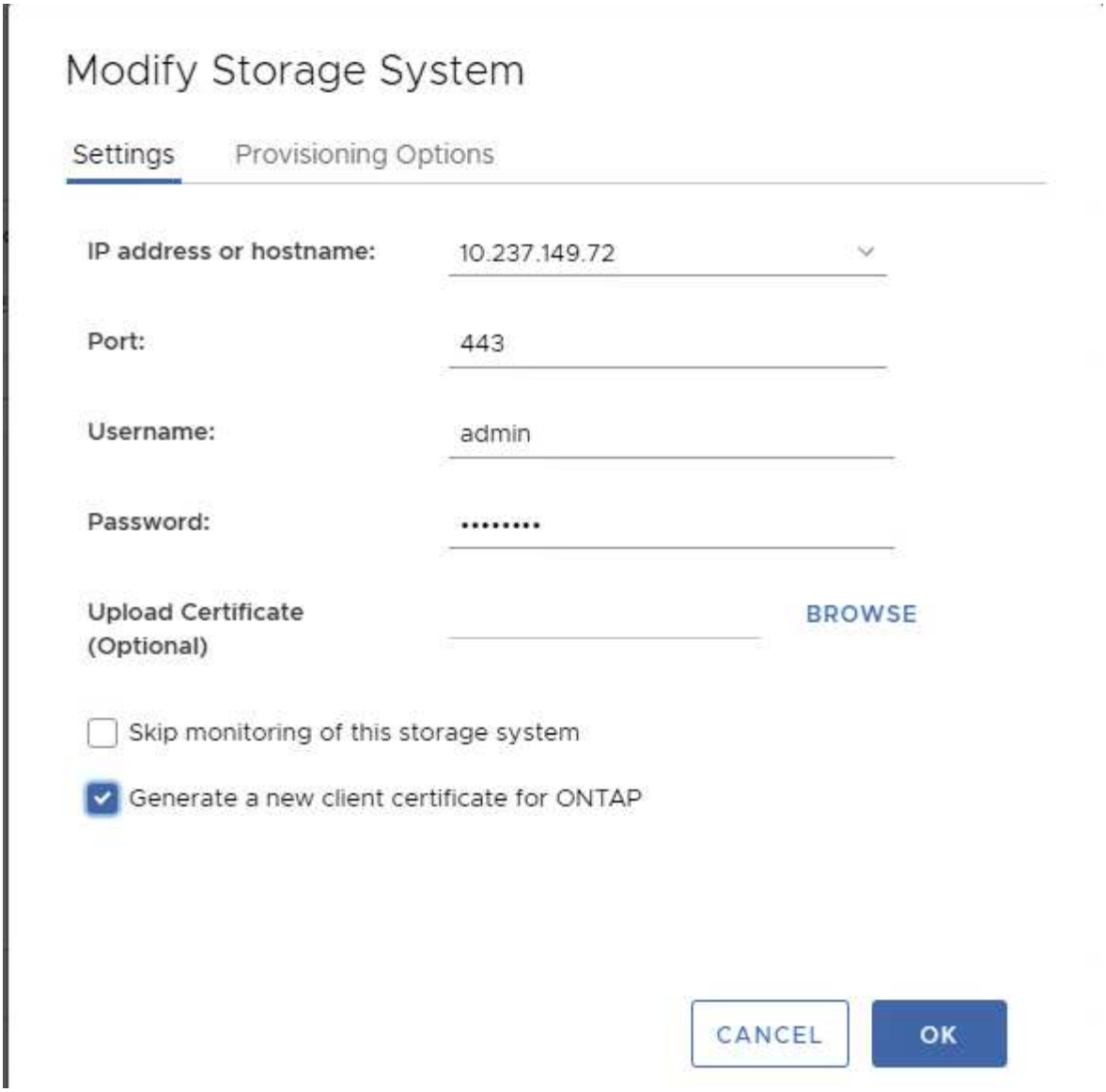

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
Authorize Cluster Certificate
Host 10.234.85.142 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
ADD

