



VMware

Enterprise applications

NetApp
May 19, 2024

Inhalt

- VMware 1
 - VMware vSphere mit ONTAP – 1
 - Virtual Volumes (VVols) mit ONTAP 46
 - VMware Site Recovery Manager mit ONTAP 72
 - VSphere Metro Storage-Cluster mit ONTAP 92
 - Produktsicherheit 122
 - Leitfaden zur Erhöhung der Sicherheit für ONTAP Tools für VMware vSphere 126

VMware

VMware vSphere mit ONTAP –

VMware vSphere mit ONTAP –

ONTAP ist seit fast 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 bietet eine Einführung in die ONTAP Lösung für vSphere sowie in die neuesten Produktinformationen und Best Practices zur Optimierung der Implementierung, Risikominderung und Vereinfachung des Managements.



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. Siehe "[NetApp Interoperabilitäts-Matrix-Tool](#)" Und "[VMware Compatibility Guide](#)" Finden Sie Details zu bestimmten Versionen.

Warum 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 Kombination von ONTAP und vSphere ermöglicht Kosteneinsparungen für Host-Hardware und VMware Software. Schützen Sie Ihre Daten außerdem zu geringeren Kosten mit konstant hoher Performance. Da virtualisierte Workloads mobil sind, können Sie mit Storage vMotion verschiedene Ansätze nutzen, um VMs auf VMFS-, NFS- oder VVols-Datstores zu verschieben. Und das alles auf ein und demselben Storage-System.

Im Folgenden sind wichtige Faktoren aufgeführt, die heutzutage von Kunden wertvoll sind:

- **Unified Storage.** Systeme mit ONTAP Software sind auf mehrere signifikante Arten vereinheitlicht. Dieser Ansatz bezog sich ursprünglich auf NAS- und SAN-Protokolle. ONTAP ist dabei weiterhin eine der führenden Plattformen für SAN und bietet in Bezug auf NAS die ursprünglichen Stärken. 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 Software sind bei VSI in der Regel kostengünstiger als herkömmliche Enterprise-Arrays, bieten zugleich 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.

- **Auf virtuellen Volumes und richtlinienbasiertem Storage-Management.** NetApp war bereits früh als Designpartner von VMware an der Entwicklung von vSphere Virtual Volumes (VVols) beteiligt und stellte architekturspezifischen Input und frühzeitig Unterstützung für VVols und VMware vSphere APIs for Storage Awareness (VASA) bereit. Durch diesen Ansatz wurde nicht nur das granulare VM-Storage-Management in VMFS integriert, sondern auch die Automatisierung der Storage-Bereitstellung durch richtlinienbasiertes Management unterstützt. Storage-Architekten können mit diesem Ansatz Storage-Pools mit unterschiedlichen Funktionen entwerfen, die von VM-Administratoren einfach genutzt werden können. ONTAP ist einer der führenden Anbieter von vVol Storage-Lösungen in der Storage-Branche, da es Hunderttausende VVols in einem einzigen Cluster unterstützt. Anbieter von Enterprise-Arrays und kleineren Flash-Arrays hingegen unterstützen gerade einmal mehrere Tausend VVols pro Array. Zudem bringt NetApp mit neuen Funktionen bei der Unterstützung von VVols 3.0 die Weiterentwicklung des granularen VM-Managements voran.
- **Storage-Effizienz.** Obwohl NetApp als erster Anbieter Deduplizierung für Produktions-Workloads bereitgestellt hat, war diese Innovation weder die erste noch die letzte in diesem Bereich. Es begann mit Snapshots, einem platzsparenden Datensicherungsmechanismus ohne Auswirkungen auf die Performance, sowie mit FlexClone Technologie, bei der sofort Lese-/Schreibkopien von VMs für die Produktion und die Nutzung von Backups erstellt werden können. Danach stellte NetApp Inline-Funktionen bereit, darunter Deduplizierung, Komprimierung und Zero-Block-Deduplizierung, mit denen sich der Storage kostspieliger SSDs maximal ausschöpfen lässt. Zuletzt wurde ONTAP um die Möglichkeit erweitert, kleinere I/O-Vorgänge und Dateien durch Data-Compaction in einen Festplattenblock zu packen. Dank der Kombination dieser Funktionen verzeichnen Kunden Einsparungen im Verhältnis von bis zu 5:1 für VSI und von bis zu 30:1 für VDI.
- **Hybrid Cloud.** ob in der Private Cloud vor Ort, in einer Public-Cloud-Infrastruktur oder in einer Hybrid Cloud, die das Beste der beiden Lösungen vereint – ONTAP Lösungen helfen Ihnen, Ihre Data Fabric zur Optimierung und zum Optimieren des Datenmanagements aufzubauen. Den Anfang machen hochperformante All-Flash-Systeme, die dann für die Datensicherung und das Cloud-Computing mit Festplatten- oder Cloud-Storage-Systemen gekoppelt werden. Zur Kostenoptimierung und Vermeidung einer Anbieterbindung stehen hierbei Azure, AWS, IBM oder Google Clouds zur Auswahl. Bei Bedarf kann die erweiterte Unterstützung für OpenStack und Containertechnologien genutzt werden. NetApp bietet darüber hinaus Cloud-basiertes Tiering und Archivierungstools (SnapMirror Cloud, Cloud Backup Service und Cloud Sync) sowie Storage-Systeme (FabricPool) für ONTAP, um die Betriebskosten zu senken und die große Reichweite der Cloud auszuschöpfen.
- *** 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.

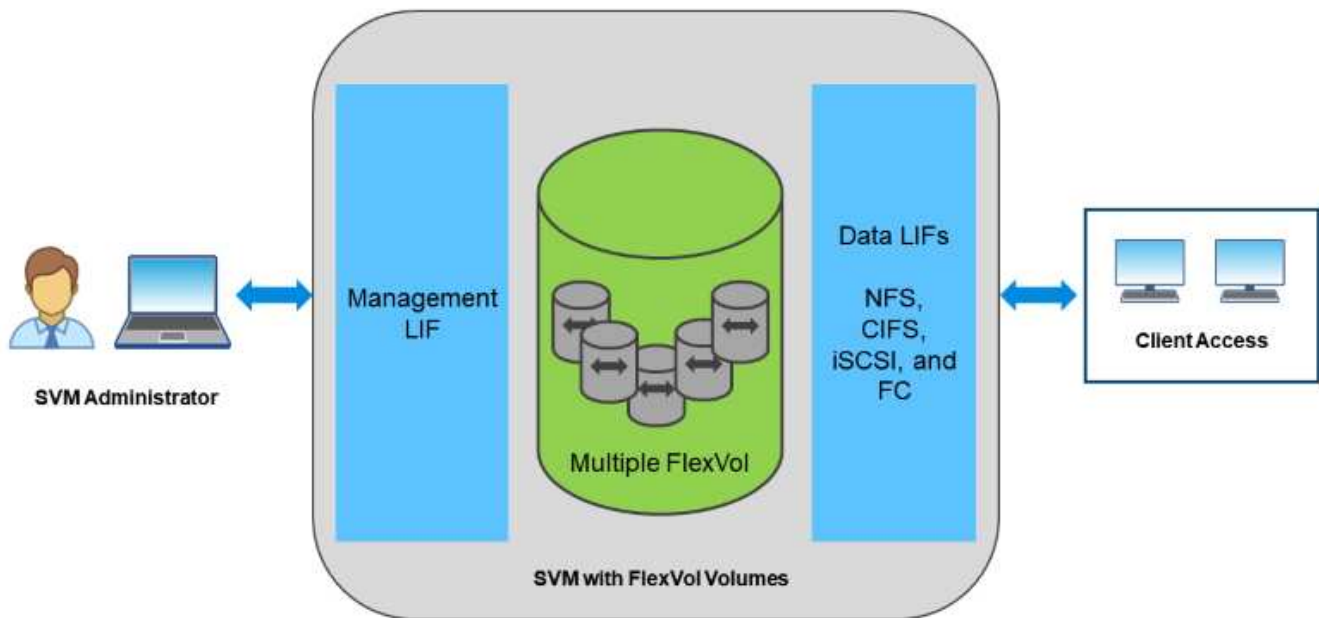
Unified Storage

NetApp 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 unter "[S3-Konfigurationsübersicht](#)".

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 Software 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 Software sind bei VSI in der Regel kostengünstiger als herkömmliche Enterprise-Arrays, bieten zugleich 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 verschiedene Standalone-Softwaretools, die gemeinsam mit ONTAP und vSphere für das Management Ihrer virtualisierten Umgebung verwendet werden können.

Die folgenden Tools sind ohne Aufpreis in der ONTAP Lizenz enthalten. In Abbildung 1 sehen Sie eine

Darstellung, wie diese Tools in Ihrer vSphere Umgebung zusammenarbeiten.

ONTAP Tools für VMware vSphere

Die ONTAP Tools für VMware vSphere sind eine Reihe von Tools, die ONTAP Storage zusammen mit vSphere verwenden. 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. Bei all diesen Vorteilen empfiehlt NetApp, bei der Verwendung von vSphere mit Systemen mit ONTAP Software diese ONTAP Tools als Best Practice zu verwenden. Sie umfasst eine Server-Appliance, Erweiterungen der Benutzeroberfläche 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 Extensions.** die UI-Erweiterungen der ONTAP-Tools vereinfachen die Arbeit von Betriebsteams und vCenter Administratoren durch die Verwendung benutzerfreundlicher, kontextabhängiger Menüs zum Managen von Hosts und Storage, Informations-Portlets und nativen Alarmfunktionen direkt in der vCenter-Benutzeroberfläche für optimierte Workflows.
- **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 Alarmer für die Monitoring-Kapazität und -Compliance mit den Profilen.
- **Storage Replication Adapter.** SRA wird zusammen mit VMware Site Recovery Manager (SRM) zum Management der Datenreplikierung zwischen Produktions- und Disaster-Recovery-Standorten sowie zum unterbrechungsfreien Testen der DR-Replikate verwendet. Diese Software hilft bei der Automatisierung der Erkennungs-, Recovery- und Sicherungsaufgaben. Sie enthält sowohl eine SRA Server-Appliance als auch SRA Adapter für den Windows SRM Server und eine SRM Appliance.

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



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-Datstores unter 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.

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

NetApp war schon früh als Design-Partner von VMware an der Entwicklung von vSphere Virtual Volumes (VVols) beteiligt und stellte architekturspezifischen Input und frühzeitig Unterstützung für VVols und VMware vSphere APIs for Storage Awareness (VASA) bereit. Durch diesen Ansatz wurde VMFS nicht nur granulares VM-Storage-Management ermöglicht, sondern auch die Automatisierung der Storage-Bereitstellung durch Storage Policy Based Management (SPBM) unterstützt.

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, die von VM-Administratoren einfach genutzt werden können. Administratoren können die Workload-Anforderungen von Virtual Machines an die bereitgestellten Storage Pools anpassen, wodurch verschiedene Einstellungen pro VM oder Virtual Disk granular kontrolliert werden können.

Bei VVols ist ONTAP eine der führenden Lösungen in der Storage-Branche, da es Hunderttausende VVols in einem einzigen Cluster unterstützt. Anbieter von Enterprise-Arrays und kleineren Flash-Arrays hingegen unterstützen gerade einmal mehrere Tausend VVols pro Array. Zudem bringt NetApp mit neuen Funktionen bei der Unterstützung von VVols 3.0 die Weiterentwicklung des granularen VM-Managements voran.



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

Datenspeicher und Protokolle

Übersicht über vSphere Datastore- und Protokollfunktionen

Sieben Protokolle können für die Anbindung von VMware vSphere ESXi Hosts an ONTAP Systeme für Datastores genutzt werden:

- FCP
- FCoE
- NVMe/FC
- NVMe/TCP
- iSCSI
- NFS v3
- NFS 4.1

FCP, FCoE, NVMe/FC, NVMe/TCP und iSCSI sind Blockprotokolle. VMware Datastores werden über das vSphere Virtual Machine File System (VMFS) gespeichert, um VMs innerhalb von ONTAP LUNs oder NVMe Namespaces zu speichern, die in einem ONTAP FlexVol Volume enthalten sind. Beachten Sie, dass VMware ab vSphere 7.0 keine Software FCoE mehr in Produktionsumgebungen unterstützt. 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. Sie können sich auch beraten ["Maximalwerte für die VMware Konfiguration"](#) Bestätigen Sie für bestimmte vSphere Versionen bestimmte Limits.

Funktion/Feature	FC/FCoE	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 Namespaces pro Server	256 Halterungen Standard-NFS. MaxVolumes ist 8. Erhöhen Sie mit den ONTAP Tools für VMware vSphere auf 256.

Funktion/Feature	FC/FCoE	ISCSI	NVMe-of	NFS
Maximale Datastore-Größe	64 TB	64 TB	64 TB	100 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/FCoE	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.
Microsoft Cluster Service (MSCS) oder Failover Clustering in einer VM	Ja.	Ja*	Ja*	Nicht unterstützt
Fehlertoleranz	Ja.	Ja.	Ja.	Ja.
Site Recovery Manager	Ja.	Ja.	Nein**	Nur V3**
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.

Kapazität/Funktion	FC/FCoE	ISCSI	NVMe-of	NFS
Natives VMware Multipathing	Ja.	Ja.	Ja, Verwendung des neuen High Performance Plug-ins (HPP)	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/FCoE	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.	Nein	Ja.
Monitoring und Host-Konfiguration mit ONTAP Tools für VMware vSphere	Ja.	Ja.	Nein	Ja.
Bereitstellung mit ONTAP Tools für VMware vSphere	Ja.	Ja.	Nein	Ja.

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

Funktion/Feature	FC/FCoE	ISCSI	NVMe-of	NFS
ONTAP Snapshots	Ja.	Ja.	Ja.	Ja.
Durch replizierte Backups unterstütztes SRM	Ja.	Ja.	Nein**	Nur V3**
Volume SnapMirror	Ja.	Ja.	Ja.	Ja.
VDMK Image-Zugriff	VADP fähige Backup-Software	VADP fähige Backup-Software	VADP fähige Backup-Software	VADP fähige Backup-Software, vSphere Client und vSphere Web Client Datastore-Browser
VDMK-Zugriff auf Dateiebene	VADP fähige Backup-Software, nur Windows	VADP fähige Backup-Software, nur Windows	VADP fähige Backup-Software, nur Windows	VADP fähige Backup-Software und Applikationen von Drittanbietern

Funktion/Feature	FC/FCoE	ISCSI	NVMe-of	NFS
NDMP-Granularität	Datenspeicher	Datenspeicher	Datenspeicher	Datastore oder VM

*NetApp empfiehlt für Microsoft Cluster die Verwendung von in-Guest iSCSI anstelle von Multiwriter-fähigen VMDKs 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. In vSphere 7 wurde eine neue Clustered VMDK-Option hinzugefügt. Dies unterscheidet sich von VMDKs mit mehreren Schreibenden, die einen Datenspeicher benötigen, der über das FC-Protokoll bereitgestellt wird, für das die Unterstützung für geclusterte VMDK aktiviert ist. Weitere Einschränkungen sind möglich. VMware's ansehen ["Einrichtung für Windows Server Failover Clustering"](#) Dokumentation für Konfigurationsrichtlinien.

**Datastores mit NVMe-of und NFS v4.1 erfordern die vSphere Replizierung. Array-basierte Replizierung wird von SRM nicht unterstützt.

Auswahl eines Storage-Protokolls

Systeme mit ONTAP Software unterstützen alle wichtigen Storage-Protokolle, sodass die Kunden das für ihre Umgebung am besten geeignete Protokoll auswählen können. Dies hängt von der vorhandenen und geplanten Netzwerkinfrastruktur und den Fähigkeiten der Mitarbeiter ab. Bei von NetApp durchgeführten Tests zeigten sich generell nur geringfügige Unterschiede zwischen Protokollen, die mit ähnlichen Übertragungsgeschwindigkeiten ausgeführt wurden. Daher empfiehlt es sich, den Schwerpunkt in erster Linie auf die Netzwerkinfrastruktur und die Fähigkeiten der Mitarbeiter und erst in zweiter Linie auf die ursprüngliche Protokoll-Performance zu legen.

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

- **Gegenwärtige Kundenumgebung.** Obwohl IT-Teams normalerweise erfahren sind, um Ethernet IP-Infrastrukturen zu managen, sind nicht alle erfahren im Management einer FC SAN Fabric. 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.** bei SAN-Protokollen sind bei Bedarf mehrere Schritte erforderlich, darunter das Vergrößern einer LUN, das erneute Erkennen der neuen Größe und das Anwachsen des Dateisystems). Obwohl eine LUN vergrößert werden kann, ist eine Reduzierung der Größe einer LUN nicht möglich. Auch das Recovery von ungenutztem Speicherplatz kann weiteren Aufwand bedeuten. NFS ermöglicht eine problemlose Größenanpassung, die durch das Storage-System automatisiert werden kann. SAN bietet über TRIM/UNMAP-Befehle des Gast-Betriebssystems eine Speicherplatzrückgewinnung, sodass Speicherplatz aus gelöschten Dateien an das Array zurückgegeben werden kann. Diese Art der Rückgewinnung von ungenutztem Speicherplatz ist bei NFS-Datenspeichern schwieriger.
- **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.

ONTAP Storage-Systeme bieten beim Erstellen von Datastores für VMs und virtuelle Festplatten ein hohes Maß an Flexibilität. Obwohl viele ONTAP Best Practices angewendet werden, wenn Datastores für vSphere mit VSC bereitgestellt werden (siehe Abschnitt ["Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen"](#)), hier 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 ONTAP kann, sollten Sie mindestens vier Datastores (FlexVol Volumes) verwenden. Durch die Verteilung der Datastores auf die Controller kann so die bestmögliche Ausnutzung der Hardware gewährleistet 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. Indessen könnte die Implementierung von Datastores als mehrere qtrees in einem einzelnen Volume in hoch automatisierten Umgebungen nützlich sein, die von Kontingenten auf Datastore-Ebene oder VM-Dateiklonen profitieren können.
- 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 100 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 Tools für die Bereitstellung von VMware vSphere Datastores verwendet Autosize standardmäßig 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 konfiguriert werden, auf die über FC, iSCSI oder FCoE zugegriffen wird. Bei VMFS können alle ESX Server in einem Cluster gleichzeitig auf herkömmliche LUNs 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 den meisten Systemen 16 TB und 128 TB auf All-SAN-Array-Systemen. Daher kann auf den meisten ONTAP Systemen ein VMFS 5 Datastore mit maximaler Größe aus vier 16-TB-LUNs erstellt werden. Für Workloads mit hohem I/O-Aufkommen und mehreren LUNs (bei High-End FAS oder AFF Systemen) können Performance-Vorteile zum Tragen kommen, allerdings werden diese durch das komplexere Management beim Erstellen, Managen und Sichern der Datastore-LUNs und ein erhöhtes Verfügbarkeitsrisiko ausgeglichen. NetApp empfiehlt im Allgemeinen, eine einzelne, große LUN für jeden Datastore zu verwenden. Und nur im Ausnahmefall, wenn größere Datastores mit über 16 TB gebraucht werden, mit Extends zu arbeiten. Analog zu dem NFS Ansatz, verteilen ONTAP Sie ebenfalls die Datastores über die Controller, um die bestmögliche Performance zu erzielen.
- 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 das Thema VM Alignment behandelt 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. Um die beste Performance und ein optimales Management zu erzielen, sollten Sie für Applikationen mit hohem I/O-Aufkommen – beispielsweise für Datenbanken und bestimmte Applikationen – keinen Datastore verwenden. Hier sind „inguest“-Ansätze via NFS oder iSCSI in Erwägung zu ziehen, die vom Gastbetriebssystem verwaltet werden oder via Raw Device Mapping (RDM). Eine Anleitung zu bestimmten Applikationen finden Sie in den technischen Berichten von NetApp für die jeweilige Applikation. Beispiel: ["Oracle-Datenbanken auf ONTAP"](#) Ein Abschnitt zur Virtualisierung mit hilfreichen 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.
- Die meisten VMs und deren Storage können im Betrieb (eingeschalteter Zustand) migriert werden. Attached Storage (nicht im Datastore) – beispielsweise in Form von ISOs, LUNs oder NFS-Volumes – aus einem anderen Storage-System muss jedoch unter Umständen im ausgeschalteten Zustand migriert werden.
- 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. Siehe ["TR-4534"](#) Finden Sie weitere Informationen. 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 ONTAP verwenden, ist es eine Best Practice, die ONTAP Tools für VMware vSphere Plug-in (ehemals Virtual Storage Console) zu installieren und zu verwenden. Dieses vCenter Plug-in vereinfacht das Storage-Management, erhöht die Verfügbarkeit und senkt die Storage-Kosten und den Betriebsaufwand – sei es bei SAN oder bei NAS. 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.

Das Plug-in ist auch die Managementoberfläche für viele Funktionen von VASA Provider für ONTAP und unterstützt das richtlinienbasierte Storage-Management mit VVols. Nach der Registrierung von ONTAP Tools für VMware vSphere erstellen Sie damit Storage-Funktionsprofile, ordnen diesen Storage zu und stellen im Laufe der Zeit die Datastore-Compliance mit den Profilen sicher. Vasa Provider verfügt auch über eine Schnittstelle zum Erstellen und Managen von vVol Datastores.

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

Allgemeines Networking

Wenn Sie vSphere mit Systemen mit ONTAP Software 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-Netzwerkports 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. Siehe ["TR-4182"](#) Für mehr Hintergrund zur Flusssteuerung.
- 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 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“.

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, FCoE, NVMe/FC, iSCSI), RDM

NetApp ONTAP bietet Block-Storage der Enterprise-Klasse für VMware vSphere unter Verwendung von iSCSI, Fibre Channel Protocol (FCP, kurz FC) und NVMe over Fabrics (NVMe-of). Nachfolgend finden Sie Best Practices zur Implementierung von Blockprotokollen für VM-Storage mit vSphere und ONTAP.

Mit vSphere gibt es drei Methoden, blockbasierten Speicher zu nutzen:

- Mit VMFS Datastores
- Mit Raw Device Mapping (RDM)

- Auf diese LUN wird von einem Software-Initiator aus einem VM-Gastbetriebssystem zugegriffen und gesteuert

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-Namespace, 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.

VSphere umfasst integrierte Unterstützung für mehrere Pfade zu Storage-Geräten. Dieses Verfahren wird als natives Multipathing (NMP) bezeichnet. NMP kann den Storage-Typ für unterstützte Storage-Systeme erkennen und den NMP-Stack automatisch so konfigurieren, dass die Funktionen des verwendeten Storage-Systems unterstützt werden.

Sowohl NMP als auch ONTAP unterstützen Asymmetric Logical Unit Access (ALUA) zur Ermittlung optimierter und nicht optimierter Pfade. In ONTAP folgt ein ALUA-optimierter Pfad auf einen direkten Datenpfad. Dabei wird ein Zielpfad auf dem Node verwendet, der die LUN hostet, auf die zugegriffen wird. ALUA ist sowohl in vSphere als auch in ONTAP standardmäßig aktiviert. NMP erkennt das ONTAP Cluster als ALUA-fähig und verwendet ein ALUA Storage-Array-Plug-in (`VMW_SATP_ALUA`) und wählt das Plug-in zur Auswahl des Round-Robin-Pfades aus (`VMW_PSP_RR`).

ESXi 6 unterstützt bis zu 256 LUNs und insgesamt bis zu 1,024 Pfade zu LUNs. ESXi erkennt keine LUNs oder Pfade, die über diese Grenzen hinausgehen. Ausgehend von dieser maximalen Anzahl an LUNs lässt das Pfadlimit vier Pfade pro LUN zu. 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).

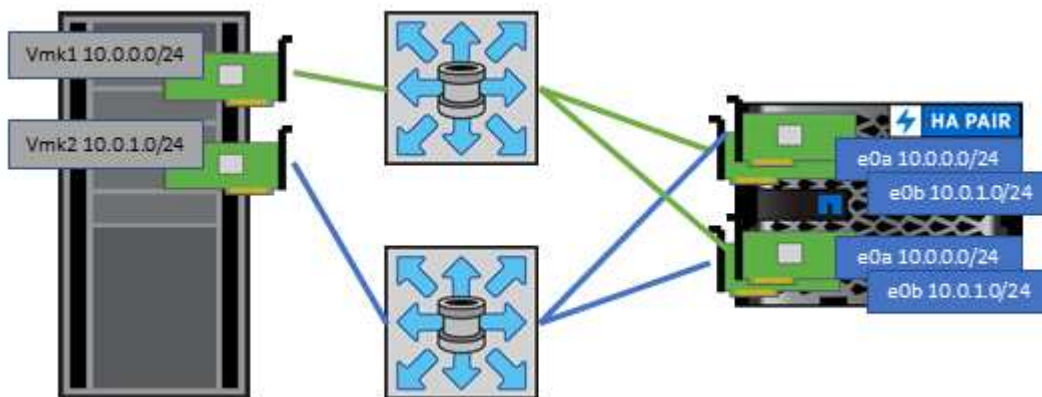
SLM beschränkt die Nodes, die Pfade an eine bestimmte LUN weitergeben. Eine Best Practice von NetApp sieht mindestens eine logische Schnittstelle (Logical Interface, LIF) pro Node pro SVM und die Verwendung von SLM vor, um die Pfade zu begrenzen, die an den Node weitergegeben werden, der die LUN und deren HA-Partner hostet. 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 im 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, indem Sie die ausführen `lun mapping remove-reporting-nodes` Befehl, um die LUN-Nodes für die Berichterstellung zu entfernen und den LUN-Zugriff auf den LUN-Eigentümer-Node und seinen HA-Partner zu beschränken.

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) und iSCSI verwendet qualifizierte iSCSI-Namen (IQNs). Der Pfad zu LUNs innerhalb des Storage 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. Das NVMe-Subsystem in ONTAP funktioniert ähnlich.

Weitere Best Practices, die berücksichtigt werden sollten:

- 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 geparkt 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

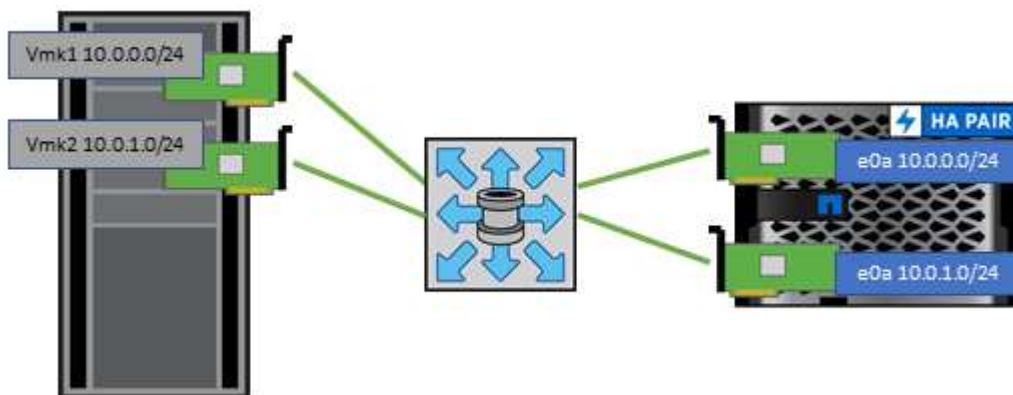
Bei NetApp ONTAP handelt es sich unter anderem um ein horizontal skalierbares NAS-Array der Enterprise-Klasse. ONTAP ermöglicht VMware vSphere den gleichzeitigen Zugriff auf NFS-verbundene Datastores von vielen ESXi Hosts und übertrifft dabei die für VMFS Dateisysteme auferlegten Grenzen bei Weitem.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

Wie bereits in erwähnt, ist hier ein Überblick gegeben ["Datenspeicher"](#) Abschnitt.

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

- 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).
- VMware unterstützt NFSv3 seit VMware Infrastructure 3. vSphere 6.0 bietet zusätzlich Unterstützung für NFSv4.1 und ermöglicht damit einige erweiterte Funktionen wie Kerberos Sicherheit. In NFSv3 wird „Client-side locking“ verwendet, in NFSv4.1 „Server-side locking“. Ein ONTAP Volume kann zwar mit beiden Protokollen exportiert werden, doch ESXi kann nur durch ein Protokoll gemountet werden. Bei diesem Einzelprotokoll-Mounting ist jedoch nicht ausgeschlossen, dass ESXi Hosts denselben Datastore auch durch eine andere Version mounten. Denken Sie daran, die beim Mounten verwendete Protokollversion anzugeben, damit alle Hosts dieselbe Version und somit auch denselben Sperrungsstil anwenden. Verwenden Sie auf verschiedenen Hosts nicht unterschiedliche NFS-Versionen. Falls möglich, prüfen Sie mithilfe von Hostprofilen die Compliance.
 - 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.
 - Weitere Informationen finden Sie in den Anmerkungen zur Interoperabilität von NFS v4.1 ["NetApp Interoperabilitäts-Matrix-Tool"](#) Für bestimmte ESXi-Patch-Level, die zur Unterstützung erforderlich sind.
 - VMware unterstützt nconnect mit NFSv3 ab vSphere 8.0U2. Weitere Informationen zu nconnect finden Sie im ["NFSv3 nConnect Funktion mit NetApp und VMware"](#)
- Zur Steuerung des Zugriffs durch vSphere Hosts kommen NFS-Exportrichtlinien zur Anwendung. Sie können eine Richtlinie für mehrere Volumes (Datastores) nutzen. Bei NFSv3 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 Exportrichtlinien mit unterschiedlichen Werten für `-anon` und `-allow-suid` Die ONTAP-Tools können zu Problemen bei der SVM-Erkennung führen. Hier sehen Sie eine Beispielrichtlinie:
 - Access Protocol: nfs (schließt nfsv3 und NFSv4 ein)
 - Client Match Spec: 192.168.42.21
 - RO-Zugriffsregel: Sys
 - RW Access Rule: Sys
 - Anonyme UID
 - Superuser: Sys
- Wenn das NetApp NFS-Plug-in für VMware VAAI verwendet wird, sollte das Protokoll auf eingestellt werden `nfs` Statt `nfs3` Wenn die Regel für die Exportrichtlinie erstellt oder geändert wird. Die Funktion für den Copy-Offload erfordert das NFSv4-Protokoll, selbst wenn das Datenprotokoll NFSv3 ist. Angeben des Protokolls als `nfs` Umfasst sowohl die NFSv3 als auch die NFSv4-Versionen.
- NFS-Datstore-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:
 - Access Protocol: nfs (schließt nfsv3 und NFSv4 ein)

- Client Match Spec: 192.168.42.21
- RO-Zugriffsregel: Sys
- RW Access Rule: Never (höchste Sicherheit für Root-Volume)
- Anonyme UID
- Superuser: Sys (auch für Root-Volume mit VAAI erforderlich)
- Verwenden Sie ONTAP Tools für VMware vSphere (die wichtigste Best Practice):
 - Mit 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.
- 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.
DRS	Ja.	Ja.

Funktionen von vSphere	NFSv3	NFSv4.1
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.

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.

Neben ONTAP 9.8 und den ONTAP Tools für VMware vSphere 9.8 und dem SnapCenter Plug-in für VMware 4.4 Versionen wurde auch die Unterstützung für Volume-gestützte FlexGroup Datastores in vSphere hinzugefügt. 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.

Weitere Informationen zu FlexGroup Volumes in ["Technische Berichte zu Volumes von FlexCache und FlexGroup"](#).

Verwenden Sie FlexGroup Volumes mit vSphere, wenn Sie einen einzelnen, skalierbaren vSphere-Datastore mit der Leistung eines vollständigen ONTAP Clusters benötigen oder wenn sehr große Klon-Workloads vorhanden sind, die von dem neuen FlexGroup-Klonmechanismus profitieren können.

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 lokale Cache wird dann verwendet, um VM-Klone bei Bedarf schnell instanziierten zu können.

Informationen zum Aktivieren des für FlexGroup optimierten Copy-Offload finden Sie unter ["Konfigurieren von ONTAP FlexGroups zum Zulassen von 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 Klone 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 FlexGroups 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.

Beachten Sie, dass VMware vSphere alle I/O-Vorgänge für einen NFS-Datastore als eine einzige Warteschlange pro Host behandelt. Die QoS-Drosselung einer VM kann die Performance anderer VMs im selben Datastore 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-Standard Einstellungen, 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 ($6 \times 8 + 10\%$) dimensionieren.
- VMware und NetApp unterstützen das NFSv4.1 Session Trunking ab ONTAP 9.14.1. In den Hinweisen zur NetApp NFS 4.1 Interoperabilitäts-Matrix finden Sie spezifische Versionsdetails. NFSv3 unterstützt nicht mehrere physische Pfade zu einem Volume, sondern beginnend mit vSphere 8.0U2 nconnect. Weitere Informationen zu nconnect finden Sie im ["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 beim Einsatz von VAAI oder FlexGroups Ihre Klon-Workloads. Die Änderung der Anzahl zusammengebender Volumes ist eine Möglichkeit zur Optimierung des FlexGroup-basierten Klonens. Ebenso wie die Anpassung der zuvor erwähnten Cache-Zeitüberschreitung.
- Verwenden Sie ONTAP Tools für VMware vSphere 9.8 oder höher, um die Performance von FlexGroup VMs mithilfe von ONTAP Kennzahlen (Dashboard und VM-Berichte) zu überwachen und QoS für einzelne VMs zu managen. 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.

Netzwerkconfiguration

Wenn Sie vSphere mit Systemen mit ONTAP Software 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- Flussssteuerung nur an den Cluster-Netzwerkports innerhalb eines ONTAP Clusters. Für die übrigen Netzwerkports, die für Daten-Traffic verwendet werden, gibt NetApp im Hinblick auf Best Practices keine weiteren Empfehlungen. Sie sollten diese Funktion nach Bedarf aktivieren oder deaktivieren. Siehe ["TR-4182"](#) Für mehr Hintergrund zur Flussssteuerung.
- 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*
Flussskontrolle	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, FCoE, NVMe/FC, iSCSI), RDM

Mit vSphere gibt es drei Methoden, blockbasierten Speicher zu nutzen:

- Mit VMFS Datastores

- Mit Raw Device Mapping (RDM)
- Auf diese LUN wird von einem Software-Initiator aus einem VM-Gastbetriebssystem zugegriffen und gesteuert

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 oder NVMe Namespaces zugegriffen wird, auf die das NVMe/FC-Protokoll zugegriffen wird. Bei VMFS können alle ESX Server in einem Cluster gleichzeitig auf herkömmliche LUNs zugreifen. Die maximale LUN-Größe beträgt bei ONTAP im Allgemeinen 16 TB; daher wird ein VMFS 5 Datastore mit einer maximalen Größe von 64 TB (siehe erste Tabelle in diesem Abschnitt) aus vier 16-TB-LUNs erstellt (alle SAN-Array-Systeme unterstützen die maximale VMFS-LUN-Größe von 64 TB). Da die ONTAP LUN-Architektur keine kleinen individuellen „Queue Depths“ aufweist, sind VMFS Datastores in ONTAP relativ problemlos in einem höheren Maße skalierbar gegenüber herkömmlichen Array-Architekturen.

VSphere umfasst integrierte Unterstützung für mehrere Pfade zu Storage-Geräten. Dieses Verfahren wird als natives Multipathing (NMP) bezeichnet. NMP kann den Storage-Typ für unterstützte Storage-Systeme erkennen und den NMP-Stack automatisch so konfigurieren, dass die Funktionen des verwendeten Storage-Systems unterstützt werden.

Sowohl NMP als auch ONTAP unterstützen Asymmetric Logical Unit Access (ALUA) zur Ermittlung optimierter und nicht optimierter Pfade. In ONTAP folgt ein ALUA-optimierter Pfad auf einen direkten Datenpfad. Dabei wird ein Zielport auf dem Node verwendet, der die LUN hostet, auf die zugegriffen wird. ALUA ist sowohl in vSphere als auch in ONTAP standardmäßig aktiviert. NMP erkennt das ONTAP Cluster als ALUA-fähig und verwendet ein ALUA Storage-Array-Plug-in (`VMW_SATP_ALUA`) und wählt das Round-Robin-Pfadauswahl-Plug-in aus (`VMW_PSP_RR`).

ESXi 6 unterstützt bis zu 256 LUNs und insgesamt bis zu 1,024 Pfade zu LUNs. Alle über diese Grenzen hinausgehenden LUNs oder Pfade werden von ESXi nicht erkannt. Ausgehend von dieser maximalen Anzahl an LUNs lässt das Pfadlimit vier Pfade pro LUN zu. 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).

SLM beschränkt die Nodes, die Pfade an eine bestimmte LUN weitergeben. Eine Best Practice von NetApp sieht mindestens eine logische Schnittstelle (Logical Interface, LIF) pro Node pro SVM und die Verwendung von SLM vor, um die Pfade zu begrenzen, die an den Node weitergegeben werden, der die LUN und deren HA-Partner hostet. 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 im 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.

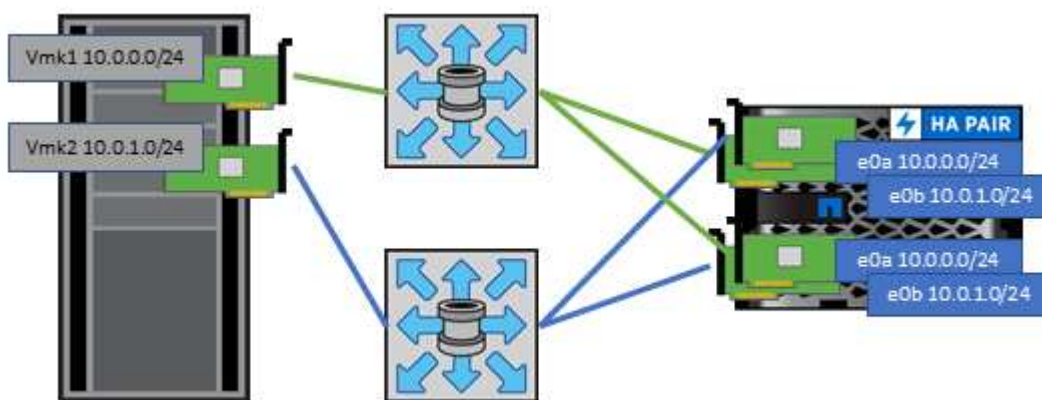
- SLM ist standardmäßig aktiviert. Sofern Sie keine Portsätze verwenden, ist keine weitere Konfiguration erforderlich.
- Für LUNs, die vor Data ONTAP 8.3 erstellt wurden, wenden Sie SLM manuell an, indem Sie den ausführen `lun mapping remove-reporting-nodes` Befehl, um die LUN-Nodes für die Berichterstellung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

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) und iSCSI verwendet qualifizierte iSCSI-Namen (IQNs). Der Pfad zu LUNs innerhalb des Storage 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. Das NVMe-Subsystem in ONTAP funktioniert ähnlich.

Weitere Best Practices, die berücksichtigt werden sollten:

- 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 geparkt 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. Verwenden Sie in ONTAP eine Single-Mode-Schnittstellengruppe mit mehreren Links zu verschiedenen Switches oder LACP mit Multimode-Schnittstellengruppen für hohe Verfügbarkeit und Vorteile bei der Link-Aggregation.
- 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"](#). In der folgenden Abbildung ist die Multipath-Konnektivität von einem vSphere Host zu einer ONTAP-LUN dargestellt.



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 zu Datastores erwähnt, gibt es bei der Verwendung von NFS mit vSphere einige Vorteile im Hinblick auf Benutzerfreundlichkeit, Storage-Effizienz und Sichtbarkeit.

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

- 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).
- Alle aktuell unterstützten Versionen von VMware vSphere können sowohl NFS v3 als auch v4.1 verwenden. Die offizielle Unterstützung für nconnect wurde in vSphere 8.0 Update 2 für NFS v3 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. Sie können mehr über die nconnect-Funktion und wie sie die Leistung verbessert unter erfahren "[NFSv3 nConnect Funktion mit NetApp und VMware](#)".

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.

Bitte beachten Sie die Hinweise in der Tabelle NFS v4.1 Interoperability im "[NetApp Interoperabilitäts-Matrix-Tool](#)". Für bestimmte ESXi-Patch-Level, die zur Unterstützung erforderlich sind.

* NFS-Exportrichtlinien werden verwendet, um den Zugriff durch vSphere-Hosts zu steuern. Sie können eine Richtlinie für mehrere Volumes (Datastores) nutzen. Bei NFSv3 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 Exportrichtlinien mit unterschiedlichen Werten für `noanon` und `allow-suid` Die ONTAP-Tools können zu Problemen bei der SVM-Erkennung führen. Hier sehen Sie eine Beispielrychtlinie:

Access Protocol: nfs3

Client-Match-Spezifikation: 192.168.42.21

RO-Zugriffsregel: Sys

RW-Zugriffsregel: Sys

Anonyme UID

Superuser: Sys

* Wenn das NetApp-NFS-Plugin für VMware VAAI verwendet wird, sollte das Protokoll auf eingestellt werden `nfs`. Wenn die Regel für die Exportrichtlinie erstellt oder geändert wird. Damit der Copy-Offload funktioniert, wird das NFSv4-Protokoll benötigt und das Protokoll als angegeben `nfs`. Beinhaltet automatisch sowohl die NFSv3- als auch die NFSv4-Versionen.

* 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 Beispielrychtlinie für das Root-Volume, bei der auch das VAAI Plug-in genutzt wird:

Access Protocol: nfs (schließt NFSv3 und NFSv4 ein)

Client-Match-Spezifikation: 192.168.42.21

RO-Zugriffsregel: Sys

RW Access Rule: Never (höchste Sicherheit für Root-Volume)

Anonyme UID

Superuser: Sys (auch für Root-Volume mit VAAI erforderlich)

* Verwenden Sie ONTAP-Tools für VMware vSphere (die wichtigste Best Practice):

Verwenden Sie ONTAP Tools für VMware vSphere zur Bereitstellung von Datastores, da es das Management von Richtlinien für den Export automatisch vereinfacht.

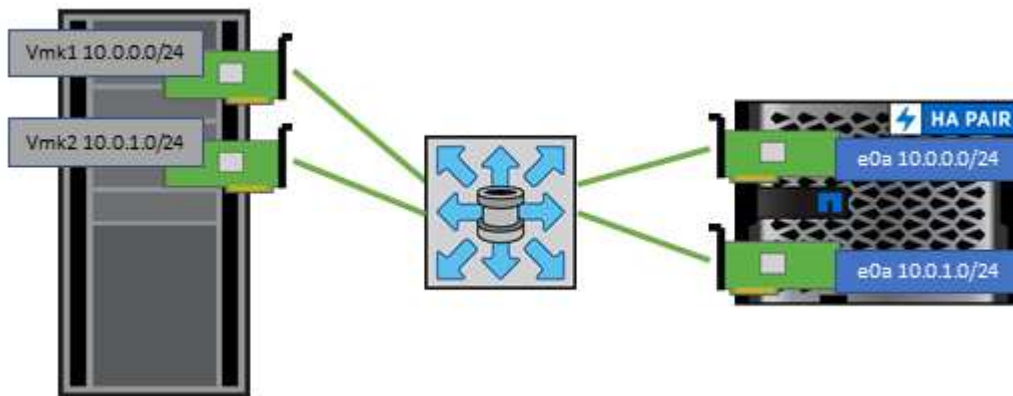
Wenn Sie Datastores für VMware-Cluster mit dem Plug-in erstellen, wählen Sie das Cluster anstelle eines einzigen ESX-Servers aus. Bei dieser Auswahl mountet der Datastore automatisch auf alle Hosts im Cluster.

Verwenden Sie die Plug-in Mount-Funktion, um vorhandene Datastores auf neue Server anzuwenden.

Wenn Sie keine ONTAP-Tools für VMware vSphere verwenden, verwenden Sie eine einzige Exportrichtlinie für alle Server oder für jeden Cluster von Servern, bei dem eine zusätzliche Zugriffskontrolle erforderlich ist.

* 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 geeignet. 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 4.000 ist für NTFS-Partitionen auf NFS-Datastores in Ordnung. 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.
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.

Funktionen von vSphere	NFSv3	NFSv4.1
Kerberos Authentifizierung	Nein	Ja (Erweiterung mit vSphere 6.5 und höher zur Unterstützung von AES, krb5i)
Multipathing-Unterstützung	Nein	Ja (ONTAP 9.14.1)

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.

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 hängen bleiben, 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.

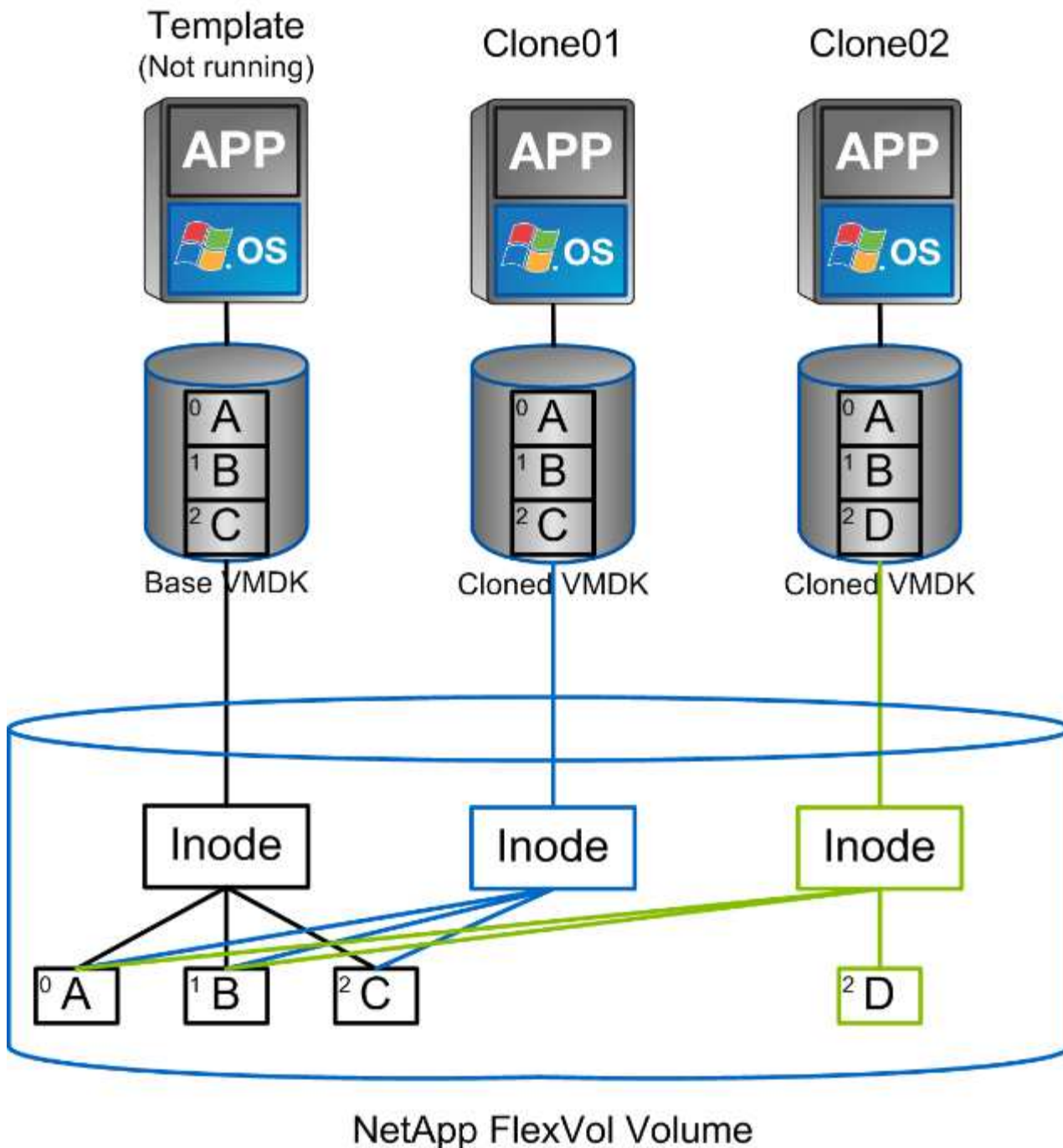
Klonen von VMs und Datastores

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 Software 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 Klon 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 den Betrieb nur auf „kalte“ (ausgeschalteten) VMs in einem NAS-Datastore, während Vorgänge auf heißen VMs (Klonen und Storage vMotion) ebenfalls für SAN verlagert werden. ONTAP nutzt je nach Quelle, Ziel und installierten Produktlizenzen den effizientesten

Ansatz. Diese Funktion wird auch von VMware Horizon View unterstützt.

- SRA (wird mit VMware 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 kopiert / zurückgesichert 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. Die Verlagerung von Kopien in einen herkömmlichen Datastore, bei dem ein FlexVol Volume verwendet wird, kann mit einer Lizenzierung von FlexClone schnell und effizient sein. Kopien zwischen FlexVol Volumes sind jedoch unter Umständen langsamer. 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 Anwendungsfälle 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

Zu den größten Stärken von ONTAP für vSphere zählt, dass Sie Ihre VMs sichern und schnell wiederherstellen können und dass Sie diese Funktion mit dem SnapCenter Plugin für VMware vSphere einfach in vCenter managen können.

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.

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 Plug-ins, um transaktionsorientierte Daten – beispielsweise SQL Server oder Oracle Daten – zu sichern. Diese Snapshots unterscheiden sich von den VMware (Konsistenz-)Snapshots und sind für längerfristigen Schutz geeignet. VMware Snapshots sind nur **"Empfehlenswert"** Für den kurzfristigen Einsatz aufgrund von Performance und anderen Auswirkungen.

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, direkt mit dem Gastbetriebssystem verbundenen iSCSI-LUNs oder VMDK-Dateien in VMFS oder NFS-Datstores 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. Zusätzlich zum Backup und Recovery unterstützen die Plug-ins auch das Klonen von Datenbanken zu Entwicklungs- oder Testzwecken.

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



Falls Sie erweiterte Disaster-Recovery-Funktionen nutzen möchten, sollten Sie in Betracht ziehen, NetApp SRA für ONTAP mit VMware Site Recovery Manager zu kombinieren. Dadurch wird die Replizierung von Datastores an einen DR-Standort unterstützt. Darüber hinaus werden unterbrechungsfreie Tests in der DR-Umgebung ermöglicht, indem die replizierten Datastores geklont werden. Das Recovery nach einem Ausfall und die erneute Sicherung der Produktion nach Behebung des Ausfalls wurden durch die in SRA integrierte Automatisierung ebenfalls vereinfacht.

Um ein Höchstmaß an Hochverfügbarkeit zu gewährleisten, ziehen Sie eine VMware vSphere Metro Storage Cluster (vMSC) Konfiguration mit NetApp MetroCluster in Erwägung. VMSC ist eine von VMware zertifizierte Lösung mit einer Kombination aus synchroner Replizierung und Array-basiertem Clustering. Sie bietet dieselben Vorteile wie ein Hochverfügbarkeits-Cluster, ist aber zum Schutz vor Standortausfällen auf separate Standorte verteilt. NetApp MetroCluster bietet kostengünstige Konfigurationen für die synchrone Replizierung mit transparentem Recovery nach dem Ausfall einer einzelnen Storage-Komponente sowie Recovery mit nur einem Befehl im Falle eines Standortausfalls. VMSC wird in ausführlicher 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 Software 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-Datstores

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.

Hinweis: 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-Datenspeichern weiterhin gelten.

VMFS-Datenspeicher

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 Datenspeicher

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.

Hinweis: VVols erfordern die Verwendung von ONTAP-Tools für VMware vSphere, die als VASA Provider für ONTAP fungiert. Siehe ["VMware vSphere Virtual Volumes \(VVols\) mit ONTAP"](#) Für VVols 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 Software 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 Klon 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.

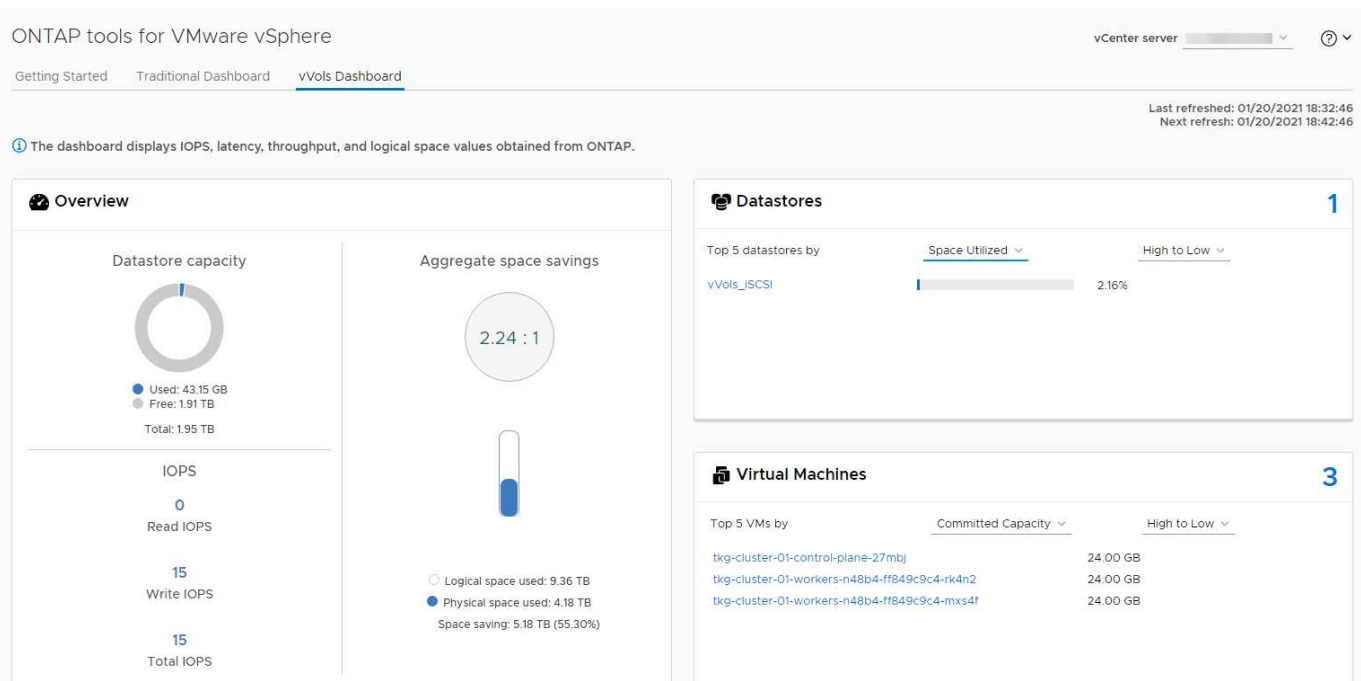
Richtlinienbasiertes Storage-Management und VVols

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 dann 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.

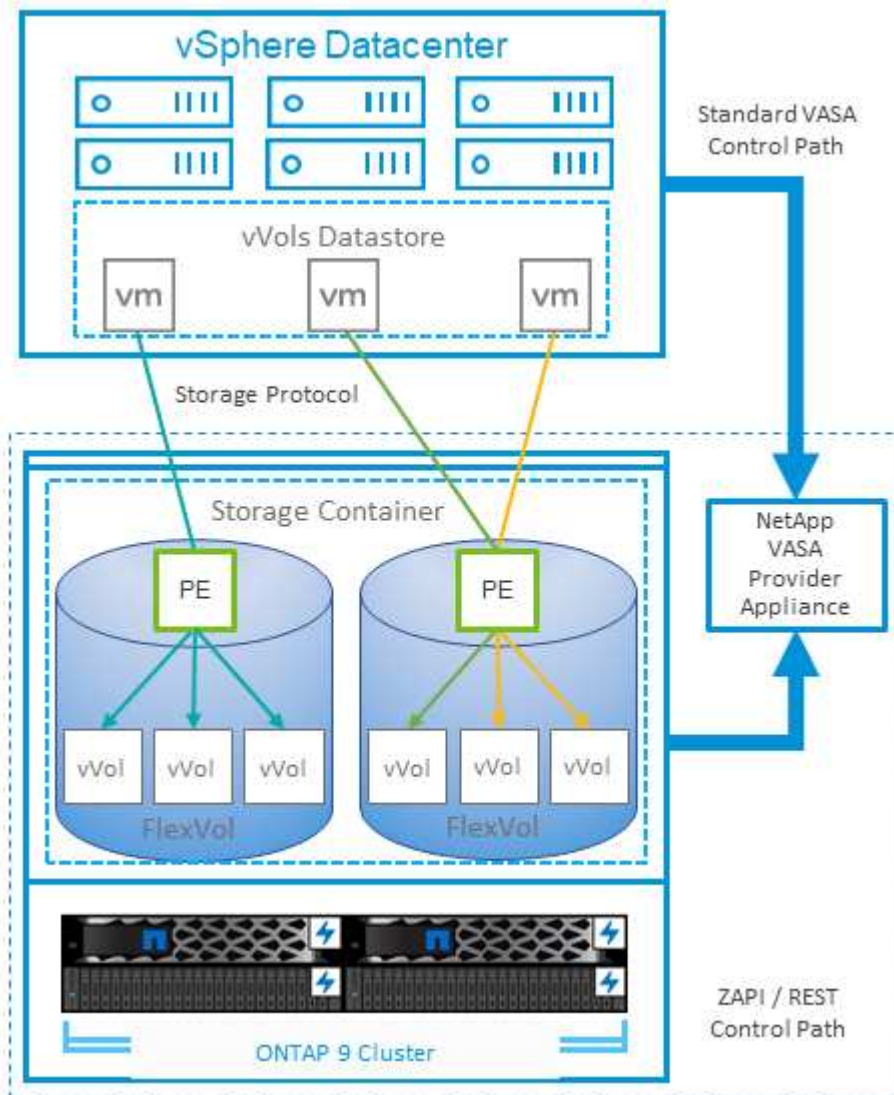
VASA stellt die Technologie bereit, mit der der Storage abgefragt und eine Reihe von Storage-Funktionen an vCenter zurückgegeben werden können. VASA Provider stellen die Übersetzung zwischen den Storage-System-APIs und -Konstrukten einerseits und den von vCenter erkannten VMware APIs bereit. NetApp VASA 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:

- **First-Party-Angebote.** Amazon FSX for NetApp ONTAP, Google Cloud NetApp Volumes und Azure NetApp Files for ANF bieten hochperformante, Multiprotokoll-gemanagte Storage-Services in den führenden Public-Cloud-Umgebungen. Sie können direkt von VMware Cloud on AWS (VMC on AWS),

Azure VMware Solution (AVS) und Google Cloud VMware Engine (GCVE) als Datastores oder Storage für Gastbetriebssysteme (GOS) und Rechnungenstanzen verwendet werden.

- **Cloud Volumes ONTAP.** die NetApp Cloud Volumes ONTAP Datenmanagement-Software bietet Kontrolle, Schutz, Flexibilität und Effizienz für Ihre Unternehmensdaten in der gewünschten Cloud. Cloud Volumes ONTAP ist eine Cloud-native Datenmanagement-Software auf der Basis von ONTAP Storage. Nutzen Sie diese Technologie zusammen mit Cloud Manager, um Cloud Volumes ONTAP Instanzen gemeinsam mit Ihren lokalen ONTAP Systemen zu implementieren und zu managen. Nutzen Sie erweiterte NAS- und iSCSI SAN-Funktionen mit einheitlichem Datenmanagement einschließlich Snapshots und SnapMirror Replizierung.
- **Cloud-Services.** mit BlueXP Backup und Recovery oder SnapMirror Cloud sichern Sie Daten von lokalen Systemen, die Public-Cloud-Storage nutzen. Cloud Sync hilft bei der Migration und bei der Synchronisierung Ihrer Daten in NAS-, Objektspeicher- und Cloud Volumes Service-Storage. BlueXP Disaster Recovery bietet eine kostengünstige und effiziente Lösung zur Nutzung von NetApp Technologien als Grundlage für eine robuste und fähige Disaster-Recovery-Lösung für DR in die Cloud, DR in On-Premises-Umgebungen und lokale Umgebungen.
- **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.