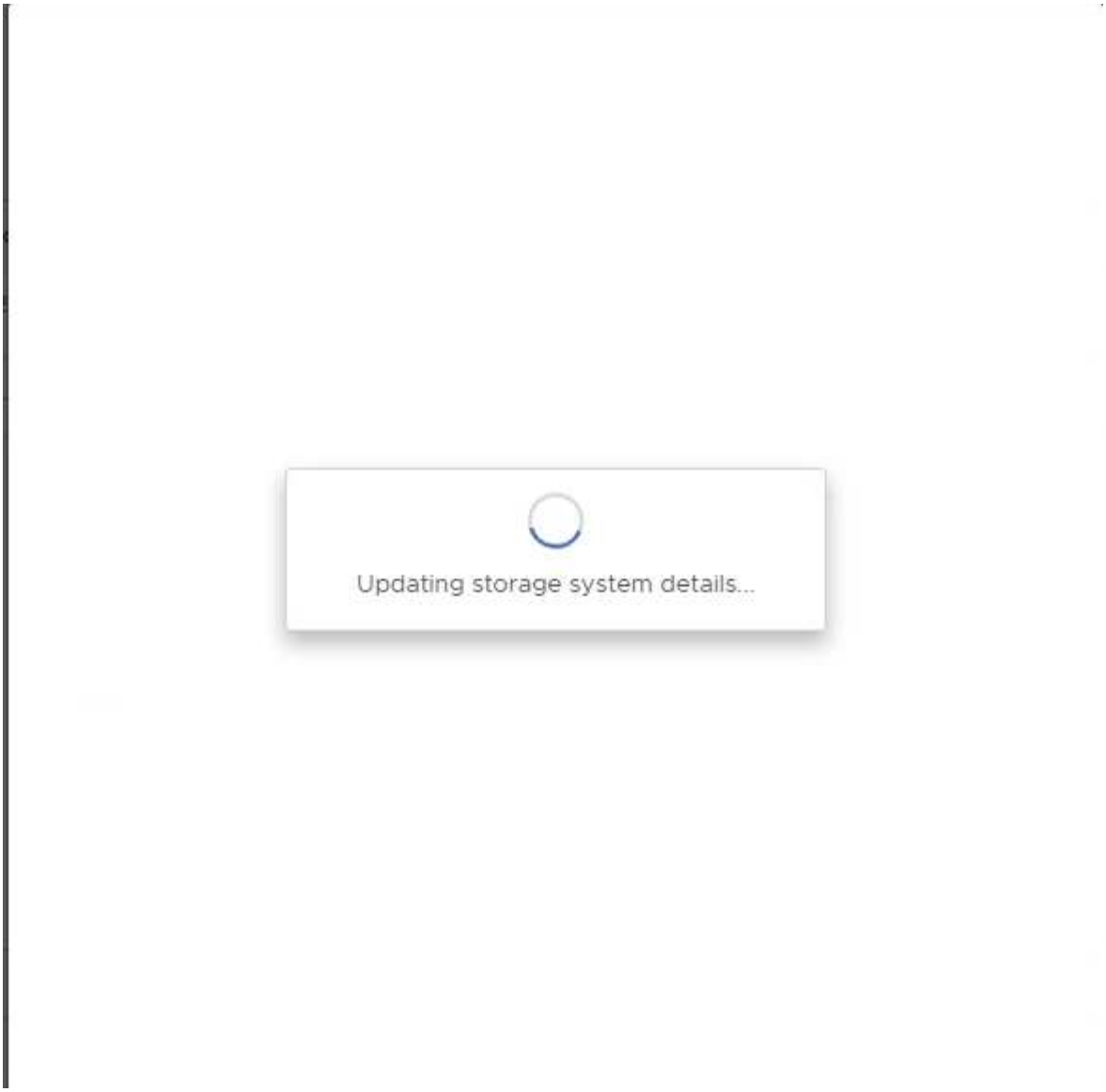


Cluster-Bearbeitung

Während der Cluster-Bearbeitung gibt es zwei Szenarien:

- Wenn das ONTAP-Zertifikat abläuft, muss der Benutzer das neue Zertifikat erhalten und hochladen.
- Wenn das OTV-Zertifikat abläuft, kann der Benutzer es durch Aktivieren des Kontrollkästchens neu generieren.
  - *Generieren Sie ein neues Client-Zertifikat für ONTAP.*


Modify Storage System
Settings
Provisioning Options
IP address or hostname:
10.237.149.72
Port:
443
Username:
admin
Password:
Upload Certificate (Optional)
BROWSE
Skip monitoring of this storage system
Generate a new client certificate for ONTAP
CANCEL
OK



ONTAP Tools 9.13 HTTPS-Zertifikat

Standardmäßig verwendet ONTAP-Tools ein selbstsigniertes Zertifikat, das bei der Installation automatisch erstellt wird, um den HTTPS-Zugriff auf die Web-Benutzeroberfläche zu sichern. Funktionen der ONTAP Tools:

1. HTTPS-Zertifikat neu generieren

Während der Installation der ONTAP-Tools wird ein HTTPS-CA-Zertifikat installiert und das Zertifikat wird im Keystore gespeichert. Der Benutzer hat die Möglichkeit, das HTTPS-Zertifikat über die maint-Konsole neu zu generieren.