Ziehen Sie bei dem Entwurf Ihrer VM-basierten Applikationen zukünftige Cloud-Mobilität in Erwägung. Anstatt beispielsweise Applikations- und Datendateien gemeinsam zu platzieren, verwenden Sie einen separaten LUN- oder NFS-Export für die Daten. Damit können Sie VM und Daten getrennt zu Cloud-Services migrieren.

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

- ["Cloud Volumes ONTAP-Dokumentation"](#)
- ["ONTAP Select-Dokumentation"](#)
- ["BlueXP Backup- und Recovery-Dokumentation"](#)
- ["BlueXP 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 Software vereinfachen die Sicherung sämtlicher Daten durch Verschlüsselung im Ruhezustand. NetApp Storage Encryption (NSE) verwendet Self-Encrypting Drives 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. Sie können ein Upgrade durchführen und mit der Nutzung von IT beginnen, ohne dass es zu Unterbrechungen für Ihre Clients oder Applikationen kommt. Außerdem sind sie gemäß FIPS 140-2 Level 1 Standard 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 Software-Verschlüsselung umfasst einen Onboard-Schlüsselmanager ohne zusätzliche Kosten und erleichtert den Einstieg ohne hochverfügbare Verschlüsselungsmanagement-Server, deren Erwerb und Nutzung ein hohes Maß an Komplexität mit sich bringt.
- **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 das Onboard-Verschlüsselungsmanagement, 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"](#)

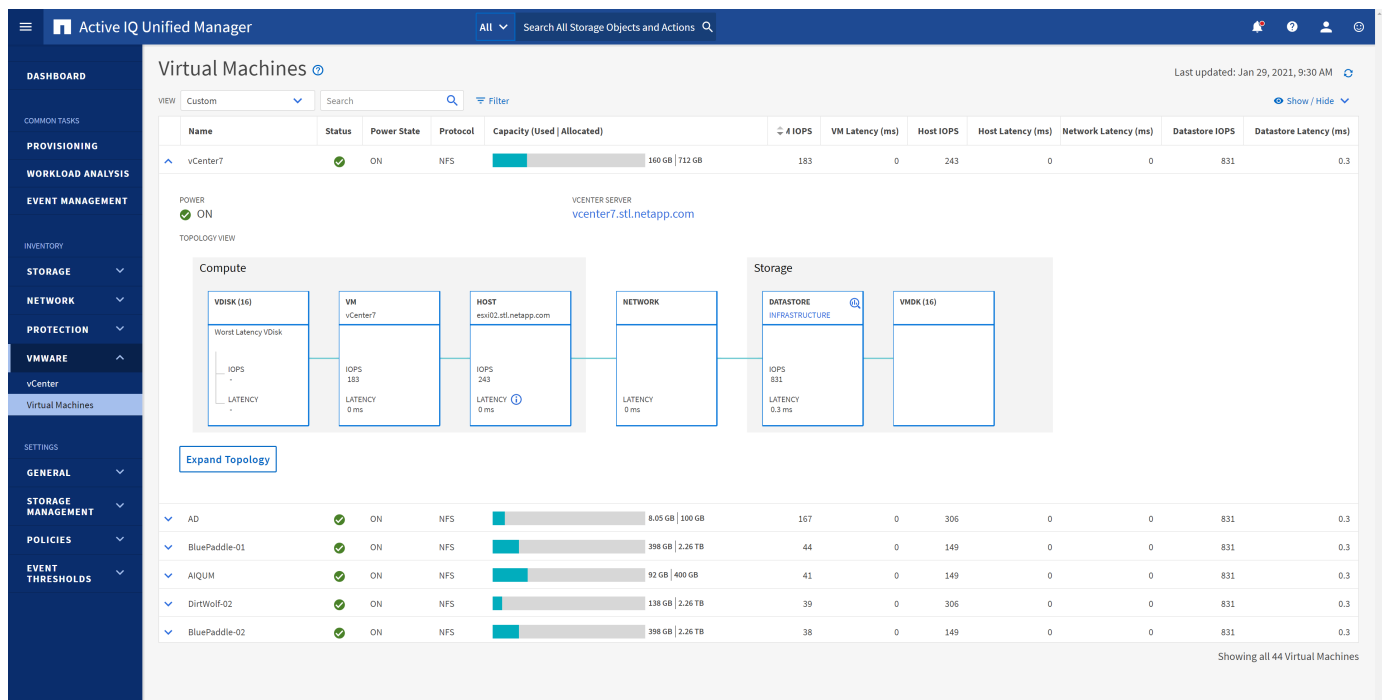
- "Leitfäden zur Erhöhung der Sicherheit"
- "Produktdokumentation zu ONTAP Sicherheit und Datenverschlüsselung"

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.

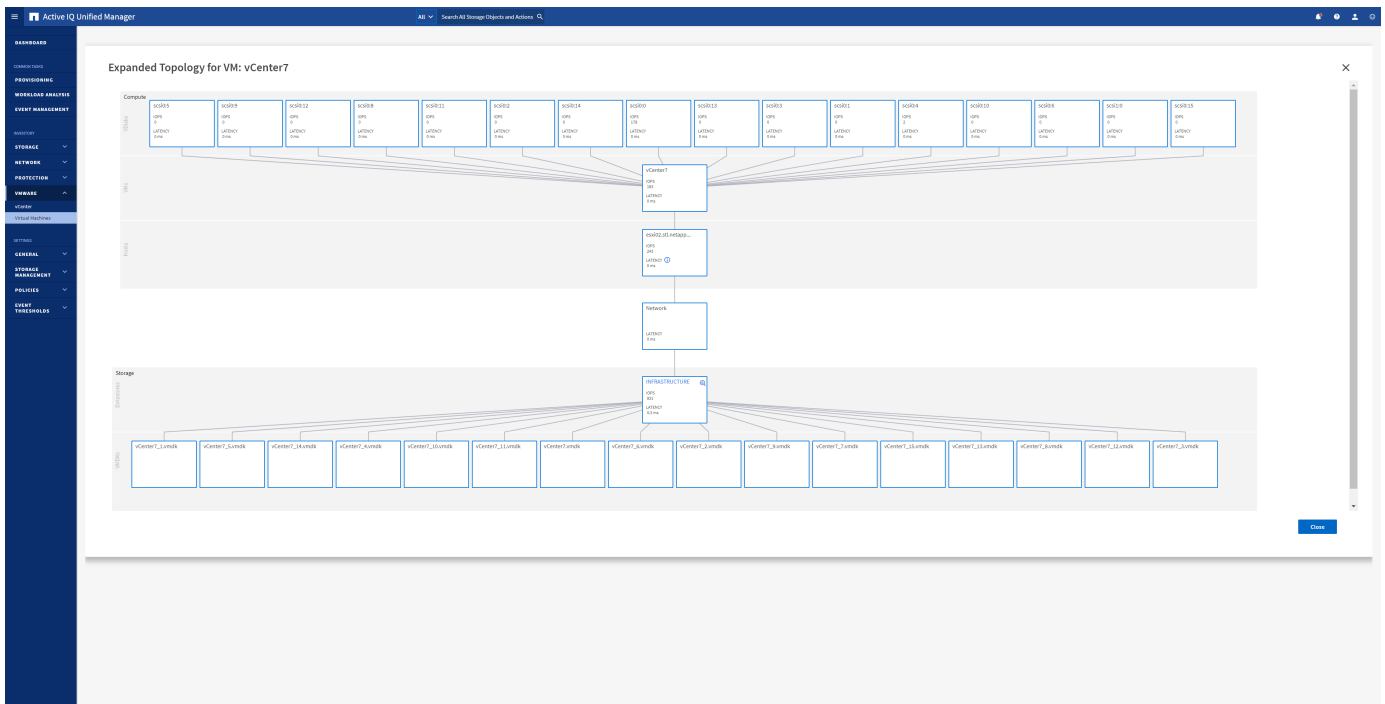
Eine typische Implementierung einer virtuellen Infrastruktur auf ONTAP setzt auf verschiedene Komponenten, die auf Computing-, Netzwerk- und Storage-Ebenen verteilt sind. Alle Performance-Einbußen bei einer VM-Applikation können aufgrund einer Kombination aus Latenzen auftreten, die bei den verschiedenen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

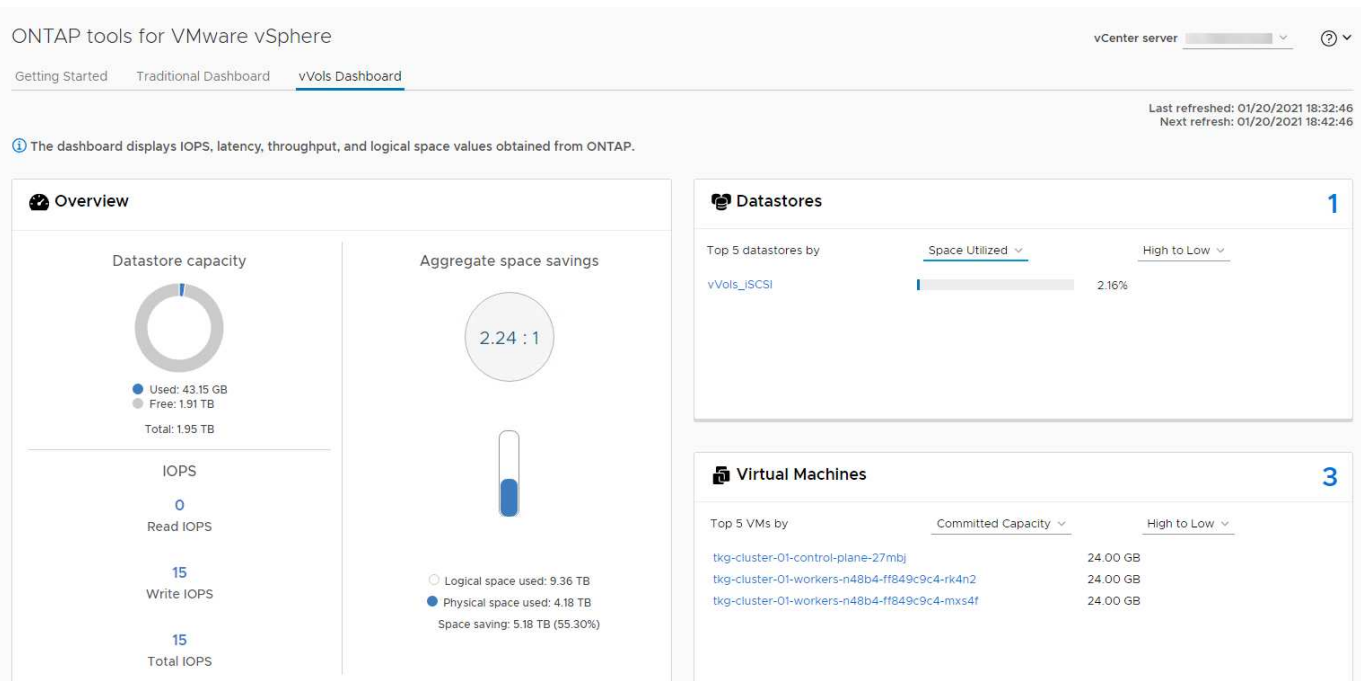
VMware vSphere APIs for Storage Awareness (VASA) erleichtern einem Storage-Administrator die Konfiguration von Datastores mit klar definierten Funktionen. Der VM-Administrator kann sie zudem im Bedarfsfall jederzeit nutzen, um VMs bereitzustellen, ohne dass eine Interaktion stattfinden muss.

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 dann 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.

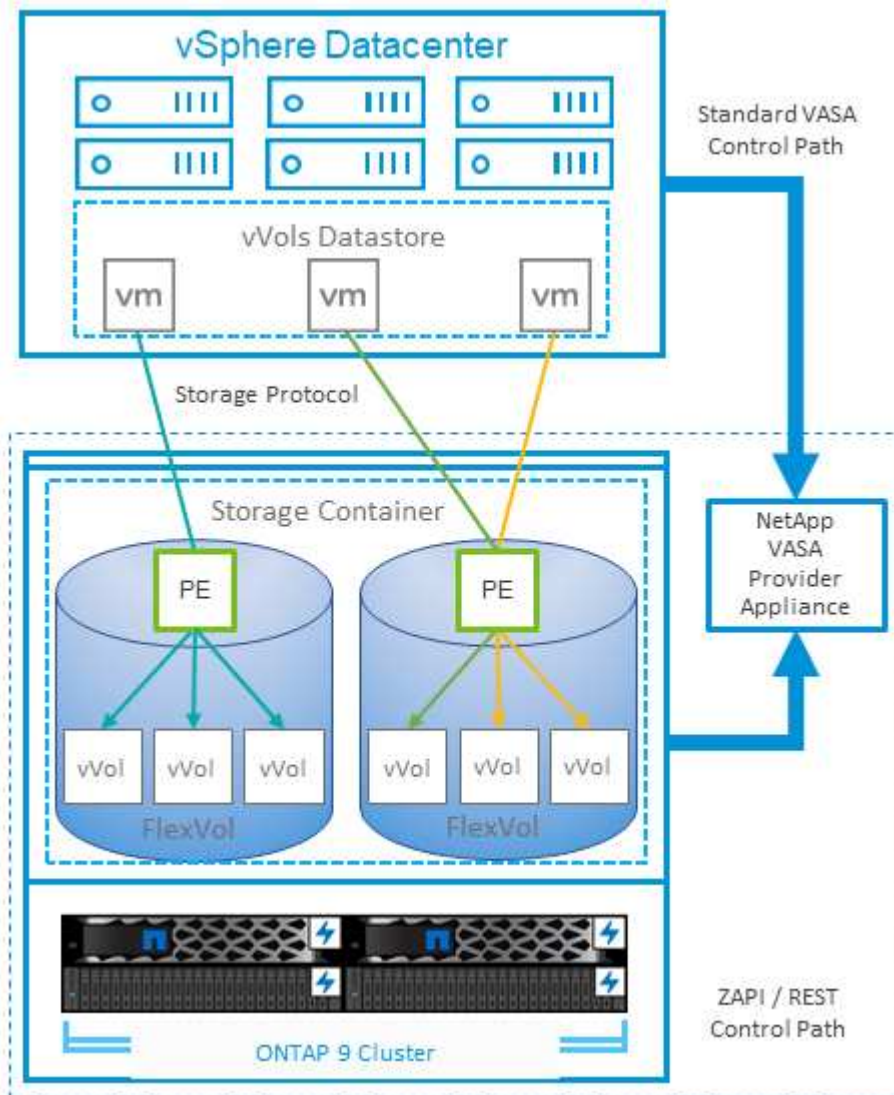
VASA stellt die Technologie bereit, mit der der Storage abgefragt und eine Reihe von Storage-Funktionen an vCenter zurückgegeben werden können. VASA Provider stellen die Übersetzung zwischen den Storage-System-APIs und -Konstrukten einerseits und den von vCenter erkannten VMware APIs bereit. NetApp VASA 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 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.

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: Klicken Sie im Dashboard „Zusammenfassung“ im Portlet „Hostsysteme“ auf „Einstellungen bearbeiten“ oder klicken Sie mit der rechten Maustaste auf den Host in vCenter. Navigieren Sie dann zu „ONTAP-Tools“ > „Empfohlene Werte festlegen“.

Im Folgenden finden Sie die derzeit empfohlenen Host-Einstellungen für die Versionen 9.8-9.13.

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 "VMware KB 2007427"	Nein
VMFS3.EnableVMFS6Entmappen	Standard beibehalten (1) Weitere Informationen finden Sie unter "VMware vSphere APIs – Array-Integration (VAAI)"	Nein

NFS-Einstellungen		
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
SunRPC.MaxConnPerIP	VSphere 7.0 oder höher: Auf 128 einstellen.	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
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



1 - die erweiterte NFS-Konfigurationsoption MaxQueueDepth funktioniert möglicherweise nicht wie vorgesehen bei der Verwendung von VMware vSphere ESXi 7.0.1 und VMware vSphere ESXi 7.0. Bitte referenzieren "[VMware KB 86331](#)" Finden Sie 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:

- In hochperformanten Umgebungen oder bei Tests der Performance mit einem einzelnen LUN-Datastore sollte die Einstellung der Lastverteilung für die Round-Robin (VMW_PSP_RR) Path Selection Policy (PSP) von der standardmäßigen IOPS-Einstellung 1000 auf einen Wert 1 geändert werden. Siehe VMware KB ["2069356"](#) Finden Sie weitere Informationen.
- In vSphere 6.7 Update 1 hat VMware einen neuen Lastausgleichsmechanismus für das Round Robin PSP System eingeführt. Bei der Auswahl des optimalen Pfads für I/O berücksichtigt die neue Option die I/O-Bandbreite und die Pfadlatenz. Möglicherweise profitieren Sie von der Verwendung in Umgebungen mit nicht gleichwertiger Pfadverbindung, z. B. bei mehr Netzwerk-Hops auf einem Pfad als auf einem anderen oder bei Verwendung eines NetApp All-SAN-Array-Systems. Siehe ["Pfadauswahl-Plug-ins und -Richtlinien"](#) Finden Sie weitere Informationen.

Zusätzliche Dokumentation

Für FCP und iSCSI mit vSphere 7 finden Sie weitere Details unter ["Verwenden Sie VMware vSphere 7.x mit ONTAP"](#)

Für FCP und iSCSI mit vSphere 8 finden Sie weitere Details unter ["Verwenden Sie VMware vSphere 8.x mit ONTAP"](#)

Für NVMe-of mit vSphere 7 finden Sie weitere Informationen unter ["Für NVMe-of finden Sie weitere Details unter NVMe-of Host Configuration for ESXi 7.x with ONTAP"](#)

Für NVMe-of mit vSphere 8 finden Sie weitere Informationen unter ["Für NVMe-of finden Sie weitere Details unter NVMe-of Host Configuration for ESXi 8.x with ONTAP"](#)

Virtual Volumes (VVols) mit ONTAP

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 1 aktualisiert, die von der Version 9.12 der ONTAP Tools unterstützt werden.

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. Zu diesen Objekten gehören LUNs, Dateien und jetzt auch vSphere 8. NVMe namespaces. NetApp arbeitete eng mit VMware als Referenzpartner für VVols zusammen, die im Jahr 2015 für vSphere 6 veröffentlicht wurden, und erneut als Design-Partner für VVols, die NVMe over Fabrics in vSphere 8 verwenden. 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 des virtuellen Volumes

Der Virtual Volume Datastore ist eine logische Datastore-Darstellung eines VVols-Containers, der von einem VASA Provider erstellt und gemanagt wird. Der Container ist ein Pool an Storage-Kapazität, der aus den vom VASA Provider gemanagten Storage-Systemen bereitgestellt wird. ONTAP Tools unterstützen die Zuweisung mehrerer FlexVol Volumes (auch als Backup Volumes bezeichnet) einem einzelnen VVols-Datastore. Diese VVols Datastores können über mehrere Nodes in einem ONTAP Cluster verteilt werden. Dabei werden Flash- und Hybrid-Systeme mit unterschiedlichen Funktionen kombiniert. Der Administrator kann neue FlexVol Volumes mithilfe des Bereitstellungsassistenten oder DER REST-API erstellen oder vorab erstellte FlexVol Volumes für die Storage-Sicherung auswählen, sofern diese verfügbar sind.

Virtual Volumes (VVols)

VVols sind die Dateien und Festplatten der Virtual Machines, die tatsächlich im VVols Datastore gespeichert sind. Der Begriff vVol (Singular) bezieht sich auf eine einzelne spezifische Datei, LUN oder Namespace. ONTAP erstellt NVMe-Namespace, LUNs oder Dateien, je nachdem, welches Protokoll der Datastore verwendet. Es gibt mehrere unterschiedliche Typen von VVols. Die gängigsten sind Konfiguration (Metadateien), Daten (virtuelle Festplatte oder VMDK) und Swap (das beim Einschalten der VM erstellt wird). VVols, die durch die Verschlüsselung von VMware VM geschützt sind, haben einen anderen Typ. 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, alle erforderlichen Storage-Funktionen zu nutzen, um VMs bereitzustellen, ohne mit ihrem Storage-Team interagieren zu müssen. Vor VASA konnten VM-Administratoren VM-Storage-Richtlinien definieren, mussten dann aber gemeinsam mit ihren Storage-Administratoren geeignete Datastores ermitteln – oft anhand der Dokumentation oder von Namenskonventionen. Mit VASA können vCenter Administratoren mit den entsprechenden Berechtigungen eine Reihe von Storage-Funktionen definieren, mit denen vCenter Benutzer dann VMs bereitstellen können. Durch die Zuordnung zwischen VM-Storage-Richtlinie und Datastore-Storage-Funktionsprofil kann in vCenter eine Liste kompatibler Datastores zur Auswahl angezeigt werden. Außerdem können andere Technologien wie Aria (ehemals vRealize) Automation oder Tanzu Kubernetes Grid aktiviert werden, um automatisch Storage aus einer zugewiesenen Richtlinie auszuwählen. Dieser Ansatz wird als richtlinienbasiertes Storage-Management bezeichnet. Während Storage-Funktionsprofile und -Richtlinien auch bei herkömmlichen Datastores verwendet werden können, konzentrieren wir uns hier auf VVols Datastores.

Es gibt zwei Elemente:

Storage Capability Profile (SCP)

Ein Storage-Funktionsprofil (Storage Capability Profile, SCP) ist eine Form von Storage-Vorlage. Damit können vCenter Administratoren festlegen, welche Storage-Funktionen benötigt werden, ohne dass ein Verständnis für das Management dieser Funktionen in ONTAP erforderlich ist. Mit Hilfe einer Vorlage können Administratoren problemlos Storage-Services auf konsistente und vorhersehbare Weise bereitstellen. Zu den in einem SCP beschriebenen Funktionen zählen Performance, Protokolle, Storage-Effizienz und weitere Funktionen. Die spezifischen Funktionen sind je nach Version unterschiedlich. Sie werden mit dem Menü ONTAP Tools für VMware vSphere in der vCenter UI erstellt. SIE können AUCH REST-APIs zum Erstellen von SCPs verwenden. Sie können manuell durch Auswahl einzelner Funktionen erstellt oder automatisch aus vorhandenen (herkömmlichen) Datenspeichern generiert werden.

VM-Speicherrichtlinie

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 bietet einen vereinfachten Ansatz, da Sie ein SCP einfach auswählen können, anstatt Sie zur Angabe einzelner Regeln zu zwingen.

Wie oben erwähnt, kann die Verwendung von Richtlinien zur Vereinfachung der Bereitstellung von Volumes beitragen. Wählen Sie einfach eine entsprechende Richtlinie aus. VASA Provider zeigt VVols-Datastores an, die diese Richtlinie unterstützen, und platziert das vVol in einem individuellen, konformen FlexVol Volume (Abbildung 1).

Bereitstellung der VM mithilfe der Storage-Richtlinie

New Virtual Machine

- ✓ 1 Select a creation type
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine (Requires Key Management Server)

VM Storage Policy

Platinum

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	Type	Clu
<input checked="" type="radio"/>	vVolsiSCSI	Compatible	100 GB	40.74 GB	64.88 GB	vVol	
<input type="radio"/>	vVolsNFS2202...	Compatible	2 TB	36.88 GB	1.96 TB	vVol	
<input type="radio"/>	local-esx01	Incompatible	3.63 TB	1.46 GB	3.63 TB	VMFS 6	
<input type="radio"/>	local-esx07	Incompatible	1.81 TB	3.85 GB	1.81 TB	VMFS 6	
<input type="radio"/>	local-esx08	Incompatible	1.69 TB	1.43 GB	1.69 TB	VMFS 6	
<input type="radio"/>	local-esx09	Incompatible	1.81 TB	3.85 GB	1.81 TB	VMFS 6	
<input type="radio"/>	local-esx15	Incompatible	3.63 TB	1.46 GB	3.63 TB	VMFS 6	
<input type="radio"/>	tier001_ds	Incompatible	22 TB	23.73 TB	18.09 TB	NFS v3	

CANCEL

BACK

NEXT

Sobald eine VM bereitgestellt ist, prüft der VASA Provider weiterhin die Compliance und alarmiert den VM-Administrator mit einem Alarm in vCenter, wenn das Backup-Volume nicht mehr mit der Richtlinie konform ist (Abbildung 2).

Einhaltung von VM-Storage-Richtlinien

Storage Policies



VM Storage Policies

AFF_VASA10

VM Storage Policy Compliance

⊗ Noncompliant

Last Checked Date

5/20/2022, 12:59:35 PM

VM Replication Groups

[CHECK COMPLIANCE](#)

NetApp VVols Unterstützung

ONTAP unterstützt die VASA Spezifikation seit ihrer ersten Version im Jahr 2012. Während andere NetApp Storage-Systeme VASA unterstützen, konzentriert sich dieses Dokument auf die derzeit unterstützten Versionen von ONTAP 9.

ONTAP

Neben ONTAP 9 auf AFF, ASA und FAS Systemen unterstützt NetApp VMware-Workloads auf ONTAP Select, Amazon FSX for NetApp mit VMware Cloud on AWS, Azure NetApp Files mit der Azure VMware Lösung, Cloud Volumes Service mit Google Cloud VMware Engine und NetApp Private Storage in Equinix, die spezifische Funktionalität kann jedoch je nach Dienstanbieter und verfügbarer Netzwerkverbindung variieren. Es ist auch möglich, von vSphere Guests auf Daten zuzugreifen, die in diesen Konfigurationen sowie auf Cloud Volumes ONTAP gespeichert sind.

Zum Zeitpunkt der Veröffentlichung sind Hyperscaler-Umgebungen nur auf herkömmliche NFS v3-Datastores beschränkt. Daher sind VVols nur mit lokalen ONTAP Systemen oder Cloud-vernetzten Systemen verfügbar, die die gesamten Funktionen von On-Premises-Systemen bereitstellen, z. B. von NetApp Partnern und Service-Providern auf der ganzen Welt.

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 die VVols-Unterstützung mit VASA 2.0 einführte, bezeichnete das Unternehmen das System

als „ein Integrations- und Management-Framework zur Bereitstellung eines neuen Betriebsmodells für externen Storage (SAN/NAS)“. Dieses Betriebsmodell bietet zusammen mit ONTAP Storage mehrere Vorteile.

Richtlinienbasiertes Management

Wie in Abschnitt 1.2 beschrieben, ermöglicht richtlinienbasiertes Management die Bereitstellung und das Management von VMs anhand von vordefinierten Richtlinien. Dies bietet verschiedene Vorteile FÜR IT-Abläufe:

- **Beschleunigung.** durch ONTAP Tools muss der vCenter Administrator keine Tickets mehr für die Storage-Bereitstellung beim Storage Team öffnen. ONTAP-Tools RBAC-Rollen in vCenter und im ONTAP System ermöglichen jedoch unabhängigen Teams (z. B. Storage-Teams) oder unabhängigen Aktivitäten desselben Teams, indem bei Bedarf der Zugriff auf bestimmte Funktionen eingeschränkt wird.
- **Intelligenterer 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 es, bei Bedarf die Storage-Kapazität bis zur individuellen Aggregatebene anzuzeigen und bei niedrigem Kapazitätsbedarf mehrere Alarmebenen bereitzustellen.

Granulares VM-Management auf dem modernen SAN

SAN-Storage-Systeme mit Fibre Channel und iSCSI wurden als erste von VMware für ESX unterstützt, allerdings fehlten ihnen die Managementmöglichkeiten individueller VM-Dateien und Festplatten aus dem Storage-System. Stattdessen werden LUNs bereitgestellt und VMFS managt die einzelnen Dateien. Dadurch wird es für das Storage-System schwierig, die Storage-Performance, das Klonen und den Schutz einzelner VMs direkt zu managen. VVols bieten Storage-Granularität, die Kunden, die NFS-Storage bereits nutzen, mit den robusten, hochperformanten SAN-Funktionen von ONTAP.

Mit vSphere 8 und ONTAP Tools für VMware vSphere 9.12 und höher sind nun dieselben granularen Steuerelemente, die von VVols für ältere SCSI-basierte Protokolle verwendet werden, in dem modernen Fibre-Channel-SAN unter Verwendung von NVMe over Fabrics verfügbar, um noch höhere Performance im großen Maßstab zu ermöglichen. Mit vSphere 8.0 Update 1 ist es jetzt möglich, eine umfassende End-to-End-NVMe-Lösung mit VVols zu implementieren, ohne dass eine I/O-Verschiebung im Hypervisor-Storage-Stack erforderlich ist.

Bessere Auslagerungsmöglichkeiten

VAAI bietet zwar eine Vielzahl an Operationen, die auf Storage verlagert werden, doch bestehen einige Lücken, die vom VASA Provider behoben werden. SAN VAAI kann keine von VMware gemanagten Snapshots in das Storage-System auslagern. NFS VAAI kann über VM gemanagte Snapshots auslagern, aber es gibt Einschränkungen, bei denen eine VM mit nativen Storage-Snapshots platziert wird. Da VVols individuelle LUNs, Namespaces oder Dateien für Virtual-Machine-Festplatten 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 zudem nicht das Verlagern von Klonvorgängen bei Migrationen mit heißem

(eingeschaltetem) Storage vMotion. Die VM muss ausgeschaltet sein, um bei Verwendung von VAAI mit herkömmlichen NFS-Datstores das Verlagern der Migration zu ermöglichen. Der VASA Provider in ONTAP ermöglicht nahezu sofortige, Storage-effiziente Klone für heiße und kalte Migrationen. Zudem unterstützt er nahezu sofortige Kopien für Volume-übergreifende Migrationen von VVols. Aufgrund dieser enormen Vorteile hinsichtlich der Storage-Effizienz können Sie die VVols Workloads unter dem optimal nutzen **"Effizienz-Garantie"** Programm. Auch wenn Volume-übergreifende Klone mit VAAI nicht Ihren Anforderungen entsprechen, werden Sie wahrscheinlich aufgrund der Verbesserungen bei den Kopien mit VVols eine geschäftliche Herausforderung bewältigen können.

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 VMware Tanzu Kubernetes Grid [TKG] Volumes.
 - Bereitstellung von Amazon EBS-ähnlichen Services über unabhängiges VMDK Lifecycle Management
- **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 werden schnell innerhalb eines einzelnen Volumes oder über mehrere Volumes in einem ONTAP Cluster hinweg erstellt – ein Vorteil im Vergleich zu herkömmlichen VAAI-fähigen Klonen. Außerdem sind sie Storage-effizient. Klone innerhalb eines Volumes nutzen ONTAP-Datei-Klone, die wie FlexClone Volumes sind und speichern nur Änderungen aus der Quell-vVol-Datei/LUN/Namespaces. Dadurch werden langfristige VMs für Produktions- oder andere Applikationszwecke schnell erstellt, benötigen nur minimalen Speicherplatz und profitieren vom Schutz auf VM-Ebene (durch das NetApp SnapCenter Plug-in für VMware vSphere, von VMware gemanagte Snapshots oder VADP-Backup) und Performance-Management (mit ONTAP QoS).
- 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 Services können über FCDs bereitgestellt werden, da eine FCD-VMDK, wie der Name schon andeutet, eine erstklassige Antwort in vSphere ist und einen Lebenszyklus hat, der unabhängig von den VMs gemanagt werden kann, an die es angeschlossen werden kann.

Verwendung von VVols mit ONTAP

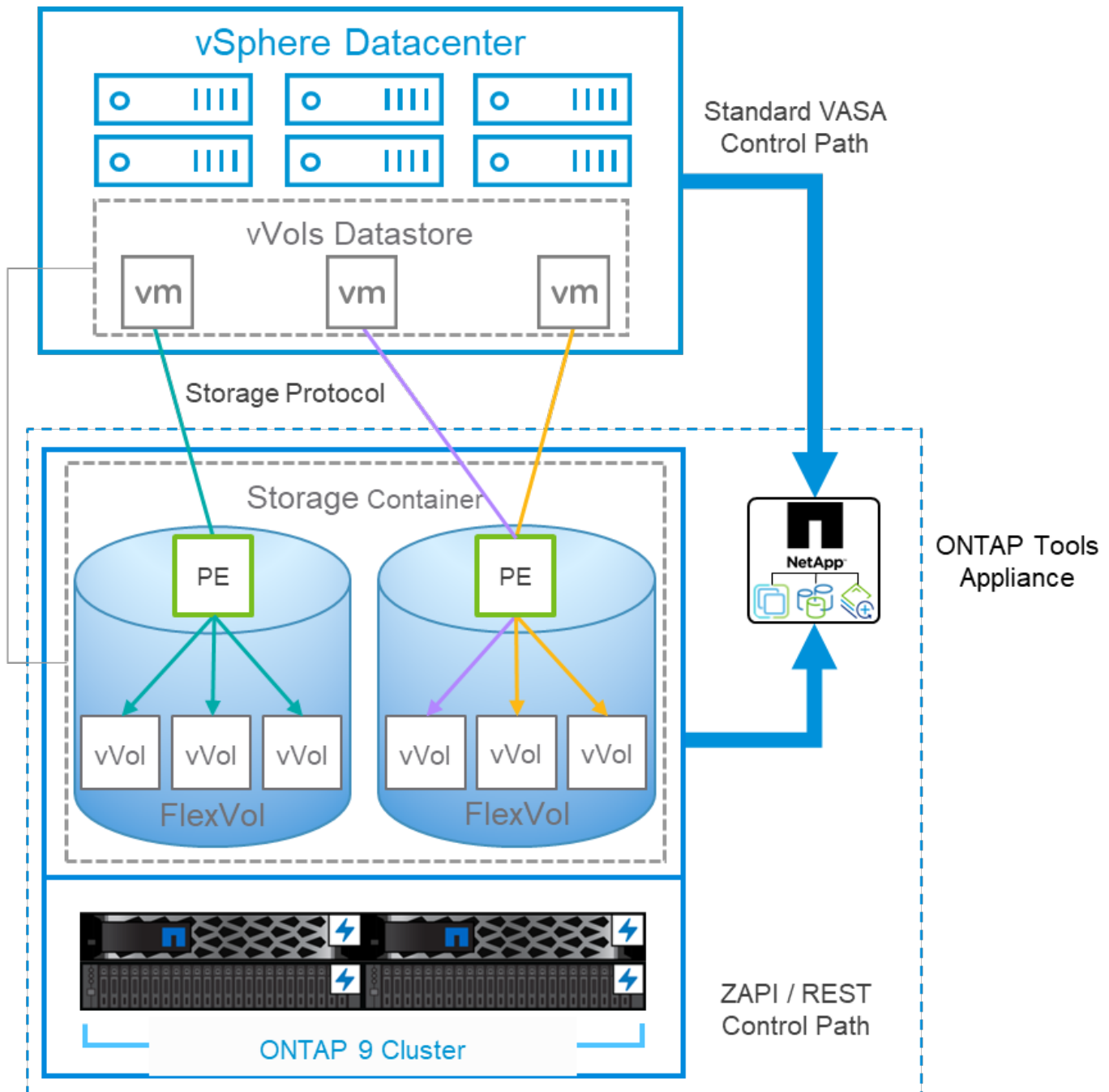
Für die Verwendung von VVols mit ONTAP muss die VASA Provider Software als Bestandteil der virtuellen ONTAP Tools für die VMware vSphere Appliance integriert sein.

Zu den ONTAP-Tools gehören außerdem vCenter-UI-Erweiterungen, REST-API-Server, Storage Replication Adapter für VMware Site Recovery Manager, Monitoring- und Host-Konfigurationstools sowie eine Reihe von Berichten, mit denen Sie Ihre VMware-Umgebung besser managen können.

Produkte und Dokumentation

Die ONTAP FlexClone Lizenz (in ONTAP One enthalten) und die ONTAP Tools Appliance sind die einzigen zusätzlichen Produkte, die für die Verwendung von VVols in Verbindung mit ONTAP erforderlich sind. Die neuesten Versionen der ONTAP Tools werden als einzige vereinheitlichte Appliance bereitgestellt und auf ESXi ausgeführt. Sie bieten die Funktionen von ehemals drei verschiedenen Appliances und Servern. Bei VVols ist es wichtig, die vCenter UI-Erweiterungen der ONTAP Tools oder REST-APIs als allgemeine Managementtools und Benutzeroberflächen für ONTAP Funktionen mit vSphere zusammen mit dem VASA Provider, der bestimmte VVols Funktionen bereitstellt, zu verwenden. Die SRA Komponente ist für herkömmliche Datastores enthalten, doch VMware Site Recovery Manager verwendet keine SRA für VVols. Stattdessen werden neue Services in SRM 8.3 und höher implementiert, bei denen der VASA-Provider für die VVols-Replizierung genutzt wird.

ONTAP nutzt die VASA Provider Architektur unter Verwendung von iSCSI oder FCP



Produktinstallation

Bei Neuinstallationen implementieren Sie die virtuelle Appliance in Ihrer vSphere Umgebung. Aktuelle Versionen der ONTAP Tools werden sich automatisch bei Ihrem vCenter registrieren und VASA Provider standardmäßig aktivieren. Zusätzlich zu den ESXi-Host- und vCenter-Server-Informationen benötigen Sie auch die IP-Adresskonfigurationsdetails für die Appliance. Wie bereits erwähnt, muss für VASA Provider die Lizenz ONTAP FlexClone bereits auf allen ONTAP Clustern installiert sein, die Sie für VVols verwenden möchten. Die Appliance verfügt über einen integrierten Watchdog, um die Verfügbarkeit zu gewährleisten. Als Best Practice sollte sie mit VMware High Availability und optional mit Fault Tolerance-Funktionen konfiguriert werden. Weitere Informationen finden Sie in Abschnitt 4.1. Installieren oder verschieben Sie die ONTAP Tools Appliance oder vCenter Server Appliance (VCSA) nicht auf VVols Storage, da dies verhindern kann, dass die Appliances neu gestartet werden.

In-Place-Upgrades von ONTAP Tools werden über die ISO-Datei für Upgrades unterstützt, die auf der NetApp Support Website (NSS) zum Download zur Verfügung steht. Befolgen Sie die Anweisungen des Bereitstellungs- und Setup-Handbuchs, um die Appliance zu aktualisieren.

Informationen zur Dimensionierung Ihrer virtuellen Appliance und zum Verständnis der Konfigurationsbeschränkungen finden Sie in diesem Knowledge Base-Artikel: ["Leitfaden zur Dimensionierung für ONTAP Tools für VMware vSphere"](#)

Produktdokumentation

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

["Für die vollständige Dokumentation Repository, besuchen Sie diesen Link zu docs.netapp.com"](#)

Los geht's

- ["Versionshinweise"](#)
- ["Erfahren Sie mehr über ONTAP Tools für VMware vSphere"](#)
- ["ONTAP-Tools Schnellstartanleitung"](#)
- ["Implementierung von ONTAP Tools"](#)
- ["Upgrade von ONTAP-Tools"](#)

Verwenden Sie ONTAP-Tools

- ["Bereitstellung herkömmlicher Datastores"](#)
- ["Bereitstellung von VVols Datastores"](#)
- ["Konfigurieren Sie die rollenbasierte Zugriffssteuerung"](#)
- ["Konfigurieren Sie die Remote-Diagnose"](#)
- ["Konfigurieren Sie Hochverfügbarkeit"](#)

Sicherung und Management von Datenspeichern

- ["Sicherung herkömmlicher Datastores" Mit SRM](#)
- ["Sicherung von auf VVols basierenden Virtual Machines" Mit SRM](#)
- ["Überwachen Sie herkömmliche Datenspeicher und Virtual Machines"](#)
- ["Überwachen Sie VVols Datastores und Virtual Machines"](#)

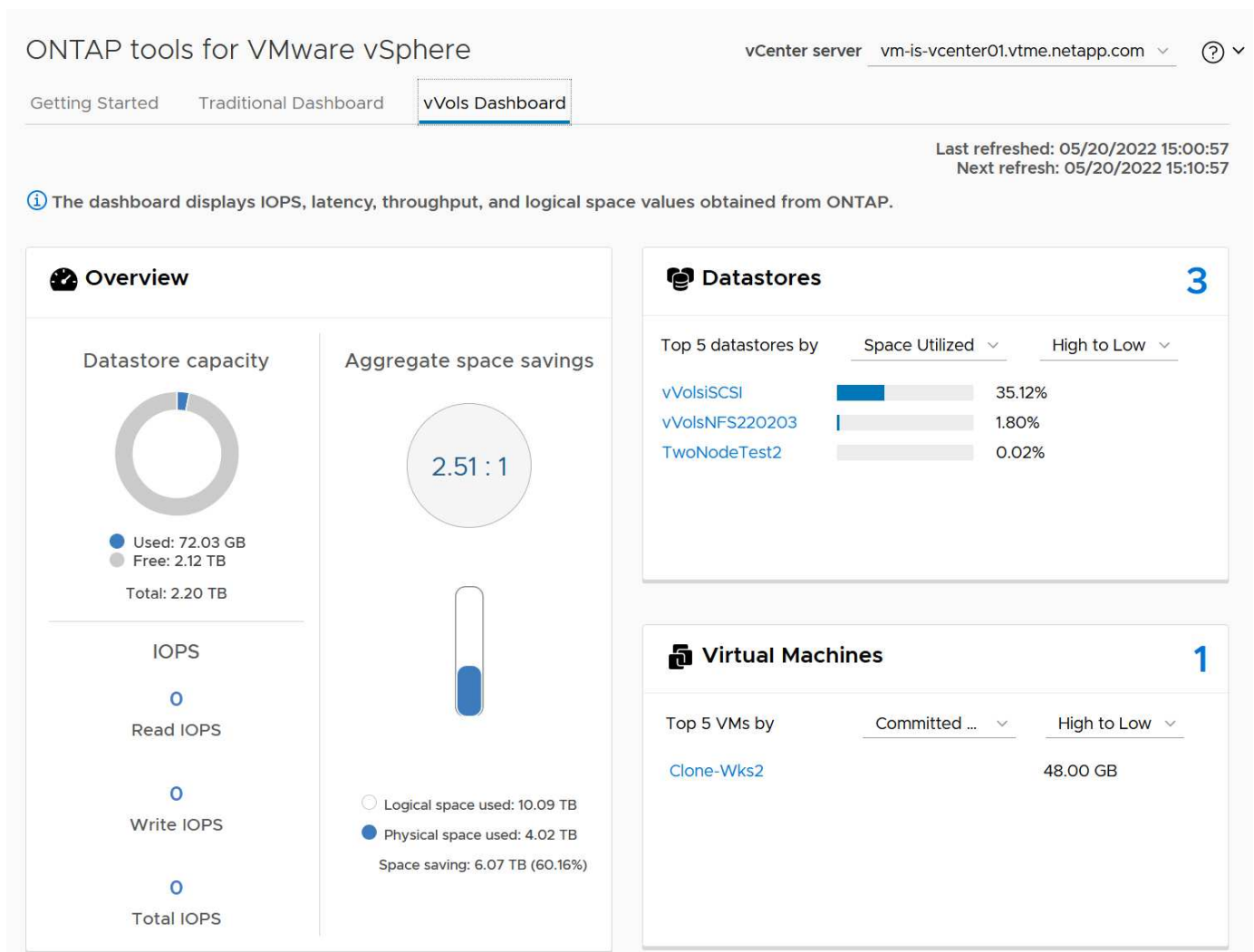
Zusätzlich zur Produktdokumentation gibt es möglicherweise Artikel aus der Support Knowledgebase, die hilfreich sein könnten.

- ["So führen Sie eine VASA Provider Disaster Recovery - Resolution Guide durch"](#)

VASA Provider Dashboard

Vasa Provider umfasst ein Dashboard mit Performance- und Kapazitätsinformationen für einzelne VVols VMs. Diese Informationen stammen direkt von ONTAP für die vVol Dateien und LUNs, einschließlich Latenz, IOPS, Durchsatz und Uptime für die Top 5 VMs sowie Latenz und IOPS für die Top 5 Datastores. Bei Verwendung von ONTAP 9.7 oder höher ist sie standardmäßig aktiviert. Es kann bis zu 30 Minuten dauern, bis die ersten Daten abgerufen und im Dashboard angezeigt werden.

ONTAP Tools VVols Dashboard



Best Practices In Sich Vereint

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, die durch VMware definiert sind (siehe veröffentlicht ["Konfigurationsmaxima"](#)). In der folgenden Tabelle sind bestimmte ONTAP-Limits für Größe und Anzahl von VVols zusammengefasst. Prüfen Sie immer das ["NetApp Hardware Universe"](#) Für aktualisierte Grenzwerte für Anzahl und Größe der LUNs und Dateien.

ONTAP VVols Grenzen

Kapazität/Funktion	SAN (SCSI oder NVMe-of)	NFS
Maximale VVols-Größe	62 tib*	62 tib*
Maximale Anzahl VVols pro FlexVol Volume	1024	2 Milliarden
Maximale Anzahl VVols pro ONTAP Node	Bis zu 12,288**	50 Milliarden
Maximale Anzahl VVols pro ONTAP-Paar	Bis zu 24,576**	50 Milliarden
Maximale Anzahl von VVols pro ONTAP Cluster	Bis zu 98,304**	Keine spezifische Cluster-Beschränkung
Maximale QoS-Objekte (gemeinsam genutzte Richtliniengruppe und individuelle VVols Service-Level)	12,000 bis ONTAP 9.3; 40,000 mit ONTAP 9.4 und höher	

- Größenbeschränkung auf Basis von ASA Systemen oder AFF und FAS Systemen mit ONTAP 9.12.1P2 und höher
 - Die Anzahl der SAN-VVols (NVMe-Namespaces oder LUNs) variiert je nach Plattform. Prüfen Sie immer das ["NetApp Hardware Universe"](#) Für aktualisierte Grenzwerte für Anzahl und Größe der LUNs und Dateien.

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 anhand von ONTAP Best Practices und unter Einhaltung der definierten Storage-Funktionsprofile 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 „Hühnchen- und Eiersituation“ führen, wenn Sie die Appliances neu starten müssen, da sie nicht in der Lage sind, während sie neu starten ihre eigenen VVols abzuheben. 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.

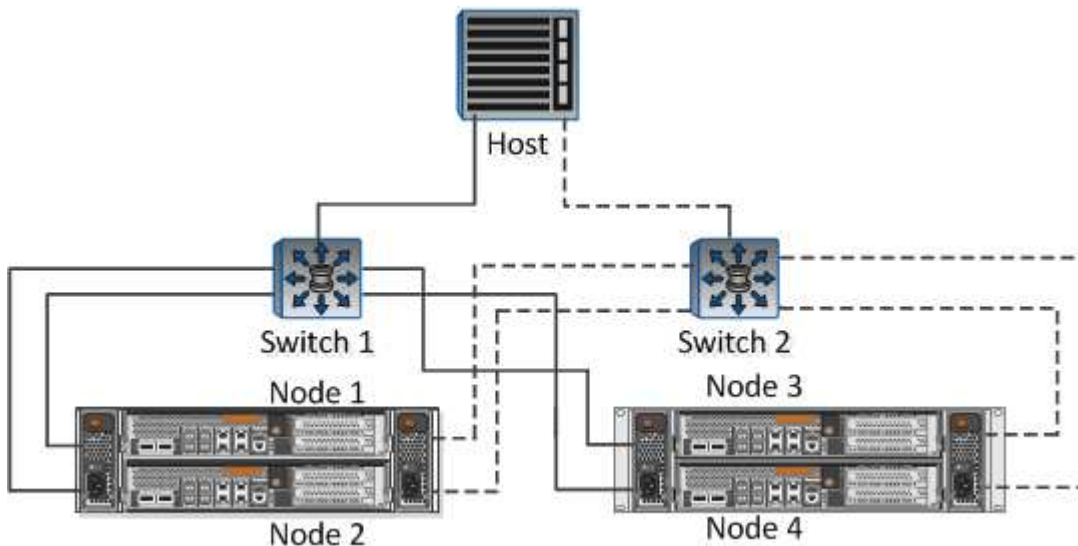
Unterstützte Storage-Funktionen wie QoS, Personality und mehr haben sich in verschiedenen Versionen des VASA Providers verändert, einige sind von der ONTAP Version abhängig. Die Verwendung verschiedener Versionen in einem ONTAP-Cluster oder das Verschieben von VVols zwischen Clustern mit unterschiedlichen

Versionen können zu unerwartetem Verhalten oder Compliance-Alarmen führen.

Zonen Sie Ihre Fibre Channel Fabric vor der Verwendung von NVMe/FC oder 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 Unterstützung FlexVols nach Ihren Bedürfnissen.*

Es ist durchaus 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.

Speicherfähigkeitsprofile (SCPs) einfach halten.

Vermeiden Sie die Angabe von Funktionen, die nicht erforderlich sind, indem Sie sie auf beliebig festlegen. Dadurch werden Probleme beim Auswählen oder Erstellen von FlexVol-Volumes minimiert. Wenn bei VASA

Provider 7.1 und älteren Versionen beispielsweise die Komprimierung mit der SCP-Standardeinstellung „Nein“ beibehalten wird, wird versucht, die Komprimierung selbst auf einem AFF-System zu deaktivieren.

Verwenden Sie die Standard-SCPs als Beispielvorlagen, um Ihre eigenen zu erstellen.

Die im Lieferumfang enthaltenen SCPs sind für die meisten allgemeinen Anwendungen geeignet, aber Ihre Anforderungen können unterschiedlich sein.

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.

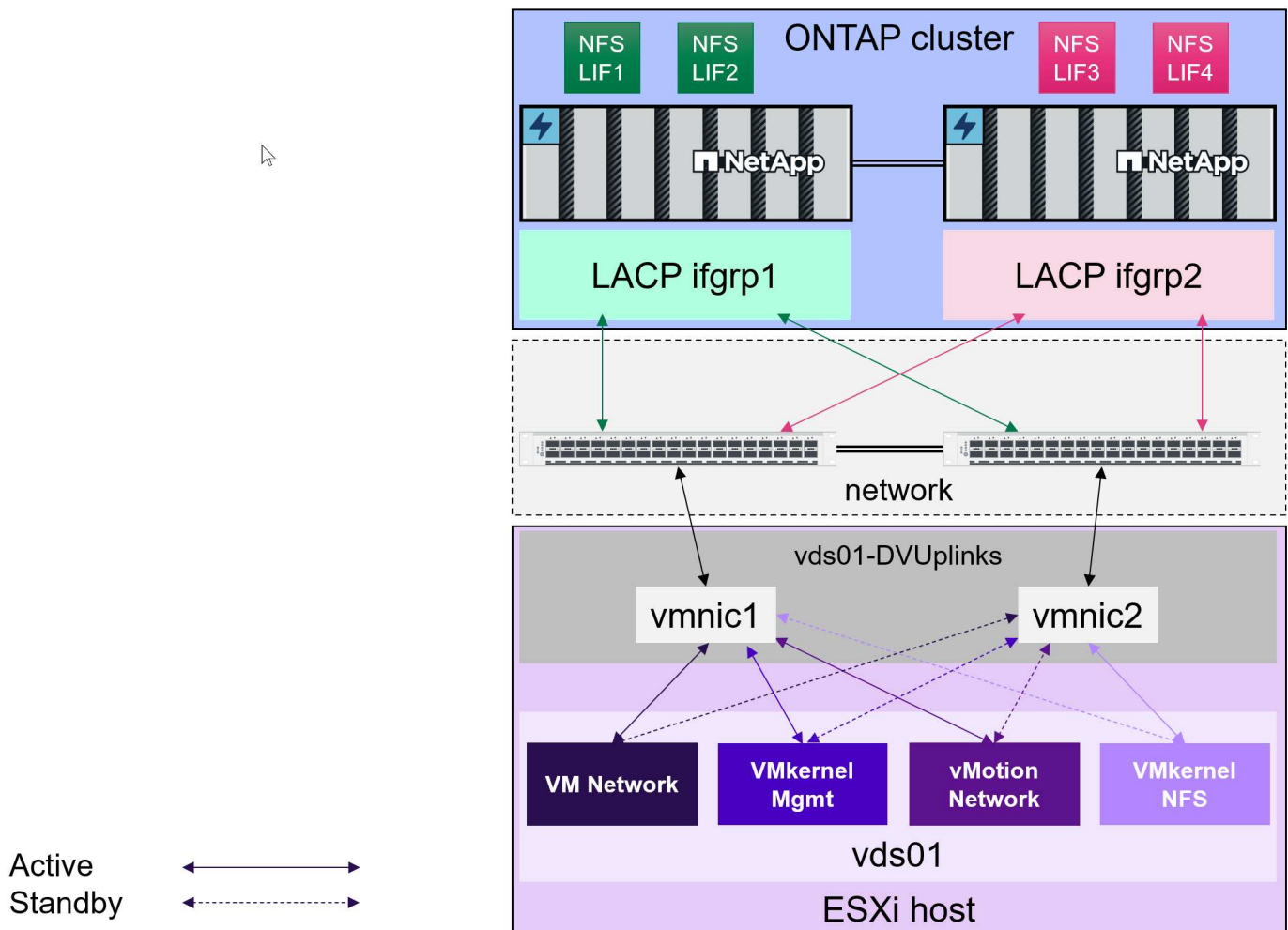
Stellen Sie sicher, dass Sie ausreichend Daten-LIFs haben.

Erstellen Sie mindestens zwei LIFs pro Node und HA-Paar. Je nach Workload werden weitere erforderlich.

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



Implementierung von VVols Storage

Zum Erstellen von VVols Storage für Ihre VMs sind verschiedene Schritte erforderlich.

Die ersten beiden Schritte sind für eine bestehende vSphere-Umgebung, die ONTAP für herkömmliche Datastores verwendet, möglicherweise nicht erforderlich. Möglicherweise verwenden Sie bereits ONTAP Tools für das Management, die Automatisierung und die Berichterstellung mit Ihrem VMFS- oder herkömmlichen NFS-basierten Storage. Diese Schritte werden im folgenden Abschnitt näher erläutert.

1. Storage Virtual Machine (SVM) und deren Protokollkonfiguration erstellen. Sie wählen zwischen NVMe/FC, NFSv3, NFSv4.1, iSCSI, FCP oder eine Kombination dieser Optionen. Sie können entweder die Assistenten von ONTAP System Manager oder die Cluster Shell-Befehlszeile verwenden.
 - 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.
 - Derzeit können Volumes erstellt werden, doch es ist einfacher, sie vom Assistenten „*Provisioning Datastore*“ erstellen zu lassen. Die einzige Ausnahme von dieser Regel ist, wenn Sie eine VVols Replizierung mit VMware Site Recovery Manager verwenden möchten. Die Einrichtung solcher FlexVol Volumes mit bestehenden SnapMirror Beziehungen ist einfacher. Beachten Sie, dass QoS auf keinen Volumes für VVols aktiviert wird, da diese über SPBM und ONTAP Tools gemanagt werden sollen.
2. Implementieren Sie ONTAP Tools für VMware vSphere mit der von der NetApp Support-Website heruntergeladenen OVA.
3. Konfigurieren Sie ONTAP Tools für Ihre Umgebung.
 - Fügen Sie den ONTAP-Cluster zu den ONTAP-Tools unter *Storage Systems* hinzu
 - ONTAP Tools und SRA unterstützen zwar Anmeldedaten auf Cluster- und SVM-Ebene, doch unterstützt der VASA Provider nur Zugangsdaten auf Cluster-Ebene für Storage-Systeme. Der Grund dafür ist, dass viele der für VVols verwendeten APIs nur auf Cluster-Ebene verfügbar sind. Wenn Sie daher VVols verwenden möchten, müssen Sie die ONTAP-Cluster mit den Anmeldedaten für den Cluster-Umfang hinzufügen.
 - Wenn sich Ihre ONTAP-Daten-LIFs in unterschiedlichen Subnetzen von Ihren VMkernel-Adaptern befinden, müssen Sie die VMkernel-Adapter-Subnetze zur Liste der ausgewählten Subnetze im Einstellungsmenü der ONTAP-Tools hinzufügen. Standardmäßig sichern ONTAP Tools Ihren Storage-Datenverkehr nur durch lokalen Subnetzzugriff.
 - Die ONTAP Tools enthalten mehrere vordefinierte Richtlinien, die verwendet werden können oder sehen [Verwalten von VMs mithilfe von Richtlinien](#) Anleitung zum Erstellen von SCPs.
4. Verwenden Sie das Menü „*ONTAP Tools*“ in vCenter, um den Assistenten „*Provisioning Datastore*“ zu starten.
5. Geben Sie einen aussagekräftigen Namen ein, und wählen Sie das gewünschte Protokoll aus. Sie können auch eine Beschreibung des Datastore angeben.
6. Wählen Sie einen oder mehrere SCPs aus, die vom VVols-Datastore unterstützt werden sollen. Dadurch werden alle ONTAP-Systeme herausgefiltert, die nicht mit dem Profil übereinstimmen. Wählen Sie in der Ergebnisliste den gewünschten Cluster und die gewünschte SVM aus.
7. Verwenden Sie den Assistenten, um neue FlexVol-Volumes für jeden der angegebenen SCPs zu erstellen, oder verwenden Sie vorhandene Volumes, indem Sie das entsprechende Optionsfeld auswählen.
8. Erstellen Sie VM-Richtlinien für jedes SCP, das im Datastore verwendet wird, über das Menü „*Policies and Profiles*“ in der vCenter UI.
9. Wählen Sie den Storage-Regelsatz „NetApp.Clustered.Data.ONTAP.VP.vvol“ aus. Der Storage-Regelsatz „NetApp.Clustered.Data.ONTAP.VP.VASA10“ gilt für die SPBM-Unterstützung bei Datastores ohne VVols

10. Beim Erstellen einer VM-Speicherrichtlinie geben Sie das Storage Capability Profile nach Namen an. Sie können in diesem Schritt auch die SnapMirror Richtlinienabstimmung über die Registerkarte „Replication“ und über die Registerkarte „Tags“ konfigurieren. Beachten Sie, dass Tags bereits erstellt werden müssen, um ausgewählt werden zu können.
11. Erstellen Sie Ihre VMs, indem Sie unter Select Storage die VM Storage Policy und kompatiblen Datenspeicher auswählen.

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. Migrationsvorgänge werden für SAN VMFS zu VVols Migrationen mit vSphere 6.0 und höher verlagert, jedoch nicht von NAS VMDKs zu VVols.

Verwalten von VMs mithilfe von Richtlinien

Um die Storage-Bereitstellung mit richtlinienbasiertem Management zu automatisieren, müssen wir

- Definieren Sie mit Storage Capability Profiles (SCPs) die Funktionen des Speichers (ONTAP-Knoten und FlexVol-Volume).
- Erstellen Sie VM-Storage-Richtlinien, die den definierten SCPs zugeordnet sind.

NetApp hat die Funktionen und die Zuordnung ab VASA Provider 7.2 vereinfacht, wobei die Verbesserungen in späteren Versionen fortgeführt werden. Dieser Abschnitt konzentriert sich auf diesen neuen Ansatz. Frühere Versionen unterstützten eine größere Anzahl von Funktionen und erlaubten die individuelle Zuordnung zu Storage-Richtlinien, allerdings wird dieser Ansatz nicht mehr unterstützt.

Funktionen des Storage-Funktionsprofils nach ONTAP-Tools

SCP-Fähigkeit	Fähigkeitswerte	Release-Unterstützung	Hinweise
Komprimierung	Ja, Nein, Alle	Alle	Obligatorisch für AFF ab 7.2.
Deduplizierung	Ja, Nein, Alle	Alle	Mandatory für AFF in 7.2 und später.
Verschlüsselung	Ja, Nein, Alle	7.2 und höher	Wählt/erstellt ein verschlüsseltes FlexVol-Volume. ONTAP-Lizenz erforderlich.
Maximale IOPS	<number>	7.1 und später, aber Unterschiede	Aufgeführt unter QoS Policy Group für 7.2 und höher. Siehe Performance Management mit ONTAP Tools 9.10 und höher . Finden Sie weitere Informationen.

SCP-Fähigkeit	Fähigkeitswerte	Release-Unterstützung	Hinweise
* Persönlichkeit*	A FF, FAS	7.2 und höher	FAS beinhaltet auch andere nicht-All Flash FAS Systeme wie beispielsweise ONTAP Select. AFF umfasst ASA.
Protokoll	NFS, NFS 4.1, iSCSI, FCP, NVMe/FC, Alle	7.1 und früher, 9.10 und höher	7.2-9.8 ist effektiv "jede". Ebenfalls ab 9.10, wo NFS 4.1 und NVMe/FC in die ursprüngliche Liste aufgenommen wurden.
Speicherplatzreserve (Thin Provisioning)	Dünn, Dick, (Beliebig)	Alle, aber Unterschiede	7.1 und früher als Thin Provisioning bezeichnet, wodurch auch beliebige Werte zulässig sind. Genannt Space Reserve in 7.2. Alle Releases sind standardmäßig Thin.
Tiering-Richtlinie	Beliebig, Keine, Snapshot, Automatisch	7.2 und höher	Verwendet für FabricPool - erfordert AFF oder ASA mit ONTAP 9.4 oder höher. Nur Snapshot ist empfohlen, wenn eine lokale S3 Lösung wie NetApp StorageGRID nicht verwendet wird.

Erstellen Von Storage-Funktionsprofilen

NetApp VASA Provider verfügt über mehrere vordefinierte SCPs. Neue SCPs können manuell über die vCenter UI oder über die Automatisierung mit REST-APIs erstellt werden. Durch das Angeben von Funktionen in einem neuen Profil, das Klonen eines vorhandenen Profils oder das automatische Generieren von Profilen aus bestehenden herkömmlichen Datastores. Dies erfolgt über die Menüs unter ONTAP Tools. Verwenden Sie *Storage Capability Profiles*, um ein Profil zu erstellen oder zu klonen, und *Storage Mapping*, um ein Profil automatisch zu generieren.

Storage-Funktionen für ONTAP Tools 9.10 und höher

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

General

Specify a name and description for the storage capability profile. ?

Name:

Description:

CANCEL

NEXT

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary

Platform

Platform:

CANCEL

BACK

NEXT

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol**
- 4 Performance
- 5 Storage attributes
- 6 Summary

Protocol

Protocol:

Any

Any
FCP
NFS
NFS 4.1
iSCSI
NVMe/FC

CANCEL

BACK

NEXT

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance**
- 5 Storage attributes
- 6 Summary

Performance

☐ None ⓘ

☒ QoS policy group ⓘ

Min IOPS: 1000

Max IOPS:

☒ Unlimited

CANCEL

BACK

NEXT

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes**
- 6 Summary

Storage attributes

Deduplication:	Yes
Compression:	Yes
Space reserve:	Thin
Encryption:	Yes
Tiering policy (FabricPool):	Snapshot

CANCEL
BACK
NEXT

Create Storage Capability Profile

- 1 General
- 2 Platform
- 3 Protocol
- 4 Performance
- 5 Storage attributes
- 6 Summary**

Summary

Name:	New_SCP
Description:	N/A
Platform:	All Flash FAS (AFF)
Protocol:	Any
Min IOPS:	1000 IOPS
Max IOPS:	Unlimited
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	Yes
Tiering policy (FabricPool):	Snapshot

CANCEL
BACK
FINISH

Erstellen von VVols Datastores

Nachdem die erforderlichen SCPs erstellt wurden, können sie auch zur Erstellung des VVols-Datastores (und optional auch FlexVol Volumes für den Datastore) verwendet werden. 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 einen oder mehrere SCPs aus, die vom Datastore unterstützt werden sollen, und wählen Sie dann aus vorhandenen FlexVol Volumes aus bzw. stellen Sie neue FlexVol Volumes für den Datastore bereit. Geben Sie schließlich das Standard-SCP für den Datastore an, das für VMs verwendet wird, für die kein durch die Richtlinie angegebenes SCP angegeben ist, sowie für Swap-VVols (diese erfordern keinen hochperformanten Storage).

Erstellen von VM-Storage-Richtlinien

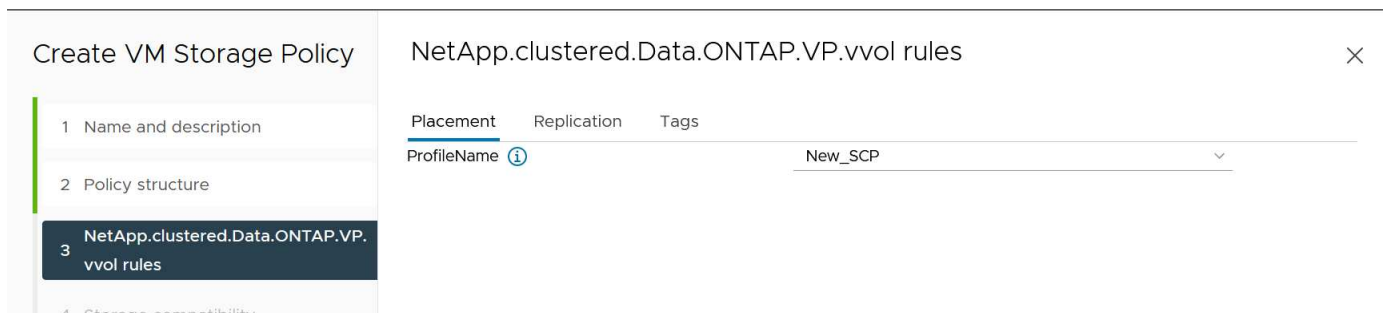
VM-Storage-Richtlinien managen in vSphere optionale Funktionen wie Storage I/O Control oder vSphere Encryption. Sie werden auch zusammen mit VVols verwendet, um spezifische Storage-Funktionen auf die VM

anzuwenden. Verwenden Sie den Storage-Typ „NetApp.Clustered.Data.ONTAP.VP.vvol“ und die Regel „ProfileName“, um mithilfe der Richtlinie ein bestimmtes SCP auf VMs anzuwenden. Ein Beispiel hierfür mit den ONTAP Tools VASA Provider finden Sie unter [Link:vmware-vmols-ontap.HTML#Best Practices](#)[Beispiel für eine Netzwerkkonfiguration mit VVols über NFS v3]. Regeln für Storage „NetApp.Clustered.Data.ONTAP.VP.VASA10“ sollen mit Datastores ohne VVols verwendet werden.

Frühere Versionen sind ähnlich, aber wie in erwähnt [Funktionen des Storage-Funktionsprofils nach ONTAP-Tools](#), Ihre Optionen variieren.

Sobald die Storage-Richtlinie erstellt wurde, kann sie verwendet werden, wenn neue VMs bereitgestellt werden, wie in dargestellt ["Bereitstellung der VM mithilfe der Storage-Richtlinie"](#). Richtlinien zur Nutzung von Performance-Management-Funktionen mit VASA Provider 7.2 finden Sie in [Performance Management mit ONTAP Tools 9.10 und höher](#).

Erstellen der Richtlinie für den VM-Storage mit ONTAP Tools VASA Provider 9.10



Performance Management mit ONTAP Tools 9.10 und höher

- ONTAP Tools 9.10 verwendet einen eigenen Algorithmus für optimierte Platzierung, um ein neues vVol im besten FlexVol Volume in einem VVols Datastore zu platzieren. Die Platzierung basiert auf dem angegebenen SCP und übereinstimmenden FlexVol-Volumes. Dadurch wird sichergestellt, dass der Datastore und der zugrunde liegende Storage die angegebenen Performance-Anforderungen erfüllen können.
- Wenn sich Funktionen für die Performance wie Min. Und Max. Ändern, muss die spezifische Konfiguration entsprechend verändert werden.
 - **Min und Max IOPS** können in einem SCP angegeben und in einer VM Policy verwendet werden.
 - Wenn Sie die IOPS im SCP ändern, wird die QoS auf den VVols erst geändert, wenn die VM-Richtlinie bearbeitet und dann auf die VMs angewendet wird, die sie verwenden (siehe [Storage-Funktionen für ONTAP Tools 9.10 und höher](#)). Oder erstellen Sie ein neues SCP mit den gewünschten IOPS und ändern Sie die Richtlinie, um es zu verwenden (und erneut auf VMs anzuwenden). Im Allgemeinen wird empfohlen, einfach separate SCPs und VM-Storage-Richtlinien für verschiedene Service-Ebenen zu definieren und einfach die VM-Storage-Richtlinie für die VM zu ändern.
 - AFF- und FAS-Persönlichkeiten haben unterschiedliche IOPS-Einstellungen. Sowohl Min. Als auch Max. Sind auf AFF verfügbar. Nicht-All Flash FAS Systeme können jedoch nur die IOPS-Maximaleinstellungen verwenden.
- In einigen Fällen muss ein vVol nach einer Richtlinienänderung (entweder manuell oder automatisch durch VASA Provider und ONTAP) migriert werden:
 - Einige Änderungen erfordern keine Migration (wie beispielsweise eine Änderung der maximalen IOPS, die sofort auf die VM angewendet werden kann, wie oben beschrieben).
 - Wenn die Richtlinienänderung nicht vom aktuellen FlexVol Volume unterstützt werden kann, in dem

das vVol gespeichert ist (beispielsweise unterstützt die Plattform die angeforderte Verschlüsselungs- oder Tiering-Richtlinie nicht), müssen Sie die VM manuell in vCenter migrieren.

- 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

VM Storage Policies

CREATE CHECK EDIT CLONE **REAPPLY** DELETE Filter

<input type="checkbox"/>	Name	VC
<input type="checkbox"/>	Management Storage Policy - Large	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	VVol No Requirements Policy	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage Policy - Stretched Lite	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	VM Encryption Policy	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage policy - Encryption	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage Policy - Single Node	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Management Storage policy - Thin	vm-is-vcenter01.vtme.netapp.com
<input checked="" type="checkbox"/>	AFF_iSCSI_VMSP	vm-is-vcenter01.vtme.netapp.com
<input type="checkbox"/>	Host-local PMem Default Storage Policy	vm-is-vcenter01.vtme.netapp.com

1 14 items

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-Datstores 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).

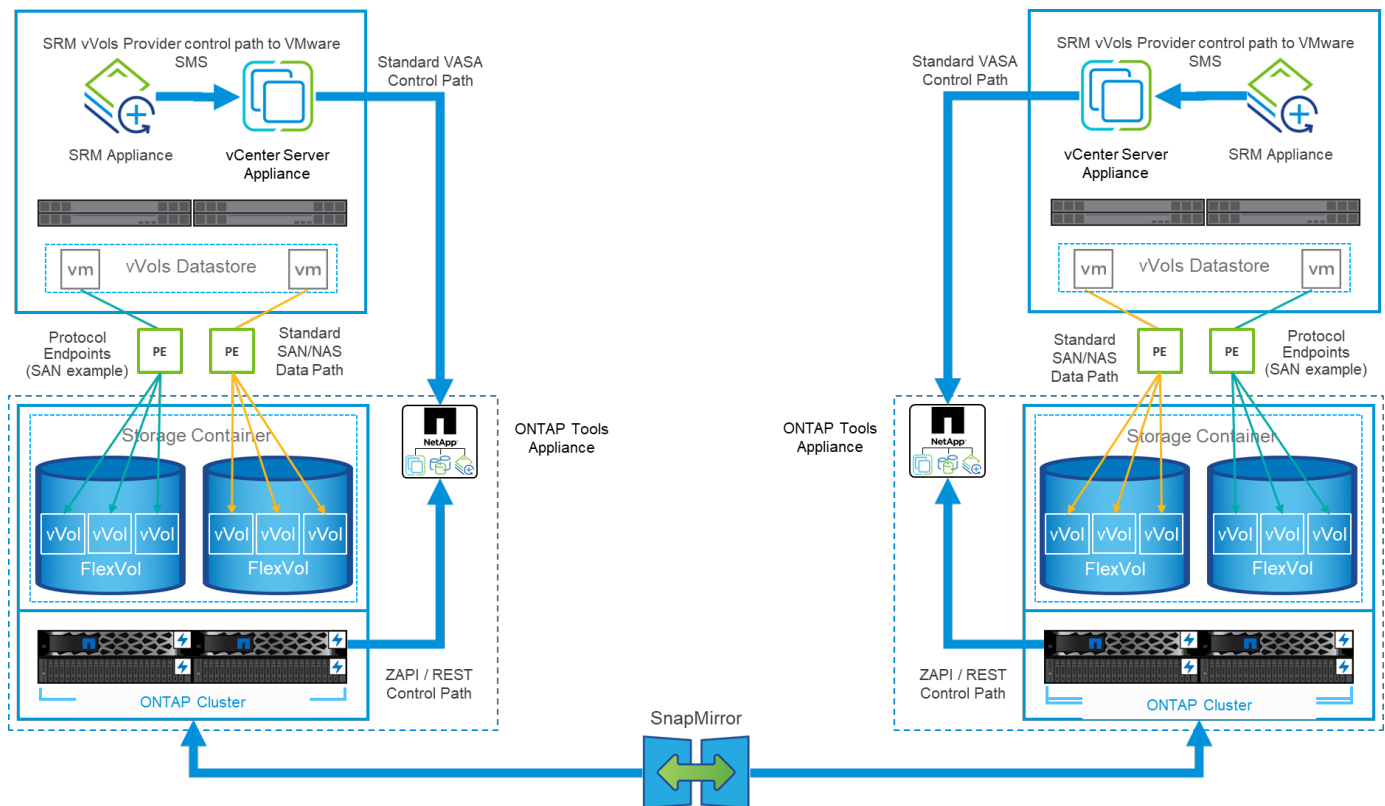
Diese Anforderung an ein Software-Tool ist für das Management der VVols Replizierung noch wichtiger. Einige Aspekte können durch native Funktionen gemanagt werden (beispielsweise werden durch VMware gemanagte Snapshots von VVols auf ONTAP verlagert, bei denen schnelle, effiziente Datei- oder LUN-Klone 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, FlexVols 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.

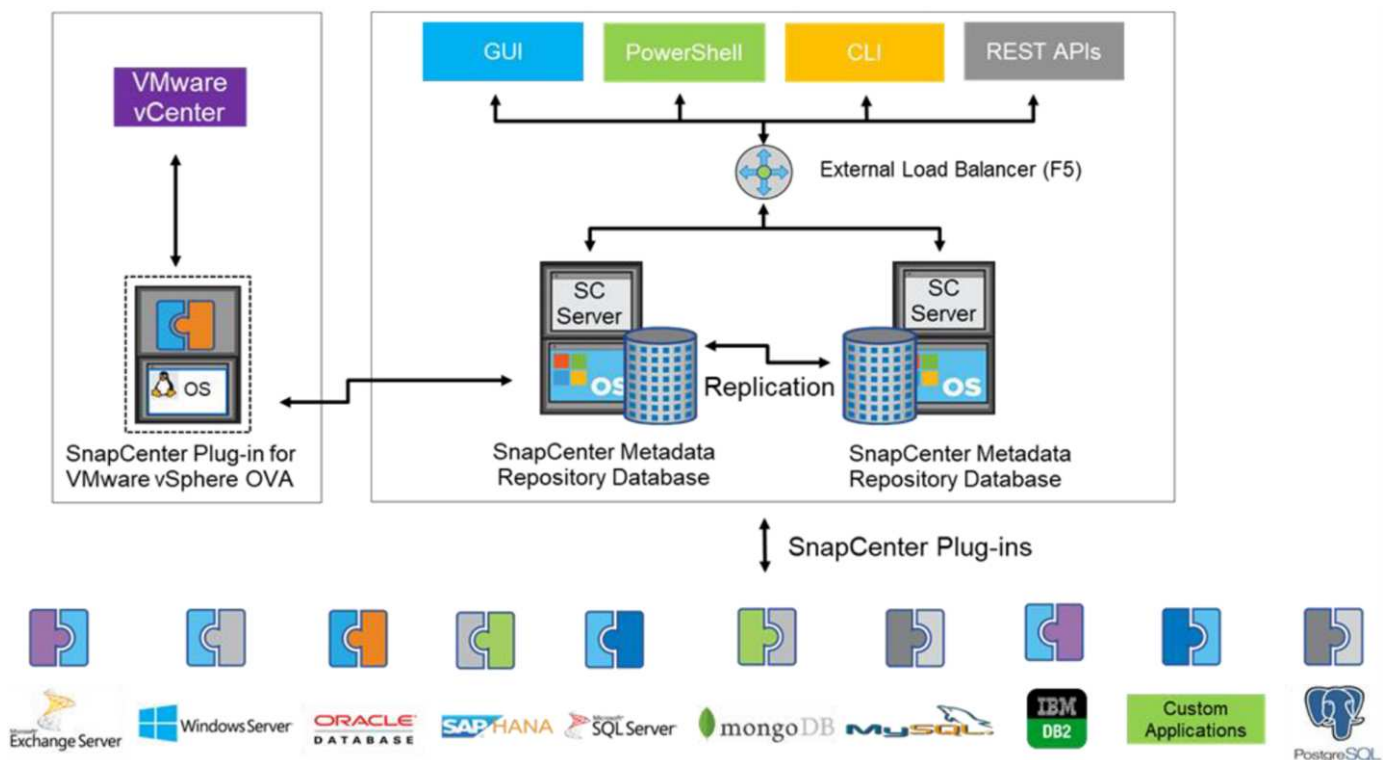
Die Unterstützung für vSphere 8.0 wurde mit SCV 4.7 eingeführt, wobei eine isolierte lokale Plug-in-Architektur verwendet wurde. Die Unterstützung für vSphere 8.0U1 wurde zu SCV 4.8 hinzugefügt, wodurch die neue Remote-Plug-in-Architektur vollständig umgestellt wurde.

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

Edit Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

✓ 5. Schedules

✓ 6. Summary

vCenter Server:

vm-is-vcenter01.vtme.netapp.com

Name:

vVols_VMs

Description:

Description

Notification:

Never

Email send from:

Error or Warnings

Email send to:

Errors

Email subject:

Always

Latest Snapshot name

☒ Enable _recent suffix for latest Snapshot Copy ⓘ

Custom snapshot format:

☐ Use custom name format for Snapshot copy

Note that the Plug-in for VMware vSphere cannot do the following:

BACK

NEXT

FINISH

CANCEL

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

Neben einer Vielzahl von Knowledgebase Artikeln zu NetApp Virtualisierungsprodukten 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 Site Recovery Manager mit ONTAP

ONTAP ist seit seiner Einführung in das moderne Datacenter im Jahr 2002 eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich um innovative Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen.

Dieses Dokument enthält eine Einführung in die ONTAP Lösung für VMware Site Recovery Manager (SRM), die branchenführende VMware Software für Disaster Recovery (DR), sowie in die neuesten Produktinformationen und Best Practices zur Optimierung der Bereitstellung, Risikominderung und Vereinfachung des fortlaufenden Managements.



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 9.12 (einschließlich NetApp Storage Replication Adapter [SRA] und VASA Provider [VP]) sowie VMware Site Recovery Manager 8.7 verwendet werden.

Vorteile von ONTAP mit SRM

Die NetApp Datenmanagementplattformen auf der Basis von ONTAP Software sind eine der am weitesten verbreiteten Storage-Lösungen für SRM. Die Gründe hierfür sind vielfältig: Eine sichere, hochperformante, einheitliche Protokoll-Datenmanagementplattform (NAS und SAN zusammen), die branchenweit definierte

Storage-Effizienz, Mandantenfähigkeit, Quality-of-Service-Kontrollen, Datensicherung mit platzsparenden Snapshots und Replizierung mit SnapMirror bietet. Dabei werden native Hybrid-Multi-Cloud-Integrationen für die Sicherung von VMware Workloads sowie eine Fülle von Automatisierungs- und Orchestrierungs-Tools blitzschnell verfügbar.

Wenn Sie SnapMirror für die Array-basierte Replizierung nutzen, profitieren Sie von einer der bewährten und ausgereiftesten Technologien von ONTAP. Mit SnapMirror profitieren Sie von sicheren und hocheffizienten Datentransfers, wobei nur geänderte Datenblöcke kopiert werden, nicht die gesamten VMs oder Datastores. Selbst diese Blöcke profitieren von Platzeinsparungen wie Deduplizierung, Komprimierung und Data-Compaction. Moderne ONTAP Systeme verwenden jetzt versionsunabhängiges SnapMirror für die flexible Auswahl von Quell- und Ziel-Clustern. SnapMirror hat sich tatsächlich zu einem der leistungsstärksten Tools für Disaster Recovery entwickelt.

Ganz gleich, ob Sie herkömmliche NFS-, iSCSI- oder Fibre Channel-Attached Datastores verwenden (jetzt mit Unterstützung für VVols Datastores) – SRM bietet Ihnen einen robusten Erstanbieter, der die besten ONTAP Funktionen für Disaster Recovery oder Planung der Datacenter-Migration und -Orchestrierung nutzt.

Wie SRM ONTAP 9 nutzt

SRM 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, 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 dieses Plug-in bei der Verwendung von vSphere bei Systemen mit ONTAP Software.
- Vasa Provider für ONTAP unterstützt 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. Es unterstützt die Unterstützung von VMware Virtual Volumes (VVols) und das Management von Storage-Funktionsprofilen (einschließlich VVols Replizierungsfunktionen) und der individuellen VM VVols Performance. Außerdem gibt es Alarmer zur Überwachung der Kapazität und der Konformität mit den Profilen. In Verbindung mit SRM ermöglicht der VASA Provider für ONTAP Unterstützung für VVols basierte Virtual Machines, ohne dass ein SRA Adapter auf dem SRM Server installiert werden muss.
- SRA wird zusammen mit SRM 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. Sie enthält sowohl eine SRA Server-Appliance als auch SRA Adapter für den Windows SRM Server und die SRM Appliance.

Nachdem Sie die SRA Adapter auf dem SRM-Server zum Schutz von Datastores außerhalb von VVols sowie zur aktivierten VVols-Replizierung in den VASA Provider-Einstellungen installiert und konfiguriert haben, können Sie mit der Aufgabe beginnen, Ihre vSphere Umgebung für die Disaster Recovery zu konfigurieren.

SRA und VASA Provider bieten eine Befehlszeilenschnittstelle für den SRM Server zum Managen der ONTAP FlexVols, die Ihre VMware Virtual Machines (VMs) enthalten, sowie zur SnapMirror Replizierung, die sie sichern.

Ab SRM 8.3 wurde ein neuer SRM VVols Provider-Kontrollpfad in den SRM Server eingeführt, der die IT in die Lage versetzt, mit dem vCenter Server und darüber hinaus ohne SRA mit dem VASA Provider zu kommunizieren. Auf diese Weise konnte der SRM Server eine wesentlich umfassendere Kontrolle über das ONTAP Cluster nutzen als bisher möglich, da VASA eine vollständige API für eine nahtlose Integration bietet.

SRM kann Ihren DR-Plan mithilfe der proprietären NetApp FlexClone Technologie unterbrechungsfrei testen, um nahezu sofortige Klone Ihrer geschützten Datenspeicher an Ihrem DR-Standort zu erstellen. SRM erstellt eine Sandbox-Umgebung für sichere Tests, damit sowohl Ihre Organisation als auch Ihre Kunden bei einem echten Ausfall geschützt sind. So können Ihre Unternehmen sicher sein, dass bei einem Ausfall ein Failover ausgeführt werden kann.

Bei einem echten Ausfall oder sogar einer geplanten Migration können Sie mit SRM 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.

SRM mit ONTAP und anderen Anwendungsfällen: Hybrid Cloud und Migration

Durch Integration Ihrer SRM-Implementierung mit erweiterten Datenmanagement-Funktionen von ONTAP lassen sich im Vergleich zu lokalen Storage-Optionen deutlich bessere Skalierungs- und Performance-Möglichkeiten erzielen. Darüber hinaus bringt sie jedoch noch mehr die Flexibilität der Hybrid Cloud. Mit der Hybrid Cloud können Sie Geld sparen, indem Sie ungenutzte Datenblöcke des High-Performance-Arrays mittels FabricPool in den bevorzugten Hyperscaler verschieben, was ein lokaler S3-Speicher wie NetApp StorageGRID sein könnte. Außerdem können Edge-basierte Systeme mit softwaredefiniertem ONTAP Select oder Cloud-basierter DR mithilfe von Cloud Volumes ONTAP (CVO) oder verwendet werden ["NetApp Private Storage in Equinix"](#) Um einen vollständig integrierten Storage-, Networking- und Computing-Service-Stack in der Cloud zu erstellen, führt Amazon Web Services (AWS), Microsoft Azure und Google Cloud Platform (GCP) zum Vorteil.

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 SRM 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.

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.

Nur bei der Verwendung von NAS-Protokollen (kein SAN-Zugriff) können Sie sogar den neuen NAS-optimierten Modus nutzen, indem Sie den folgenden Parameter einstellen (beachten Sie, dass der Name so

ist, da SRA und VASA dieselben Backend-Services in der Appliance nutzen):

1. Melden Sie sich am Bedienfeld unter an `https://<IP address>:9083` Und klicken Sie auf webbasierte CLI-Schnittstelle.
2. Führen Sie den Befehl aus `vp updateconfig -key=enable.qtree.discovery -value=true`.
3. Führen Sie den Befehl aus `vp updateconfig -key=enable.optimised.sra -value=true`.
4. Führen Sie den Befehl aus `vp reloadconfig`.

Implementieren von ONTAP-Tools und Überlegungen für VVols

Falls Sie SRM mit VVols verwenden möchten, müssen Sie den Storage mit Anmeldedaten für den Cluster-Umfang und einer Cluster-Management-LIF managen. Der Grund dafür ist, dass VASA Provider die zugrunde liegende physische Architektur verstehen muss, um die für VM Storage-Richtlinien erforderlichen Richtlinien erfüllen zu können. Wenn Sie beispielsweise eine Richtlinie haben, die All-Flash-Storage erfordert, muss der VASA Provider in der Lage sein, zu sehen, welche All-Flash-Systeme sind.

Eine weitere Best Practice bei der Implementierung besteht darin, Ihre ONTAP Tools Appliance niemals auf einem VVols Datastore zu speichern, den sie managen. Dies kann dazu führen, dass Sie den VASA Provider nicht einschalten können, da Sie die Swap-vVol für die Appliance nicht erstellen können, da die Appliance offline ist.

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.
- Wenn Sie ONTAP 9.8 oder höher verwenden, empfiehlt NetApp die Erstellung eines RBAC-Kontos mit den geringsten Berechtigungen über das Benutzermenü von ONTAP System Manager sowie die JSON-Datei, die auf der ONTAP Tools-Appliance unter verfügbar ist `https://<IP address>:9083/vsc/config/`. Verwenden Sie Ihr Administratorpasswort, um die JSON-Datei herunterzuladen. Diese Option kann für SVM oder Konten mit Cluster-Umfang verwendet werden.

Wenn Sie ONTAP 9.6 oder eine frühere Version verwenden, sollten Sie das RUC-Tool (RBAC User Creator) verwenden, das im verfügbar ist "[NetApp Support Site Tool](#)".

- Da die vCenter UI Plug-in, VASA Provider und SRA Server vollständig integrierte Services sind, müssen Sie den SRA-Adapter in SRM um Storage ebenso ergänzen wie in der vCenter UI für ONTAP-Tools. Andernfalls erkennt der SRA-Server möglicherweise nicht die Anfragen, die von SRM über den SRA-Adapter gesendet werden.
- Die NFS-Pfadprüfung wird bei der Verwendung der SVM-Scoped-Anmeldedaten nicht durchgeführt. 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-Datstores.
- 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. Beispielsweise können Sie FCP in Seite A und iSCSI in Standort B verwenden Sie sollten FCP und iSCSI nicht an Standort A verwenden Der Grund hierfür: Der SRA erstellt nicht gemischte Initiatorgruppen am Recovery-Standort, und SRM filtert nicht die Initiatorliste, die den SRA gegeben wurde.
- 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. In modernen Versionen von ONTAP 9 ist das nicht mehr erforderlich. 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 für den Versuch.

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

- Die automatische Volume-Größe sollte auf festgelegt werden `grow` Für Volumes mit SAN-Datstores und `grow_shrink` Für NFS-Datstores. Weitere Informationen zu ["Automatisches Vergrößern oder Verkleinern von Volumes"](#).
- SRM führt am besten aus, wenn die Anzahl der Datstores 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.

Storage Policy Based Management (SPBM) und VVols

Ab SRM 8.3 wird die Sicherung von VMs mit VVols Datastores unterstützt. SnapMirror Zeitpläne werden über den VASA Provider VM-Storage-Richtlinien ausgesetzt, wenn die VVols Replizierung im Einstellungsmenü der ONTAP Tools aktiviert ist, wie in den folgenden Screenshots dargestellt.

Im folgenden Beispiel wird die Aktivierung der VVols-Replizierung gezeigt.

Manage Capabilities

☒ **Enable VASA Provider**
vStorage APIs for Storage Awareness (VASA) is a set of application program interfaces (APIs) that enables vSphere vCenter to recognize the capabilities of storage arrays.

☒ **Enable vVols replication**
Enables replication of vVols when used with VMware Site Recovery Manager 8.3 or later.

☐ **Enable Storage Replication Adapter (SRA)**
Storage Replication Adapter (SRA) allows VMware Site Recovery Manager (SRM) to integrate with third party storage array technology.

Enter authentication details for VASA Provider and SRA server:

IP address or hostname:	192.168.64.7
Username:	Administrator
Password:	<input type="password"/>

CANCEL

APPLY

Der folgende Screenshot zeigt ein Beispiel zu SnapMirror Zeitplänen, die im Assistenten zur Erstellung von VM-Storage-Richtlinien angezeigt werden.

Create VM Storage Policy

- 1 Name and description
- 2 Policy structure
- 3 NetApp.clustered.Data.ONTAP.VP...
- 4 Storage compatibility
- 5 Review and finish

NetApp.clustered.Data.ONTAP.VP.vvol rules

Placement **Replication** Tags

☐ Disabled
☒ Custom

Provider: NetApp.clustered.Data.ONTAP.VP.vvolReplication

Replication ⓘ Asynchronous REMOVE

Replication Schedule ⓘ [Select Value] REMOVE
 [Select Value]
 hourly

CANCEL BACK NEXT

Der ONTAP VASA Provider unterstützt den Failover auf unterschiedlichen Storage. So kann beispielsweise ein Failover des Systems von ONTAP Select an einem Edge-Standort auf ein AFF System im Core-Datacenter durchgeführt werden. Unabhängig von Ähnlichkeit zum Storage müssen Sie für VM Storage-Richtlinien immer Storage-Richtlinien-Zuordnungen und Reverse-Mappings konfigurieren, damit die Services am Recovery-Standort die Erwartungen und Anforderungen erfüllen. Der folgende Screenshot zeigt ein Beispiel für eine Richtlinienzuordnung.

New Storage Policy Mappings

- 1 Creation mode
- 2 Recovery storage policies
- 3 Reverse mappings
- 4 Ready to complete

Recovery storage policies

Configure recovery storage policy mappings for one or more storage policies.

Search...

vc1.demo.netapp.com

☐ Host-local PMem Default Storage Policy

☐ VC1 Storage Policy *

☐ VM Encryption Policy

☐ vSAN Default Storage Policy

☐ VVol No Requirements Policy

vc2.demo.netapp.com

☐ Host-local PMem Default Storage Policy

☐ VC2 Storage Policy

☐ VM Encryption Policy

☐ vSAN Default Storage Policy

ADD MAPPINGS

vc1.demo.netapp.com	vc2.demo.netapp.com
VC1 Storage Policy	VC2 Storage Policy

1 mapping(s)

CANCEL BACK NEXT

Erstellung replizierter Volumes für VVols-Datastores

Im Gegensatz zu älteren VVols-Datastores müssen replizierte VVols Datastores von Anfang an bei aktivierter Replizierung erstellt werden. Dabei müssen sie Volumes verwenden, die vorab auf den ONTAP Systemen mit SnapMirror Beziehungen erstellt wurden. Hierfür sind vorab-Konfigurationen wie Cluster-Peering und SVM-Peering erforderlich. Diese Aktivitäten sollten von Ihrem ONTAP Administrator durchgeführt werden, da hierdurch die Zuständigkeiten zwischen denjenigen, die ONTAP Systeme an mehreren Standorten managen, und denjenigen, die hauptsächlich für vSphere Vorgänge verantwortlich sind, strikt getrennt werden können.

Dafür muss der vSphere Administrator eine neue Anforderung erfüllen. Da Volumes außerhalb der ONTAP Tools erstellt werden, ist es nicht bekannt, dass die Änderungen, die Ihr ONTAP-Administrator bis zur regelmäßigen planmäßigen Neuerfassungszeit vorgenommen hat. Daher ist es eine Best Practice, immer wieder neu zu ermitteln, wenn Sie eine Volume- oder SnapMirror Beziehung erstellen, die mit VVols verwendet werden soll. Klicken Sie einfach mit der rechten Maustaste auf den Host oder den Cluster und wählen Sie ONTAP Tools > Host- und Speicherdaten aktualisieren aus, wie im folgenden Screenshot dargestellt.



Bei VVols und SRM ist Vorsicht geboten. Niemals geschützte und ungesicherte VMs in demselben VVols Datastore zusammen. Der Grund dafür: Wenn Sie SRM für das Failover an Ihrem DR-Standort verwenden, werden nur die VMs, die Teil der Sicherungsgruppe sind, in die DR online geschaltet. Wenn Sie die Sicherung rückgängig machen (das SnapMirror aus der DR wieder in die Produktionsumgebung verschieben), können die VMs, die nicht Failover waren, überschrieben werden und wertvolle Daten enthalten.

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.

The screenshot shows the vSphere Client interface. On the left, the 'ONTAP tools' sidebar is visible with options like Overview, Storage Systems, Storage Capability Profiles, Storage Mapping, Settings, and Reports. The main area is titled 'Storage Systems' and contains a table with columns for Name, Type, and IP Address. A single entry 'cluster2' of type 'Cluster' is listed with IP address 'cluster2.demo.netapp.com'. Below this, the 'Edit Local Array Manager' dialog is open. It has a field for 'Enter a name for the array manager on "vc2.demo.netapp.com":' with the value 'vc2_array_manager'. Below that is the 'Storage Array Parameters' section, which includes a field for 'Storage Management IP Address or Hostname' containing 'cluster2.demo.netapp.com'. A red arrow points from the IP address in the table to this field. A note below the field states: 'Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.'

Allgemeines zu Replikationsgruppen

Replikationsgruppen enthalten logische Sammlungen von virtuellen Maschinen, die zusammen wiederhergestellt werden. Mit den ONTAP Tools VASA Provider werden automatisch Replikationsgruppen für Sie erstellt. 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 die Aggregat-Deduplizierung bei Volume SnapMirror 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. Sie möchten wahrscheinlich, dass Ihr Microsoft Windows Domain Controller vor Ihrem Microsoft SQL Server hochgefahren wird, was 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 einen Test-Failover durchzuführen, wenn die Konfiguration eines geschützten VM Storage geändert wird. 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 im VMware vCenter Site Recovery Manager als Array behandelt. SRM unterstützt bestimmte Array-to-Array (oder SVM-zu-SVM) Replizierungslayouts.

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

- SRM 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 SRM 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

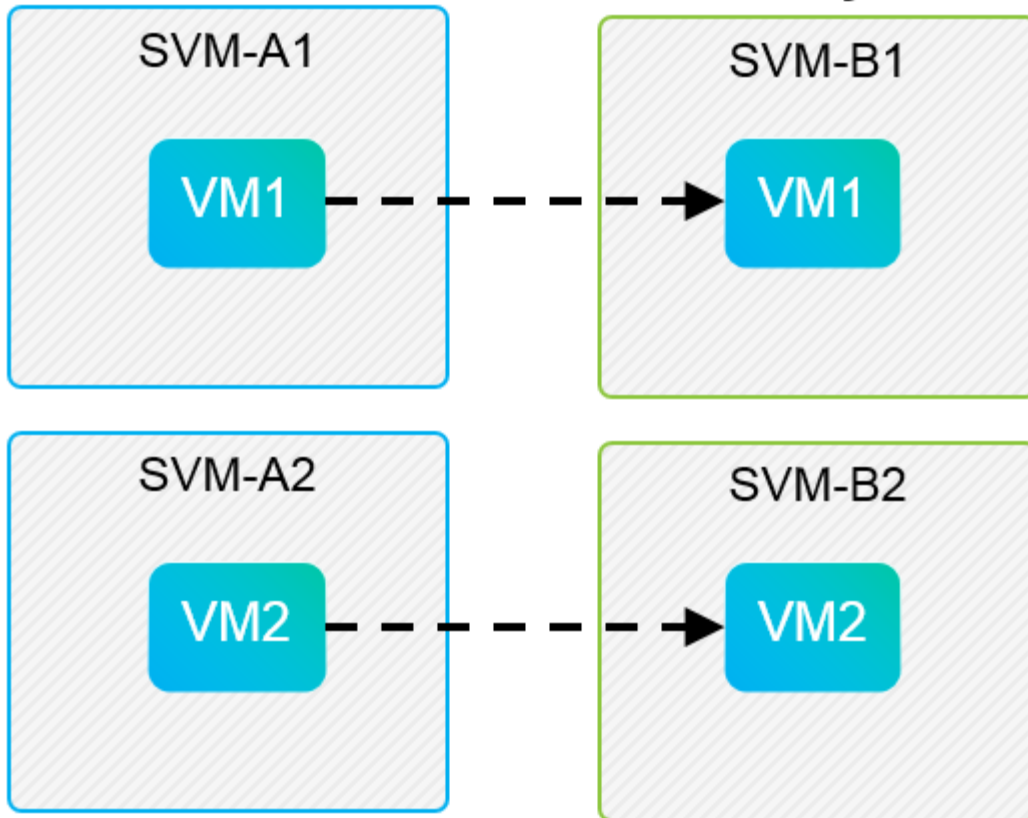
Die folgenden Abbildungen zeigen die Szenarien des SnapMirror Beziehungs-Layouts, die von SRM und SRA unterstützt werden. Jede VM in den replizierten Volumes besitzt die Daten auf nur einem SRM Array (SVM) an jedem Standort.

SnapMirror Replication



Protected Site

Recovery Site

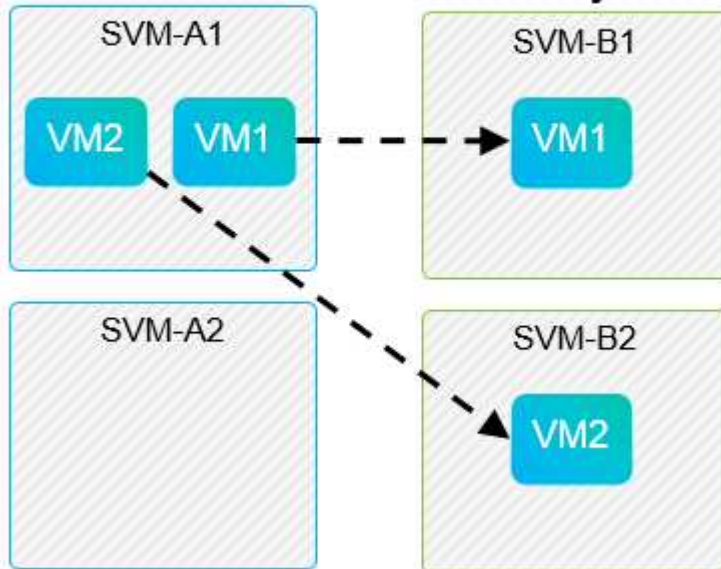


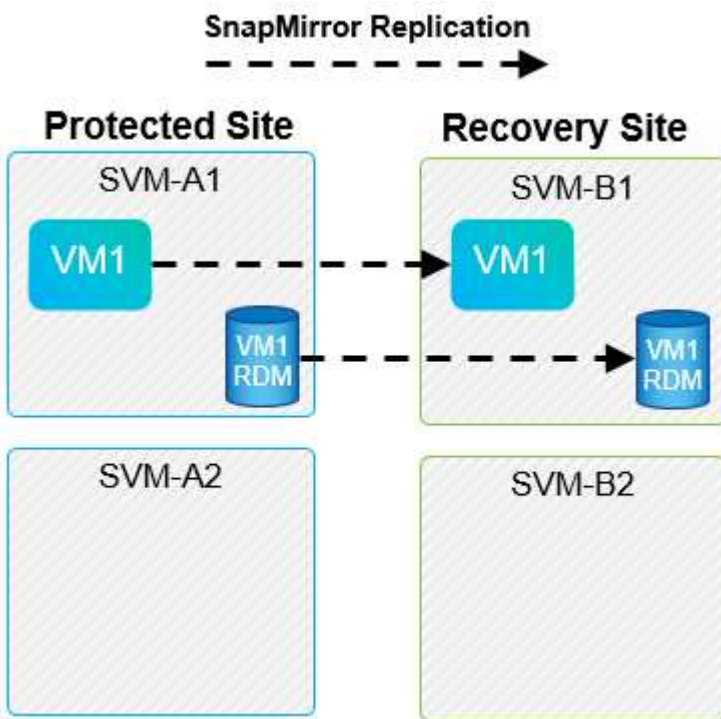
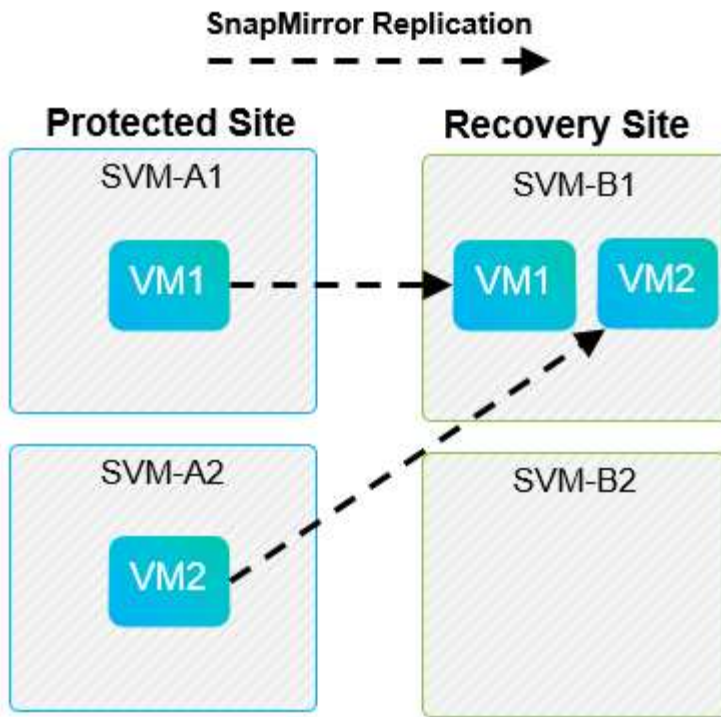
SnapMirror Replication



Protected Site

Recovery Site





Unterstützte Array Manager-Layouts

Wenn Sie in SRM 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 Peering durchgeführt `SVM3` und `SVM4` am Recovery-Standort. Sie können jedoch nur eines der beiden Array-Paare auswählen, wenn Sie eine Schutzgruppe erstellen.

New Protection Group

- Name and direction
- Type**
- Datastore groups
- Recovery plan
- Ready to complete

Type

Select the type of protection group you want to create:

- ☒ **Datastore groups (array-based replication)**
Protect all virtual machines which are on specific datastores.
- ☐ **Individual VMs (vSphere Replication)**
Protect specific virtual machines, regardless of the datastores.
- ☐ **Virtual Volumes (vVol replication)**
Protect virtual machines which are on replicated vVol storage.
- ☐ **Storage policies (array-based replication)**
Protect virtual machines with specific storage policies.

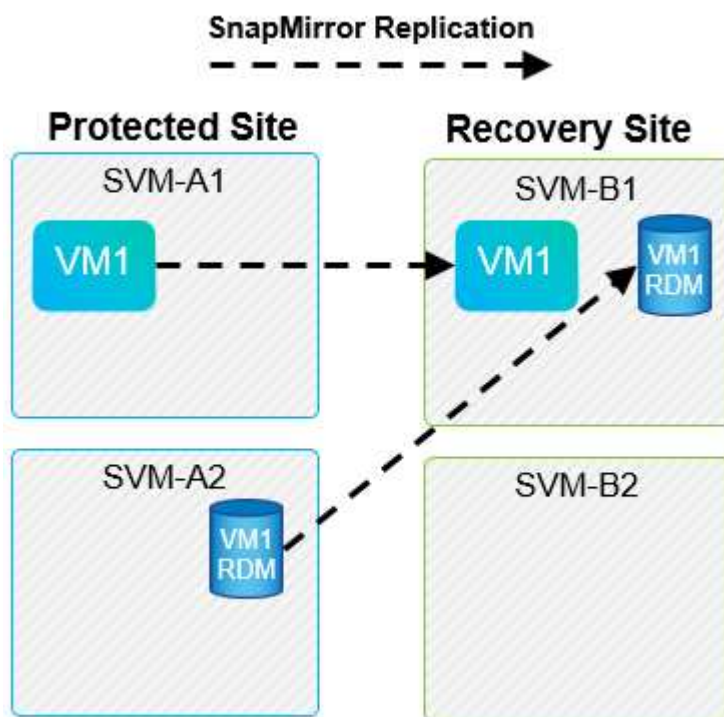
Select array pair

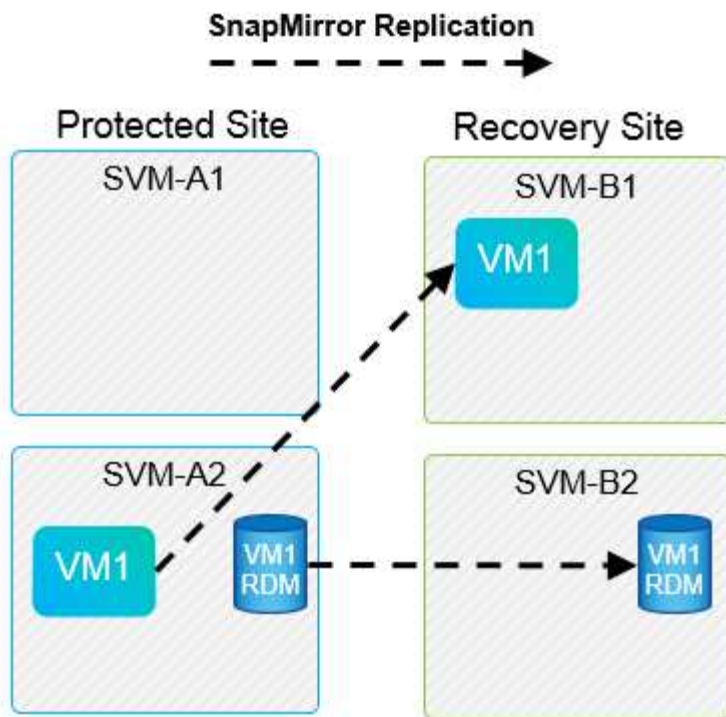
Array Pair	Array Manager Pair
<input type="radio"/> ✓ cluster1:svm1 ↔ cluster2:svm2	vc1 array manager ↔ vc2 array manager
<input type="radio"/> ✓ cluster1:svm3 ↔ cluster2:svm4	vc1 trad datastores ↔ vc2 trad datastores

CANCEL
BACK
NEXT

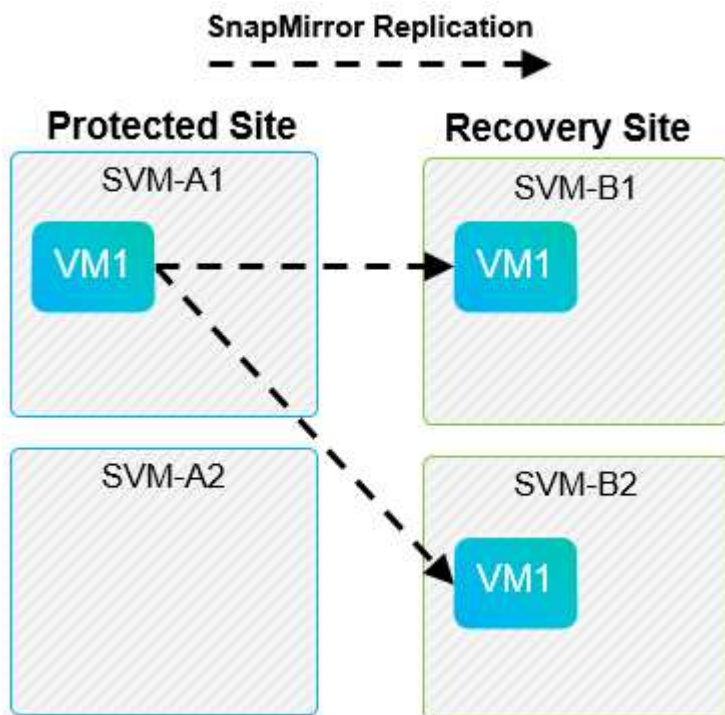
Nicht unterstützte Layouts

Nicht unterstützte Konfigurationen beinhalten Daten (VMDK oder RDM) auf mehreren SVMs, die sich im Besitz einer individuellen VM befinden. In den folgenden Abbildungen sind VM1 Kann aus dem Grund nicht für den Schutz mit SRM konfiguriert werden VM1 Verfügt über Daten auf zwei SVMs.





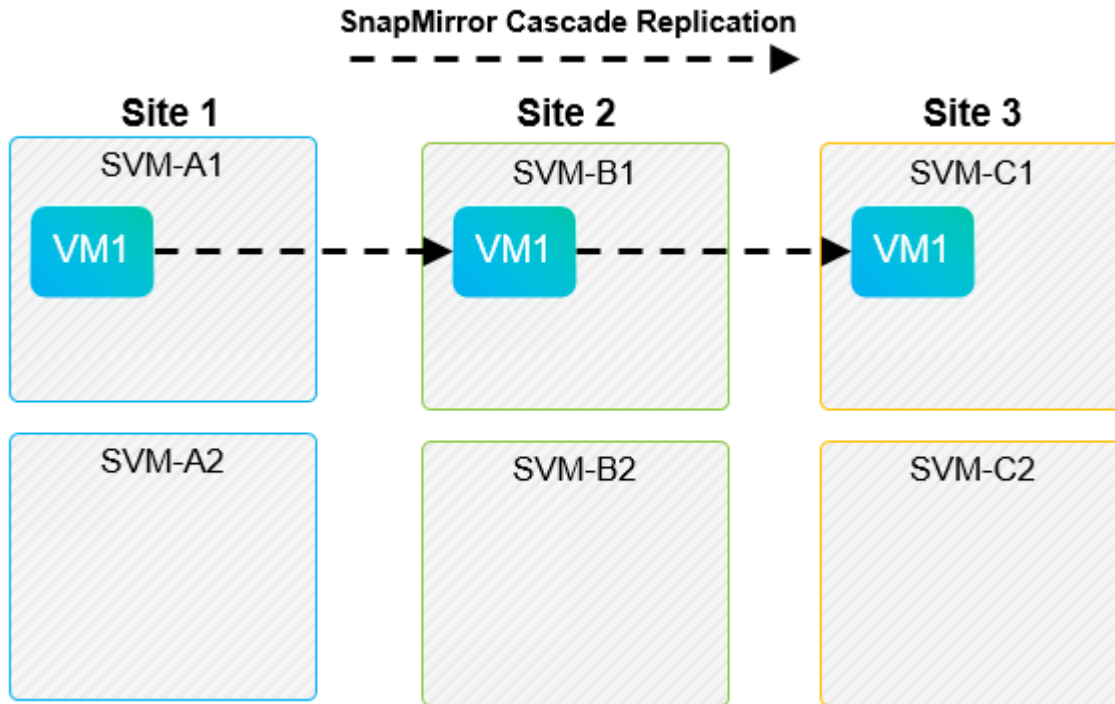
Jegliche Replizierungsbeziehungen, bei denen ein einzelnes NetApp Volume von einer Quell-SVM auf mehrere Ziele in derselben SVM oder in verschiedenen SVMs repliziert wird, werden als SnapMirror Fan-out bezeichnet. Fan-out wird mit SRM nicht unterstützt. In der folgenden Abbildung ist das Beispiel dargestellt.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



SnapMirror Kaskadierung

SRM 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 SRM 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. SRM 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 SRM Failover oder eine Umkehrung

der Replizierung stattfindet.

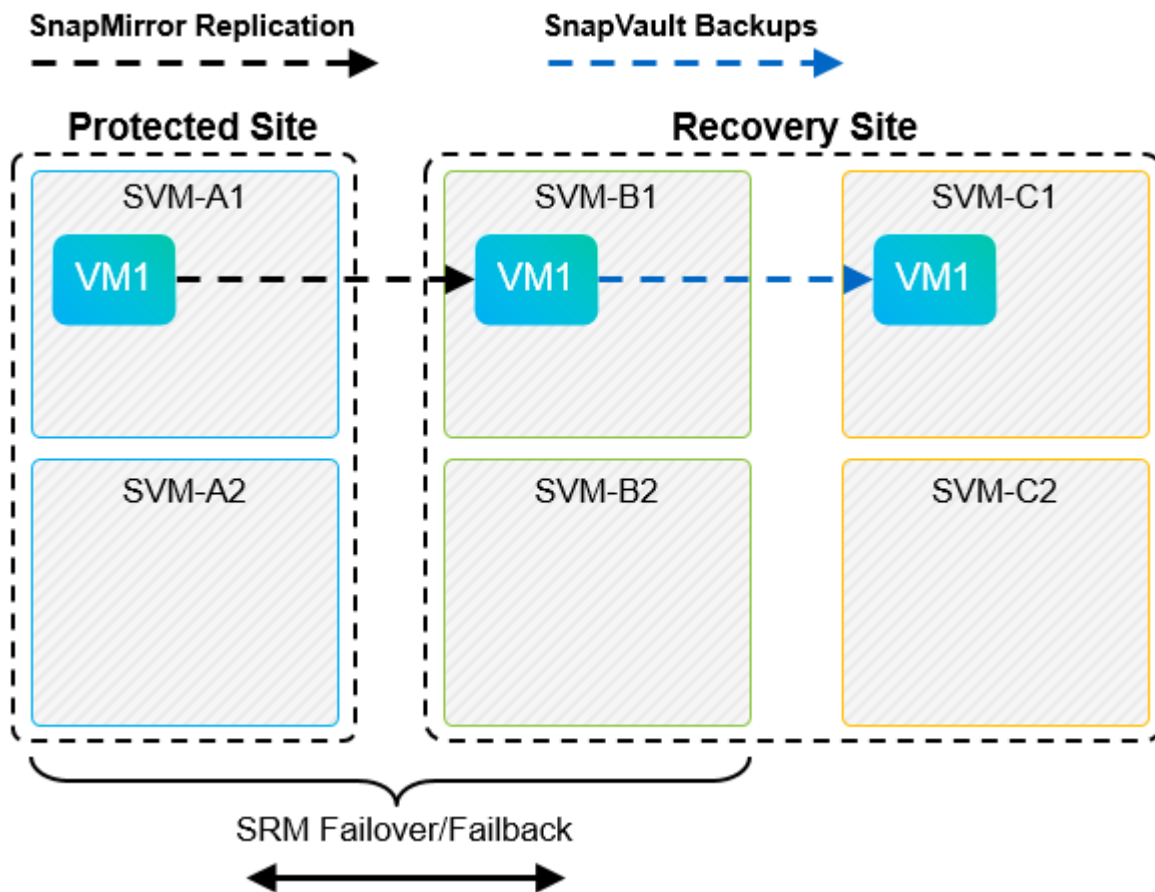
Aktuelle Informationen zu SnapMirror und SnapVault für ONTAP 9 finden Sie unter ["TR-4015 SnapMirror Configuration Best Practice Guide für ONTAP 9."](#)

Best Practices In Sich

Wenn in derselben Umgebung SnapVault und SRM 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.

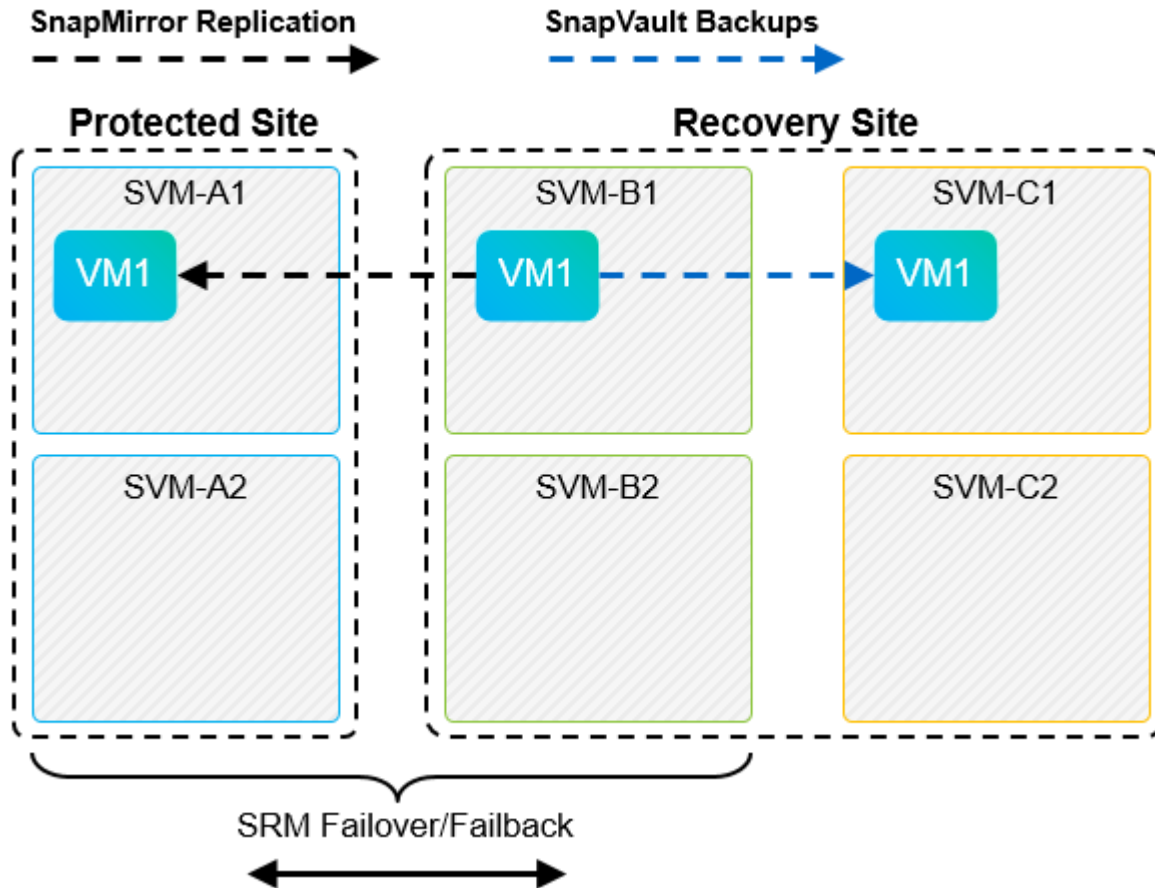
In einer VMware Umgebung verfügt jeder Datenspeicher über eine universelle eindeutige Kennung (Universal Unique Identifier, UUID) und jede VM über eine eindeutige Managed Object ID (MOID). Diese IDs werden während Failover oder Failback durch SRM nicht gepflegt. Da Datastore-UIDs und VM-MOIDs beim Failover durch SRM nicht gepflegt werden, müssen nach dem SRM 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 SRM 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 SRM ein Failback und eine zweite Umkehrung 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 SRM 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 angeordneten 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 SRM 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 SRM nicht unterstützt, da SRM während des SRM Failover oder des Test-Failovers alle FC- und iSCSI-Initiatoren in den ESXi-Hosts in der Anforderung enthält.

Best Practices In Sich

SRM 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 SRM-Ressourcenzuordnung, damit die VMs für das Failover in eine Gruppe von Hosts oder die andere konfiguriert werden.

Fehlerbehebung bei SRM bei Nutzung der VVols-Replizierung

Der Workflow in SRM unterscheidet sich deutlich, wenn VVols Replizierung mit dem verwendet wird, 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. `PreparrerFailoverReplicationGroup`: 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:

- TR-4597: VMware vSphere für ONTAP
["https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vsphere-overview.html"](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"](https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-vvols-overview.html)
- TR-4015 SnapMirror Configuration Best Practice Guide für ONTAP 9
<https://www.netapp.com/media/17229-tr4015.pdf?v=127202175503P>
- RBAC Benutzer-Creator für ONTAP
["https://mysupport.netapp.com/site/tools/tool-eula/rbac"](https://mysupport.netapp.com/site/tools/tool-eula/rbac)
- ONTAP Tools für VMware vSphere Ressourcen
["https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab"](https://mysupport.netapp.com/site/products/all/details/otv/docsandkb-tab)
- VMware Site Recovery Manager - Dokumentation
["https://docs.vmware.com/en/Site-Recovery-Manager/index.html"](https://docs.vmware.com/en/Site-Recovery-Manager/index.html)

Siehe "[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.

Lösungen für kontinuierliche Verfügbarkeit für vSphere Umgebungen

Die ONTAP-Architektur ist eine flexible und skalierbare Storage-Plattform, die SAN- (FCP, iSCSI und NVMe-of) und NAS-Services (NFS v3 und v4.1) für Datastores bietet. Die Storage-Systeme NetApp AFF, ASA und FAS nutzen das ONTAP Betriebssystem, um zusätzliche Protokolle für Gast-Storage wie S3 und SMB/CIFS anzubieten.

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 (Controller Failover on Demand oder CFOD), Hardware-Redundanz und geografische Trennung, um ein hohes Maß an Verfügbarkeit zu erreichen. 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 bietet granularen Schutz von Datenspeichern mit FCP- und iSCSI SAN-Protokollen, sodass Sie nur Workloads mit hoher Priorität selektiv schützen können. Es bietet aktiv/aktiv-Zugriff auf lokale und Remote-Standorte, im Gegensatz zu NetApp MetroCluster, die eine aktiv/Standby-Lösung ist. Derzeit ist Active Sync eine asymmetrische Lösung, bei der eine Seite der anderen bevorzugt wird, um eine bessere Performance zu bieten. Dies wird durch die ALUA-Funktionalität (Asymmetric Logical Unit Access) erreicht, die den ESXi Host automatisch informiert, welche Controller bevorzugt werden sollen. NetApp hat jedoch angekündigt, dass die aktive Synchronisierung in Kürze einen vollständig symmetrischen Zugriff ermöglichen wird.

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.

Weitere Informationen finden Sie unter ["Empfohlene Practices für VMware vSphere Metro Storage-Cluster"](#).

Was ist vSphere Metro Storage-Cluster?

vSphere Metro Storage Cluster (vMSC) ist eine zertifizierte Konfiguration, die Virtual Machines (VMs) und Container vor Ausfällen schützt. Dies wird erreicht, indem erweiterte Storage-Konzepte zusammen mit Clustern von ESXi Hosts genutzt werden, die auf verschiedene Ausfall-Domains verteilt sind, zum Beispiel Racks, Gebäude, Campus oder sogar Städte. Die NetApp MetroCluster und die Active Sync Storage-Technologien von SnapMirror sorgen für eine Sicherung von RPO=0 bzw. nahezu RPO=0 für die Host-Cluster. Mit der vMSC-Konfiguration ist sichergestellt, dass die Daten immer verfügbar sind, selbst wenn ein vollständiger physischer oder logischer „Standort“ ausfällt. Ein Speichergerät, das Teil der vMSC-Konfiguration ist, muss nach einer erfolgreichen vMSC-Zertifizierung 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)

Abhängig von den Überlegungen zur Latenz kann NetApp MetroCluster in zwei unterschiedlichen Konfigurationen für die Verwendung mit vSphere implementiert werden:

- Stretch-MetroCluster
- Fabric MetroCluster

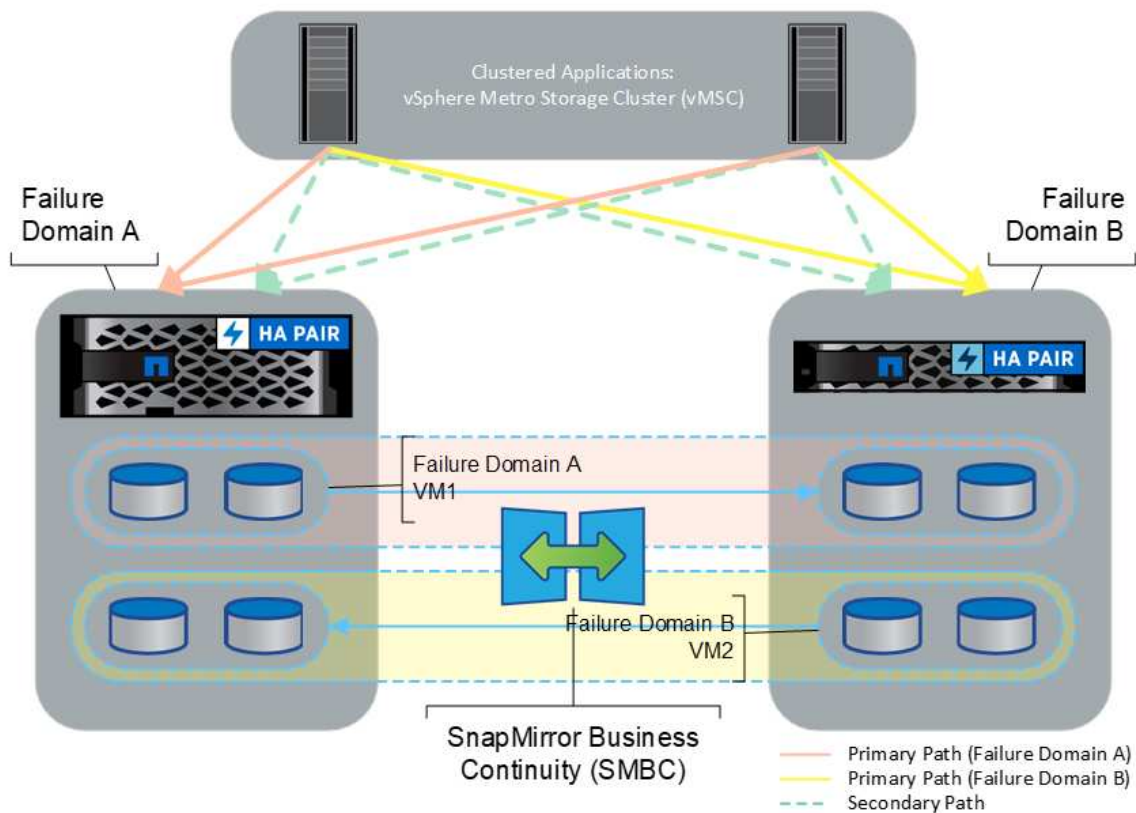
Im Folgenden finden Sie ein High-Level-Topologiediagramm von Stretch MetroCluster.



Siehe "[MetroCluster-Dokumentation](#)" Finden Sie spezifische Design- und Implementierungsinformationen für MetroCluster.

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

- Asymmetrisch
- Symmetrisch (private Vorschau in ONTAP 9.14.1)



Siehe "[NetApp Dokumente](#)" Für spezifische Design- und Implementierungsinformationen zu SnapMirror Active Sync

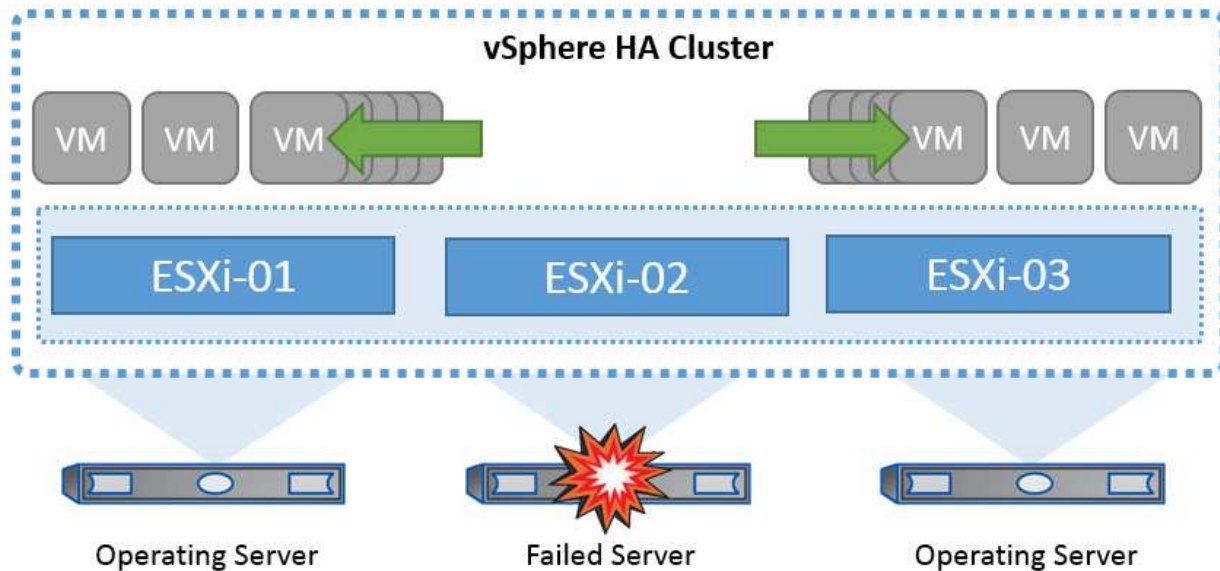
VMware vSphere Lösungsübersicht

VMware vCenter Server Appliance (VCSA) ist das leistungsstarke, zentralisierte Managementsystem und eine zentrale Konsole für vSphere, mit der Administratoren ESXi Cluster effizient betreiben können. Sie unterstützt wichtige Funktionen wie VM-Bereitstellung, vMotion Betrieb, Hochverfügbarkeit (HA), Distributed Resource Scheduler (DRS), Tanzu Kubernetes Grid und mehr. Sie ist eine wesentliche Komponente in VMware Cloud-Umgebungen und sollte im Hinblick auf die Service-Verfügbarkeit konzipiert werden.

vSphere High Availability

Die Cluster-Technologie von VMware gruppiert ESXi Server in Pools mit gemeinsam genutzten Ressourcen für Virtual Machines und stellt vSphere High Availability (HA) bereit. vSphere HA bietet benutzerfreundliche, hohe Verfügbarkeit für Anwendungen, die auf 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. Bei einem Ausfall eines Gastbetriebssystems startet vSphere HA die betroffene virtuelle Maschine auf demselben physischen Server neu. Mit vSphere HA werden geplante Ausfallzeiten reduziert, ungeplante Ausfallzeiten vermieden und eine schnelle Wiederherstellung nach Ausfällen ermöglicht.

vSphere HA Cluster Wiederherstellung von VMs aus ausgefallener Server.



Es ist wichtig zu wissen, dass VMware vSphere nicht über NetApp MetroCluster oder SnapMirror Active Sync verfügt und alle ESXi Hosts im vSphere Cluster als berechnete 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 Auswahl Teil, und einer der Hosts wird zum Master. Jeder Slave führt den Netzwerk-Heartbeat zum Master aus, und der Master wiederum führt den Netzwerk-Heartbeat auf allen Slave-Hosts aus. Der Master-Host eines vSphere HA-Clusters ist für die Erkennung des Ausfalls von Slave-Hosts verantwortlich.

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.

Best Practice

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

Antwort Der Hostisolation

Die Isolationsantwort ist eine Einstellung in vSphere HA, die die Aktion bestimmt, die auf virtuellen Maschinen ausgelöst wird, wenn ein Host in einem vSphere HA-Cluster seine Verwaltungsnetzwerkverbindungen verliert, aber weiterhin ausgeführt wird. Für diese Einstellung gibt es drei Optionen: „Disabled“, „Shut Down and Restart VMs“ und „Power Off and Restart VMs“.

„Herunterfahren“ ist besser als „Ausschalten“, das nicht die neuesten Änderungen auf Festplatte bereinigt oder Transaktionen festschreibt. Wenn virtuelle Maschinen nicht in 300 Sekunden heruntergefahren wurden, 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.

Best Practice

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 auftritt, wenn ein Speichergerät dauerhaft ausfällt oder administrativ entfernt wird und nicht zurückgegeben werden soll. Das NetApp-Speicher-Array gibt ESXi einen SCSI-Sense-Code aus, der erklärt, dass das Gerät dauerhaft verloren geht. Im Abschnitt Fehlerbedingungen und VM-Reaktion von vSphere HA können Sie konfigurieren, wie die Antwort nach dem Erkennen einer PDL-Bedingung aussehen soll.

Best Practice

NetApp empfiehlt, die „Antwort für Datastore mit PDL“ auf **„Ausschalten und Neustart von VMs“** zu setzen. Wenn dieser Zustand erkannt wird, wird eine VM sofort auf einem funktionierenden Host im vSphere HA-Cluster neu gestartet.

Alle Pfade nach unten (APD)

APD ist ein Zustand, der auftritt, wenn ein Speichergerät für den Host nicht mehr zugänglich ist und keine Pfade zum Array verfügbar sind. ESXi betrachtet dies als ein vorübergehendes Problem mit dem Gerät und erwartet, dass es wieder verfügbar 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).

Best Practice

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 die VMs neu starten kann. Wenn sie auf Conservative gesetzt ist, startet HA nur die VM neu, die vom APD betroffen ist, wenn sie weiß, dass ein anderer Host sie neu starten kann. Im Fall von aggressive, versucht HA, die VM neu zu starten, selbst wenn sie den Status anderer Hosts nicht kennt. Dies kann dazu führen, dass VMs nicht neu gestartet werden, wenn kein Host mit Zugriff auf den Datenspeicher vorhanden ist, auf dem sich dieser befindet.

Wenn der APD-Status aufgelöst ist und der Zugriff auf den Speicher wiederhergestellt wird, bevor die Zeiteinstellung überschritten wurde, startet HA die virtuelle Maschine nicht unnötig neu, es sei denn, Sie konfigurieren sie ausdrücklich 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.

Best Practice

NetApp empfiehlt, die Antwort für die APD-Wiederherstellung nach der APD-Zeitüberschreitung auf deaktiviert zu konfigurieren.

VMware DRS Implementierung für NetApp MetroCluster

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. Um standortübergreifenden Datenverkehr zu vermeiden, empfiehlt NetApp die Konfiguration der DRS Affinitätsregeln, um eine logische Trennung der VMs zu managen. So stellen Sie sicher, dass HA und DRS nur lokale Hosts verwenden, sofern es keinen vollständigen Standortausfall gibt.

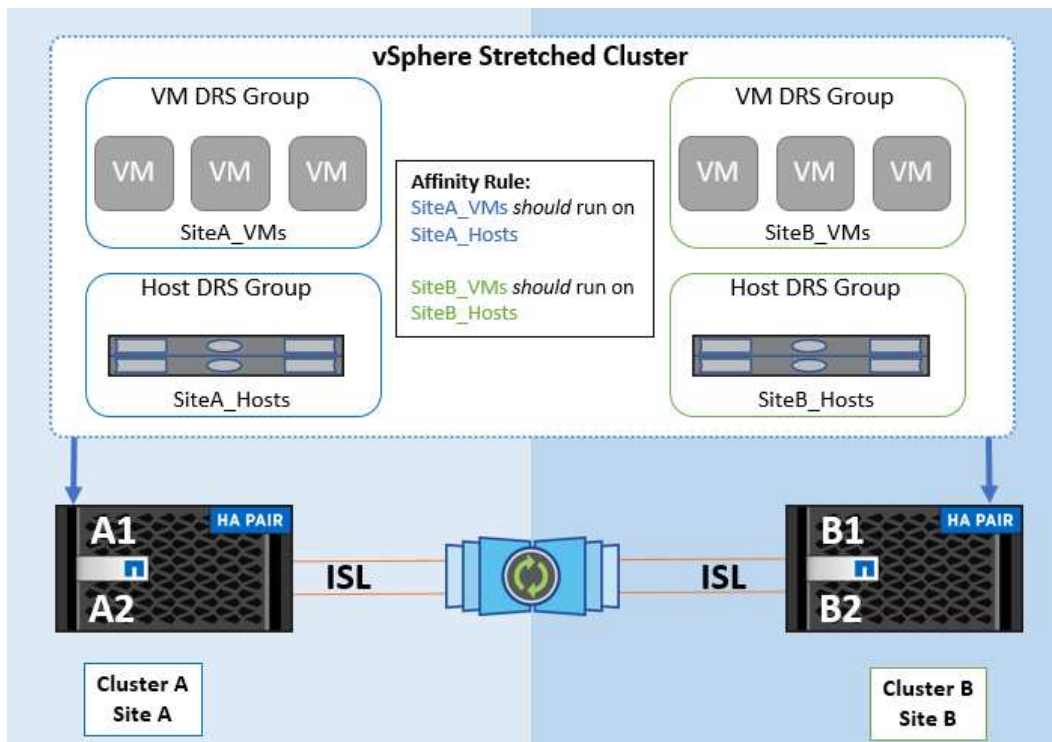
Wenn Sie eine DRS-Affinitätsregel für Ihr Cluster erstellen, können Sie festlegen, wie vSphere diese Regel während eines Failover einer virtuellen Maschine anwendet.

Es gibt zwei Arten von Regeln, die Sie vSphere HA-Failover-Verhalten angeben 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. Der Einsatz von „Must“-Regeln kann potenziell zu Serviceausfällen führen.

Die Verfügbarkeit von Services sollte immer Vorrang vor der Leistung haben. Wenn ein vollständiges Datacenter ausfällt, müssen die „Must“-Regeln Hosts aus der VM-Host-Affinitätsgruppe auswählen. Wenn das Datacenter nicht verfügbar ist, werden die Virtual Machines 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 Storage-I/O-Kontrollschwellenwerte 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.

Best Practice

NetApp empfiehlt das Erstellen von Datastore-Clustern im Hinblick auf die Storage-Standortorientierung. Das

heißt, Datastores mit Standortaffinität zu Standort A sollten nicht mit Datastore-Clustern mit Datastores mit Standortaffinität zu Standort B gemischt werden

Wenn eine virtuelle Maschine neu bereitgestellt oder mithilfe von Storage vMotion migriert wird, empfiehlt NetApp, alle für diese virtuellen Maschinen spezifischen VMware DRS-Regeln entsprechend manuell zu aktualisieren. Dadurch wird die Virtual Machine-Affinität auf Standortebene sowohl für Host als auch für Datenspeicher ermittelt und somit der Netzwerk- und Storage Overhead reduziert.

VMSC Design- und Implementierungsrichtlinien

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

NetApp-Speicherkonfiguration

Setup-Anweisungen für NetApp MetroCluster (als MCC-Konfiguration bezeichnet) finden Sie unter ["MetroCluster-Dokumentation"](#). Anweisungen für SnapMirror Active Sync 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 MetroCluster nicht nutzen, können Sie SnapMirror Active Sync verwenden, was Datastores-granulare Sicherung und aktiv/aktiv-Zugriff über diverse ONTAP Cluster in verschiedenen Ausfall-Domains hinweg bietet. SnapMirror Active Sync verwendet Konsistenzgruppen, um die Konsistenz der Schreibreihenfolge zwischen einem oder mehreren Datastores sicherzustellen. Sie können je nach Applikations- und Datastore-Anforderungen mehrere Konsistenzgruppen erstellen. Konsistenzgruppen sind insbesondere für Applikationen nützlich, die eine Datensynchronisierung zwischen mehreren Datastores erfordern. SnapMirror Active Sync unterstützt außerdem Raw Device Mapping (RDMs) und über das Gastsystem verbundenen Storage mit iSCSI-Initiatoren in-Guest. 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 handelt es sich um eine reine SAN-Konfiguration. Es können keine NFS-Datenspeicher durch SnapMirror Active Sync geschützt 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.

VMware vSphere HA

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.

Hinweis: nichts in diesem Dokument ersetzt ["Empfohlene Practices für VMware vSphere Metro Storage-Cluster"](#)

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.

New Cluster

1 Basics

2 Image

3 Review

Basics

Name

MCC Cluster

Location

Raleigh

i

vSphere DRS

i

vSphere HA

vSAN

Enable vSAN ESA

i

☒ Manage all hosts in the cluster with a single image

i

Choose how to set up the cluster's image

☒ Compose a new image

☐ Import image from an existing host in the vCenter inventory

☐ Import image from a new host

☐ Manage configuration at a cluster level

i

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.

101

vSphere HA ☒

Failures and responses

Admission Control

Heartbeat Datastores

Advanced Options

You can configure how vSphere HA responds to the failure conditions on this cluster. The following failure conditions are supported: host, host isolation, VM component protection (datastore with PDL and APD), VM and application.

Enable Host Monitoring  ☒

> Host Failure Response	Restart VMs ▾
> Response for Host Isolation	Disabled ▾
> Datastore with PDL	Power off and restart VMs ▾
> Datastore with APD	Power off and restart VMs - Conservative restart policy ▾
> VM Monitoring	Disabled ▾

CANCEL

OK

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

> Response for Host Isolation Disabled

> Datastore with PDL Power off and restart VMs

> Datastore with APD Power off and restart VMs - Conservative restart policy

▼ VM Monitoring

Enable heartbeat monitoring

VM monitoring resets individual VMs if their VMware tools heartbeats are not received within a set time. Application monitoring resets individual VMs if their in-guest heartbeats are not received within a set time.

☐ Disabled

☐ VM Monitoring Only

Turns on VMware tools heartbeats. When heartbeats are not received within a set time, the VM is reset.

☒ VM and Application Monitoring

Turns on application heartbeats. When heartbeats are not received within a set time, the VM is reset.

CANCEL OK

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

Edit Cluster Settings | MCC Cluster



vSphere HA ☒

Failures and responses Admission Control Heartbeat Datastores Advanced Options

Admission control is a policy used by vSphere HA to ensure failover capacity within a cluster. Raising the number of potential host failures will increase the availability constraints and capacity reserved.

Host failures cluster tolerates

1



Maximum is one less than number of hosts in cluster.

Define host failover capacity by

Cluster resource Percentage



Override calculated failover capacity.

Reserved failover CPU capacity: 50 % CPU

Reserved failover Memory capacity: 50 % Memory



Reserve Persistent Memory failover capacity



Override calculated Persistent Memory failover capacity

CANCEL

OK

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.

Edit Cluster Settings | MCC Cluster



vSphere DRS ☒

Automation Additional Options Power Management Advanced Options

Automation Level

Manual

DRS generates both power-on placement recommendations, and migration recommendations for virtual machines. Recommendations need to be manually applied or ignored.

Migration Threshold



Conservative
(Less
Frequent
vMotions)

(3) DRS provides recommendations when workloads are moderately imbalanced. This threshold is suggested for environments with stable workloads. (Default)

Aggressive
(More
Frequent
vMotions)

Predictive DRS



☐ Enable

Virtual Machine Automation



☒ Enable

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

vSphere HA 

Failures and responses

Admission Control

Heartbeat Datastores









Advanced Options

vSphere HA uses datastores to monitor hosts and virtual machines when the HA network has failed. vCenter Server selects 4 datastores for each host using the policy and datastore preferences specified below.

Heartbeat datastore selection policy:

- ☐ Automatically select datastores accessible from the hosts
- ☐ Use datastores only from the specified list
- ☒ Use datastores from the specified list and complement automatically if needed

Available heartbeat datastores

	Name ↑	Datastore Cluster	Hosts Mounting Datastore
<input checked="" type="checkbox"/>	 d11	N/A	2
<input checked="" type="checkbox"/>	 d12	N/A	2
<input checked="" type="checkbox"/>	 d21	N/A	2
<input checked="" type="checkbox"/>	 d22	N/A	2
<input type="checkbox"/>	 d31	N/A	2
<input type="checkbox"/>	 d32	N/A	2
<input type="checkbox"/>	 d41	N/A	2
<input type="checkbox"/>	 d42	N/A	2

11 items

CANCEL

OK

Konfigurieren Sie Die Erweiterten Optionen

Host-Fehlererkennung

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.

Siehe "core.vmware.com" Weitere Informationen.

vSphere HA 

Failures and responses

Admission Control

Heartbeat Datastores

Advanced Options

You can set advanced options that affect the behavior of your vSphere HA cluster.

 Add  Delete

Option	Value
das.ignoreRedundantNetWarning	true
das.isolationaddress0	10.61.99.100
das.isolationaddress1	10.61.99.110
das.heartbeatDsPerHost	4

4 items

CANCEL

OK

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 MCC oder SnapMirror Active Sync geschützt werden.

Siehe "core.vmware.com" Weitere Informationen.

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.

Best Practice

- 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.

Hinweis: 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 unter ["vSphere Monitoring und Performance"](#) 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 VMHost 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 VMHost 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 VMHostregeln.
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.

Create VM/Host Rule | Cluster-01

×

Name	sitea_affinity	<input checked="" type="checkbox"/> Enable rule.
Type	Virtual Machines to Hosts ▼	

Virtual machines that are members of the Cluster VM Group sitea_vms should run on host group sitea_hosts.

VM Group:

sitea_vms	▼
Should run on hosts in group	▼

Host Group:

sitea_hosts	▼
-------------	---

CANCEL

OK

VMware vSphere Storage DRS für NetApp MetroCluster

Datastore-Cluster 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.
3. Wählen Sie die Option Storage DRS aktivieren aus, und klicken Sie auf Weiter.
4. Stellen Sie alle Optionen auf Keine Automatisierung (manueller Modus) ein, und klicken Sie auf Weiter.

Best Practice

- NetApp empfiehlt, Storage DRS im manuellen Modus zu konfigurieren, sodass der Administrator entscheiden und kontrollieren kann, wann Migrationen stattfinden.

Storage DRS automation

Cluster automation level

☒ **No Automation (Manual Mode)**
vCenter Server will make migration recommendations for virtual machine storage, but will not perform automatic migrations.

☐ **Fully Automated**
Files will be migrated automatically to optimize resource usage.

1. Vergewissern Sie sich, dass das Kontrollkästchen E/A-Metrik für SDRS-Empfehlungen aktivieren aktiviert ist. Die metrischen Einstellungen können mit Standardwerten belassen werden.

New Datastore Cluster

1 Name and Location
2 Storage DRS Automation
3 **Storage DRS Runtime Settings**
4 Select Clusters and Hosts
5 Select Datastores
6 Ready to Complete

I/O Metric inclusion
Select this option if you want I/O metrics considered as a part of any SDRS recommendations or automated migrations in this data store cluster

☒ Enable I/O metric for SDRS recommendations

Storage DRS thresholds
Runtime thresholds govern when Storage DRS performs or recommends migrations (based on the selected automation level).

Space threshold: ☒ Utilized space 50 % %
Dictates the minimum level of consumed space for each datastore that is the threshold for action.

☐ Minimum free space 50 GB
Dictates the minimum level of free space for each datastore that is the threshold for action.

I/O latency threshold: 5 ms ms
Dictates the minimum I/O latency for each datastore below which I/O load balancing moves are not considered.

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

New Datastore Cluster

1 Name and Location
2 Storage DRS Automation
3 Storage DRS Runtime Settings
4 **Select Clusters and Hosts**
5 Select Datastores
6 Ready to Complete

Select all hosts and clusters that require connectivity to the datastores in the datastore cluster.

Filter (1) Selected Objects

Clusters Standalone Hosts

Filter

Name
<input checked="" type="checkbox"/> MCC HA Cluster

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

New Datastore Cluster

1 Name and Location
2 **Storage DRS Automation**
3 Storage DRS Runtime Settings
4 Select Clusters and Hosts
5 **Select Datastores**
6 Ready to Complete

Show datastores connected to all hosts

Filter

Name	Host Connection Status	Capacity	Free Space	Type
<input checked="" type="checkbox"/> sitea_infra	All Hosts Connect...	10.00 GB	10.00 GB	NFS
<input checked="" type="checkbox"/> sitea_infra2	All Hosts Connect...	10.00 GB	10.00 GB	NFS

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"](https://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, hochverfügbare Server-Cluster, Docker Container oder virtualisierte Server verwenden: Die NetApp-Technologie sorgt nahtlos für die Storage-Verfügbarkeit im Falle eines totalen Ausfalls aufgrund von Strom-, Kühlungs- oder Netzwerkkonnektivität, Herunterfahren des Storage-Arrays 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 (Network Attached Storage Logical Interfaces) in MetroCluster-Konfigurationen automatisch ein Failover durch. Storage Area Network LIFs (SAN LIFs) führen jedoch keinen Failover durch. Sie 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 NetApp-Mediator ist erforderlich, um sicherzustellen, dass ein Standort-Failover korrekt ausgeführt wird.

Ausfallszenarien für vMSC mit MCC

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.

Hinweis: Es gibt keine Änderung im MetroCluster-Verhalten in diesem Szenario, und alle Datastores bleiben 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.

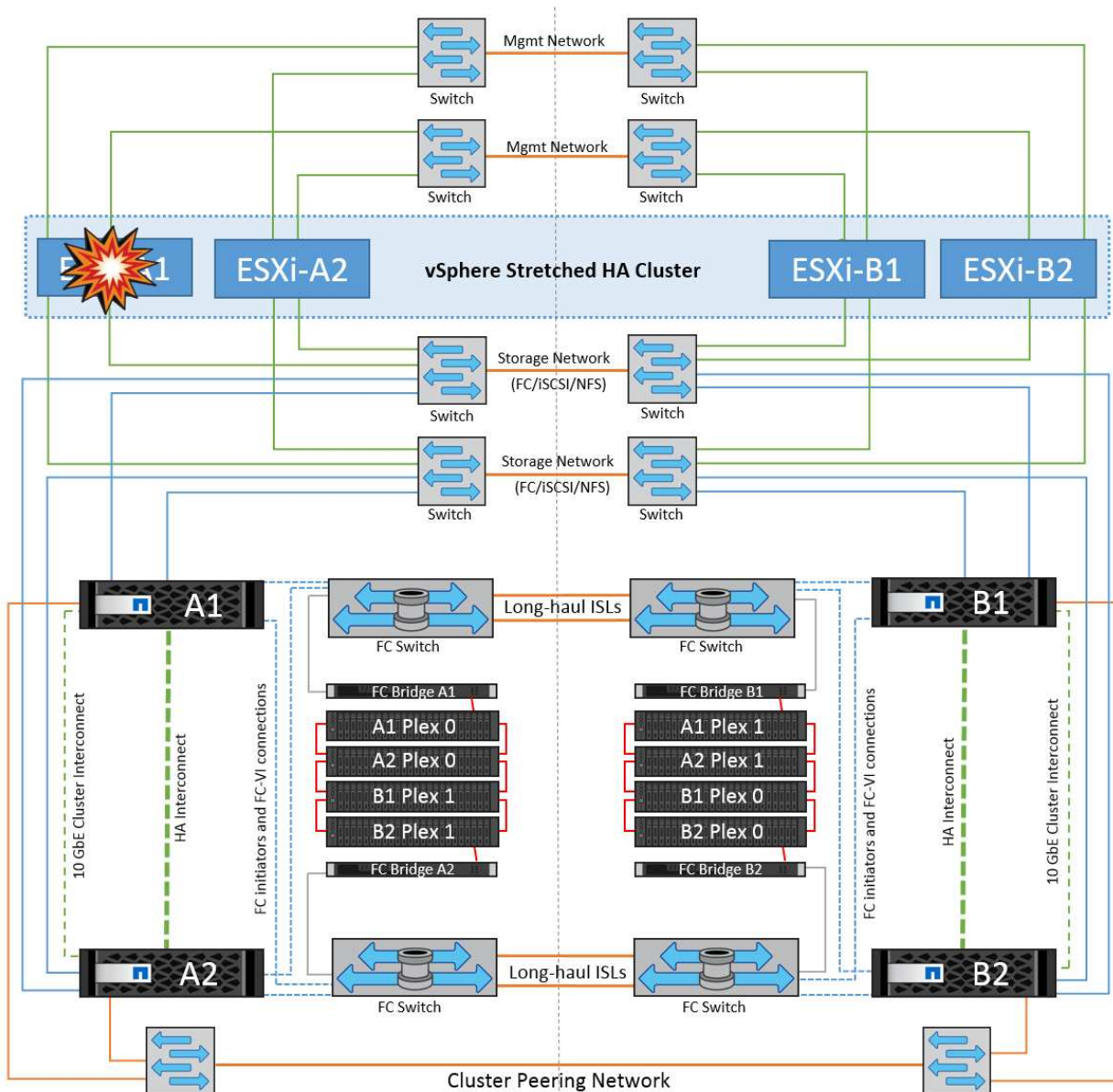
Außerdem muss bei iSCSI LUNs Multipathing konfiguriert werden, indem die VMkernel-Schnittstellen an die iSCSI-Netzwerkadapter gebunden werden. Weitere Informationen finden Sie in der vSphere-Speicherdokumentation.

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



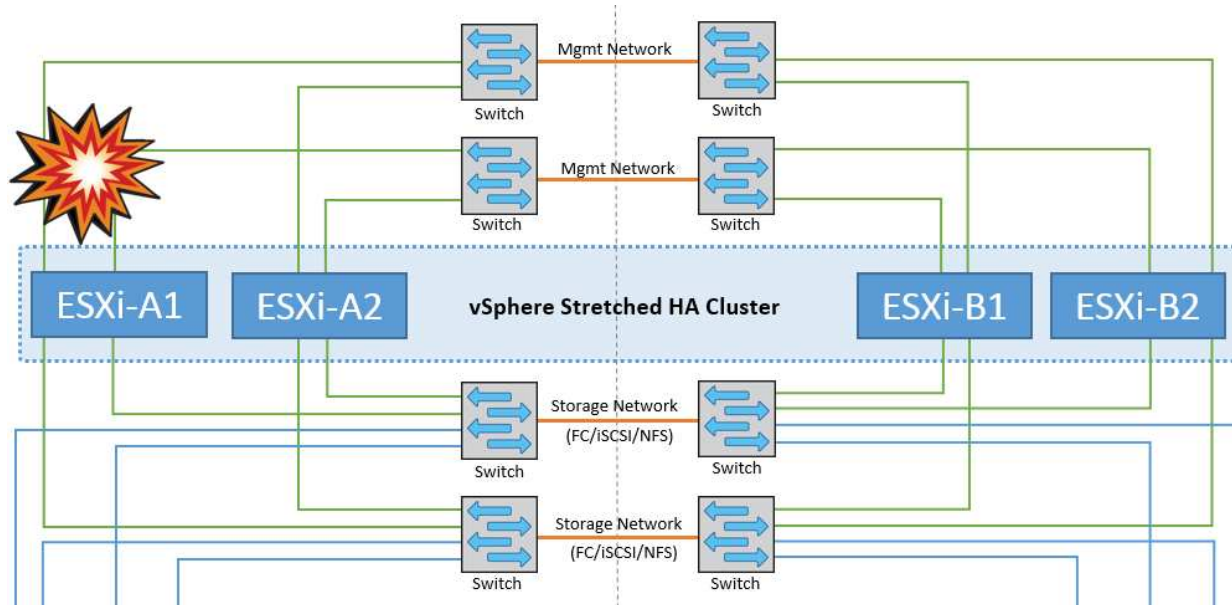
Wenn in diesem Szenario ein ESXi-Host ausfällt, erkennt der Master-Node im VMware HA-Cluster den Host-Ausfall, da er keine Netzwerk-Heartbeats mehr empfängt. Um festzustellen, ob der Host wirklich ausgefallen ist oder nur eine Netzwerkpartition ist, überwacht der Master-Knoten die Datastore-Heartbeats 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

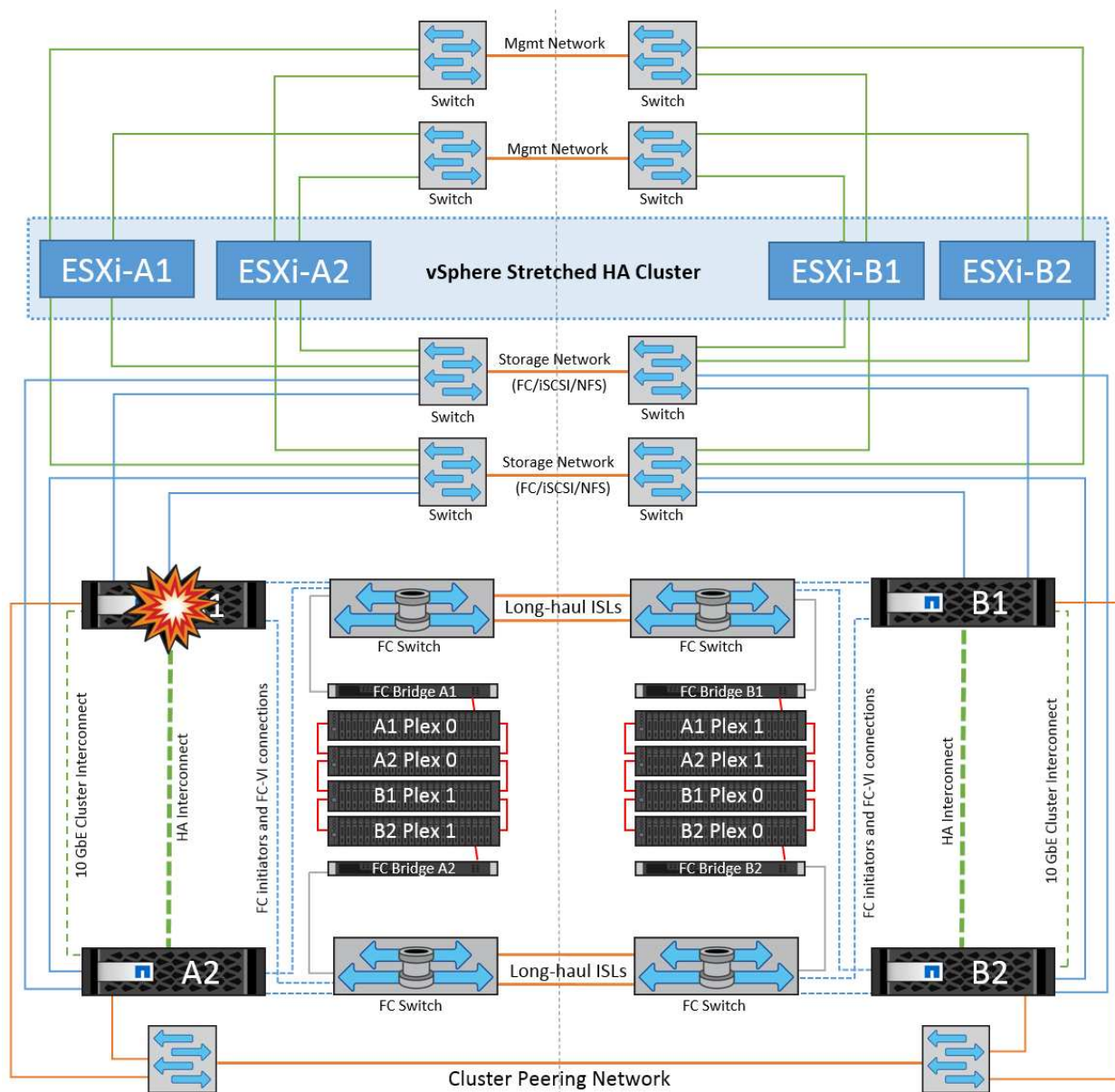


Wenn in diesem Szenario das Managementnetzwerk des ESXi-Hosts ausgefallen ist, erhält der Master-Node im HA-Cluster keine Heartbeats, wodurch dieser Host im Netzwerk isoliert wird. Um festzustellen, ob es ausgefallen ist oder nur isoliert ist, beginnt der Master-Node mit der Überwachung des Datastore-Herzschlags. 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

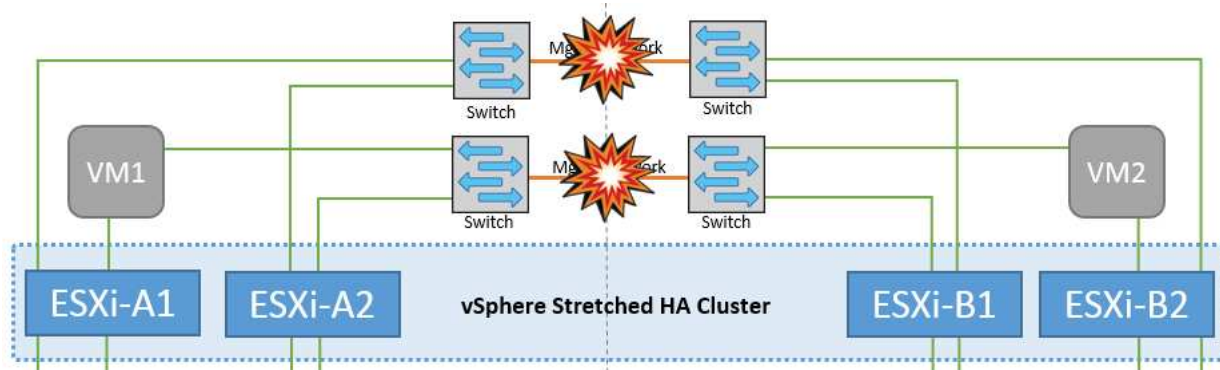
In diesem Szenario kommt es zu einem Ausfall von mehr als zwei Festplatten oder eines gesamten Shelf. Daten werden vom verbleibenden Plex ohne Unterbrechung der Datenservices bereitgestellt. Der Festplattenausfall kann sich auf einen lokalen oder einen Remote-Plex auswirken. Die Aggregate werden als degradierte 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 erstellt werden.



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

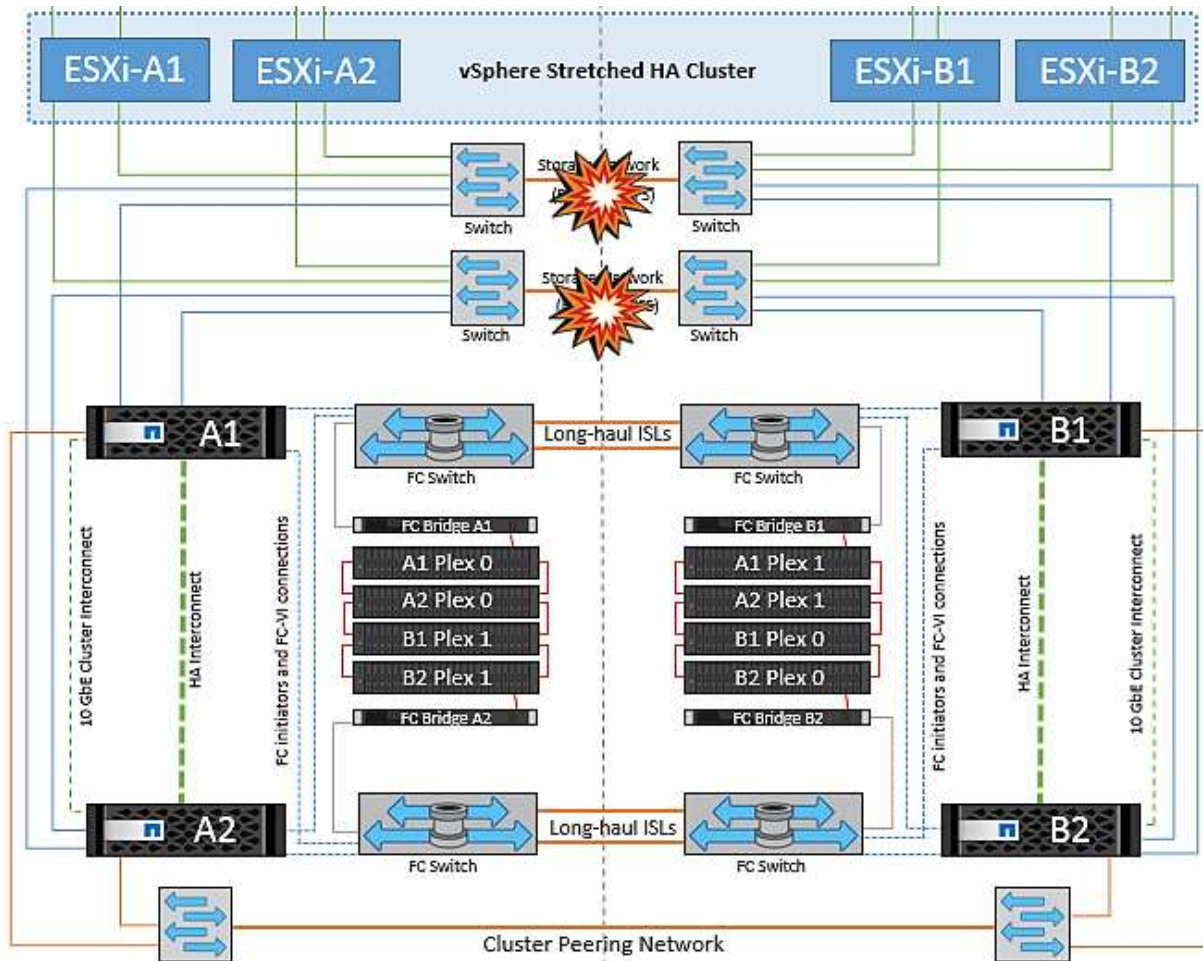
Verbindungsfehler zwischen Switches im Managementnetzwerk



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.

Hinweis: während dieser Zeit 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.

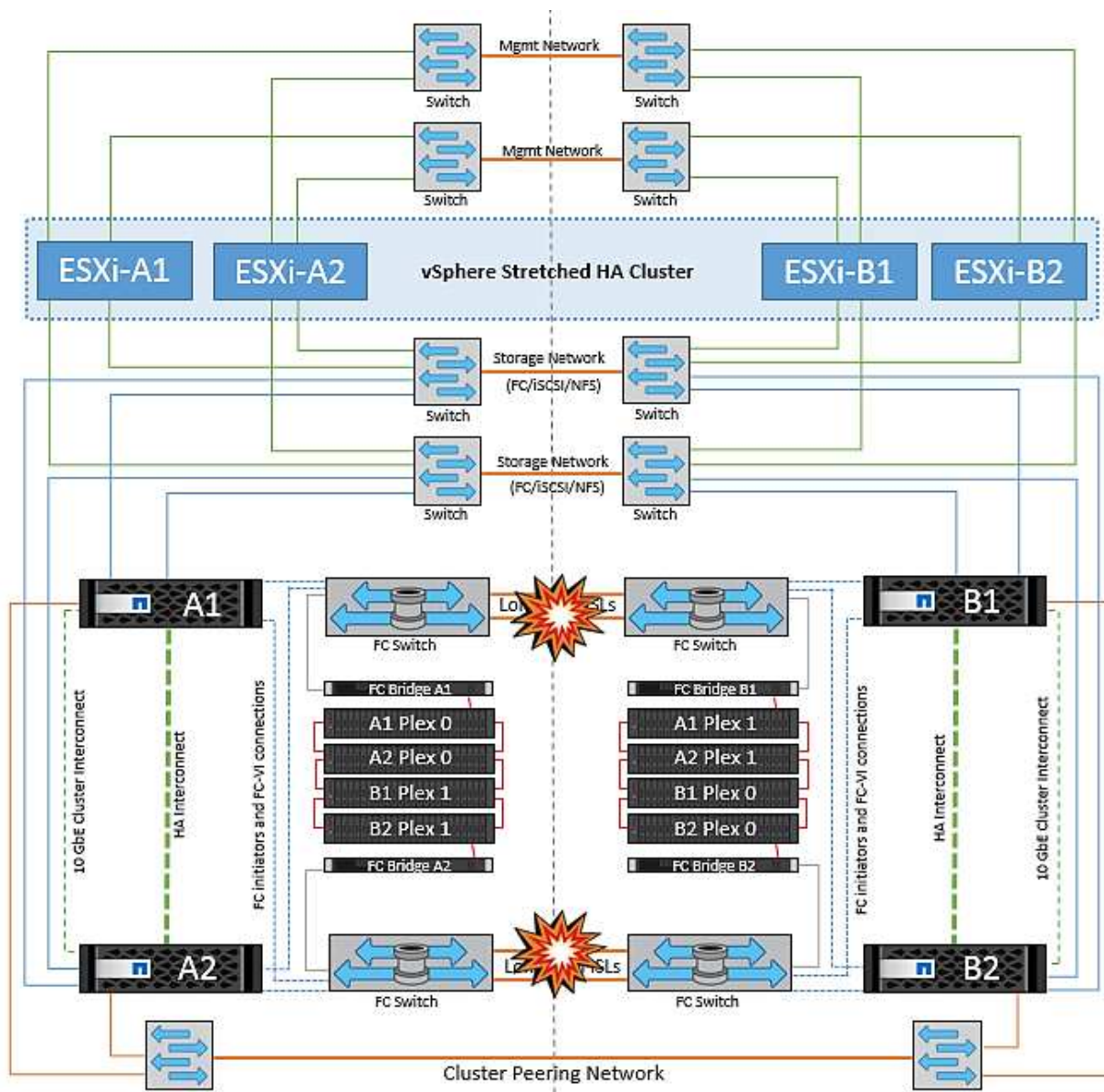
Wenn aus irgendeinem Grund die Affinitätsregel verletzt wurde (z. B. VM1, das von Standort A ausgeführt werden sollte, wo sich seine Festplatten auf lokalen Cluster A-Knoten befinden, auf einem Host an Standort B ausgeführt wird), wird der Remote-Zugriff auf das Laufwerk der virtuellen Maschine über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

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

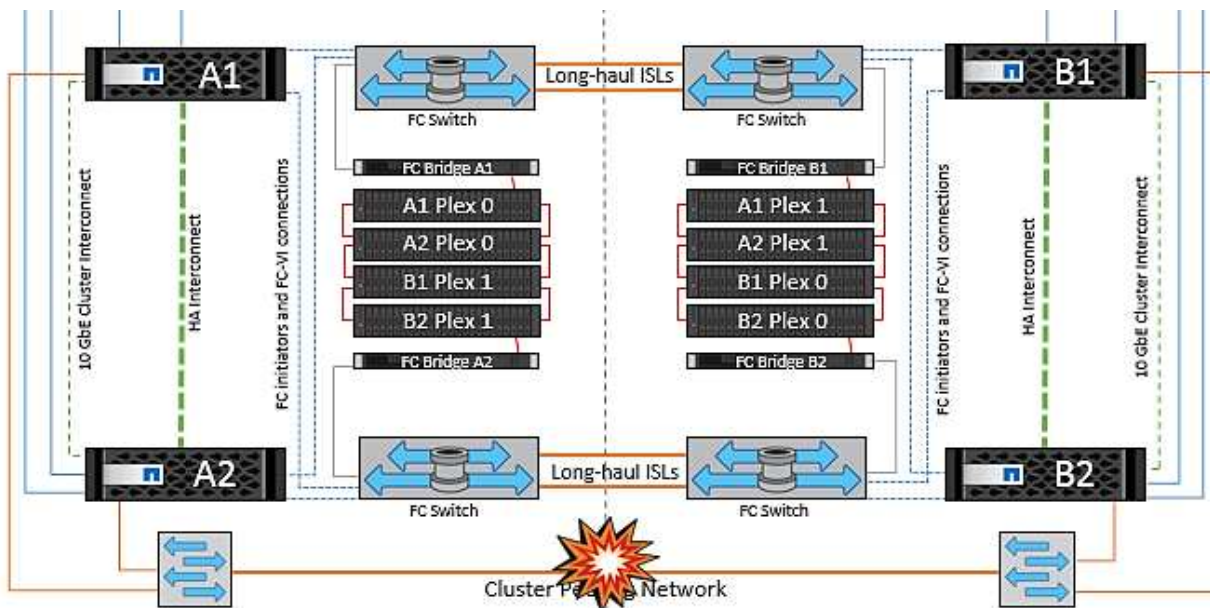
In einem Szenario, in dem ein oder mehrere ISLs ausfallen, wird der Datenverkehr über die verbleibenden Links fortgesetzt. Wenn alle ISLs auf beiden Fabrics ausfallen, sodass kein Link zwischen den Standorten für die Storage- und NVRAM-Replizierung vorhanden ist, stellt jeder Controller weiterhin seine lokalen Daten bereit. Bei der Wiederherstellung eines Minimums von einer ISL wird die Resynchronisierung 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 Wiederherstellung der Peering-Cluster-Verbindung automatisch auf das andere Cluster übertragen. 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.



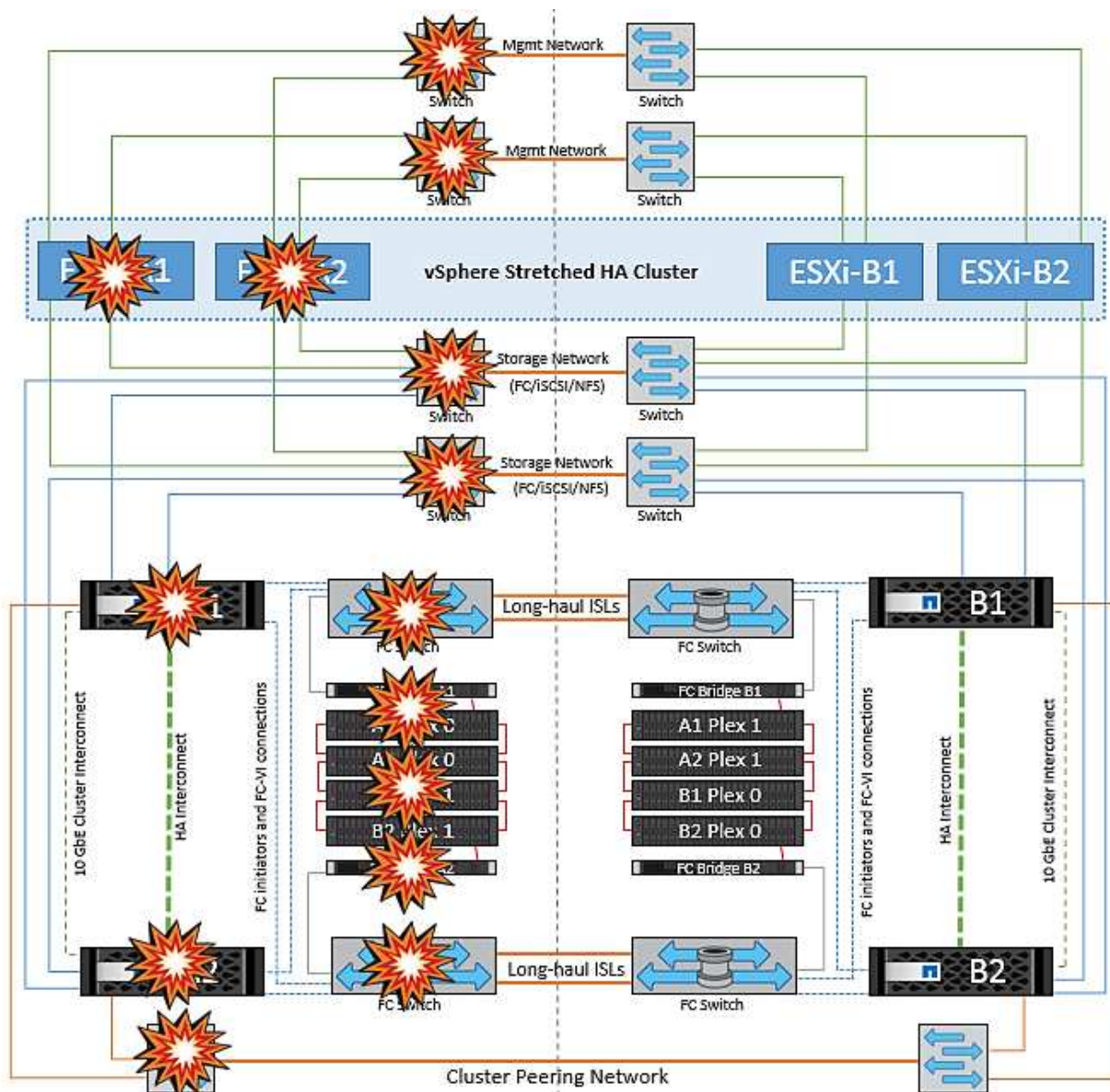
Kompletter Standortausfall

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 wieder aufzunehmen. 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).

Hinweis: der HA-Master startet die Neustartversuche erst, wenn der Platzierungsmanager geeigneten Speicher findet. Im Falle eines vollständigen Standortausfalls würde dies nach der Umschaltung der Fall sein.

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 fort dauernde 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

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 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 die Option Administration. 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).

Deploy OVF Template

- ✓ 1 Select an OVF template
- ✓ 2 Select a name and folder
- ✓ 3 Select a compute resource
- 4 Review details**
- 5 License agreements
- 6 Select storage
- 7 Select networks
- 8 Customize template
- 9 Ready to complete

Review details

Verify the template details.

Publisher	Entrust Code Signing CA - OVCS2 (Trusted certificate)
Product	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere
Version	See appliance for version
Vendor	NetApp Inc.
Description	Virtual Appliance - NetApp Inc. ONTAP tools for VMware vSphere for netapp storage systems. For more information or support please visit https://www.netapp.com/
Download size	2.2 GB
Size on disk	3.9 GB (thin provisioned)
	53.0 GB (thick provisioned)

CANCEL

BACK

NEXT

Activate
Go to Sys

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

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

Bitte 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= ';  
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 Access Points (User)

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

1. Systembenutzer: Das root-Benutzerkonto
2. Anwendungsbutzer: 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. Anwendungsbutzer

Der Anwendungsbutzer 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 Anwendungsbutzern 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.

Mutual TLS (Certificate-Based Authentication)

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.

Name		Type	IP Address	ONTAP Release	Status	Capacity	NFS VAAI	Supported Protocols
CL_sti2l-vsim-ucs59im_1678878260		Cluster	10.224.85.142	9.12.0	Normal	20.42%		

Storage Systems per page: 10 1 Item

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

i 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:

Username:

Password:

Port: 443

Advanced options

ONTAP Cluster Certificate:

☒ Automatically fetch
☐ Manually upload

CANCEL ADD

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

10.224.58.52

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

Authorize Cluster Certificate

Host 10.234.85.142 has identified itself with a self-signed certificate.

[Hide certificate](#)

Certificate Information

This certificate identifies the 10.234.85.142 host.

Issued By

Name (CN or DN): C1_sti21-vsim-ucs581m_1678878260

Issued To

Name (CN or DN): C1_sti21-vsim-ucs581m_1678878260

Validity

Issued On: 03/15/2023 11:16:06

Expires On: 03/14/2024 11:16:06

Fingerprint Information

SHA-1 Fingerprint: 2C:38:E3:5C:4B:F3:5D:3F:39:C8:CE:4A:8
2:C1:A6:EE:34:53:A0:F3

SHA-256 Fingerprint: 05:0F:FE:CD:B0:C6:FC:6F:EB:8A:FC:86:F
7:E3:EF:D4:8D:CA:02:92:9B:E1:A4:70:84:
52:F8:76:98:64:FA:23

Do you want to trust this certificate?

NO

YES

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



HTTPS-Zertifikat für ONTAP-Tools

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.

Anmelde-Banner

Das folgende Anmeldebanner wird angezeigt, nachdem der Benutzer einen

Benutzernamen in die Anmeldeaufforderung eingegeben hat. Beachten Sie bitte, 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

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 Anfragen pro Benutzer (Netzwerksicherheitsschutz :: DOS-Angriff)

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)

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

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:

```
Maintenance Console : "NetApp ONTAP tools for VMware vSphere"
Discovered interfaces: eth0 (ENABLED)
validating password policies
```

- 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:

```
Your Administrator and Database password is expired or does not match password policy:
-----
1 ) Change 'administrator' user password
2 ) Change database password
x ) Exit
Enter your choice: _
```

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

```
Changing password for administrator.
User: administrator
Enter new password:
Retype new password:

Password doesn't matches the password policy.
For security reasons, it is recommended to use a password that is of eight to thirty characters and
contains a minimum of one upper, one lower, one digit, and one special character.

Enter new password:
Retype new password:
Check if new decoder works ?
New decoder worked successfully
00-02/23 13:36:53 Your new password must be different

Error updating sra credential file

Press ENTER to continue._
```

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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