Auf die oben genannten Optionen kann in der *maint*-Konsole zugegriffen werden, indem Sie zu *'Anwendungskonfiguration' → 'Zertifikate erneut generieren' navigieren.*

Anmeldebanner für ONTAP Tools 9.13

Das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen

Benutzernamen in die Anmeldeaufforderung eingegeben hat. Beachten Sie, dass SSH standardmäßig deaktiviert ist und nur einmalige Anmeldungen zulässt, wenn sie über die VM-Konsole aktiviert werden.

```
WARNING: Unauthorized access to this system is forbidden and will be
prosecuted by law. By accessing this system, you agree that your actions
may be monitored if unauthorized usage is suspected.
```

Nachdem der Benutzer die Anmeldung über den SSH-Kanal abgeschlossen hat, wird der folgende Text angezeigt:

```
Linux UnifiedVSC 5.10.0-21-amd64 #1 SMP Debian 5.10.162-1 (2023-01-21)
x86_64
```

```
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
```

Zeitüberschreitung bei Inaktivität für ONTAP-Tools 9.13

Um unbefugten Zugriff zu verhindern, wird ein Inaktivitäts-Timeout eingerichtet, das automatisch Benutzer abmeldet, die für einen bestimmten Zeitraum inaktiv sind, während autorisierte Ressourcen verwendet werden. So wird sichergestellt, dass nur autorisierte Benutzer auf die Ressourcen zugreifen können und die Sicherheit gewahrt bleibt.

- Standardmäßig werden die vSphere Client-Sitzungen nach 120 Minuten Leerlaufzeit geschlossen, sodass sich der Benutzer erneut anmelden muss, um die Verwendung des Clients fortzusetzen. Sie können den Timeout-Wert ändern, indem Sie die Datei webclient.properties bearbeiten. Sie können das Timeout des vSphere-Clients konfigurieren "Konfigurieren Sie den Wert für die Zeitüberschreitung des vSphere-Clients"
- Die Abmeldezeit für ONTAP-Tools beträgt 30 Minuten für die Web-cli-Sitzung.

Maximale Anzahl gleichzeitiger Anforderungen pro Benutzer (Netzwerksicherheitsschutz/DOS-Angriff) ONTAP-Tools für VMware vSphere 9.13

Standardmäßig beträgt die maximale Anzahl gleichzeitiger Anfragen pro Benutzer 48. Der Root-Benutzer in ONTAP-Tools kann diesen Wert je nach den Anforderungen seiner Umgebung ändern. **Dieser Wert sollte nicht auf einen sehr hohen Wert gesetzt werden, da er einen Mechanismus gegen Denial-of-Service (DOS) Angriffe bietet.**

Benutzer können die Anzahl der maximalen gleichzeitigen Sessions und andere unterstützte Parameter in der

Datei */opt/netapp/vscserver/etc/dosfilterParams.json* ändern.

Wir können den Filter mit folgenden Parametern konfigurieren:

- ***delayMs***: Die Verzögerung in Millisekunden, die allen Anfragen über das Limit der Rate gegeben wird, bevor sie berücksichtigt werden. Geben Sie -1, um die Anfrage einfach abzulehnen.
- ***drossleMS***: Wie lange warten Sie auf Semaphore.
- ***maxRequestms***: Wie lange soll diese Anfrage laufen lassen?
- ***ipWhitelist***: Eine kommagetrennte Liste von IP-Adressen, die nicht ratenbegrenzt ist. (Dies können vCenter-, ESXi- und SRA-IPs sein)
- ***maxRequestsPerSec***: Die maximale Anzahl von Anfragen einer Verbindung pro Sekunde.

Standardwerte in der *dosfilterParams-Datei*:

```
{"delayMs":"-1",
"throttleMs":"1800000",
"maxRequestMs":"300000",
"ipWhitelist":"10.224.58.52",
"maxRequestsPerSec":"48"}
```

NTP-Konfiguration (Network Time Protocol) für ONTAP-Tools 9.13

Manchmal können Sicherheitsprobleme aufgrund von Diskrepanzen bei der Konfiguration der Netzwerkzeit auftreten. Es ist wichtig, dass alle Geräte innerhalb eines Netzwerks über genaue Zeiteinstellungen verfügen, um solche Probleme zu vermeiden.

Virtuelles Gerät

Sie können den/die NTP-Server über die Wartungskonsole in der virtuellen Appliance konfigurieren. Benutzer können die NTP-Server-Details unter der Option *System Configuration ⇒ Add New NTP Server* hinzufügen

Standardmäßig lautet der Service für NTP ntpd. Es handelt sich hierbei um einen Legacy-Service, der in bestimmten Fällen für virtuelle Maschinen nicht gut funktioniert.

Debian

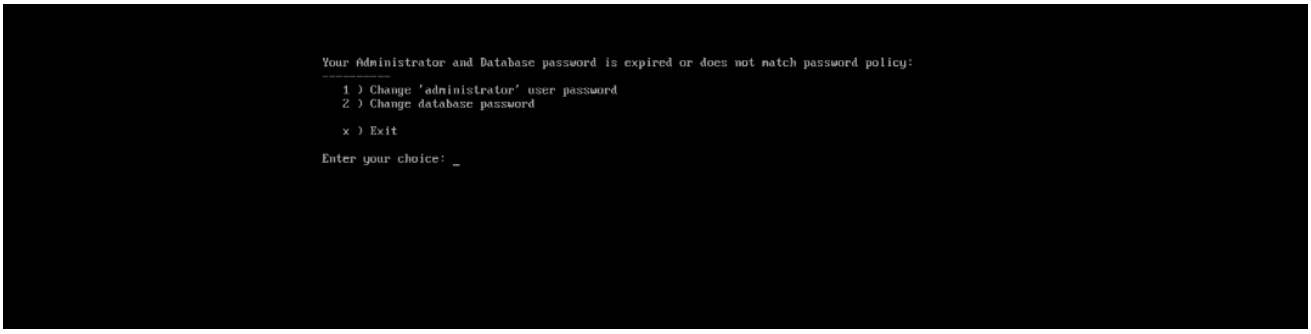
Auf Debian kann der Benutzer auf die Datei /etc/ntp.conf zugreifen, um ntp-Serverdetails zu erhalten.

Passwortrichtlinien für ONTAP-Tools 9.13

Benutzer, die ONTAP-Tools zum ersten Mal bereitstellen oder ein Upgrade auf Version 9.12 oder höher durchführen, müssen die Richtlinie für starkes Kennwort sowohl für den Administrator als auch für Datenbankbenutzer befolgen. Während des Bereitstellungsprozesses werden neue Benutzer aufgefordert, ihre Passwörter einzugeben. Für Brownfield-Benutzer, die auf Version 9.12 oder höher aktualisieren, wird die Option zur Einhaltung der Richtlinie für starke Kennwörter in der Wartungskonsole verfügbar sein.

- Sobald sich der Benutzer in der maint-Konsole anmeldet, werden die Passwörter anhand der komplexen Regelsammlung überprüft. Wenn er nicht befolgt wird, wird der Benutzer aufgefordert, das gleiche zurückzusetzen.
- Die Standardgültigkeit des Passworts beträgt 90 Tage, und nach 75 Tagen erhält der Benutzer die Benachrichtigung, das Kennwort zu ändern.
- Es ist erforderlich, in jedem Zyklus ein neues Passwort festzulegen, das System nimmt nicht das letzte Passwort als neues Passwort.
- Wenn sich ein Benutzer an der maint-Konsole anmeldet, überprüft er vor dem Laden des Hauptmenüs nach den Passwortrichtlinien wie den folgenden Screenshots:

- Wenn die Kennwortrichtlinie oder das Upgrade-Setup von ONTAP Tools 9.11 oder früher nicht verwendet wurde. Der Benutzer wird dann den folgenden Bildschirm sehen, um das Passwort zurückzusetzen:



- Wenn der Benutzer versucht, ein schwaches Passwort festzulegen oder das letzte Passwort erneut gibt, wird der Benutzer folgende Fehlermeldung sehen: