



VMware Virtualisierung

NetApp Solutions

NetApp
December 19, 2024

Inhalt

- NetApp-Lösungen für die Virtualisierung mit VMware von Broadcom 1
 - VMware vSphere mit ONTAP – 1
 - VMware vSphere Foundation 1
 - VMware Cloud Foundation 192
 - Migration von VMs 355
 - NetApp Hybrid-Multi-Cloud mit VMware Lösungen 409
 - Anwendungsfälle für die VMware Hybrid-Multi-Cloud 409
 - VMware vSphere Automation 410
 - Demos und Tutorials 433

NetApp-Lösungen für die Virtualisierung mit VMware von Broadcom

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.

Weitere Informationen finden Sie unter ["VMware vSphere mit ONTAP –"](#)

VMware vSphere Foundation

NFS Reference Guide für vSphere 8

NFS v3 Reference Guide für vSphere 8

VMware vSphere Foundation (VVF) ist eine Plattform der Enterprise-Klasse, die verschiedene virtualisierte Workloads unterstützt. Core-to-vSphere sind VMware vCenter, der ESXi-Hypervisor, Netzwerkkomponenten und verschiedene Ressourcen-Services. In Kombination mit ONTAP weisen virtualisierte Infrastrukturen auf Basis von VMware bemerkenswerte Flexibilität, Skalierbarkeit und Leistungsfähigkeit auf.

Verwendung von NFS v3 mit vSphere 8 und ONTAP Storage-Systemen

Dieses Dokument enthält Informationen zu Storage-Optionen, die für VMware Cloud vSphere Foundation unter Verwendung von NetApp All-Flash-Arrays verfügbar sind. Unterstützte Storage-Optionen werden durch spezielle Anweisungen zur Implementierung von NFS-Datstores abgedeckt. Außerdem wird VMware Live Site Recovery für Disaster Recovery bei NFS-Datenspeichern vorgestellt. Und schließlich wird der autonome Ransomware-Schutz von NetApp für NFS-Storage überprüft.

Anwendungsfälle

Anwendungsfälle in dieser Dokumentation:

- Storage-Optionen für Kunden, die einheitliche Umgebungen sowohl in privaten als auch in öffentlichen Clouds benötigen.
- Implementierung einer virtuellen Infrastruktur für Workloads
- Skalierbare Storage-Lösung, die auf neue Anforderungen zugeschnitten ist, auch wenn sie nicht direkt auf die Anforderungen von Computing-Ressourcen ausgerichtet ist
- Sichern Sie VMs und Datstores mit dem SnapCenter Plug-in für VMware vSphere.
- Verwendung von VMware Live Site Recovery für Disaster Recovery von NFS-Datenspeichern.
- Ransomware-Erkennungsstrategie, die mehrere Schutzschichten auf ESXi Host- und Gast-VM-Ebene

umfasst.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Lösungsarchitekten, die flexiblere Storage-Optionen für VMware Umgebungen benötigen und ihre TCO maximieren möchten.
- Lösungsarchitekten, die auf der Suche nach VVF Storage-Optionen sind, die Datensicherungs- und Disaster Recovery-Optionen bei den großen Cloud-Providern bieten.
- Storage-Administratoren, die spezifische Anweisungen zur Konfiguration von VVVF mit NFS-Storage benötigen.
- Storage-Administratoren, die spezifische Anweisungen zum Schutz von VMs und Datenspeichern auf ONTAP Storage benötigen.

Technologischer Überblick

Das NFS v3 VVVF Referenzhandbuch für vSphere 8 besteht aus den folgenden Hauptkomponenten:

VMware vSphere Foundation

VMware vCenter, eine zentrale Komponente von vSphere Foundation, ist eine zentralisierte Managementplattform für Konfiguration, Kontrolle und Administration von vSphere-Umgebungen. VCenter dient als Basis für das Management virtualisierter Infrastrukturen. Administratoren können so VMs, Container und ESXi-Hosts innerhalb der virtuellen Umgebung implementieren, überwachen und managen.

Die VVF Lösung unterstützt sowohl native Kubernetes-Workloads als auch Workloads, die auf Virtual Machines basieren. Wichtige Komponenten:

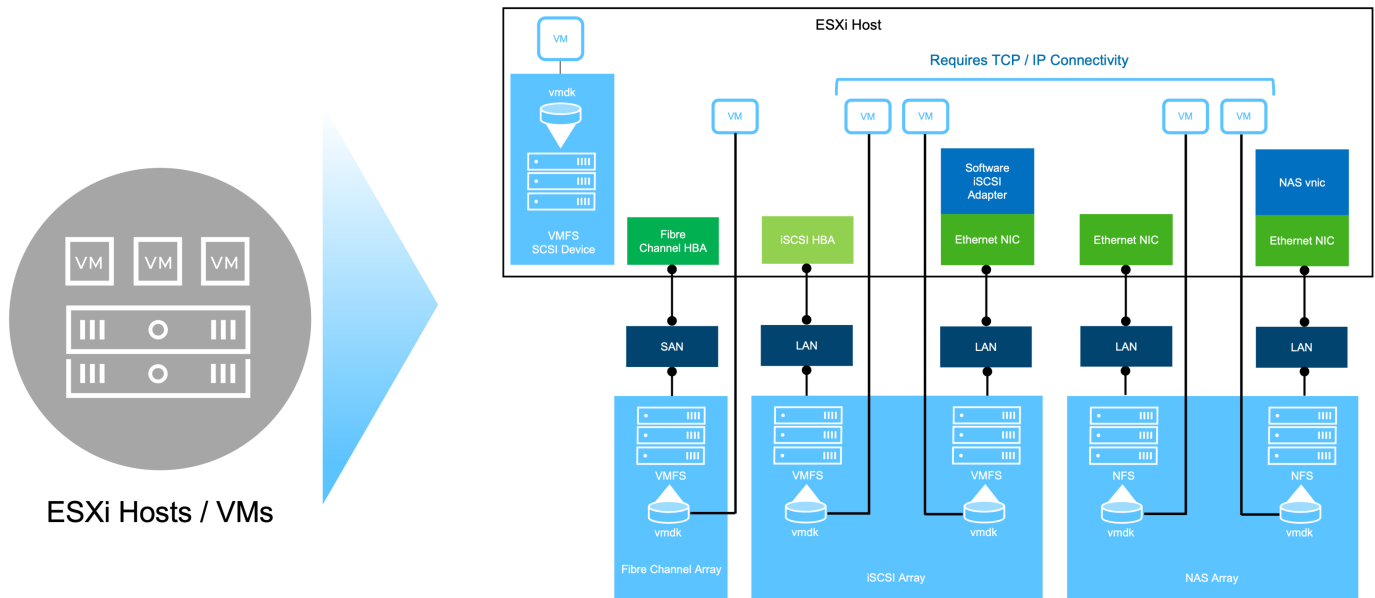
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware Tanzu Kubernetes Grid Service für vSphere
- vSphere Distributed Switch

Weitere Informationen zu VVF-enthaltenen Komponenten finden Sie unter Architektur und Planung. "[VMware vSphere Product Live Comparison](#)"

VVF Storage-Optionen

Im Mittelpunkt einer erfolgreichen und leistungsstarken virtuellen Umgebung steht Storage. Storage – ob mit VMware Datastores oder mit Gast verbundenen Anwendungsfällen – sorgt für die optimale Nutzung Ihrer Workloads, da Sie den besten Preis pro GB wählen können, der den größten Mehrwert bietet und gleichzeitig die Unterauslastung reduziert. 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.

VMware Storage-Optionen sind in der Regel als herkömmliche Storage- und softwaredefinierte Storage-Angebote organisiert. Herkömmliche Storage-Modelle umfassen lokalen und Netzwerk-Storage, während softwaredefinierte Storage-Modelle vSAN und VMware Virtual Volumes (VVols) umfassen.



<https://docs.vmware.com/en/VMware-vSphere/8.0/vsphere-storage/GUID-F602EB17-8D24-400A-9B05-196CEA66464F.html> ["Einführung in Storage in einer vSphere Umgebung"] Weitere Informationen zu unterstützten Storage-Typen für VMware vSphere Foundation finden Sie unter.

NetApp ONTAP

Es gibt zahlreiche überzeugende Gründe, warum sich Zehntausende Kunden für ONTAP als primäre Storage-Lösung für vSphere entschieden haben. Hierzu zählen:

1. **Unified Storage System:** ONTAP bietet ein Unified Storage-System, das sowohl SAN- als auch NAS-Protokolle unterstützt. Diese Vielseitigkeit ermöglicht die nahtlose Integration verschiedener Storage-Technologien in einer einzigen Lösung.
2. **Robuste Datensicherung:** ONTAP bietet robuste Datensicherungsfunktionen durch platzsparende Snapshots. Diese Snapshots ermöglichen effiziente Backup- und Recovery-Prozesse und gewährleisten so die Sicherheit und Integrität von Applikationsdaten.
3. **Umfassende Verwaltungstools:** ONTAP bietet eine Fülle von Tools, die bei der effektiven Verwaltung von Anwendungsdaten helfen sollen. Diese Tools optimieren das Storage-Management, verbessern die betriebliche Effizienz und vereinfachen die Administration.
4. **Storage-Effizienz:** ONTAP enthält verschiedene standardmäßig aktivierte Storage-Effizienz-Funktionen, die zur Optimierung der Speicherauslastung, zur Senkung von Kosten und zur Verbesserung der Gesamtsystemleistung entwickelt wurden.

Die Verwendung von ONTAP mit VMware bietet ein hohes Maß an Flexibilität bei den gegebenen Applikationsanforderungen. Die folgenden Protokolle werden als VMware Datastore mit ONTAP unterstützt: * FCP * FCoE * NVMe/FC * NVMe/TCP * iSCSI * NFS v3 * NFS v4.1

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.

Rein Flash-basierte NetApp Arrays

NetApp AFF (All Flash FAS) ist eine Produktreihe von All-Flash-Storage-Arrays. Es wurde für hochperformante Storage-Lösungen mit niedriger Latenz für Enterprise-Workloads entwickelt. Die AFF Series kombiniert die Vorteile der Flash-Technologie mit den Datenmanagementfunktionen von NetApp und bietet Unternehmen eine leistungsstarke und effiziente Storage-Plattform.

Die Produktpalette von AFF umfasst sowohl Die Modelle Der A-Serie als auch der C-Serie.

All-NVMe-Flash-Arrays der NetApp A-Serie wurden für hochperformante Workloads entwickelt und bieten eine äußerst niedrige Latenz und hohe Ausfallsicherheit. Dadurch sind sie für geschäftskritische Applikationen geeignet.

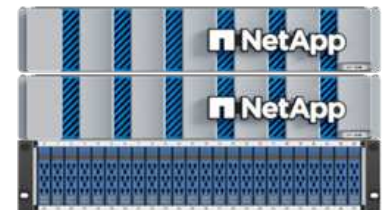
AFF A70



AFF A90



AFF A1K



QLC Flash-Arrays der C-Serie richten sich an Anwendungsfälle mit höherer Kapazität, die die Geschwindigkeit von Flash mit der Wirtschaftlichkeit von Hybrid Flash bieten.

AFF C250



AFF C400



AFF C800



Unterstützte Storage-Protokolle

Die AFF unterstützen alle Standardprotokolle, die bei der Virtualisierung verwendet werden, sowohl für Datstores als auch für Gast-verbundenen Storage. Hierzu zählen NFS, SMB, iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE), NVME over Fabrics und S3. Kunden können frei wählen, was für ihre Workloads und Applikationen am besten geeignet ist.

NFS - NetApp AFF bietet Unterstützung für NFS und ermöglicht den dateibasierten Zugriff auf VMware-Datstores. Mit dem NFS verbundene Datstores von vielen ESXi-Hosts übersteigen die für VMFS-Dateisysteme auferlegten Beschränkungen bei Weitem. Die Verwendung von NFS mit vSphere bietet einige Vorteile im Hinblick auf Benutzerfreundlichkeit und Storage-Effizienz. ONTAP umfasst Dateizugriffsfunktionen, die für das NFS-Protokoll verfügbar sind. Sie können einen NFS-Server aktivieren und Volumes oder qtrees exportieren.

Designberatung für NFS-Konfigurationen finden Sie im ["Dokumentation des NAS-Storage-Managements"](#).

iSCSI - NetApp AFF bietet robuste Unterstützung für iSCSI und ermöglicht den Zugriff auf Speichergeräte auf Blockebene über IP-Netzwerke. Die nahtlose Integration mit iSCSI-Initiatoren ermöglicht eine effiziente Bereitstellung und Verwaltung von iSCSI-LUNs. Die erweiterten Funktionen von ONTAP wie Multi-Pathing, CHAP-Authentifizierung und ALUA-Unterstützung

Designanleitungen zu iSCSI-Konfigurationen finden Sie im ["Referenzdokumentation zur SAN-Konfiguration"](#).

Fibre Channel - NetApp AFF bietet umfassende Unterstützung für Fibre Channel (FC), eine Hochgeschwindigkeits-Netzwerktechnologie, die häufig in Storage Area Networks (SANs) verwendet wird. ONTAP lässt sich nahtlos in FC-Infrastrukturen integrieren und bietet zuverlässigen und effizienten Zugriff auf Storage-Geräte auf Blockebene. Mit Funktionen wie Zoning, Multi-Pathing und Fabric Login (FLOGI) wird die Performance optimiert, die Sicherheit erhöht und die nahtlose Konnektivität in FC-Umgebungen sichergestellt.

Informationen zum Design von Fibre-Channel-Konfigurationen finden Sie im ["Referenzdokumentation zur SAN-Konfiguration"](#).

NVMe over Fabrics - NetApp ONTAP unterstützen NVMe over Fabrics. NVMe/FC ermöglicht die Verwendung von NVMe-Storage-Geräten über Fibre-Channel-Infrastruktur und NVMe/TCP über Storage-IP-Netzwerke.

Eine Anleitung zum Design für NVMe finden Sie unter ["Konfiguration, Support und Einschränkungen von NVMe"](#).

Aktiv/aktiv-Technologie

Rein Flash-basierte NetApp Arrays ermöglichen aktiv/aktiv-Pfade durch beide Controller. Dadurch muss das Host-Betriebssystem nicht auf einen Ausfall eines aktiven Pfads warten, bevor der alternative Pfad aktiviert wird. Das bedeutet, dass der Host alle verfügbaren Pfade auf allen Controllern nutzen kann und sicherstellen kann, dass immer aktive Pfade vorhanden sind, unabhängig davon, ob sich das System in einem stabilen Zustand befindet oder ob ein Controller Failover durchgeführt wird.

Weitere Informationen finden Sie in ["Datensicherung und Disaster Recovery"](#) der Dokumentation.

Storage-Garantien

NetApp bietet mit All-Flash-Arrays von NetApp eine einzigartige Auswahl an Storage-Garantien. Einzigartige Vorteile:

Storage-Effizienz-Garantie: mit der Storage-Effizienz-Garantie erzielen Sie eine hohe Performance bei gleichzeitiger Minimierung der Storage-Kosten. 4:1 für SAN-Workloads. **Ransomware Recovery-Garantie:** Garantierte Datenwiederherstellung im Falle eines Ransomware-Angriffs.

Ausführliche Informationen finden Sie im ["NetApp AFF Landing Page"](#).

NetApp ONTAP Tools für VMware vSphere

Eine leistungsstarke Komponente von vCenter ist die Möglichkeit, Plug-ins oder Erweiterungen zu integrieren, die die Funktionalität weiter verbessern und zusätzliche Funktionen bieten. Diese Plug-ins erweitern die Management-Funktionen von vCenter und ermöglichen Administratoren die Integration von Lösungen, Tools und Services von Drittanbietern in ihre vSphere-Umgebung.

NetApp ONTAP Tools for VMware ist eine umfassende Suite an Tools, die mithilfe der vCenter Plug-in-Architektur das Lifecycle Management von Virtual Machines in VMware Umgebungen vereinfachen. Diese Tools lassen sich nahtlos in das VMware Ecosystem integrieren und ermöglichen so eine effiziente Datastore-

Bereitstellung und unverzichtbaren Schutz für Virtual Machines. Mit den ONTAP Tools für VMware vSphere können Administratoren Storage-Lifecycle-Management-Aufgaben mühelos managen.

Umfassende ONTAP-Tools 10 Ressourcen finden Sie ["ONTAP Tools für VMware vSphere – Dokumentationsressourcen"](#).

Sehen Sie sich die Implementierungslösung ONTAP Tools 10 unter an ["Konfigurieren Sie NFS-Datastores für vSphere 8 mit den ONTAP-Tools 10"](#)

NetApp NFS Plug-in für VMware VAAI

Das NetApp NFS Plug-in für VAAI (vStorage APIs zur Array-Integration) optimiert Storage-Vorgänge, indem bestimmte Aufgaben an das NetApp Storage-System abgegeben werden. Dies führt zu einer verbesserten Performance und Effizienz. Dazu gehören Vorgänge wie das vollständige Kopieren, das Nullsetzen von Blöcken und die Hardware-gestützte Sperrung. Darüber hinaus optimiert das VAAI-Plug-in die Storage-Auslastung, indem die über das Netzwerk übertragene Datenmenge bei Bereitstellung und Klonvorgängen von Virtual Machines reduziert wird.

Das NetApp NFS-Plug-in für VAAI kann von der NetApp Support-Website heruntergeladen werden. Es wird mithilfe der ONTAP Tools für VMware vSphere auf ESXi Hosts hochgeladen und installiert.

Weitere Informationen finden Sie unter ["NetApp NFS Plug-in für VMware VAAI Dokumentation"](#) .

SnapCenter Plug-in für VMware vSphere

Das SnapCenter Plug-in für VMware vSphere (SCV) ist eine Softwarelösung von NetApp, die umfassende Datensicherung für VMware vSphere Umgebungen bietet. Er vereinfacht und optimiert den Prozess des Schutzes und des Managements von Virtual Machines (VMs) und Datastores. SCV verwendet Storage-basierten Snapshot und Replikation zu sekundären Arrays, um kürzere Recovery Time Objectives zu erreichen.

Das SnapCenter Plug-in für VMware vSphere bietet folgende Funktionen in einer einheitlichen Oberfläche, die in den vSphere Client integriert ist:

Policy-basierte Snapshots - mit SnapCenter können Sie Richtlinien für die Erstellung und Verwaltung von anwendungskonsistenten Snapshots von virtuellen Maschinen (VMs) in VMware vSphere definieren.

Automatisierung - automatisierte Snapshot-Erstellung und -Verwaltung auf Basis definierter Richtlinien unterstützen einen konsistenten und effizienten Datenschutz.

Schutz auf VM-Ebene - granularer Schutz auf VM-Ebene ermöglicht effizientes Management und Recovery einzelner virtueller Maschinen.

Funktionen zur Storage-Effizienz - durch die Integration in NetApp Storage-Technologien können Storage-Effizienz-Funktionen wie Deduplizierung und Komprimierung für Snapshots erzielt werden, was die Speicheranforderungen minimiert.

Das SnapCenter-Plug-in orchestriert die Stilllegung von Virtual Machines in Verbindung mit hardwarebasierten Snapshots auf NetApp Storage-Arrays. Die SnapMirror Technologie wird eingesetzt, um Backup-Kopien auf sekundäre Storage-Systeme einschließlich in der Cloud zu replizieren.

Weitere Informationen finden Sie im ["Dokumentation zum SnapCenter Plug-in für VMware vSphere"](#).

Die Integration von BlueXP ermöglicht 3-2-1-1-Backup-Strategien zur Erweiterung von Datenkopien auf Objekt-Storage in der Cloud.

Weitere Informationen zu 3-2-1-1-Backup-Strategien mit BlueXP finden Sie unter ["3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs"](#).

Anweisungen zur schrittweisen Bereitstellung des SnapCenter-Plug-ins finden Sie in der Lösung ["Schützen Sie VMs in VCF-Workload-Domänen mit dem SnapCenter Plug-in für VMware vSphere"](#).

Überlegungen zum Storage

Durch die Nutzung von ONTAP NFS-Datenspeichern mit VMware vSphere erhalten Sie eine hochperformante, einfach zu managende und skalierbare Umgebung, die mit blockbasierten Storage-Protokollen nicht erreichbar ist. Diese Architektur kann zu einer Verzehnfachung der Datastore-Dichte und einer entsprechenden Reduzierung der Datenspeicher führen.

NConnect for NFS: ein weiterer Vorteil der Nutzung von NFS ist die Möglichkeit, die **nConnect** Funktion zu nutzen. NConnect ermöglicht mehrere TCP Verbindungen für NFS v3 Datastore Volumes, wodurch ein höherer Durchsatz erzielt wird. Dies erhöht die Parallelität und bei NFS-Datastores. Kunden, die Datastores mit NFS Version 3 implementieren, können die Anzahl der Verbindungen zum NFS-Server erhöhen und so die Auslastung der ultraschnellen Netzwerkschnittstellenkarten maximieren.

Ausführliche Informationen zu nConnect finden Sie unter ["NFS nConnect Funktion mit VMware und NetApp"](#).

Session-Trunking für NFS: ab ONTAP 9.14.1 können Clients, die NFSv4.1 verwenden, Session-Trunking nutzen, um mehrere Verbindungen zu verschiedenen LIFs auf dem NFS-Server aufzubauen. Dies ermöglicht schnellere Datentransfers und verbessert die Ausfallsicherheit durch Multipathing. Das Trunking erweist sich besonders beim Export von FlexVol Volumes an Clients, die Trunking unterstützen, wie z. B. VMware und Linux Clients, oder bei der Verwendung von NFS über RDMA-, TCP- oder pNFS-Protokollen.

Weitere Informationen finden Sie unter ["Übersicht über NFS Trunking"](#).

FlexVol Volumes: NetApp empfiehlt die Verwendung von **FlexVol** Volumes für die meisten NFS Datastores. Obwohl größere Datastores die Storage-Effizienz und betriebliche Vorteile verbessern können, sollte mindestens vier Datastores (FlexVol Volumes) verwendet werden, um VMs auf einem einzelnen ONTAP Controller zu speichern. Administratoren implementieren normalerweise Datastores, die von FlexVol Volumes mit Kapazitäten von 4 TB bis 8 TB unterstützt werden. Diese Größe sorgt für ein gutes Gleichgewicht zwischen Performance, einfacher Verwaltung und Datensicherung. Administratoren können klein anfangen und den Datenspeicher nach Bedarf skalieren (bis zu maximal 100 TB). Kleinere Datastores ermöglichen ein schnelleres Recovery nach Backups oder Ausfällen und lassen sich innerhalb des Clusters zügig verschieben. Dieser Ansatz ermöglicht eine maximale Performance-Auslastung der Hardwareressourcen und ermöglicht Datenspeicher mit verschiedenen Recovery-Richtlinien.

FlexGroup Volumes: für Szenarien, die einen großen Datastore erfordern, empfiehlt NetApp die Verwendung von **FlexGroup** Volumes. FlexGroup Volumes weisen praktisch keine Beschränkungen hinsichtlich Kapazität und Anzahl der Dateien auf. Administratoren können so problemlos einen sehr großen Single Namespace bereitstellen. Die Verwendung von FlexGroup Volumes ist ohne zusätzlichen Wartungs- oder Managementaufwand verbunden. Für eine Performance mit FlexGroup Volumes sind keine diversen Datastores erforderlich, da sie sich per se skalieren lassen. Durch die Verwendung von ONTAP und FlexGroup Volumes mit VMware vSphere lassen sich einfache und skalierbare Datenspeicher erstellen, die die volle Leistung des gesamten ONTAP Clusters ausschöpfen.

Schutz durch Ransomware

Die NetApp ONTAP Datenmanagement-Software bietet eine umfassende Suite integrierter Technologien, die Sie vor Ransomware-Angriffen schützen, sie erkennen und bei Angriffen eine Wiederherstellung ermöglichen. Die in ONTAP integrierte NetApp SnapLock Compliance Funktion verhindert das Löschen von Daten, die auf einem aktivierten Volume mithilfe von WORM (Write Once, Read Many) Technologie mit erweiterter

Datenaufbewahrung gespeichert sind. Nachdem der Aufbewahrungszeitraum festgelegt ist und die Snapshot Kopie gesperrt ist, kann selbst ein Storage-Administrator mit vollständigen System-Privileges oder ein Mitglied des NetApp Supportteams die Snapshot Kopie nicht löschen. Noch wichtiger ist jedoch, dass ein Hacker mit kompromittierten Zugangsdaten die Daten nicht löschen kann.

NetApp garantiert, dass wir Ihre geschützten NetApp® Snapshot™ Kopien auf geeigneten Arrays wiederherstellen können, und wenn dies nicht der Fall ist, werden wir Ihre Organisation entschädigen.

Weitere Informationen über die Ransomware Recovery Garantie, siehe: "[Ransomware Recovery-Garantie](#)".

```
https://docs.netapp.com/us-en/ontap/anti-ransomware/["Autonome Ransomware-Schutz - Übersicht"]Weitere Informationen finden Sie im.
```

Sehen Sie sich die vollständige Lösung im Dokumentationscenter von NetApps Solutions an: "[Autonomer Ransomware-Schutz für NFS-Storage](#)"

Überlegungen zur Disaster Recovery

NetApp bietet den weltweit sichersten Storage. NetApp kann Sie dabei unterstützen, Ihre Daten- und Applikationsinfrastruktur zu schützen, Daten zwischen lokalem Storage und der Cloud zu verschieben und dafür zu sorgen, dass sie Cloud-übergreifend zur Verfügung stehen. ONTAP verfügt über leistungsstarke Datensicherungs- und Sicherheitstechnologien, die Kunden vor Notfällen schützen, indem sie Bedrohungen proaktiv erkennen und Daten und Applikationen schnell wiederherstellen.

VMware Live Site Recovery, früher als VMware Site Recovery Manager bekannt, bietet optimierte, richtlinienbasierte Automatisierung zum Schutz virtueller Maschinen innerhalb des vSphere Web-Clients. Über den Storage Replication Adapter als Teil der ONTAP Tools für VMware nutzt diese Lösung die erweiterten Datenmanagement-Technologien von NetApp. Durch die Nutzung der Funktionen von NetApp SnapMirror für die Array-basierte Replizierung können VMware Umgebungen von einer der zuverlässigsten und ausgereiftesten Technologien von ONTAP profitieren. SnapMirror sorgt für sichere und hocheffiziente Datentransfers, indem lediglich die geänderten File-Systemblöcke kopiert werden, und keine vollständigen VMs oder Datastores. Zudem profitieren diese Blöcke von platzsparenden Techniken wie Deduplizierung, Komprimierung und Data-Compaction. Mit der Einführung versionsunabhängiger SnapMirror in modernen ONTAP Systemen profitieren Sie von der flexiblen Auswahl Ihrer Quell- und Ziel-Cluster. SnapMirror hat sich wirklich zu einem leistungsstarken Tool für Disaster Recovery entwickelt und bietet in Kombination mit Live-Site-Recovery im Vergleich zu alternativen Lösungen für lokalen Storage verbesserte Skalierbarkeit, Performance und Kosteneinsparungen.

Weitere Informationen finden Sie im "[Überblick über VMware Site Recovery Manager](#)".

Sehen Sie sich die vollständige Lösung im Dokumentationscenter von NetApps Solutions an: "[Autonomer Ransomware-Schutz für NFS-Storage](#)"

BlueXP DRaaS (Disaster Recovery as a Service) für NFS ist eine kostengünstige Disaster-Recovery-Lösung für VMware-Workloads, die auf lokalen ONTAP-Systemen mit NFS-Datastores ausgeführt werden. Es nutzt die NetApp SnapMirror-Replizierung, um sich vor Standortausfällen und Datenbeschädigung, z. B. Ransomware-Angriffen, zu schützen. Dieser Service ist in die NetApp BlueXP Konsole integriert und ermöglicht das einfache Management und die automatische Erkennung von VMware vCenter und ONTAP Storage. Unternehmen können Disaster-Recovery-Pläne erstellen und testen und durch Replikation auf Blockebene eine Recovery Point Objective (RPO) von bis zu 5 Minuten erreichen. BlueXP DRaaS nutzt die FlexClone-Technologie von ONTAP für platzsparende Tests ohne Auswirkungen auf die Produktionsressourcen. Der Service orchestriert Failover- und Failback-Prozesse, sodass geschützte Virtual Machines mit minimalem Aufwand am designierten Disaster Recovery-Standort bereitgestellt werden können. Im Vergleich zu anderen

bekanntesten Alternativen bietet BlueXP DRaaS diese Funktionen zu einem Bruchteil der Kosten. Dies ist eine effiziente Lösung für Unternehmen, die Disaster-Recovery-Vorgänge für ihre VMware Umgebungen mit ONTAP Storage-Systemen einrichten, testen und durchführen.

Sehen Sie sich die vollständige Lösung im Dokumentationscenter von NetApp Solutions an: ["DR unter Verwendung von BlueXP DRaaS für NFS-Datstores"](#)

Lösungsübersicht

In dieser Dokumentation behandelte Lösungen:

- **NFS nConnect-Funktion mit NetApp und VMware.** Klicken Sie auf, ["Hier"](#) um die Bereitstellungsschritte anzuzeigen.
 - **Verwenden Sie ONTAP Tools 10, um NFS Datstores für vSphere 8 zu konfigurieren.** Klicken Sie auf, ["Hier"](#) um die Bereitstellungsschritte anzuzeigen.
 - **Deploy and use the SnapCenter Plug-in for VMware vSphere to protect and restore VMs.** Klicken Sie auf, ["Hier"](#) um die Bereitstellungsschritte anzuzeigen.
 - **Disaster Recovery von NFS-Datenspeichern mit VMware Site Recovery Manager.** Klicken Sie auf, ["Hier"](#) um die Bereitstellungsschritte anzuzeigen.
 - **Autonomer Ransomware-Schutz für NFS-Storage.** Klicken Sie auf, ["Hier"](#) um die Bereitstellungsschritte anzuzeigen.

NFS nConnect Funktion mit NetApp und VMware

Ab VMware vSphere 8.0 U1 (als Tech-Preview) ermöglicht die nconnect Funktion mehrere TCP-Verbindungen für NFS v3 Datastore Volumes für einen höheren Durchsatz. Kunden, die NFS-Datstore verwenden, können nun die Anzahl der Verbindungen zum NFS-Server erhöhen und so die Auslastung von Hochgeschwindigkeits-Netzwerkkarten maximieren.



Das Feature ist allgemein verfügbar für NFS v3 mit 8.0 U2, siehe Speicher Abschnitt auf ["Versionshinweise zu VMware vSphere 8.0 Update 2"](#). Die Unterstützung für NFS v4.1 wurde mit vSphere 8.0 U3 hinzugefügt. Weitere Informationen finden Sie unter ["Versionshinweise zu vSphere 8.0 Update 3"](#)

Anwendungsfälle

- Hosten Sie mehr virtuelle Maschinen pro NFS-Datstore auf demselben Host.
- Steigern Sie die Performance des NFS-Datstore.
- Sie können Services auf einem höheren Tier für VM- und Container-basierte Applikationen anbieten.

Technische Details

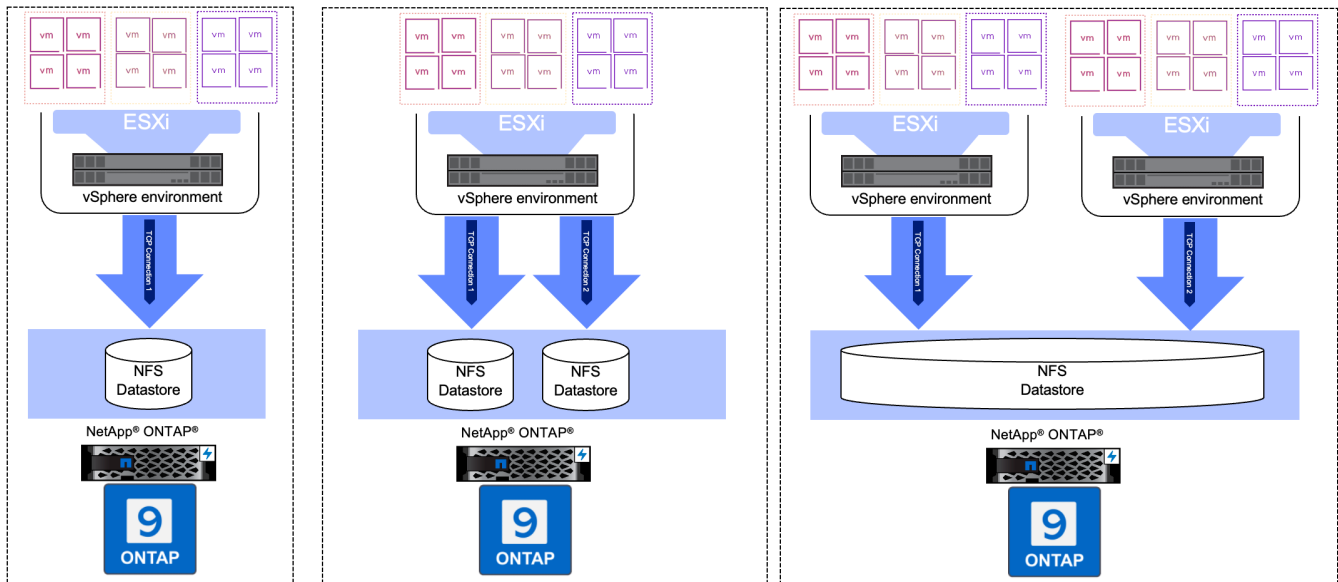
Der Zweck von nconnect besteht darin, mehrere TCP-Verbindungen pro NFS-Datstore auf einem vSphere-Host zur Verfügung zu stellen. Dadurch werden Parallelität und Performance von NFS-Datstores verbessert. Wenn in ONTAP ein NFS-Mount eingerichtet wird, wird eine Verbindungs-ID (CID) erstellt. Diese CID ermöglicht bis zu 128 gleichzeitige Operationen während des Fluges. Wenn diese Zahl vom Client überschritten wird, führt ONTAP eine Form der Flusskontrolle durch, bis sie einige verfügbare Ressourcen freisetzen kann, wenn andere Vorgänge abgeschlossen sind. Diese Pausen liegen in der Regel nur wenige Mikrosekunden, aber im Verlauf von Millionen von Operationen können sich diese summieren und

Performance-Probleme verursachen. Nconnect kann die 128-Grenze nehmen und sie mit der Anzahl der nconnect-Sitzungen auf dem Client multiplizieren, was mehr gleichzeitige Vorgänge pro CID ermöglicht und möglicherweise Leistungsvorteile bietet. Weitere Details finden Sie unter "[NFS Best Practice und Implementierungsleitfaden](#)"

Standard-NFS-Datenspeicher

Um die Performance-Einschränkungen einer einzelnen Verbindung mit einem NFS-Datastore zu beheben, werden zusätzliche Datastores gemountet oder weitere Hosts hinzugefügt, um die Verbindung zu erhöhen.

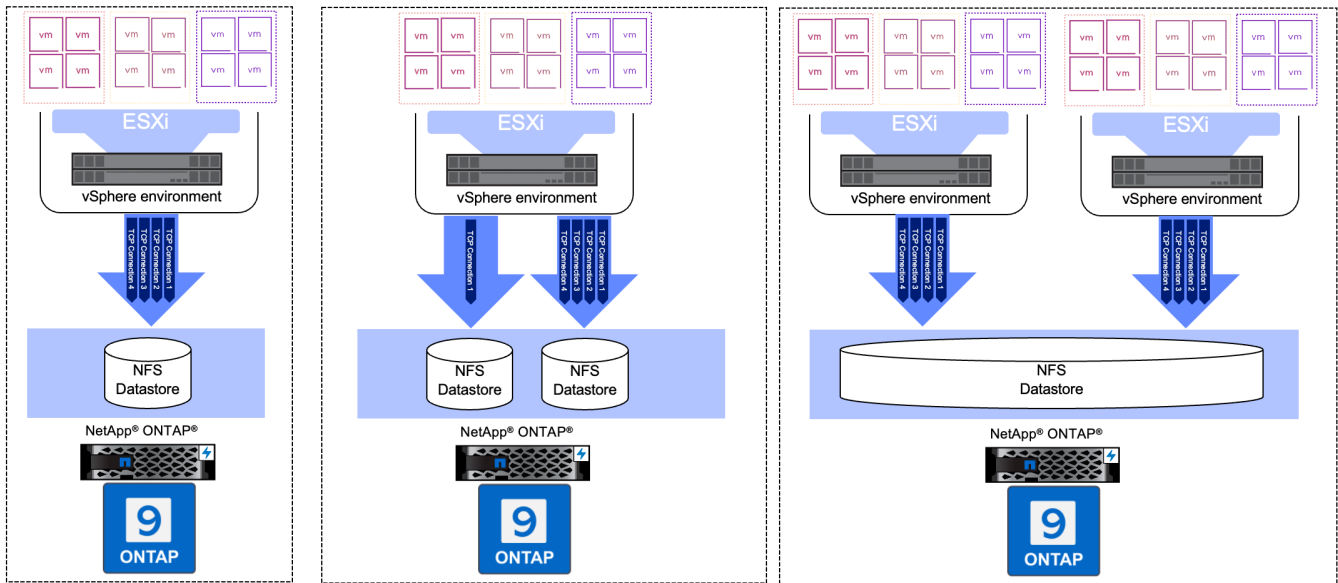
Without nConnect feature with NetApp and VMware



Mit nConnect NFS Datastore

Sobald der NFS-Datastore mit ONTAP Tools oder mit anderen Optionen erstellt wurde, kann die Anzahl der Verbindungen pro NFS-Datastore mithilfe von vSphere CLI, PowerCLI, govc Tool oder anderen API-Optionen geändert werden. Um Performance-Probleme zusammen mit vMotion zu vermeiden, halten Sie die Anzahl der Verbindungen für den NFS-Datastore auf allen vSphere-Hosts, die Teil des vSphere-Clusters sind, unverändert.

With nConnect feature with NetApp and VMware



Voraussetzung

Um die nconnect-Funktion zu nutzen, sollten die folgenden Abhängigkeiten erfüllt sein.

ONTAP-Version	VSphere Version	Kommentare
9.8 oder höher	8 Update 1	Tech Preview mit Option zur Erhöhung der Anzahl der Verbindungen.
9.8 oder höher	8 Update 2	Allgemein verfügbar mit der Option, die Anzahl der Verbindungen zu erhöhen und zu verringern.
9.8 oder höher	8 Update 3	NFS 4.1 und Multi-Path-Unterstützung.

Aktualisieren Sie die Nummer der Verbindung zum NFS-Datenspeicher

Wenn ein NFS-Datenspeicher mit ONTAP Tools oder mit vCenter erstellt wird, wird eine einzelne TCP-Verbindung verwendet. Um die Anzahl der Verbindungen zu erhöhen, kann vSphere CLI verwendet werden. Der Referenzbefehl ist unten dargestellt.

```

# Increase the number of connections while creating the NFS v3 datastore.
esxcli storage nfs add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To specify the number of connections while mounting the NFS 4.1
datastore.
esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v <datastore_name> -s
<remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the number of connections for existing NFSv3
datastore.
esxcli storage nfs param set -v <datastore_name> -c
<number_of_connections>
# For NFSv4.1 datastore
esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# To set VMkernel adapter for an existing NFS 4.1 datastore
esxcli storage nfs41 param set -I <NFS_Server_FQDN_or_IP>:vmk2 -v
<datastore_name> -c <number_of_connections>

```

Oder verwenden Sie PowerCLI ähnlich wie unten gezeigt

```

$datastoreSys = Get-View (Get-VMHost host01.vsphere.local).ExtensionData
.ConfigManager.DatastoreSystem
$nfSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfSpec.RemoteHost = "nfs_server.ontap.local"
$nfSpec.RemotePath = "/DS01"
$nfSpec.LocalPath = "DS01"
$nfSpec.AccessMode = "readWrite"
$nfSpec.Type = "NFS"
$nfSpec.Connections = 4
$datastoreSys.CreateNasDatastore($nfSpec)

```

Hier ist das Beispiel für die Erhöhung der Anzahl der Verbindung mit govc Tool.

```

$env.GOV_C_URL = 'vcenter.vsphere.local'
$env.GOV_C_USERNAME = 'administrator@vsphere.local'
$env.GOV_C_PASSWORD = 'XXXXXXXXXX'
$env.GOV_C_Datastore = 'DS01'
# $env.GOV_C_INSECURE = 1
$env.GOV_C_HOST = 'host01.vsphere.local'
# Increase number of connections while creating the datastore.
govc host.esxcli storage nfs add -H nfs_server.ontap.local -v DS01 -s
/DS01 -c 2
# For NFS 4.1, replace nfs with nfs41
govc host.esxcli storage nfs41 add -H <NFS_Server_FQDN_or_IP> -v
<datastore_name> -s <remote_share> -c <number_of_connections>
# To utilize specific VMkernel adapters while mounting, use the -I switch
govc host.esxcli storage nfs41 add -I <NFS_Server_FQDN_or_IP>:vmk1 -I
<NFS_Server_FQDN_or_IP>:vmk2 -v <datastore_name> -s <remote_share> -c
<number_of_connections>
# To increase or decrease the connections for existing datastore.
govc host.esxcli storage nfs param set -v DS01 -c 4
# For NFSv4.1 datastore
govc host.esxcli storage nfs41 param set -v <datastore_name> -c
<number_of_connections>
# View the connection info
govc host.esxcli storage nfs list

```

Siehe ["VMware KB-Artikel 91497"](#) Finden Sie weitere Informationen.

Designüberlegungen

Die maximale Anzahl von auf ONTAP unterstützten Verbindungen hängt vom Storage-Plattformmodell ab. Suchen Sie auf exec_ctx ["NFS Best Practice und Implementierungslaufplan"](#) Finden Sie weitere Informationen.

Wenn die Anzahl der Verbindungen pro NFSv3-Datastore erhöht wird, nimmt die Anzahl der NFS-Datastores, die auf diesem vSphere Host gemountet werden können, ab. Insgesamt werden pro vSphere-Host 256 Verbindungen unterstützt. Prüfen ["VMware KB-Artikel 91481"](#) Für Datastore-Begrenzungen pro vSphere-Host.



VVol Datastore unterstützt keine nConnect-Funktion. Protokollendpunkte werden jedoch auf die Verbindungsgrenze angerechnet. Bei der Erstellung von vVol Datastores wird für jeden Daten-LIF der SVM ein Protokollendpunkt erstellt.

Konfigurieren Sie NFS-Datastores für vSphere 8 mit den ONTAP-Tools 10

Die ONTAP Tools für VMware vSphere 10 verfügen über eine Next-Generation-Architektur, die native Hochverfügbarkeit und Skalierbarkeit für VASA Provider (und unterstützt iSCSI und NFS VVols) ermöglicht. Dies vereinfacht das Management mehrerer VMware vCenter Server und ONTAP Cluster.

In diesem Szenario werden wir die Implementierung und Verwendung von ONTAP Tools für VMware vSphere 10 und die Konfiguration eines NFS-Datenspeichers für vSphere 8 demonstrieren.

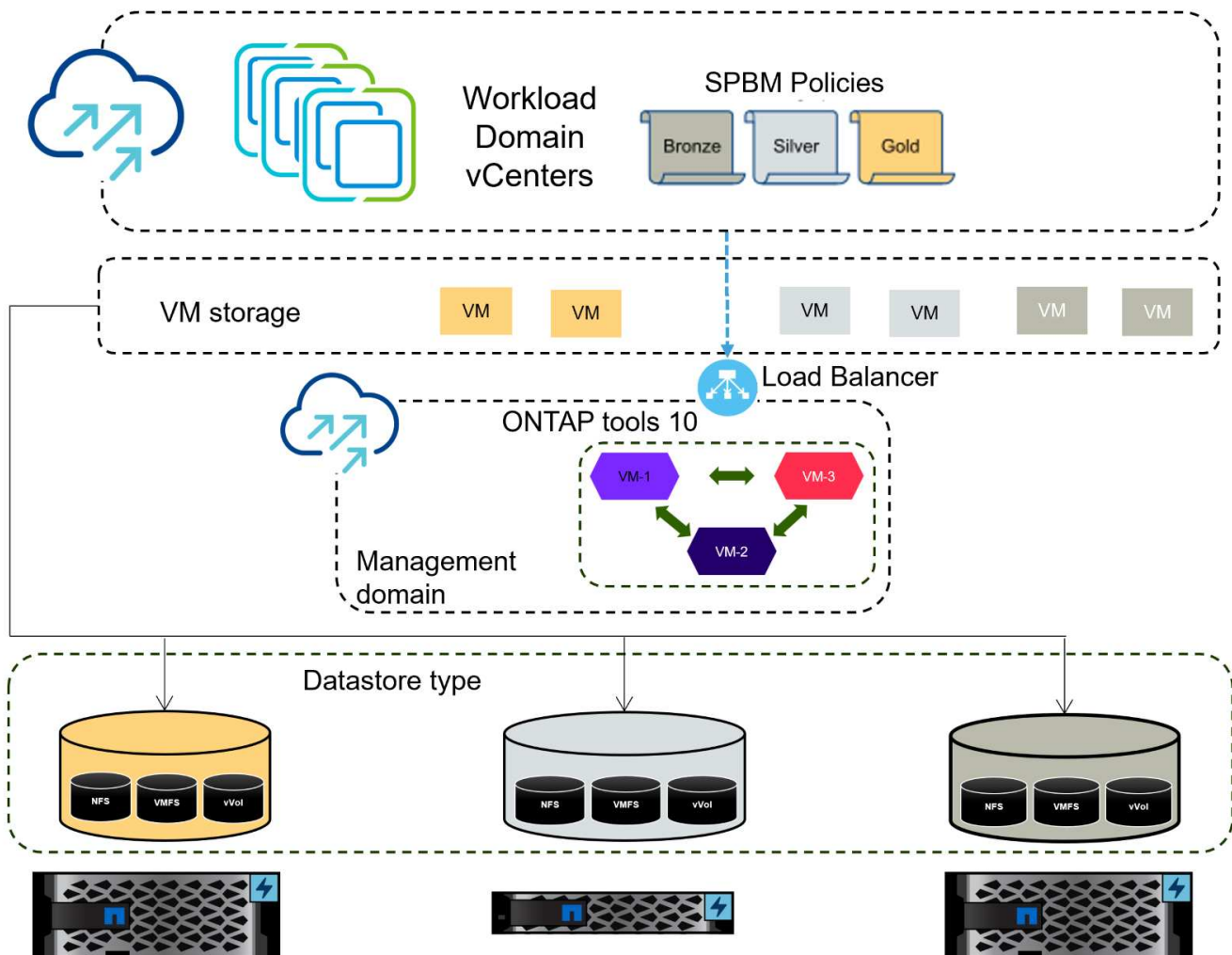
Lösungsüberblick

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für NFS-Traffic erstellen.
- Erstellen Sie eine verteilte Portgruppe für das NFS-Netzwerk auf dem vSphere 8-Cluster.
- Erstellen Sie auf den ESXi Hosts im vSphere 8-Cluster einen VMkernel-Adapter für NFS.
- Implementieren Sie die ONTAP Tools 10 und registrieren Sie sich beim vSphere 8 Cluster.
- Erstellen Sie einen neuen NFS-Datstore auf dem vSphere 8-Cluster.

Der Netapp Architektur Sind

Im folgenden Diagramm werden die Architekturkomponenten eines ONTAP Tools für die Implementierung von VMware vSphere 10 dargestellt.



Voraussetzungen

Diese Lösung erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die vSphere 8-Cluster-Implementierung ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Die ONTAP-Tools für VMware vSphere 10 OVA-Vorlage wurde von der NetApp Support-Website heruntergeladen.

NetApp empfiehlt ein redundantes Netzwerkdesign für NFS und liefert Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Je nach den Architektur Anforderungen ist es üblich, NFS mit einem einzigen oder mehreren Subnetzen bereitzustellen.

Siehe "[Best Practices für die Ausführung von NFS mit VMware vSphere](#)" Für detaillierte Informationen speziell zu VMware vSphere.

Eine Anleitung zum Netzwerk mit ONTAP mit VMware vSphere finden Sie im "[Netzwerkconfiguration – NFS](#)" Der Dokumentation zu NetApp Enterprise-Applikationen.

Umfassende ONTAP-Tools 10 Ressourcen finden Sie "[ONTAP Tools für VMware vSphere – Dokumentationsressourcen](#)".

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um die ONTAP Tools 10 zu implementieren und sie zum Erstellen eines NFS-Datenspeichers in der VCF-Managementdomäne zu verwenden:

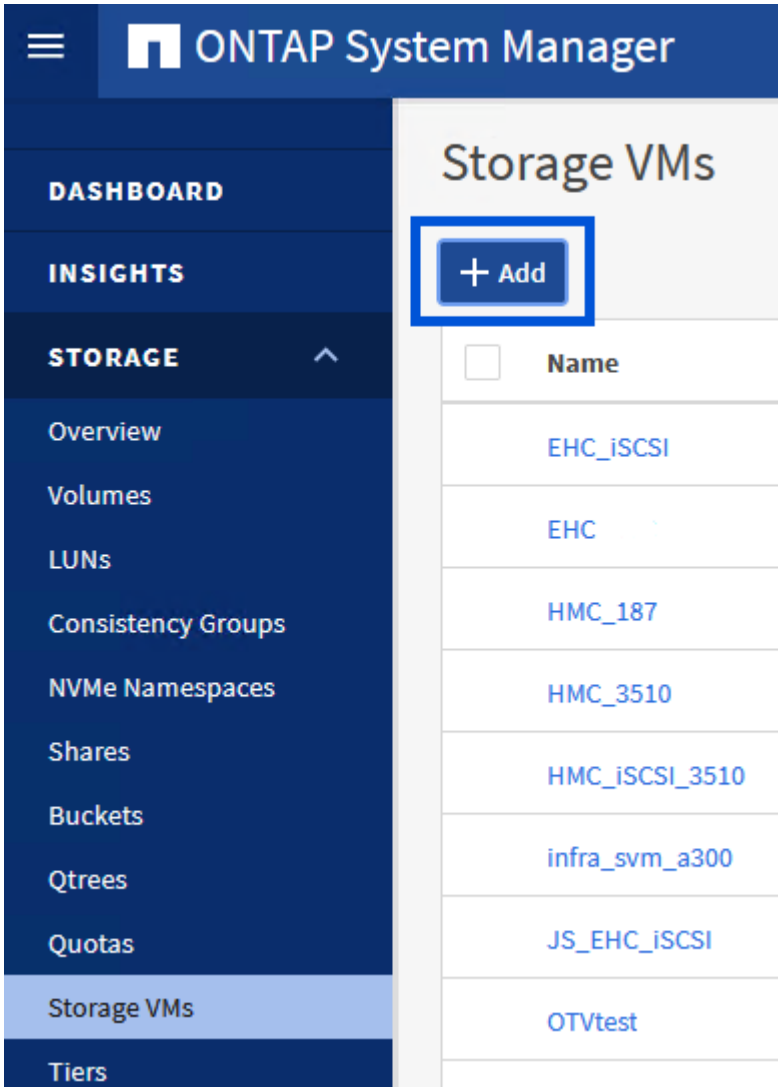
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

Storage-VM und LIFs erstellen

Führen Sie die folgenden Schritte aus, um eine SVM sowie mehrere LIFs für NFS-Datenverkehr zu erstellen.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf **+ Hinzufügen**, um zu starten.



2. Im **Add Storage VM** Wizard geben Sie einen **Namen** für die SVM an, wählen Sie den **IP Space** aus und klicken dann unter **Access Protocol** auf die Registerkarte **SMB/CIFS, NFS, S3** und aktivieren Sie das Kontrollkästchen **enable NFS**.

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default


Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



Es ist nicht notwendig, hier die Schaltfläche **NFS-Client-Zugriff zulassen** zu aktivieren, da ONTAP-Tools für VMware vSphere verwendet werden, um den Datastore-Bereitstellungsprozess zu automatisieren. Dazu gehört auch die Bereitstellung des Client-Zugriffs für die ESXi-Hosts.

3. Geben Sie im Abschnitt **Network Interface** die **IP-Adresse**, **Subnetzmaske** und **Broadcast Domain und Port** für die erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert sein, um allgemeine Einstellungen für alle verbleibenden LIFs zu verwenden oder separate Einstellungen zu verwenden.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

4. Wählen Sie aus, ob das Storage VM Administration-Konto aktiviert werden soll (für mandantenfähige Umgebungen), und klicken Sie auf **Speichern**, um die SVM zu erstellen.

Storage VM Administration

Manage administrator account

Save

Cancel

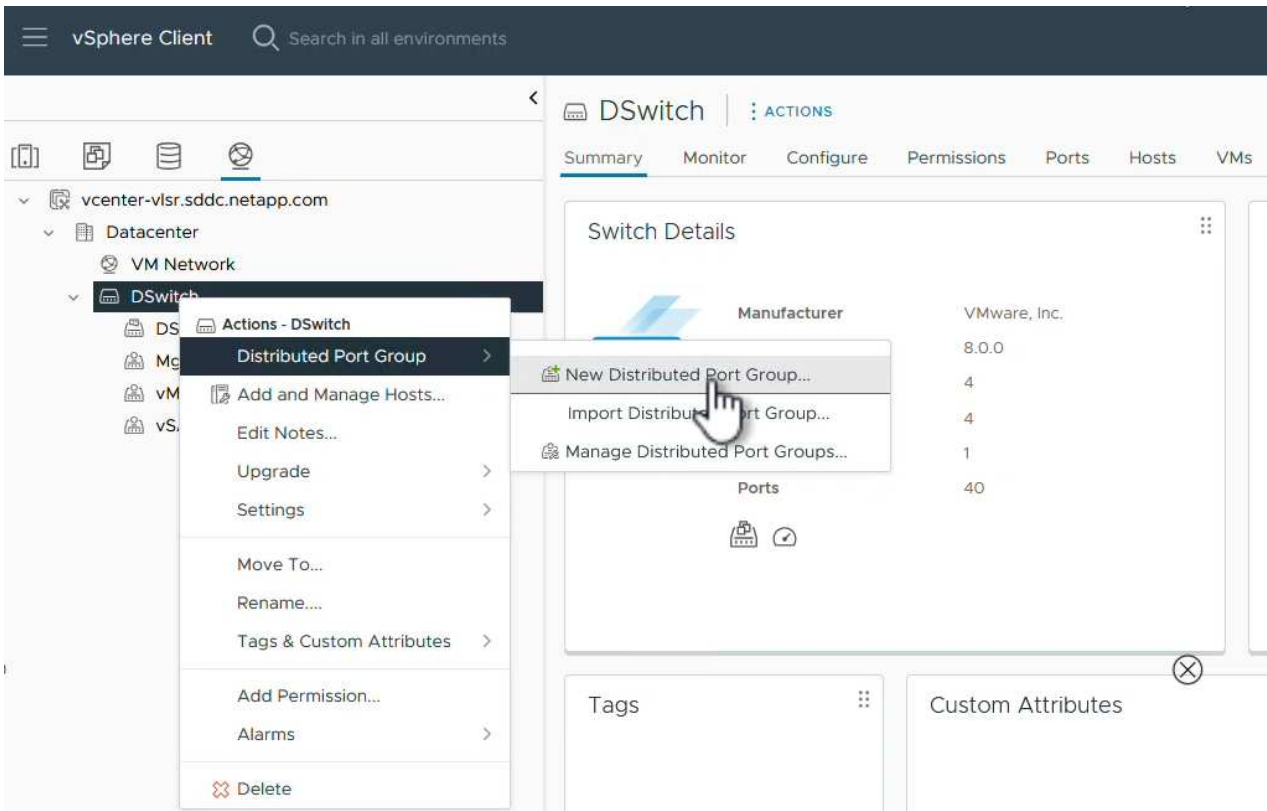
Richten Sie das Netzwerk für NFS auf ESXi-Hosts ein

Die folgenden Schritte werden für den VI Workload Domain Cluster mithilfe des vSphere Clients durchgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client in der Management- und Workload-Domäne einheitlich ist.

Erstellen Sie eine verteilte Portgruppe für NFS-Datenverkehr

Gehen Sie wie folgt vor, um eine neue verteilte Portgruppe für das Netzwerk zu erstellen, die NFS-Datenverkehr übertragen soll:

1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workload-Domäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen von **New Distributed Port Group...** aus.



2. Geben Sie im Assistenten **New Distributed Port Group** einen Namen für die neue Portgruppe ein und klicken Sie auf **Next**, um fortzufahren.
3. Füllen Sie auf der Seite **Configure settings** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige VLAN-ID angeben. Klicken Sie auf **Weiter**, um fortzufahren.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic ?

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

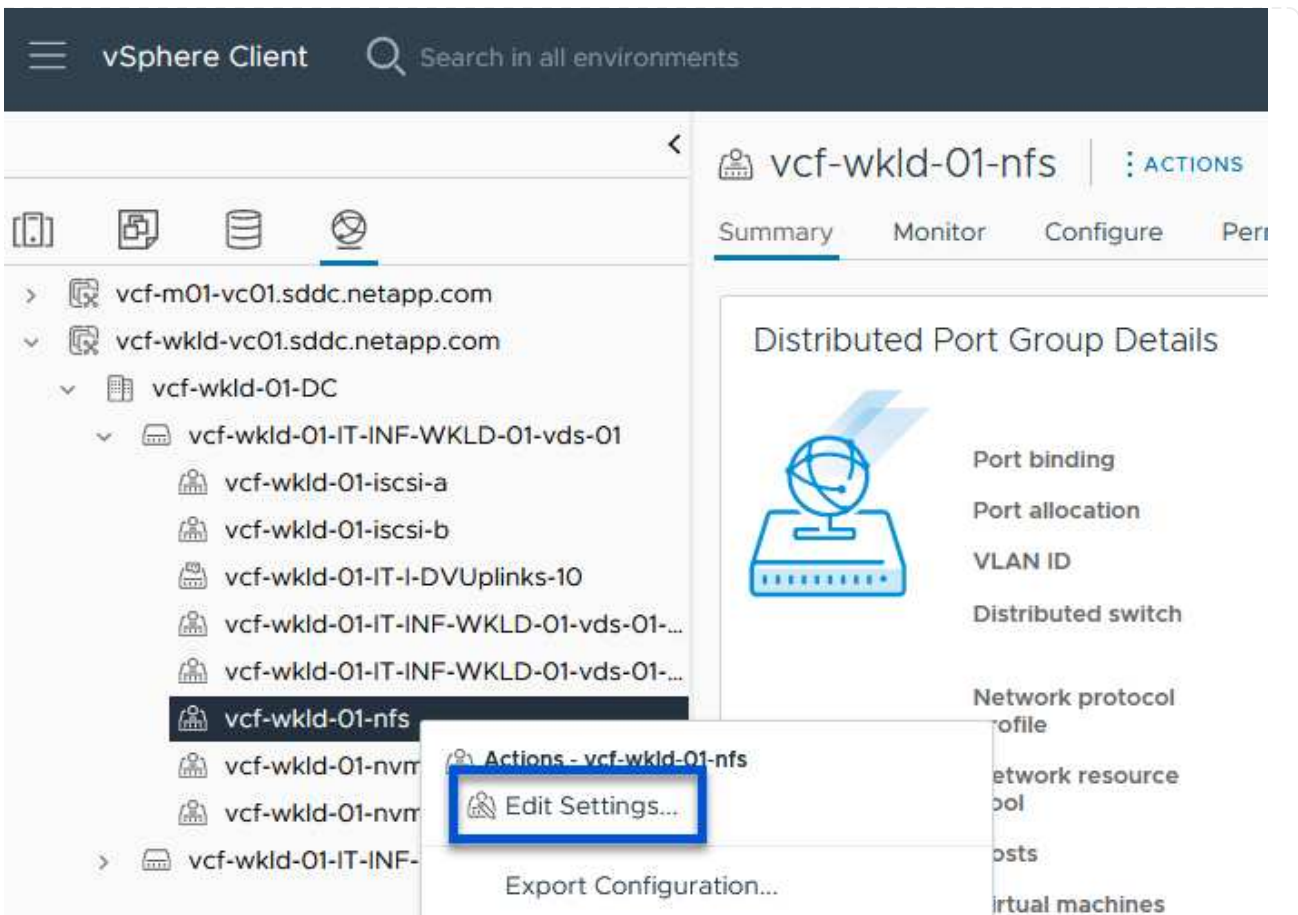
Customize default policies configuration

CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Nachdem die Portgruppe erstellt wurde, navigieren Sie zur Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.



6. Navigieren Sie auf der Seite **Distributed Port Group - Einstellungen bearbeiten** im linken Menü zu **Teaming und Failover**. Aktivieren Sie Teaming für die Uplinks, die für NFS-Verkehr verwendet werden sollen, indem Sie sicherstellen, dass sie sich im Bereich **Active Uplinks** befinden. Verschieben Sie alle nicht verwendeten Uplinks nach unten zu **unused Uplinks**.

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

Uplink 1

Uplink 2

Standby uplinks

Unused uplinks

CANCEL

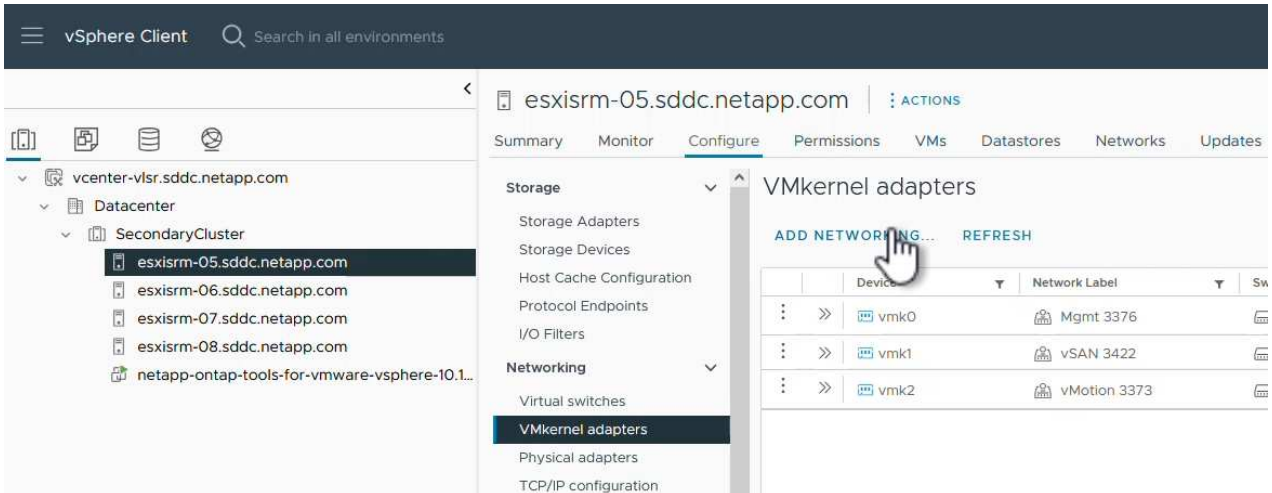
OK

7. Wiederholen Sie diesen Vorgang für jeden ESXi-Host im Cluster.

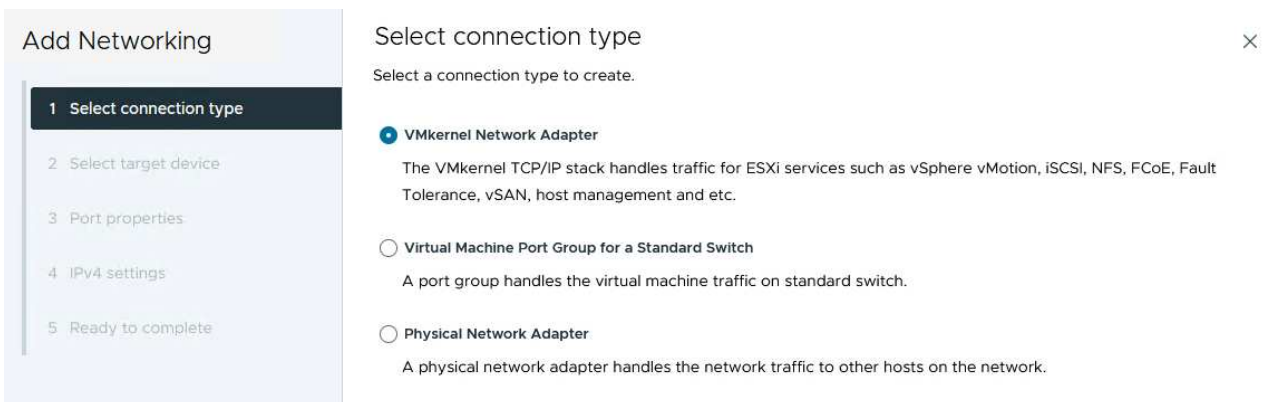
Erstellen Sie auf jedem ESXi-Host einen VMkernel-Adapter

Wiederholen Sie diesen Vorgang auf jedem ESXi-Host in der Workload-Domäne.

1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts in der Workload-Domäneninventarisierung. Wählen Sie auf der Registerkarte **Configure VMkernel Adapter** und klicken Sie auf **Add Networking...**, um zu starten.



2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für NFS aus.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	Mgmt 3376	--	DSwitch
<input checked="" type="radio"/>	NFS 3374	--	DSwitch
<input type="radio"/>	vMotion 3373	--	DSwitch
<input type="radio"/>	vSAN 3422	--	DSwitch

Manage Columns 4 items

CANCEL

BACK

NEXT

4. Behalten Sie auf der Seite **Port Properties** die Standardeinstellungen (keine aktivierten Dienste) bei und klicken Sie auf **Weiter**, um fortzufahren.
5. Geben Sie auf der Seite **IPv4 settings** die **IP-Adresse**, **Subnetzmaske** ein, und geben Sie eine neue Gateway-IP-Adresse ein (nur bei Bedarf). Klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings**
- 5 Ready to complete

IPv4 settings



Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

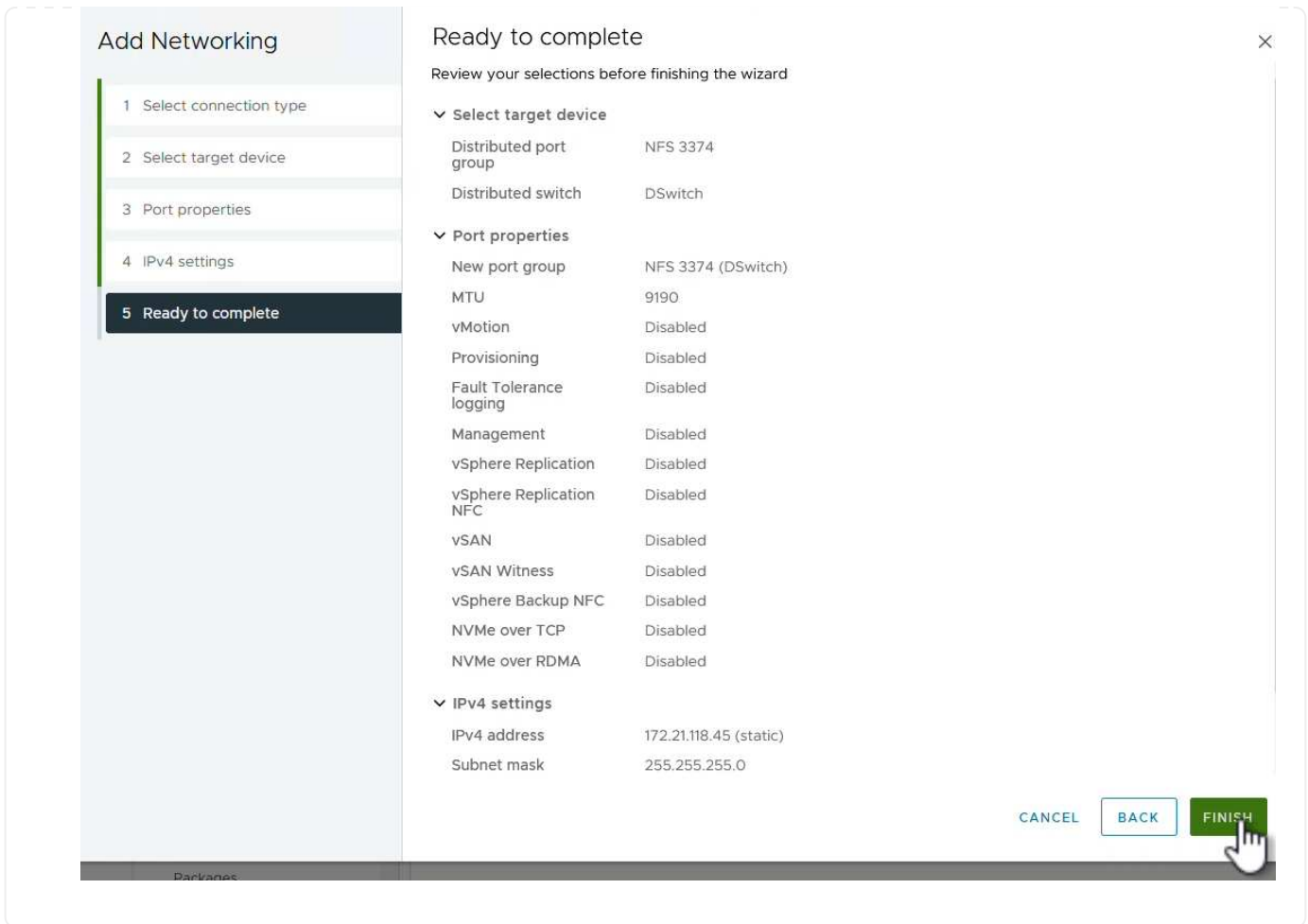
DNS server addresses

CANCEL

BACK

NEXT

6. Überprüfen Sie Ihre Auswahl auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um den VMkernel-Adapter zu erstellen.



Bereitstellung und Verwendung der ONTAP-Tools 10 zur Konfiguration des Speichers

Die folgenden Schritte werden auf dem vSphere 8-Cluster mit dem vSphere-Client durchgeführt. Dazu gehören die Implementierung von OTV, die Konfiguration des ONTAP Tools Manager und die Erstellung eines VVols NFS-Datastore.

Die vollständige Dokumentation zum Bereitstellen und Verwenden von ONTAP-Tools für VMware vSphere 10 finden Sie unter "[Implementieren Sie ONTAP-Tools für VMware vSphere](#)".

Implementieren Sie ONTAP-Tools für VMware vSphere 10

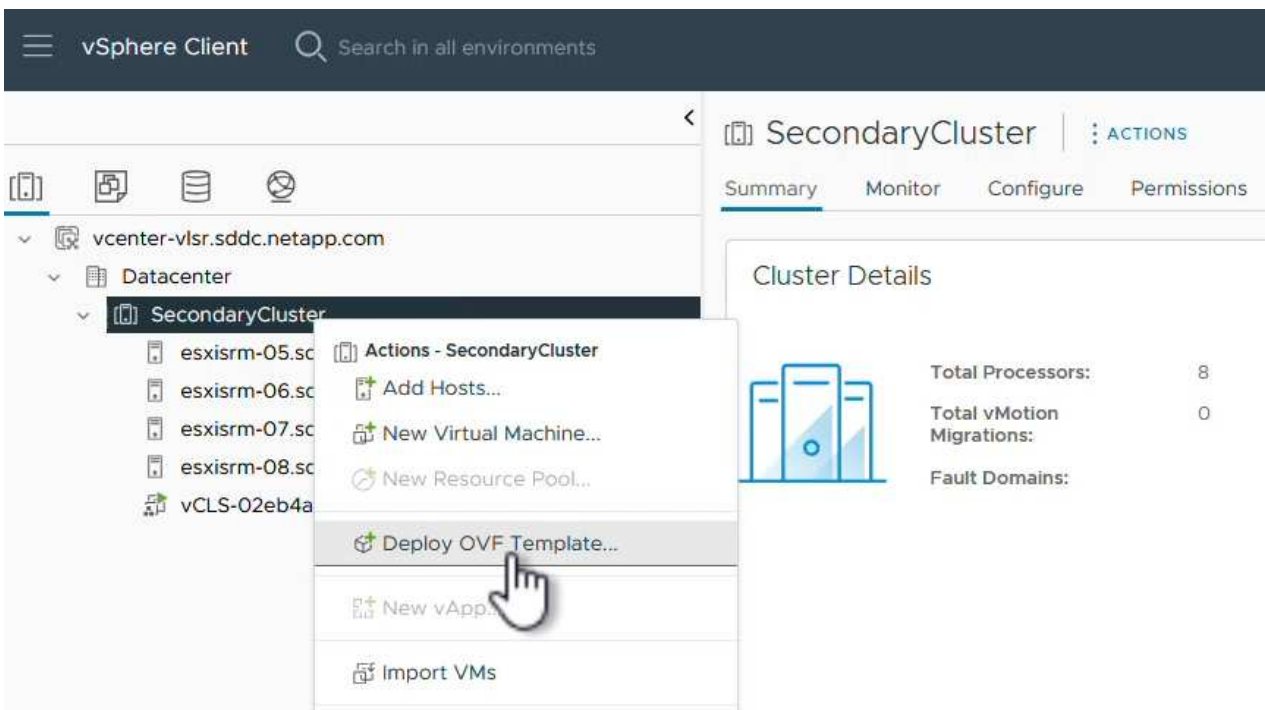
Die ONTAP Tools für VMware vSphere 10 werden als VM-Appliance implementiert und verfügen über eine integrierte vCenter UI zum Managen von ONTAP Storage. ONTAP Tools 10 verfügt über ein neues globales Management-Portal für das Management von Verbindungen zu mehreren vCenter Servern und ONTAP Storage Back-Ends.



In einem Szenario ohne Hochverfügbarkeit sind drei verfügbare IP-Adressen erforderlich. Dem Load Balancer wird eine IP-Adresse zugewiesen, eine weitere für die Kubernetes-Kontrollebene und die verbleibende Adresse für den Node. In einer HA-Implementierung sind zusätzlich zu den ersten drei für den zweiten und dritten Node zwei zusätzliche IP-Adressen erforderlich. Vor der Zuweisung sollten die Hostnamen den IP-Adressen in DNS zugeordnet werden. Es ist wichtig, dass sich alle fünf IP-Adressen im gleichen VLAN befinden, das für die Bereitstellung ausgewählt wird.

Füllen Sie die folgenden Schritte aus, um ONTAP Tools für VMware vSphere zu implementieren:

1. Rufen Sie das OVA-Image der ONTAP-Tools auf "[NetApp Support Website](#)", und laden Sie es in einen lokalen Ordner herunter.
2. Melden Sie sich bei der vCenter Appliance für den vSphere 8-Cluster an.
3. Klicken Sie in der vCenter-Appliance-Oberfläche mit der rechten Maustaste auf den Management-Cluster und wählen Sie **Deploy OVF Template...** aus



4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei für ONTAP-Tools aus.

Deploy OVF Template

1 Select an OVF template

- 2 Select a name and folder
- 3 Select a compute resource
- 4 Review details
- 5 Select storage
- 6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie zum Speicherort der Konfigurations- und Festplattendateien einen lokalen Datastore oder vSAN Datastore aus.

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 Configuration
- 7 Select storage**
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

VM Storage Policy

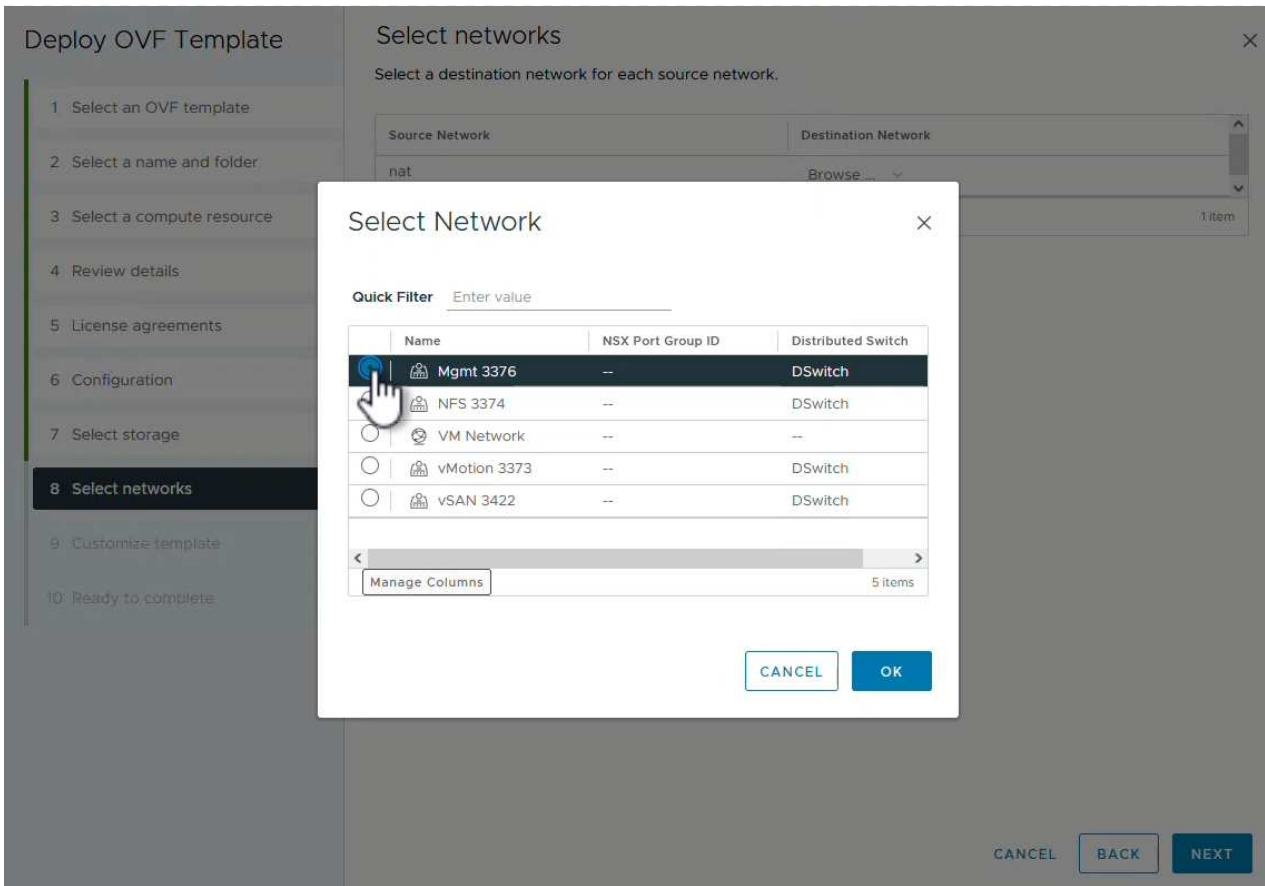
Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
vsanDatastore	--	799.97 GB	26.05 GB	783.98 GB

Items per page 10 1 item

Compatibility

7. Wählen Sie auf der Seite Netzwerk auswählen das Netzwerk aus, das für den Verwaltungsdatenverkehr verwendet wird.



8. Wählen Sie auf der Konfigurationsseite die zu verwendende Bereitstellungskonfiguration aus. In diesem Szenario wird die einfache Bereitstellungsmethode verwendet.



ONTAP Tools 10 umfasst verschiedene Implementierungskonfigurationen, einschließlich Hochverfügbarkeitsimplementierungen mit mehreren Nodes. Dokumentation zu allen Bereitstellungskonfigurationen und -Voraussetzungen finden Sie unter "[Voraussetzungen für die Bereitstellung von ONTAP-Tools für VMware vSphere](#)".

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 Configuration**
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Configuration

Select a deployment configuration

<input checked="" type="radio"/> Easy deployment (S)	Description Deploy local provisioner Non-HA Small single node instance of ONTAP tools	
<input type="radio"/> Easy deployment (M)		
<input type="radio"/> Advanced deployment (S)		
<input type="radio"/> Advanced deployment (M)		
<input type="radio"/> High-Availability deployment (S)		
<input type="radio"/> High-Availability deployment (M)		
<input type="radio"/> High-Availability deployment (L)		
<input type="radio"/> Recovery		
8 Items		

CANCEL

BACK

NEXT

9. Geben Sie auf der Seite Vorlage anpassen alle erforderlichen Informationen ein:

- Anwendungsbenutzername zur Registrierung des VASA-Providers und SRA im vCenter-Server.
- Aktivieren Sie ASUP für automatisierten Support.
- ASUP Proxy-URL, falls erforderlich
- Administratorbenutzername und -Kennwort.
- NTP-Server.
- Wartungsbutzerpasswort für den Zugriff auf Managementfunktionen von der Konsole aus.
- Load Balancer-IP.
- Virtuelle IP für die K8s-Kontrollebene:
- Primäre VM zur Auswahl der aktuellen VM als primäre VM (für HA-Konfigurationen)
- Hostname für die VM
- Geben Sie die erforderlichen Felder für Netzwerkeigenschaften an.

Klicken Sie auf **Weiter**, um fortzufahren.

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 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Customize the deployment properties of this software solution.

! 10 properties have invalid values X

System Configuration		8 settings
Application username(*)	Username to assign to the Application	<input type="text" value="vsphere-services"/>
Application password(*)	Password to assign to the Application	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
Enable ASUP	Select this checkbox to enable ASUP	<input checked="" type="checkbox"/>
ASUP Proxy URL	Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.	<input type="text"/>
Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '.', ':', '-' special characters are supported	<input style="border: 1px solid #f00;" type="text"/>
Administrator password(*)	Password to assign to the Administrator	<input type="password"/>

CANCEL BACK NEXT

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 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template**
- 10 Ready to complete

Customize template

Maintenance user password(*)	Password to assign to maint user account	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
Deployment Configuration		3 settings
Load balancer IP(*)	Load balancer IP (*)	<input type="text" value="172.21.120.57"/>
Virtual IP for K8s control plane(*)	Provide the virtual IP address for K8s control plane	<input type="text" value="172.21.120.58"/>
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools.	<input checked="" type="checkbox"/>
Node Configuration		10 settings
HostName(*)	Specify the hostname for the VM	<input style="border: 1px solid #f00;" type="text"/>
IP Address(*)	Specify the IP address for the appliance	<input style="border: 1px solid #f00;" type="text"/>
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack.	<input type="text"/>

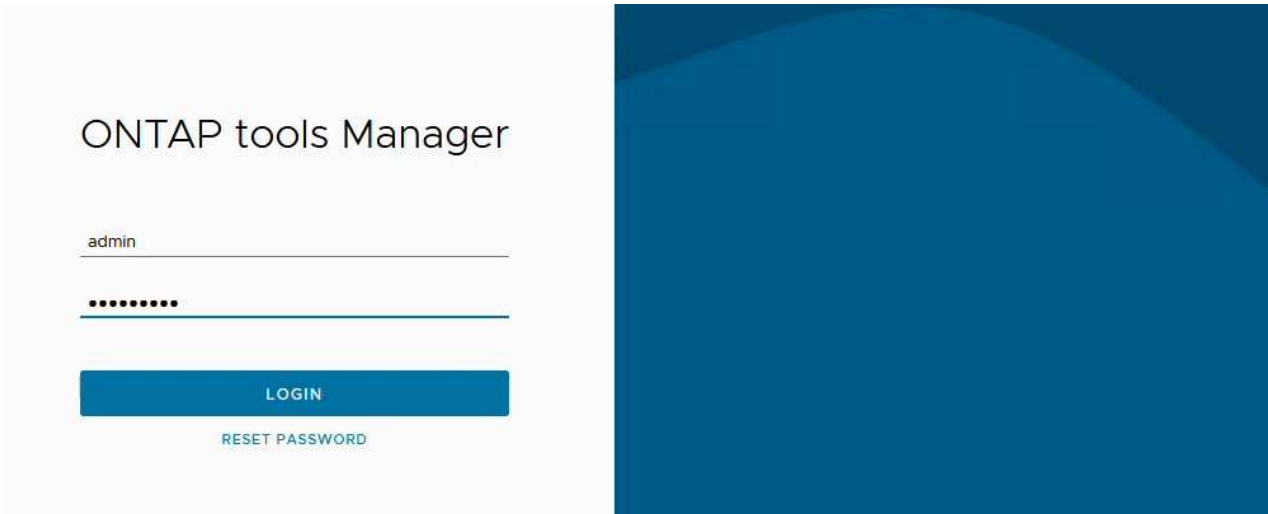
CANCEL BACK NEXT

10. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertigstellen, um mit der Bereitstellung der ONTAP Tools Appliance zu beginnen.

Verbinden Sie das Storage Back-End und vCenter Server mit den ONTAP Tools 10.

Der ONTAP-Tools-Manager wird verwendet, um globale Einstellungen für ONTAP-Tools 10 zu konfigurieren.

1. Sie erhalten Zugriff auf ONTAP Tools Manager, indem <https://<loadBalanceIP>:8443/virtualization/ui/> Sie in einem Webbrowser zu navigieren und sich mit den während der Implementierung angegebenen administrativen Anmeldeinformationen anmelden.



2. Klicken Sie auf der Seite **erste Schritte** auf **Gehe zu Speicher-Backends**.

Getting Started



ONTAP tools Manager allows you to manage ONTAP Storage Backends and associate them with vCenters. You can also download support log bundles.



Storage Backends

Add, modify, and remove storage backends.

[Go to Storage Backends](#)



vCenters

Add, modify, and remove vCenters and associate storage backends with them.

[Go to vCenters](#)



Log Bundles

Generate and download log bundles for support purposes.

[Go to Log Bundles](#)

Don't show again

3. Klicken Sie auf der Seite **Speicher-Backends** auf **ADD**, um die Zugangsdaten eines ONTAP-Speichersystems einzugeben, das mit den ONTAP-Tools 10 registriert werden soll.

ONTAP tools Manager

Storage Backends

The ESXi hosts use Storage Backends for data storage.


Name	Type	IP Address or FQDN
This list is empty!		

4. Geben Sie im Feld **Speicher-Backend hinzufügen** die Anmeldeinformationen für das ONTAP-Speichersystem ein.

Add Storage Backend

Hostname: * 172.16.9.25

Username: * admin

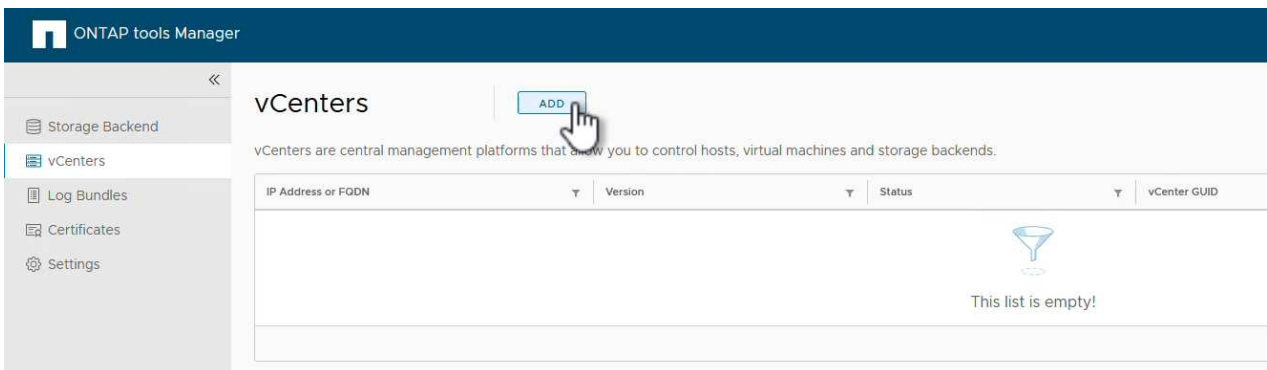
Password: * ●●●●●●●● 

Port: * 443

CANCEL

ADD 

5. Klicken Sie im linken Menü auf **vCenters** und dann auf **ADD**, um die Zugangsdaten eines vCenter-Servers einzugeben, der mit den ONTAP-Tools 10 registriert werden soll.



The screenshot shows the ONTAP tools Manager interface. The left sidebar contains a menu with options: Storage Backend, vCenters (highlighted), Log Bundles, Certificates, and Settings. The main content area is titled 'vCenters' and includes an 'ADD' button with a hand cursor pointing to it. Below the button is a table with columns: IP Address or FQDN, Version, Status, and vCenter GUID. The table is currently empty, with a message 'This list is empty!' and a funnel icon centered below it.

6. Geben Sie im Feld **Add vCenter** die Anmeldeinformationen für das ONTAP-Speichersystem ein.

Add vCenter

Server IP Address or FQDN: *

Username: *

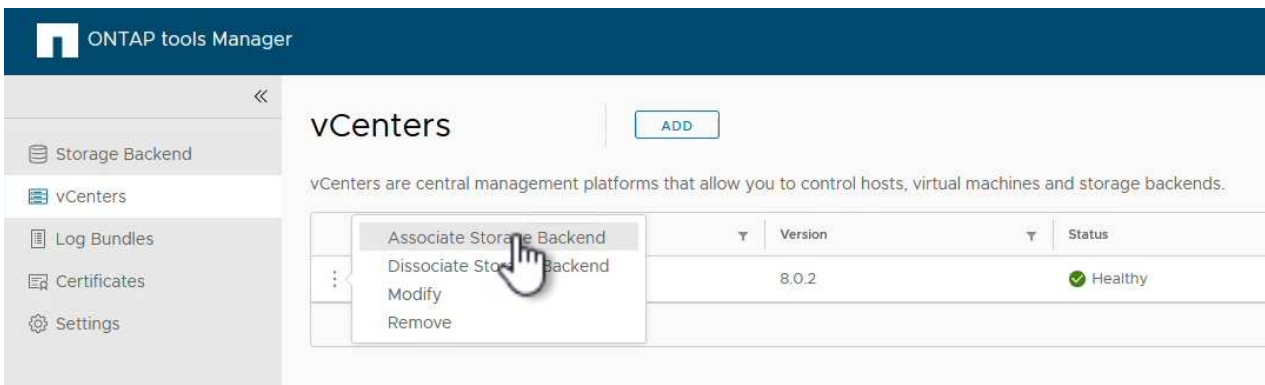
Password: * 

Port: *

CANCEL

ADD 


- Wählen Sie im vertikalen drei-Punkt-Menü für den neu ermittelten vCenter-Server **Speicher-Backend zuordnen** aus.



ONTAP tools Manager

vCenters

vCenters are central management platforms that allow you to control hosts, virtual machines and storage backends.

	Version	Status
 Associate Storage Backend Dissociate Storage Backend Modify Remove	8.0.2	Healthy

- Wählen Sie im Feld **Speicher-Backend zuordnen** das ONTAP-Speichersystem aus, das dem vCenter-Server zugeordnet ist, und klicken Sie auf **Associate**, um die Aktion abzuschließen.

Associate Storage Backend

vcenter-vlsr.sddc.netapp.com



Storage Backend

ntaphci-a300e9u25

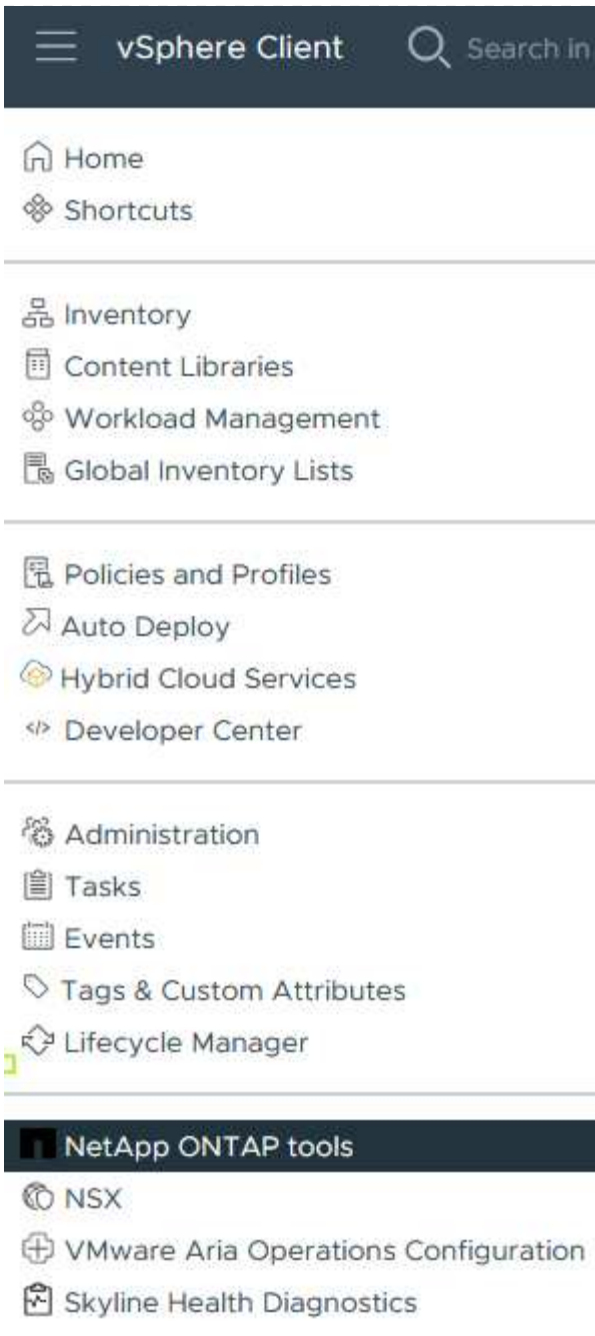


CANCEL

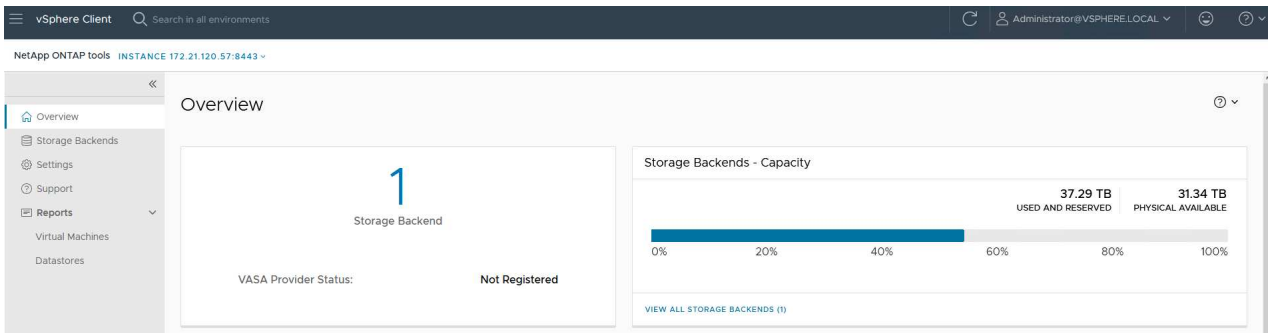
ASSOCIATE



9. Um die Installation zu überprüfen, melden Sie sich beim vSphere-Client an und wählen Sie im linken Menü **NetApp ONTAP Tools** aus.



10. Im Dashboard der ONTAP-Tools sollten Sie sehen, dass ein Speicher-Back-End mit dem vCenter Server verknüpft war.

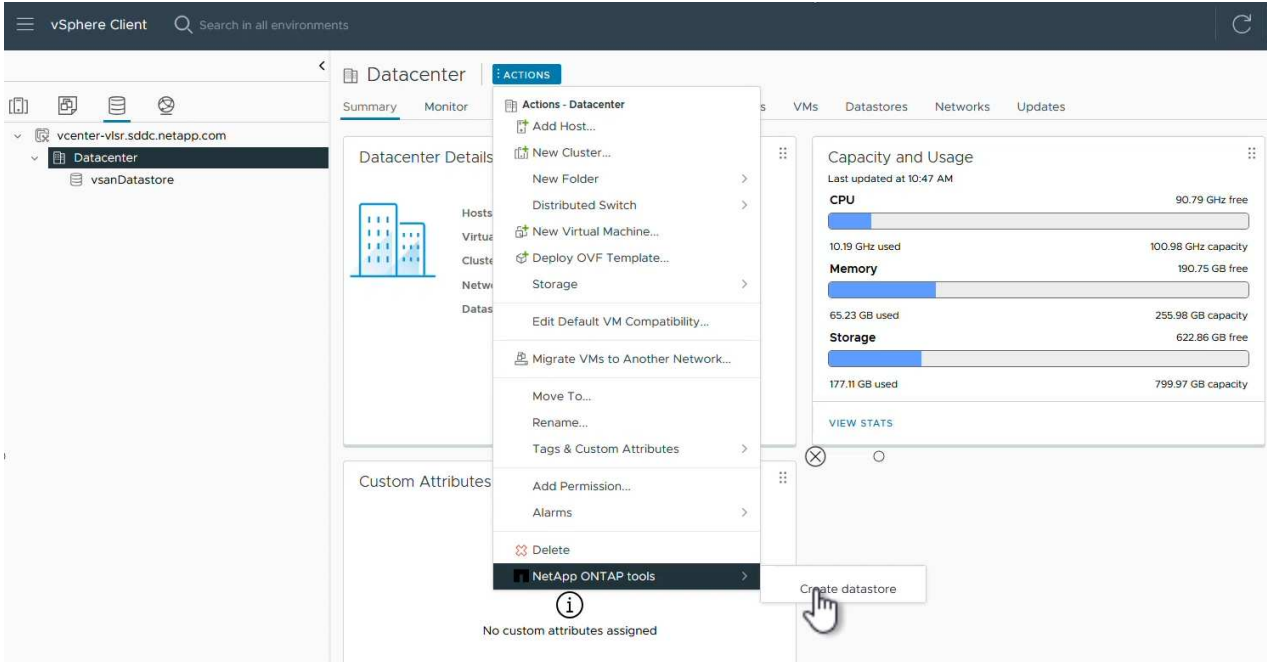




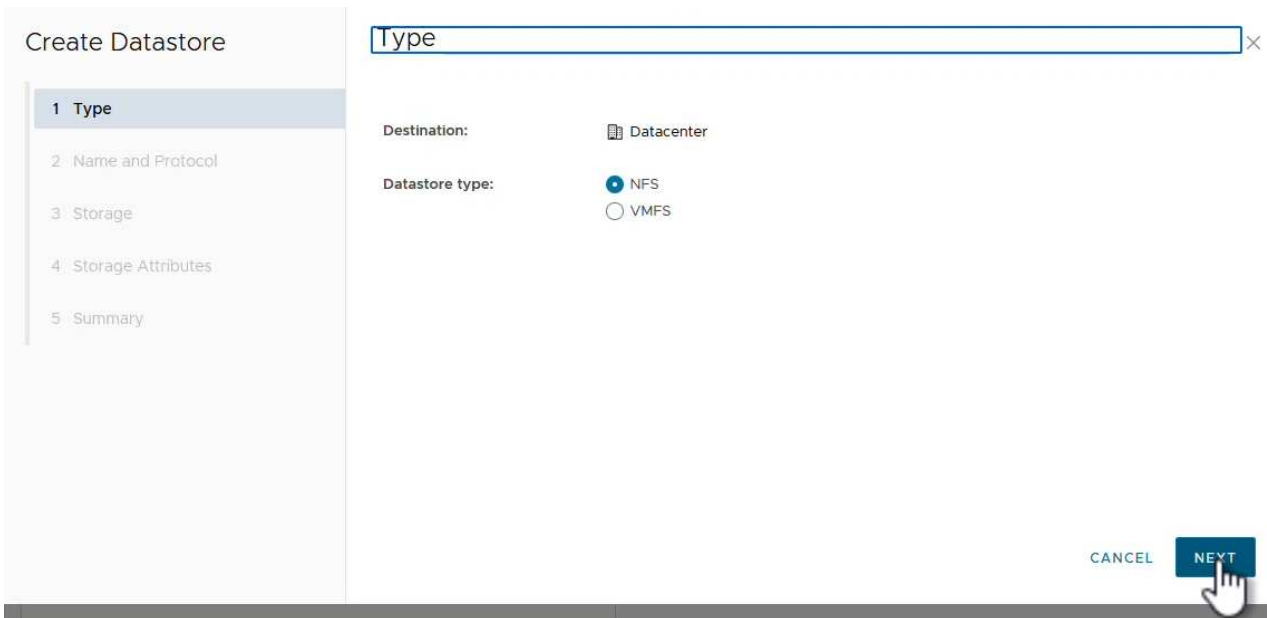
Erstellen Sie einen NFS-Datystore mit ONTAP-Tools 10

Führen Sie die folgenden Schritte aus, um einen ONTAP-Datystore zu implementieren, der auf NFS ausgeführt wird, und mit ONTAP-Tools 10 zu verwenden.

1. Navigieren Sie im vSphere-Client zum Speicherbestand. Wählen Sie im Menü **ACTIONS** die Option **NetApp ONTAP Tools > Datystore erstellen**.



2. Klicken Sie auf der Seite **Typ** des Assistenten Datystore erstellen auf das NFS-Optionsfeld und dann auf **Weiter**, um fortzufahren.



3. Geben Sie auf der Seite **Name und Protokoll** den Namen, die Größe und das Protokoll für den Datastore ein. Klicken Sie auf **Weiter**, um fortzufahren.

The screenshot shows the 'Create Datastore' wizard in the 'Name and Protocol' step. On the left, a sidebar lists five steps: 1 Type, 2 Name and Protocol (highlighted), 3 Storage, 4 Storage Attributes, and 5 Summary. The main area is titled 'Name and Protocol' and contains the following fields:

- Datastore name:** NFS_DS1
- Size:** 2 TB (with a note: 'Minimum supported size is 1 GB.')
- Protocol:** NFS 3
- Advanced Options:** (expanded section)
- Datastore Cluster:** (empty dropdown)

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

4. Wählen Sie auf der Seite **Storage** eine Plattform (filtert das Speichersystem nach Typ) und eine Speicher-VM für das Volume aus. Wählen Sie optional eine benutzerdefinierte Exportrichtlinie aus. Klicken Sie auf **Weiter**, um fortzufahren.

The screenshot shows the 'Create Datastore' wizard in the 'Storage' step. On the left, the sidebar lists five steps: 1 Type, 2 Name and Protocol, 3 Storage (highlighted), 4 Storage Attributes, and 5 Summary. The main area is titled 'Storage' and contains the following fields:

- Platform: *** Performance (A)
- Storage VM: *** VCF_NFS (with ID: ntaphci-a300e9u25 (172.16.9.25))
- Advanced Options:** (expanded section)
- Custom Export Policy:** Search or specify policy name (with a note: 'Choose an existing policy or give a new name to the default policy.')

At the bottom right, there are three buttons: CANCEL, BACK, and NEXT. A mouse cursor is pointing at the NEXT button.

5. Wählen Sie auf der Seite **Speicherattribute** das zu verwendende Speicheraggregat und optional erweiterte Optionen wie Platzreservierung und Servicequalität aus. Klicken Sie auf **Weiter**, um fortzufahren.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 Summary

Storage Attributes

Specify the storage details for provisioning the datastore.

Aggregate: * EHCaggr02 (16.61 TB Free) ▾

Volume: A new volume will be created automatically.

^ Advanced Options

Space Reserve: * Thin ▾

Enable QoS

CANCEL

BACK

NEXT

6. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf Fertig stellen, um mit der Erstellung des NFS-Datastore zu beginnen.

Create Datastore

- 1 Type
- 2 Name and Protocol
- 3 Storage
- 4 Storage Attributes
- 5 Summary

Summary

A new datastore will be created with these settings.

Type

Destination: Datacenter

Datastore type: NFS

Name and Protocol

Datastore name: NFS_DS1

Size: 2 TB

Protocol: NFS 3

Storage

Platform: Performance (A)

Storage VM: VCF_NFS

CANCEL

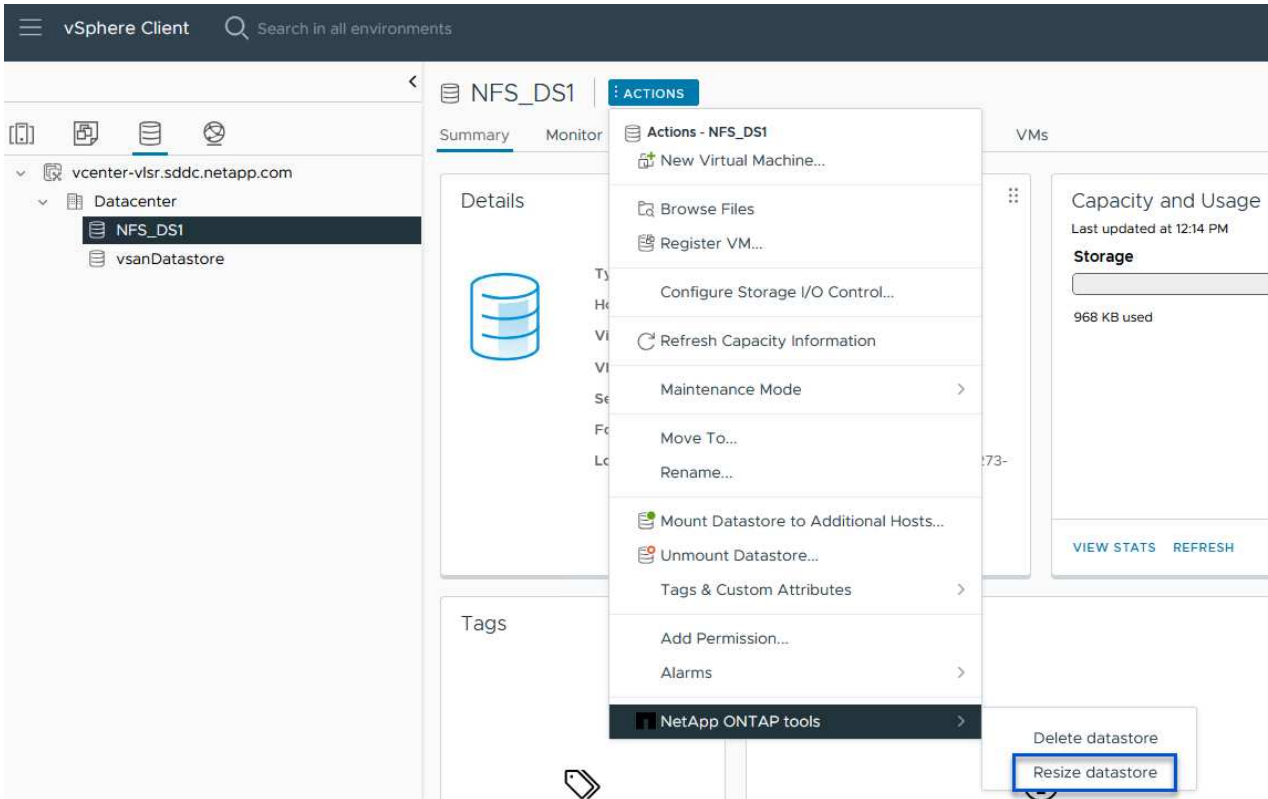
BACK

FINISH

Größe eines NFS-Datenspeichers mit ONTAP-Tools ändern 10

Führen Sie die folgenden Schritte durch, um die Größe eines vorhandenen NFS-Datenspeichers mithilfe von ONTAP-Tools zu ändern: 10.

1. Navigieren Sie im vSphere-Client zum Speicherbestand. Wählen Sie im Menü **ACTIONS** die Option **NetApp ONTAP Tools > Datastore skalieren**.



2. Füllen Sie im Assistenten **Resize Datastore** die neue Größe des Datastore in GB aus und klicken Sie auf **Resize**, um fortzufahren.

Resize Datastore | NFS_DS1

Volume Details

Volume Name:	NFS_DS1
Total Size:	2.1 TB
Used Size:	968 KB
Snapshot Reserve (%):	5
Thin Provisioned:	Yes


Size

Current Datastore Size:	2 TB
New Datastore Size (GB): *	3000

CANCEL

RESIZE

3. Überwachen Sie den Fortschritt des Jobs in der Größenänderung im Bereich **Letzte Aufgaben**.

Task Name	Target	Status	Details
Expand Datastore	vcenter-vlsr.sddc.net app.com	100% 	Expand datastore initiated with job id 2807

Weitere Informationen

Eine vollständige Liste der ONTAP Tools für VMware vSphere 10 finden Sie unter "[ONTAP Tools für VMware vSphere – Dokumentationsressourcen](#)".

Weitere Informationen zur Konfiguration von ONTAP-Speichersystemen finden Sie im "[ONTAP 10-Dokumentation](#)" Center.

Verwenden Sie VMware Site Recovery Manager für die Disaster Recovery von NFS-Datenspeichern

Die Nutzung von ONTAP Tools für VMware vSphere 10 und den Site Replication Adapter (SRA) in Verbindung mit VMware Site Recovery Manager (SRM) ist ein wichtiger Bestandteil von Disaster-Recovery-Maßnahmen. ONTAP Tools 10 bieten robuste Storage-Funktionen, einschließlich nativer Hochverfügbarkeit und Skalierbarkeit für den VASA Provider und unterstützen iSCSI und NFS VVols. Dadurch wird die Datenverfügbarkeit sichergestellt und das Management mehrerer VMware vCenter Server und ONTAP Cluster vereinfacht. Durch den Einsatz von SRA mit VMware Site

Recovery Manager können Unternehmen eine nahtlose Replizierung und ein Failover von Virtual Machines und Daten zwischen Standorten erzielen und so effiziente Disaster-Recovery-Prozesse ermöglichen. Die Kombination aus ONTAP-Tools und SRA ermöglicht Unternehmen, kritische Workloads zu schützen, Ausfallzeiten zu minimieren und die Business Continuity auch bei unvorhergesehenen Ereignissen oder Ausfällen aufrechtzuerhalten.

Die ONTAP Tools 10 vereinfachen das Storage-Management und die Effizienzfunktionen, verbessern die Verfügbarkeit und senken 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.

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.

In diesem Szenario wird die Implementierung und der Einsatz von VMware Site Recovery Manager zum Schutz von Datenspeichern demonstriert und sowohl ein Test als auch ein abschließender Failover auf einen sekundären Standort durchgeführt. Außerdem werden der Schutz und das Failback besprochen.

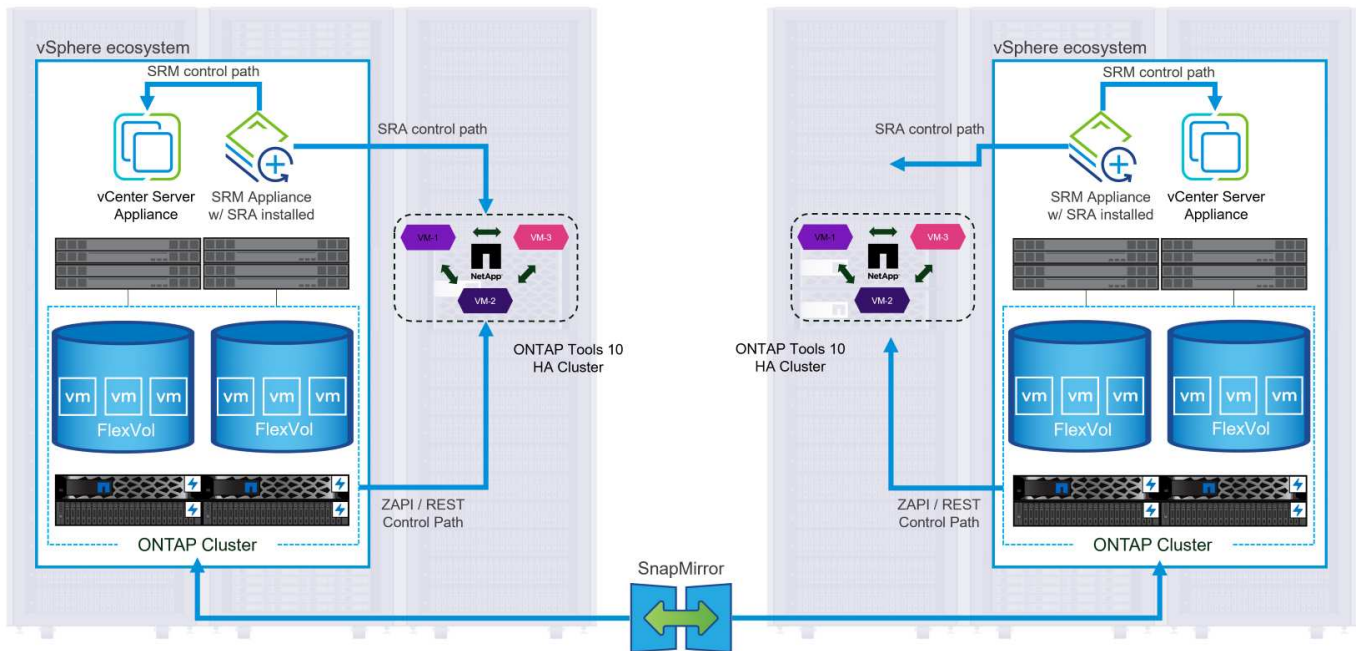
Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Konfigurieren Sie SRM mit vCenter Servern am primären und sekundären Standort.
- Installieren Sie den SRA Adapter für ONTAP Tools für VMware vSphere 10 und registrieren Sie sich bei vCenters.
- Erstellung von SnapMirror Beziehungen zwischen Quell- und Ziel-ONTAP-Storage-Systemen
- Konfigurieren Sie Site Recovery für SRM.
- Führen Sie Tests und ein abschließendes Failover durch.
- Besprechen Sie Datensicherheit und Failback.

Der Netapp Architektur Sind

Das folgende Diagramm zeigt eine typische VMware Site Recovery-Architektur mit ONTAP Tools für VMware vSphere 10, die in einer Hochverfügbarkeitskonfiguration mit 3 Nodes konfiguriert sind.



Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- vSphere 8 Cluster werden sowohl an den primären als auch an den sekundären Standorten installiert und bieten ein geeignetes Netzwerk für die Kommunikation zwischen Umgebungen.
- ONTAP Storage-Systeme an primären und sekundären Standorten mit dedizierten physischen Daten-Ports an ethernet-Switches für NFS Storage-Datenverkehr.
- ONTAP-Tools für VMware vSphere 10 sind installiert und beide vCenter-Server registriert.
- VMware Site Recovery Manager-Appliances wurden für den primären und sekundären Standort installiert.
 - Bestandszuordnungen (Netzwerk, Ordner, Ressource, Speicherrichtlinie) wurden für SRM konfiguriert.

NetApp empfiehlt ein redundantes Netzwerkdesign für NFS und liefert Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Je nach den Architektur Anforderungen ist es üblich, NFS mit einem einzigen oder mehreren Subnetzen bereitzustellen.

Siehe "[Best Practices für die Ausführung von NFS mit VMware vSphere](#)" Für detaillierte Informationen speziell zu VMware vSphere.

Eine Anleitung zum Netzwerk mit ONTAP mit VMware vSphere finden Sie im "[Netzwerk Konfiguration – NFS](#)" Der Dokumentation zu NetApp Enterprise-Applikationen.

NetApp-Dokumentation zur Verwendung von ONTAP Storage mit VMware SRM finden Sie unter "[VMware Site Recovery Manager mit ONTAP](#)"

Implementierungsschritte

In den folgenden Abschnitten werden die Implementierungsschritte zur Implementierung und zum Testen einer VMware Site Recovery Manager Konfiguration mit einem ONTAP Storage-System beschrieben.

Erstellung einer SnapMirror Beziehung zwischen ONTAP Storage-Systemen

Zwischen den ONTAP Quell- und Ziel-Storage-Systemen muss eine SnapMirror Beziehung hergestellt werden, damit die Datastore Volumes gesichert werden können.

In der Dokumentation von ONTAP "[HIER](#)" finden Sie alle Informationen zum Erstellen von SnapMirror Beziehungen für ONTAP Volumes.

Schritt-für-Schritt-Anweisungen sind im folgenden Dokument, befindet "[HIER](#)". Im Folgenden wird beschrieben, wie Cluster Peer- und SVM-Peer-Beziehungen erstellt und anschließend SnapMirror Beziehungen für jedes Volume erstellt werden. Diese Schritte können in ONTAP System Manager oder über die ONTAP CLI ausgeführt werden.

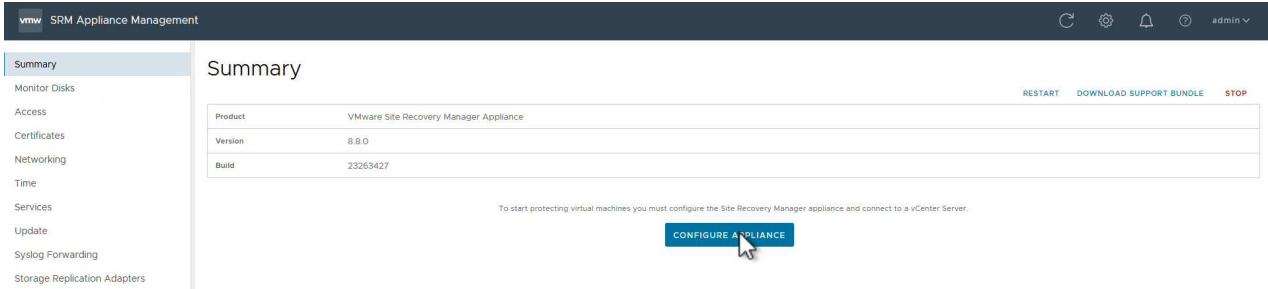
Konfigurieren Sie die SRM-Appliance

Führen Sie die folgenden Schritte aus, um die SRM-Appliance und den SRA-Adapter zu konfigurieren.

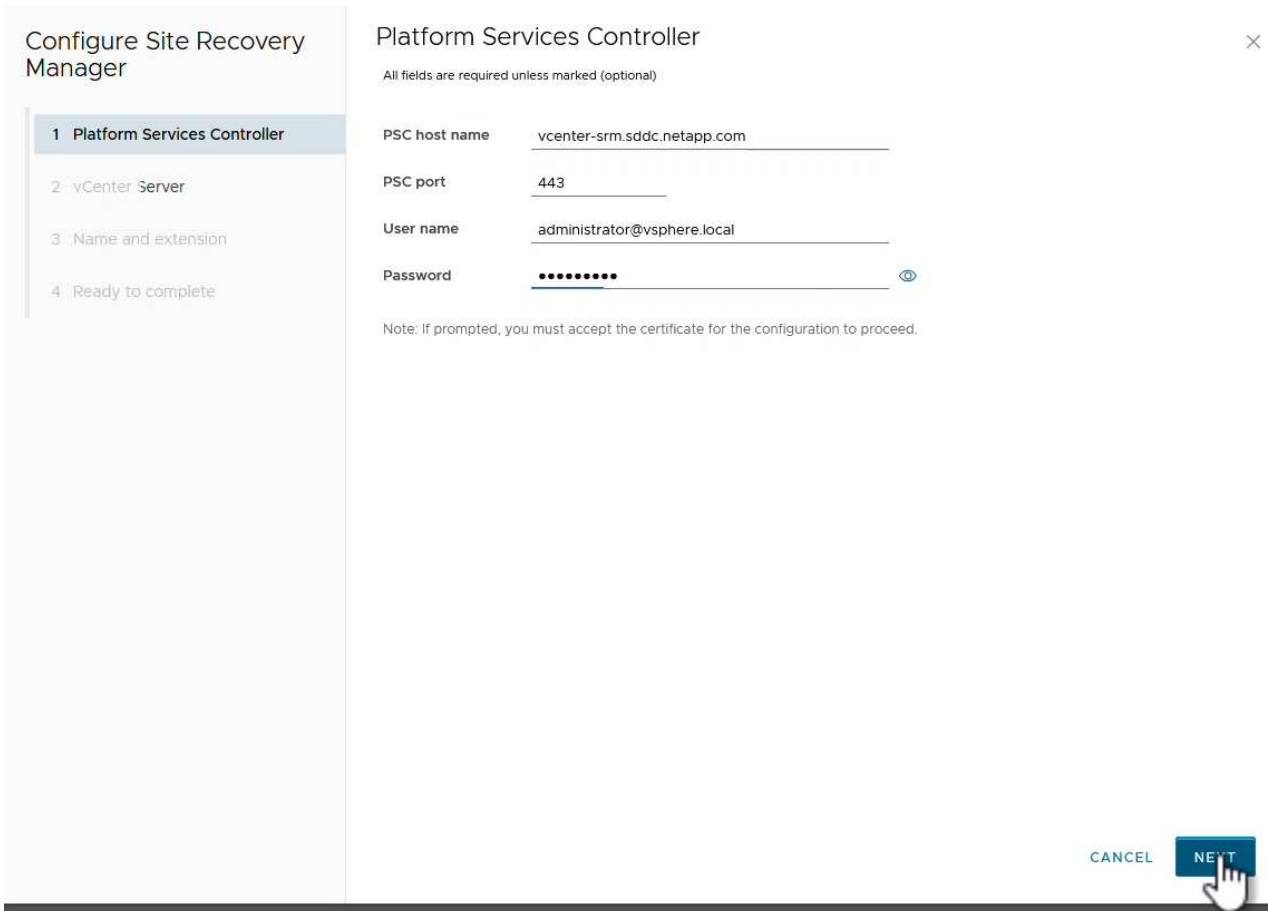
Verbinden Sie die SRM-Appliance für primäre und sekundäre Standorte

Die folgenden Schritte müssen sowohl für den primären als auch für den sekundären Standort durchgeführt werden.

1. Navigieren Sie in einem Webbrowser zu https://<SRM_appliance_IP>:5480 und melden Sie sich an. Klicken Sie auf **Gerät konfigurieren**, um zu beginnen.



2. Geben Sie auf der Seite **Platform Services Controller** des Assistenten Site Recovery Manager konfigurieren die Anmeldeinformationen des vCenter-Servers ein, für den SRM registriert wird. Klicken Sie auf **Weiter**, um fortzufahren.



3. Sehen Sie sich auf der Seite **vCenter Server** den verbundenen Vserver an und klicken Sie auf

Weiter, um fortzufahren.

4. Geben Sie auf der Seite **Name and Extension** einen Namen für den SRM-Standort, eine Administrator-E-Mail-Adresse und den lokalen Host ein, der von SRM verwendet werden soll. Klicken Sie auf **Weiter**, um fortzufahren.

The screenshot shows a web-based configuration wizard for Site Recovery Manager. On the left, a sidebar titled 'Configure Site Recovery Manager' lists four steps: 1 Platform Services Controller, 2 vCenter Server, 3 Name and extension (highlighted), and 4 Ready to complete. The main area is titled 'Name and extension' and contains the following fields and options:

- Site name:** 'Site 2' (with a note: 'A unique display name for this Site Recovery Manager site.')
- Administrator email:** 'josh.powell@netapp.com' (with a note: 'An email address to use for system notifications.')
- Local host:** 'srm-site2.sddc.netapp.com' (with a note: 'The address on the local host to be used by Site Recovery Manager.')
- Extension ID:** Radio buttons for 'Default extension ID (com.vmware.vcDr)' (selected) and 'Custom extension ID'. A note below states: 'The default extension ID is recommended for most configurations. For shared recovery site installations, in which multiple sites connect to a shared recovery site, use a unique custom extension ID for each SRM pair.'
- Extension ID:** 'com.vmware.vcDr-'
- Organization:** (empty field)
- Description:** (empty field)

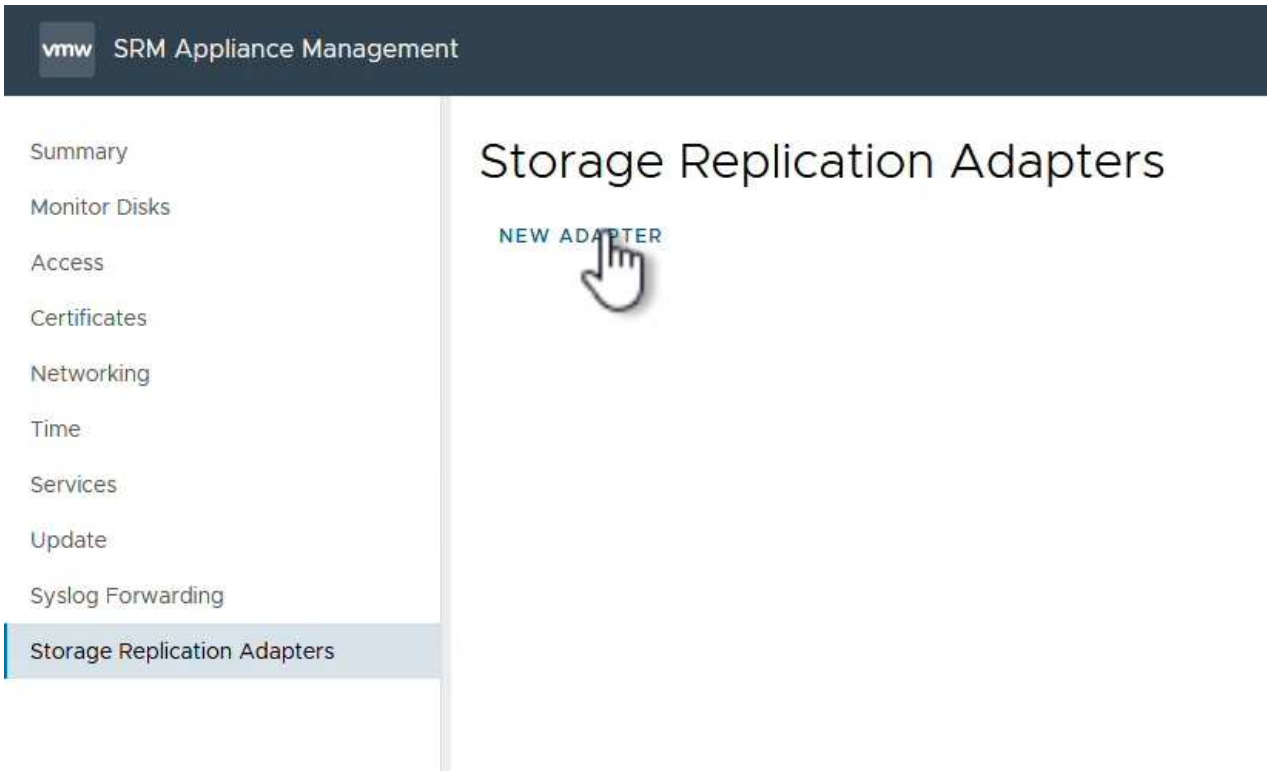
At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is pointing at the 'NEXT' button.

5. Überprüfen Sie auf der Seite **Ready to Complete** die Zusammenfassung der Änderungen

Konfigurieren Sie SRA auf der SRM-Appliance

Führen Sie die folgenden Schritte aus, um SRA auf der SRM-Appliance zu konfigurieren:

1. Laden Sie die SRA für ONTAP-Tools 10 unter herunter "[NetApp Support Website](#)" und speichern Sie die Datei tar.gz in einem lokalen Ordner.
2. Klicken Sie in der SRM Management Appliance auf **Storage Replication Adapter** im linken Menü und dann auf **New Adapter**.



3. Befolgen Sie die Schritte auf der Dokumentationswebsite ONTAP Tools 10 unter "[Konfigurieren Sie SRA auf der SRM-Appliance](#)". Sobald der SRA abgeschlossen ist, kann er mit SRA über die bereitgestellte IP-Adresse und Anmeldedaten des vCenter Servers kommunizieren.

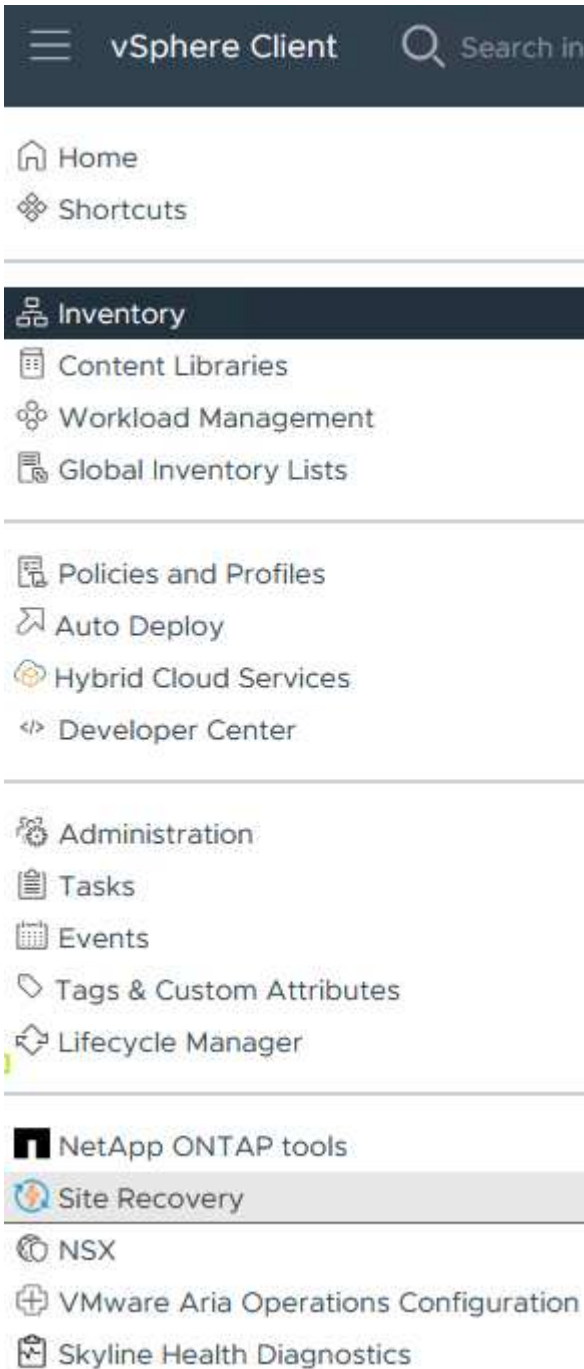
Konfigurieren Sie Site Recovery für SRM

Führen Sie die folgenden Schritte aus, um Standortpairing, Schutzgruppen,

Konfigurieren Sie die Standortanpairing für SRM

Der folgende Schritt wird im vCenter Client des primären Standorts durchgeführt.

1. Klicken Sie im vSphere-Client im linken Menü auf **Site Recovery**. Ein neues Browserfenster wird für die SRM-Management-UI am primären Standort geöffnet.



2. Klicken Sie auf der Seite **STANDORTWIEDERHERSTELLUNG** auf **NEUES STANDORTPAAR**.

Before you can use Site Recovery, you must configure the connection between the Site Recovery Manager server and vSphere Replication server instances on the protected and recovery sites. This is known as a site pair.

[NEW SITE PAIR](#)[Learn More](#)

- Überprüfen Sie auf der Seite **Pair type** des **New Pair Wizard**, ob der lokale vCenter Server ausgewählt ist, und wählen Sie den **Pair Typ** aus. Klicken Sie auf **Weiter**, um fortzufahren.

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

Pair type

Select a local vCenter Server.

vCenter Server

vcenter-vlsr.sddc.netapp.com

Pair type

Pair with a peer vCenter Server located in a different SSO domain

Pair with a peer vCenter Server located in the same SSO domain

CANCEL NEXT

- Geben Sie auf der Seite **Peer vCenter** die Zugangsdaten des vCenter am sekundären Standort ein und klicken Sie auf **Find vCenter Instances**. Überprüfen Sie, ob die vCenter-Instanz erkannt wurde, und klicken Sie auf **Weiter**, um fortzufahren.

New Pair

1 Pair type

2 Peer vCenter Server

3 Services

4 Ready to complete

Peer vCenter Server



All fields are required unless marked (optional)

Enter the Platform Services Controller details for the peer vCenter Server.

PSC host name

PSC port

User name

Password

FIND VCENTER SERVER INSTANCES

Select a vCenter Server you want to pair.

vCenter Server

- vcenter-srm.sddc.netapp.com

CANCEL

BACK

NEXT

5. Aktivieren Sie auf der Seite **Services** das Kontrollkästchen neben der vorgeschlagenen Standortkopplung. Klicken Sie auf **Weiter**, um fortzufahren.

New Pair

- 1 Pair type
- 2 Peer vCenter Server
- 3 Services
- 4 Ready to complete

Services

The following services were identified on the selected vCenter Server instances. Select the ones you want to pair.

Service	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com
<input checked="" type="checkbox"/> Site Recovery Manager (com.vmware.vc...	Site 1	Site 2

CANCEL

BACK

NEXT

6. Überprüfen Sie auf der Seite **Ready to Complete** die vorgeschlagene Konfiguration und klicken Sie dann auf die Schaltfläche **Finish**, um die Standortanordnung zu erstellen
7. Das neue Standortpaar und seine Zusammenfassung können auf der Übersichtsseite angezeigt werden.

Summary

RECONNECT

BREAK SITE PAIR



vCenter Server: [vcenter-vlsr.sddc.netapp.com](#) [vcenter-srm.sddc.netapp.com](#)
vCenter Version: 8.0.2, 22385739 8.0.2, 22385739
vCenter Host Name: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443
Platform Services Controller: vcenter-vlsr.sddc.netapp.com:443 vcenter-srm.sddc.netapp.com:443

Site Recovery Manager

EXPORT/IMPORT SRM CONFIGURATION

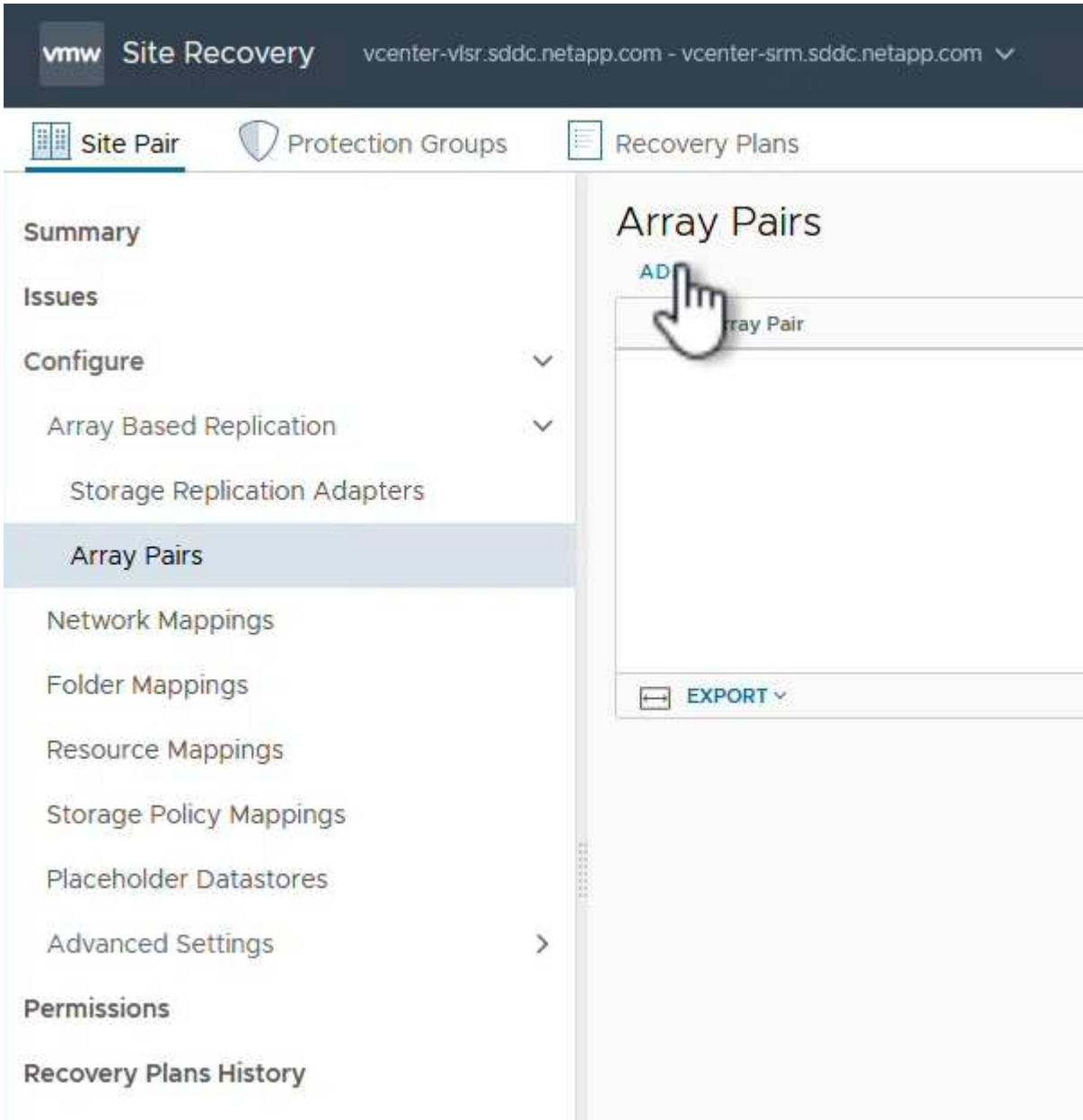
Protection Groups: 0 Recovery Plans: 0

Name	Site 1 RENAME	Site 2 RENAME
Server	srm-site1.sddc.netapp.com:443 ACTIONS	srm-site2.sddc.netapp.com:443 ACTIONS
Version	8.8.0, 23263429	8.8.0, 23263429
ID	com.vmware.vcDr	com.vmware.vcDr
Logged in as	VSPHERE.LOCAL\Administrator	VSPHERE.LOCAL\Administrator
Remote SRM connection	✓ Connected	✓ Connected

Fügen Sie ein Array-Paar für SRM hinzu

Der folgende Schritt wird in der Oberfläche „Standortwiederherstellung“ des primären Standorts durchgeführt.

1. Navigieren Sie in der Benutzeroberfläche für die Standortwiederherstellung im linken Menü zu **Konfigurieren > Array-basierte Replikation > Array Pairs**. Klicken Sie auf **ADD**, um zu beginnen.



2. Überprüfen Sie auf der Seite **Speicherreplikationsadapter** des Assistenten **Array Pair hinzufügen**, ob der SRA-Adapter für den primären Standort vorhanden ist, und klicken Sie auf **Weiter**, um fortzufahren.

Add Array Pair

1 Storage replication adapter

- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Storage replication adapter

Select a storage replication adapter (SRA):

	Storage Replication Adapter	Status	Vendor	Version	Stretched Storage
	NetApp Storage Replication Ada...	OK	NetApp	10.1	Not Support...

Items per page: AUTO 1 items

CANCEL

NEXT

3. Geben Sie auf der Seite **Local Array Manager** einen Namen für das Array am primären Standort, den FQDN des Speichersystems, die SVM-IP-Adressen, die NFS bereitstellen, und optional die Namen bestimmter Volumes ein, die ermittelt werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Local array manager

Array managers allow Site Recovery Manager to communicate with array based replication storage systems.

Enter a name for the array manager on "vcenter-vlsr.sddc.netapp.com":

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname
Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses
Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name
Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list
Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list
Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

4. Geben Sie im **Remote Array Manager** dieselben Informationen wie im letzten Schritt für das ONTAP-Speichersystem am sekundären Standort ein.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs
- 5 Ready to complete

Remote array manager

Do not create a remote array manager now.

Enter a name for the array manager on "vcenter-srm.sddc.netapp.com":

Array_2

Storage Array Parameters

Storage System connection parameters

Storage Management IP Address or Hostname ontap-destination.sddc.netapp.com

Enter the cluster management IP address/hostname. To connect directly to a Storage Virtual Machine(SVM), enter the SVM management IP address/hostname.

NFS Hostnames or IP Addresses 172.21.118.51

Comma separated list of Hostnames or IP addresses that serve NFS to ESX hosts. Leave blank for SAN only.

Storage Virtual Machine(SVM) Name SRM_NFS

Provide Storage Virtual Machine(SVM) name. Leave blank if connecting directly to an SVM.

Volume include list |

Comma separated list of strings in volume names to discover. Leave blank to discover all. Example: srm,sql,win.

Volume exclude list |

Comma separated list of strings in volume names to exclude. Leave blank to exclude none. Example: home,dept,tmp.

CANCEL

BACK

NEXT

5. Wählen Sie auf der Seite **Array pairs** die zu aktivierenden Array-Paare aus und klicken Sie auf **Weiter**, um fortzufahren.

Add Array Pair

- 1 Storage replication adapter
- 2 Local array manager
- 3 Remote array manager
- 4 Array pairs**
- 5 Ready to complete

Array pairs

Select the array pairs to enable:

<input checked="" type="checkbox"/>	vcenter-vlsr.sddc.netapp.com	vcenter-srm.sddc.netapp.com	Status
<input checked="" type="checkbox"/>	ontap-source:SQL_NFS (Array_1)	ontap-destination:SRM_NFS (Array_2)	Ready to be enabled

1 1 items

CANCEL

BACK

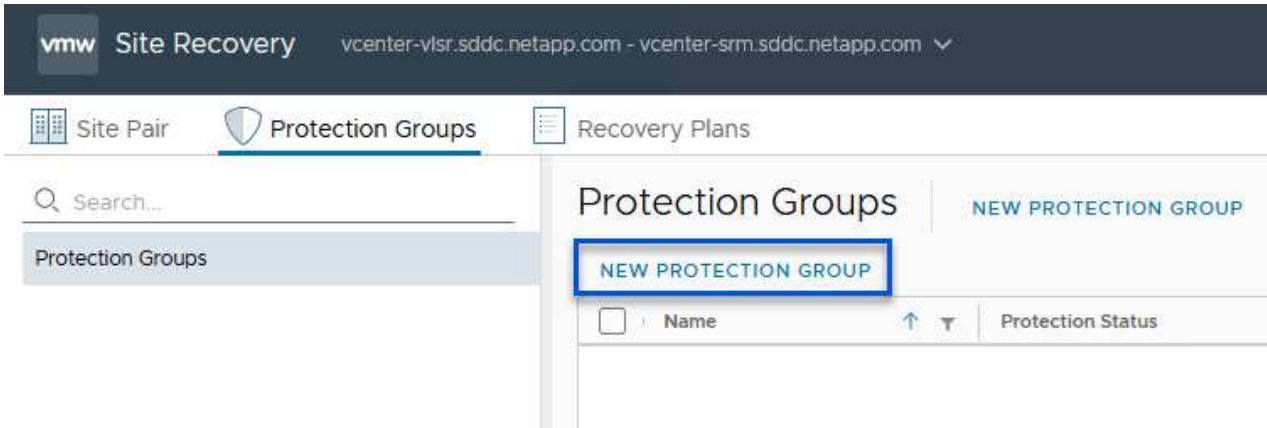
NEXT

6. Überprüfen Sie die Informationen auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um das Array-Paar zu erstellen.

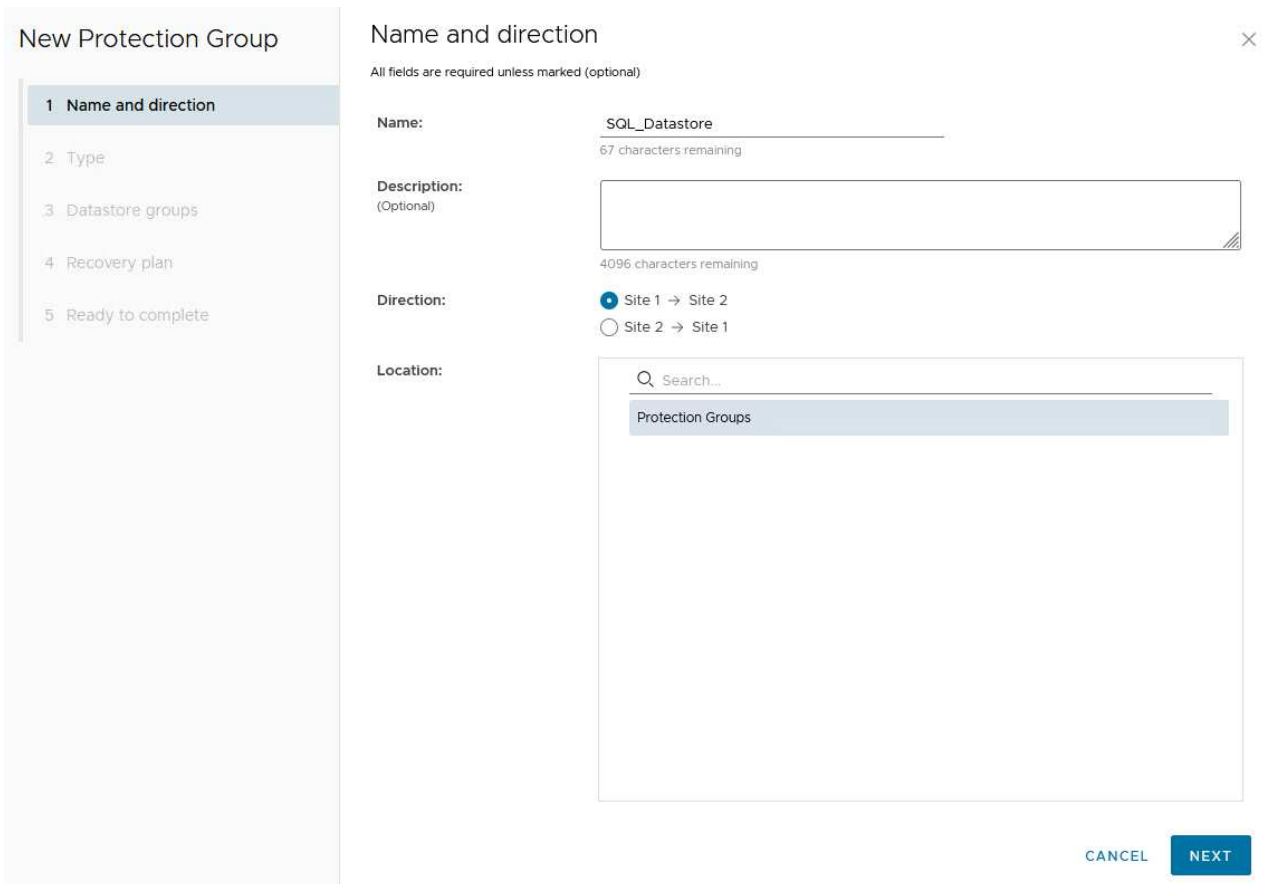
Konfigurieren Sie Schutzgruppen für SRM

Der folgende Schritt wird in der Oberfläche „Standortwiederherstellung“ des primären Standorts durchgeführt.

1. Klicken Sie in der Site Recovery Oberfläche auf die Registerkarte **Schutzgruppen** und dann auf **Neue Schutzgruppe**, um zu beginnen.



2. Geben Sie auf der Seite **Name und Richtung** des **New Protection Group**-Assistenten einen Namen für die Gruppe ein und wählen Sie die Standortrichtung zum Schutz der Daten aus.

The screenshot shows the 'New Protection Group' wizard in the 'Name and direction' step. On the left, a sidebar lists the steps: 1. Name and direction (selected), 2. Type, 3. Datastore groups, 4. Recovery plan, and 5. Ready to complete. The main area is titled 'Name and direction' and contains the following fields:

- Name:** A text input field containing 'SQL_Datastore' with a character count of '67 characters remaining'.
- Description:** An optional text area with a character count of '4096 characters remaining'.
- Direction:** Two radio button options: 'Site 1 → Site 2' (selected) and 'Site 2 → Site 1'.
- Location:** A search dropdown menu with 'Protection Groups' selected.

At the bottom right, there are 'CANCEL' and 'NEXT' buttons.

3. Wählen Sie auf der Seite **Typ** den Typ der Schutzgruppe (Datastore, VM oder vVol) aus und wählen Sie das Array-Paar aus. Klicken Sie auf **Weiter**, um fortzufahren.

New Protection Group

- 1 Name and direction
- 2 Type**
- 3 Datastore groups
- 4 Recovery plan
- 5 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.

Select array pair

Array Pair	Array Manager Pair
<input checked="" type="radio"/> <input checked="" type="checkbox"/> ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2	nfs_array1 ↔ nfs_Array2
<input type="radio"/> <input checked="" type="checkbox"/> ontap-source:SQL_NFS ↔ ontap-destination:SRM_NFS	Array_1 ↔ Array_2

Items per page: AUTO 2 array pairs

[CANCEL](#) [BACK](#) [NEXT](#)

4. Wählen Sie auf der Seite **Datastore groups** die Datastores aus, die in die Schutzgruppe aufgenommen werden sollen. VMs, die sich derzeit auf dem Datenspeicher befinden, werden für jeden ausgewählten Datenspeicher angezeigt. Klicken Sie auf **Weiter**, um fortzufahren.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Datastore groups

Select the datastore groups to be part of this protection group. Datastore groups contain datastores which must be recovered together.

[SELECT ALL](#) [CLEAR SELECTION](#)

<input checked="" type="checkbox"/>	Datastore Group	Status
<input checked="" type="checkbox"/>	NFS_DS1	Add to this protection group

1 Items per page: [AUTO](#) 1 datastore groups

The following virtual machines are in the selected datastore groups:

Virtual Machine	Datastore	Status
SQLSRV-01	NFS_DS1	Add to this protection group
SQLSRV-03	NFS_DS1	Add to this protection group
SQLSRV-02	NFS_DS1	Add to this protection group

[CANCEL](#) [BACK](#) [NEXT](#)

5. Wählen Sie auf der Seite **Wiederherstellungsplan** optional die Schutzgruppe zu einem Wiederherstellungsplan hinzufügen. In diesem Fall ist der Wiederherstellungsplan noch nicht erstellt, sodass **nicht zum Wiederherstellungsplan hinzufügen** ausgewählt ist. Klicken Sie auf **Weiter**, um fortzufahren.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete

Recovery plan



You can optionally add this protection group to a recovery plan.

- Add to existing recovery plan
- Add to new recovery plan
- Do not add to recovery plan now

 The protection group cannot be recovered unless it is added to a recovery plan.

CANCEL

BACK

NEXT

6. Überprüfen Sie auf der Seite **Ready to Complete** die neuen Parameter der Schutzgruppe und klicken Sie auf **Finish**, um die Gruppe zu erstellen.

New Protection Group

- 1 Name and direction
- 2 Type
- 3 Datastore groups
- 4 Recovery plan
- 5 Ready to complete**

Ready to complete



Review your selected settings.

Name	SQL_Datastore
Description	
Protected site	Site 1
Recovery site	Site 2
Location	Protection Groups
Protection group type	Datastore groups (array-based replication)
Array pair	ontap-source:NFS_Array1 ↔ ontap-destination:NFS_Array2 (nfs_array1 ↔ nfs_array2)
Datastore groups	NFS_DS1
Total virtual machines	3
Recovery plan	none

CANCEL

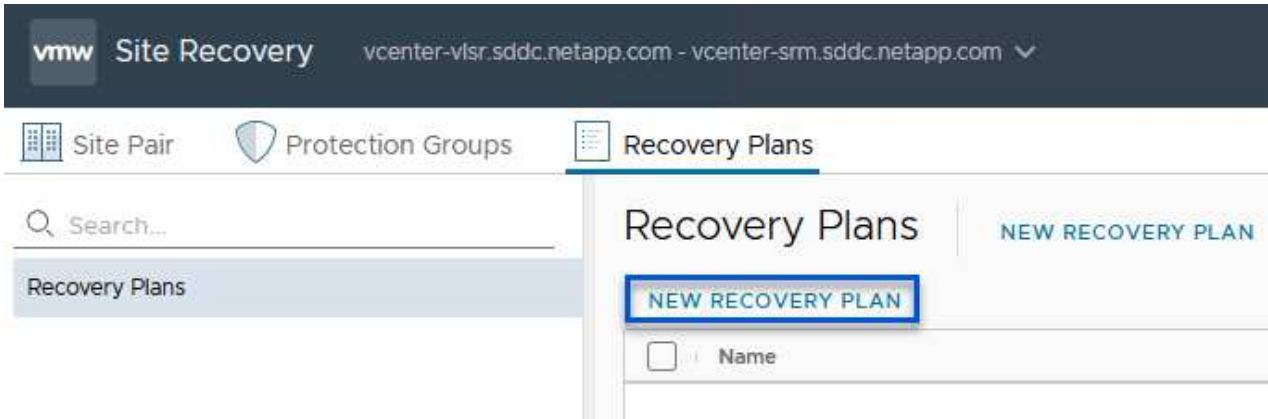
BACK

FINISH

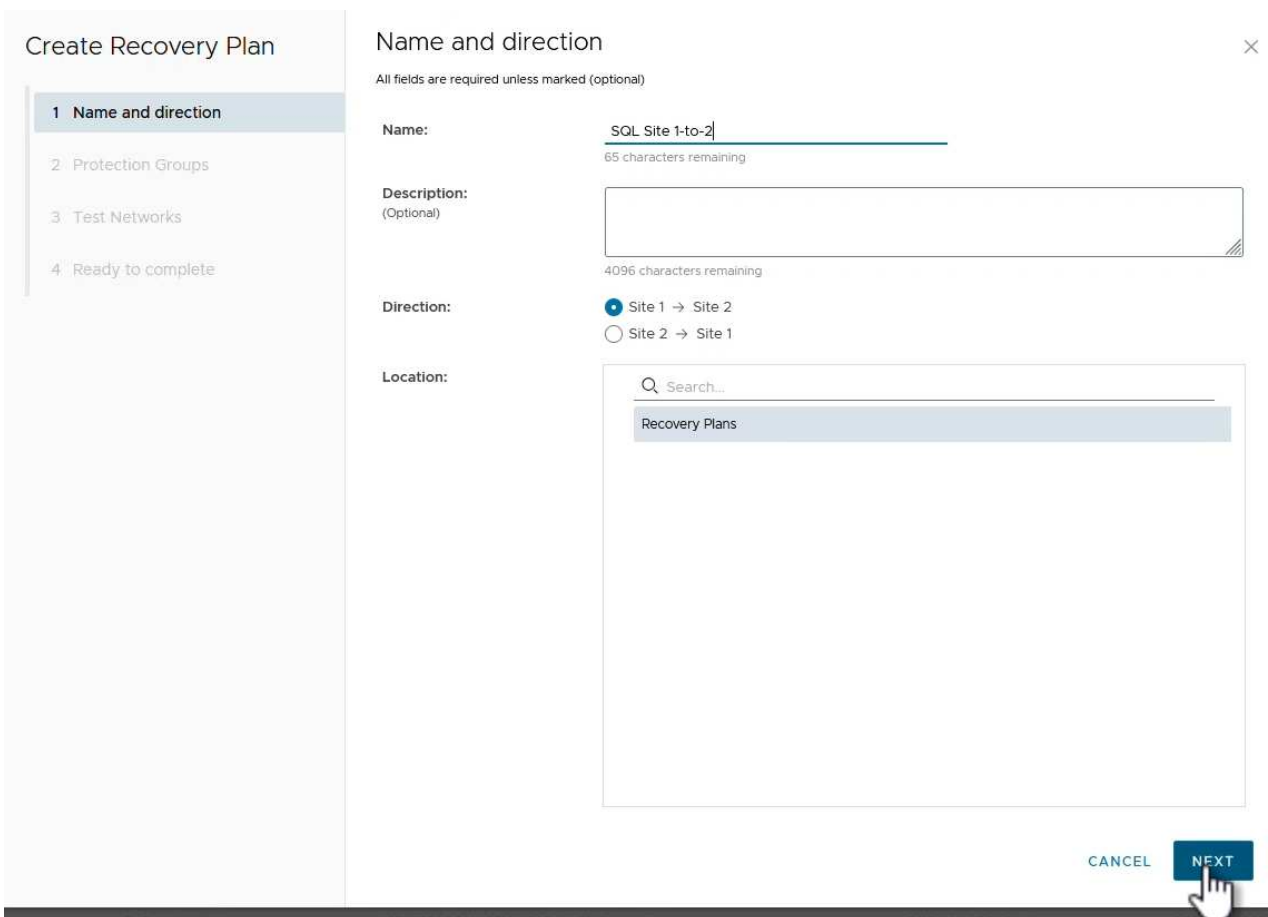
Konfiguration des Recovery-Plans für SRM

Der folgende Schritt wird in der Oberfläche „Standortwiederherstellung“ des primären Standorts durchgeführt.

1. Klicken Sie in der Benutzeroberfläche der Standortwiederherstellung auf die Registerkarte **Wiederherstellungsplan** und dann auf **Neuer Wiederherstellungsplan**, um zu beginnen.



2. Geben Sie auf der Seite **Name und Richtung** des Assistenten **Wiederherstellungsplan erstellen** einen Namen für den Wiederherstellungsplan ein und wählen Sie die Richtung zwischen Quell- und Zielstandort aus. Klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Schutzgruppen** die zuvor erstellten Schutzgruppen aus, die in den Wiederherstellungsplan aufgenommen werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.

Create Recovery Plan

- 1 Name and direction
- 2 Protection Groups**
- 3 Test Networks
- 4 Ready to complete

Protection Groups ×

All Selected (1)

<input checked="" type="checkbox"/>	Name	Description
<input checked="" type="checkbox"/>	SQL_Datastore	

Items per page: AUTO 1 group(s)

CANCEL BACK **NEXT**

4. Konfigurieren Sie auf dem **Test Networks** bestimmte Netzwerke, die während des Tests des Plans verwendet werden. Wenn keine Zuordnung vorhanden ist oder kein Netzwerk ausgewählt ist, wird ein isoliertes Testnetzwerk erstellt. Klicken Sie auf **Weiter**, um fortzufahren.

Create Recovery Plan

- 1 Name and direction
- 2 Protection Groups
- 3 Test Networks
- 4 Ready to complete

Test Networks

Select the networks to use while running tests of this plan.

i If "Use site-level mapping" is selected and no such mapping exists, an isolated test network will be created.

Recovery Network	↑ ↓	Test Network	
Datacenter > DPortGroup	☰	Use site-level mapping	CHANGE
Datacenter > Mgmt 3376	☰	Mgmt 3376	CHANGE
Datacenter > NFS 3374	☰	NFS 3374	CHANGE
Datacenter > VLAN 181	☰	Use site-level mapping	CHANGE
Datacenter > VM Network	☰	Use site-level mapping	CHANGE
Datacenter > vMotion 3373	☰	Use site-level mapping	CHANGE
Datacenter > vSAN 3422	☰	Use site-level mapping	CHANGE

7 network(s)

CANCEL
BACK
NEXT

5. Überprüfen Sie auf der Seite **Ready to Complete** die ausgewählten Parameter und klicken Sie dann auf **Finish**, um den Wiederherstellungsplan zu erstellen.

Disaster Recovery-Vorgänge mit SRM

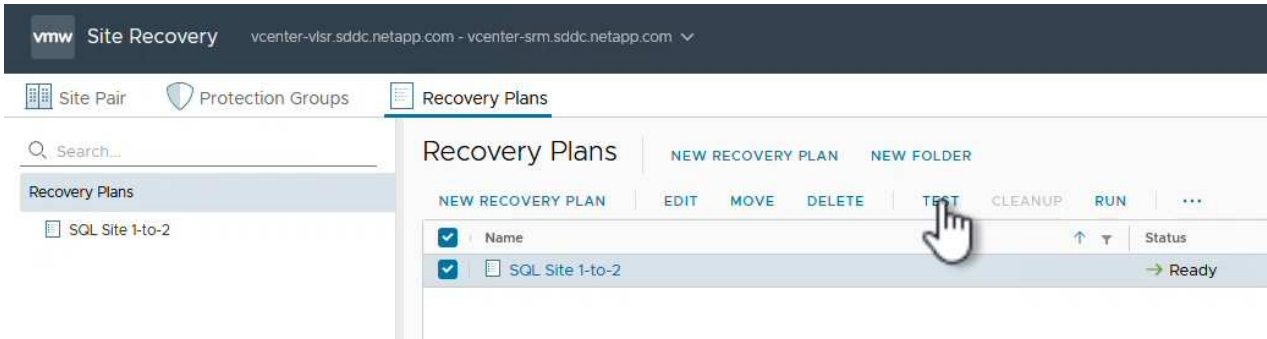
In diesem Abschnitt werden verschiedene Funktionen der Verwendung von Disaster Recovery mit SRM behandelt, darunter das Testen von Failover, das Durchführen von Failovers, das Durchführen von Datensicherung und Failback.

https://docs.netapp.com/us-en/ontap-apps-dbs/vmware/vmware-srm-operational_best_practices.html ["Best Practices für betriebliche Prozesse"] Weitere Informationen zur Verwendung von ONTAP Storage mit Disaster-Recovery-Vorgängen durch SRM finden Sie unter.

Testen des Failover mit SRM

Der folgende Schritt wird in der Benutzeroberfläche für die Standortwiederherstellung ausgeführt.

1. Klicken Sie in der Benutzeroberfläche für die Standortwiederherstellung auf die Registerkarte **Wiederherstellungsplan** und wählen Sie dann einen Wiederherstellungsplan aus. Klicken Sie auf die Schaltfläche **Test**, um den Failover zum sekundären Standort zu testen.

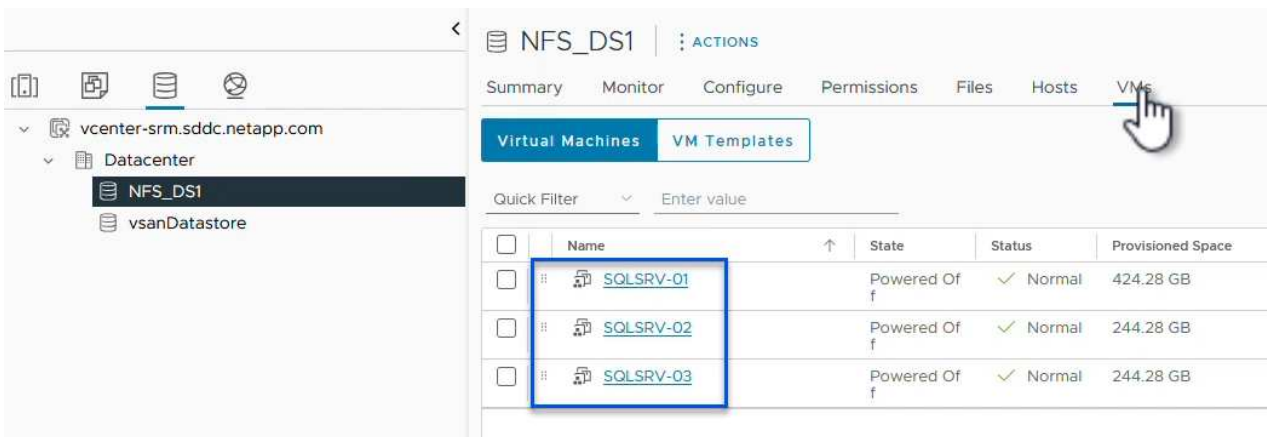


2. Sie können den Fortschritt des Tests im Aufgabenbereich Site Recovery sowie im Aufgabenbereich vCenter anzeigen.

The screenshot shows the 'Recent Tasks' section of the VMware Site Recovery console. It displays a table with columns: 'Task Name', 'Target', 'Status', 'Initiator', and 'Queued For'. The table contains four rows of tasks.

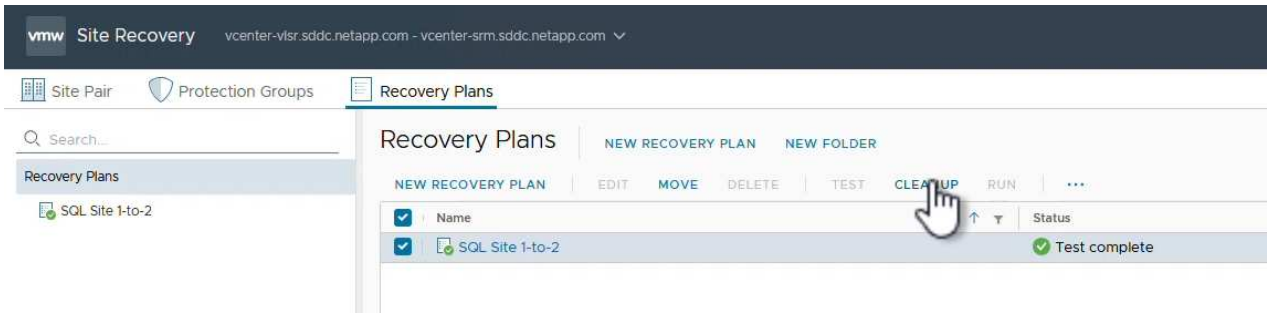
Task Name	Target	Status	Initiator	Queued For
Test Recovery Plan	vcenter-vlsr.sddc.netapp.com	6 %	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	11 ms
Create Recovery Plan	vcenter-vlsr.sddc.netapp.com	✓ Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	10 ms
Set virtual machine custom value	SQLSRV-02	✓ Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	4 ms
Set virtual machine custom value	SQLSRV-01	✓ Completed	VSPHERE.LOCAL\SRM-d1369bbb-62c6...	3 ms

3. SRM sendet Befehle über den SRA an das sekundäre ONTAP Storage-System. Eine FlexClone des letzten Snapshots wird auf dem sekundären vSphere-Cluster erstellt und gemountet. Der neu gemountete Datastore kann im Storage Inventory angezeigt werden.



4. Wenn der Test abgeschlossen ist, klicken Sie auf **Cleanup**, um den Datenspeicher zu entsperren und

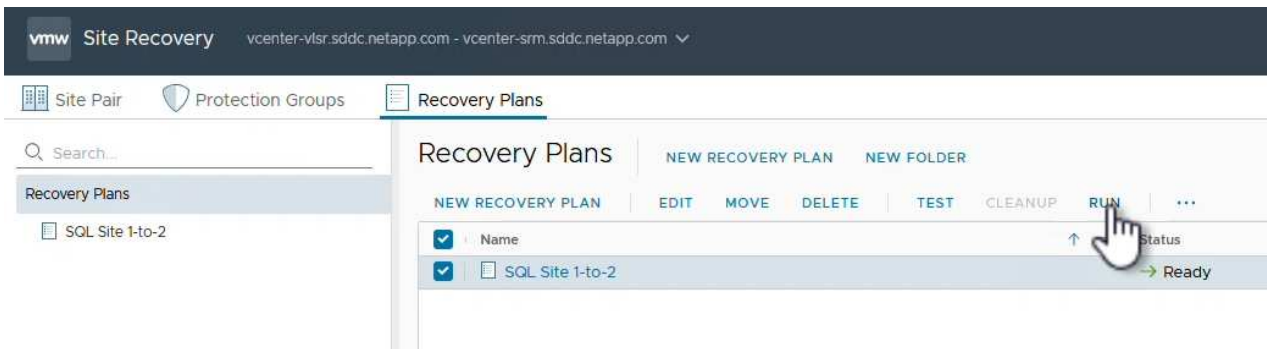
zur ursprünglichen Umgebung zurückzukehren.



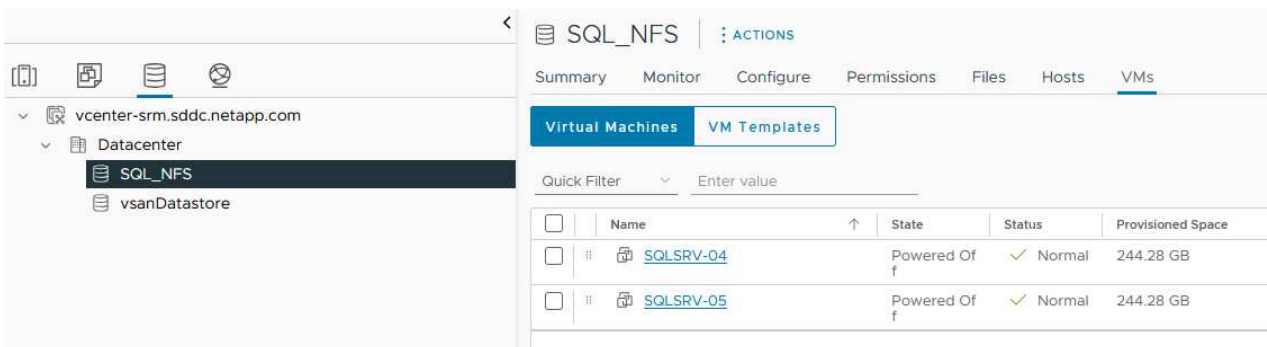
Ausführen des Recovery-Plans mit SRM

Führen Sie eine vollständige Recovery und einen Failover auf den sekundären Standort durch.

1. Klicken Sie in der Benutzeroberfläche für die Standortwiederherstellung auf die Registerkarte **Wiederherstellungsplan** und wählen Sie dann einen Wiederherstellungsplan aus. Klicken Sie auf die Schaltfläche **Ausführen**, um den Failover zum sekundären Standort zu starten.



2. Sobald der Failover abgeschlossen ist, werden der gemountete Datastore und die VMs am sekundären Standort registriert.



Nach Abschluss eines Failovers sind in SRM zusätzliche Funktionen möglich.

Reschutz: Sobald der Recovery-Prozess abgeschlossen ist, übernimmt der zuvor vorgesehene Recovery-Standort die Rolle des neuen Produktionsstandorts. Es ist jedoch zu beachten, dass die SnapMirror-Replizierung während des Recovery-Vorgangs unterbrochen wird, sodass der neue Produktionsstandort

anfällig für zukünftige Katastrophen ist. Um einen kontinuierlichen Schutz zu gewährleisten, wird empfohlen, einen neuen Schutz für den neuen Produktionsstandort einzurichten, indem er an einen anderen Standort repliziert wird. In Fällen, an denen der ursprüngliche Produktionsstandort weiterhin funktionsfähig bleibt, kann der VMware-Administrator ihn als neuen Recovery-Standort neu zuweisen und so die Sicherungsrichtung effektiv umkehren. Hervorzuheben ist, dass ein erneuter Schutz nur bei nicht katastrophalen Ausfällen möglich ist, sodass die Wiederherstellbarkeit der ursprünglichen vCenter-Server, ESXi-Server, SRM-Server und der entsprechenden Datenbanken möglich ist. Wenn diese Komponenten nicht verfügbar sind, müssen eine neue Schutzgruppe und ein neuer Wiederherstellungsplan erstellt werden.

Failback: Ein Failback-Vorgang ist ein Reverse Failover, der Vorgänge zum ursprünglichen Standort zurückgibt. Es ist wichtig sicherzustellen, dass der ursprüngliche Standort wieder funktionsfähig ist, bevor der Failback-Prozess gestartet wird. Um ein reibungsloses Failback zu gewährleisten, wird empfohlen, ein Test-Failover durchzuführen, nachdem der erneute Schutz abgeschlossen wurde und bevor das abschließende Failback ausgeführt wird. Diese Vorgehensweise dient als Überprüfungsschritt, der bestätigt, dass die Systeme am ursprünglichen Standort den Betrieb vollständig handhaben können. Mit diesem Ansatz können Sie Risiken minimieren und einen zuverlässigeren Übergang zurück zur ursprünglichen Produktionsumgebung sicherstellen.

Weitere Informationen

NetApp-Dokumentation zur Verwendung von ONTAP Storage mit VMware SRM finden Sie unter ["VMware Site Recovery Manager mit ONTAP"](#)

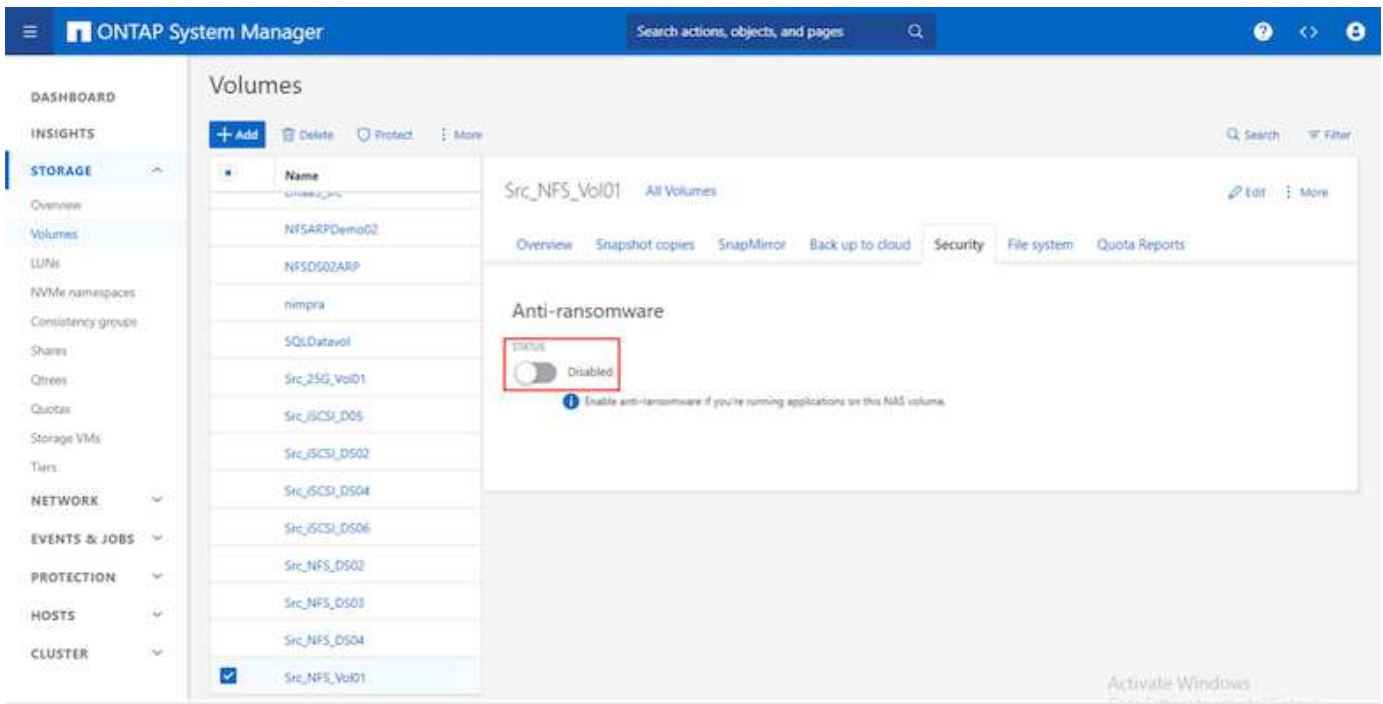
Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

Autonomer Ransomware-Schutz für NFS-Storage

Um die Ausbreitung zu verhindern und teure Ausfallzeiten zu vermeiden, ist es wichtig, Ransomware so früh wie möglich zu erkennen. Eine effektive Strategie zur Erkennung von Ransomware muss mehrere Schutzebenen auf ESXi Host- und Gast-VM-Ebene umfassen. Während mehrere Sicherheitsmaßnahmen implementiert werden, um einen umfassenden Schutz vor Ransomware-Angriffen zu bieten, bietet ONTAP dem gesamten Verteidigungsansatz zusätzliche Schutzschichten. Um nur einige Funktionen zu nennen: Snapshots, Autonomer Ransomware-Schutz, manipulationssichere Snapshots usw.

Sehen wir uns an, wie die oben genannten Funktionen mit VMware zusammenarbeiten, um Daten vor Ransomware zu schützen und wiederherzustellen. Um vSphere und Gast-VMs vor Angriffen zu schützen, müssen verschiedene Maßnahmen ergriffen werden, darunter Segmentierung, Einsatz von EDR/XDR/SIEM für Endpunkte und Installation von Sicherheitsupdates sowie Einhaltung der entsprechenden Härtingsrichtlinien. Jede virtuelle Maschine, die sich auf einem Datastore befindet, hostet auch ein Standardbetriebssystem. Stellen Sie sicher, dass die Produktsuiten für Anti-Malware-Produkte von Unternehmensservern installiert und regelmäßig aktualisiert werden, was ein wesentlicher Bestandteil einer mehrschichtigen Ransomware-Schutzstrategie ist. Aktivieren Sie darüber hinaus Autonomous Ransomware Protection (ARP) auf dem NFS-Volume, das den Datastore versorgt. ARP nutzt integriertes ML zur automatischen Erkennung von Ransomware mit Blick auf die Volume-Workload-Aktivität und Datenentropie. ARP kann über die integrierte Management-Schnittstelle von ONTAP oder System Manager konfiguriert werden und ist für einzelne Volumes aktiviert.

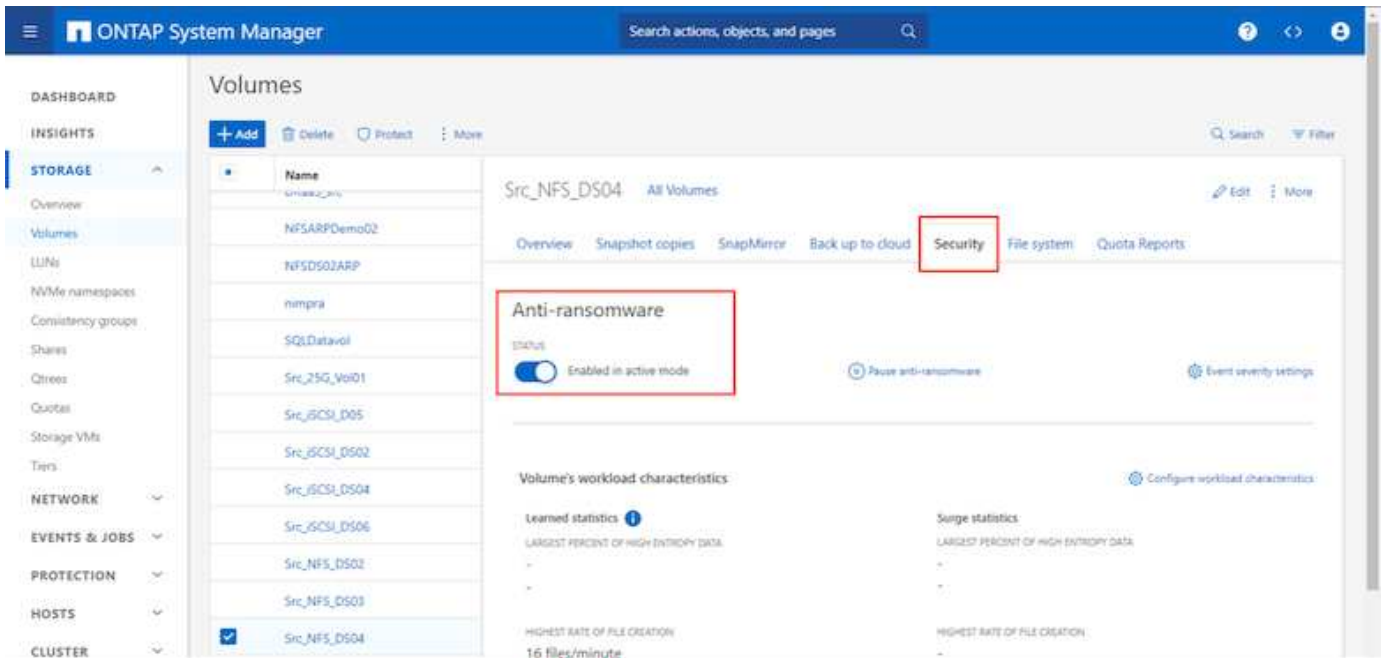


Mit dem neuen NetApp ARP/AI, das sich derzeit in der Tech Preview befindet, ist kein Lernmodus erforderlich. Stattdessen ist ein direkter Weg in den aktiv-Modus mit seiner KI-gestützten Ransomware-Erkennungsfunktion möglich.



Mit ONTAP One sind alle diese Funktionen komplett kostenlos. Greifen Sie auf die robuste Suite von NetApp für Datensicherung, Sicherheit und alle Funktionen von ONTAP zu, ohne sich über Lizenzierungshindernisse Gedanken machen zu müssen.

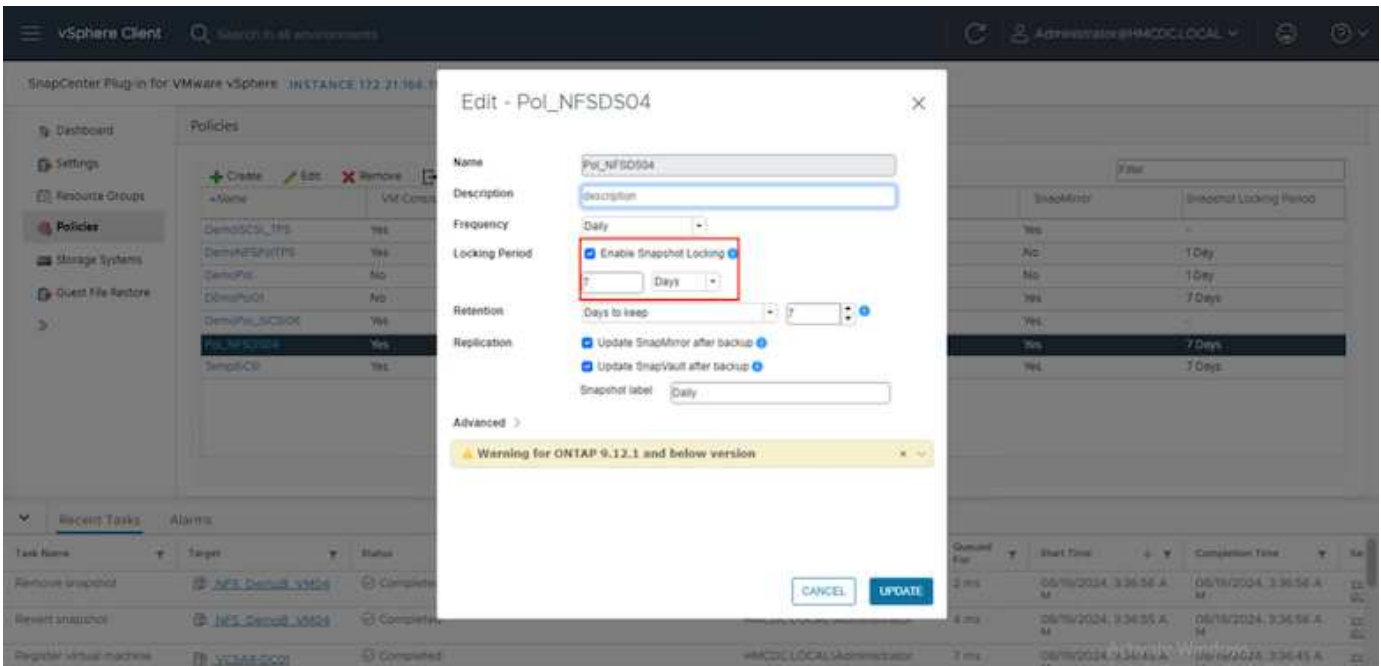
Im aktiven Modus wird nach der abnormalen Volume-Aktivität gesucht, die möglicherweise ein Ransomware-Angriff sein könnte. Wenn anormale Aktivitäten erkannt werden, wird sofort eine automatische Snapshot Kopie erstellt. Dadurch wird ein Wiederherstellungspunkt so nah wie möglich an der Infektion mit Dateien erstellt. ARP kann Änderungen in VM-spezifischen Dateierweiterungen auf einem NFS-Volume außerhalb der VM erkennen, wenn dem verschlüsselten Volume eine neue Erweiterung hinzugefügt oder die Dateierweiterung geändert wird.



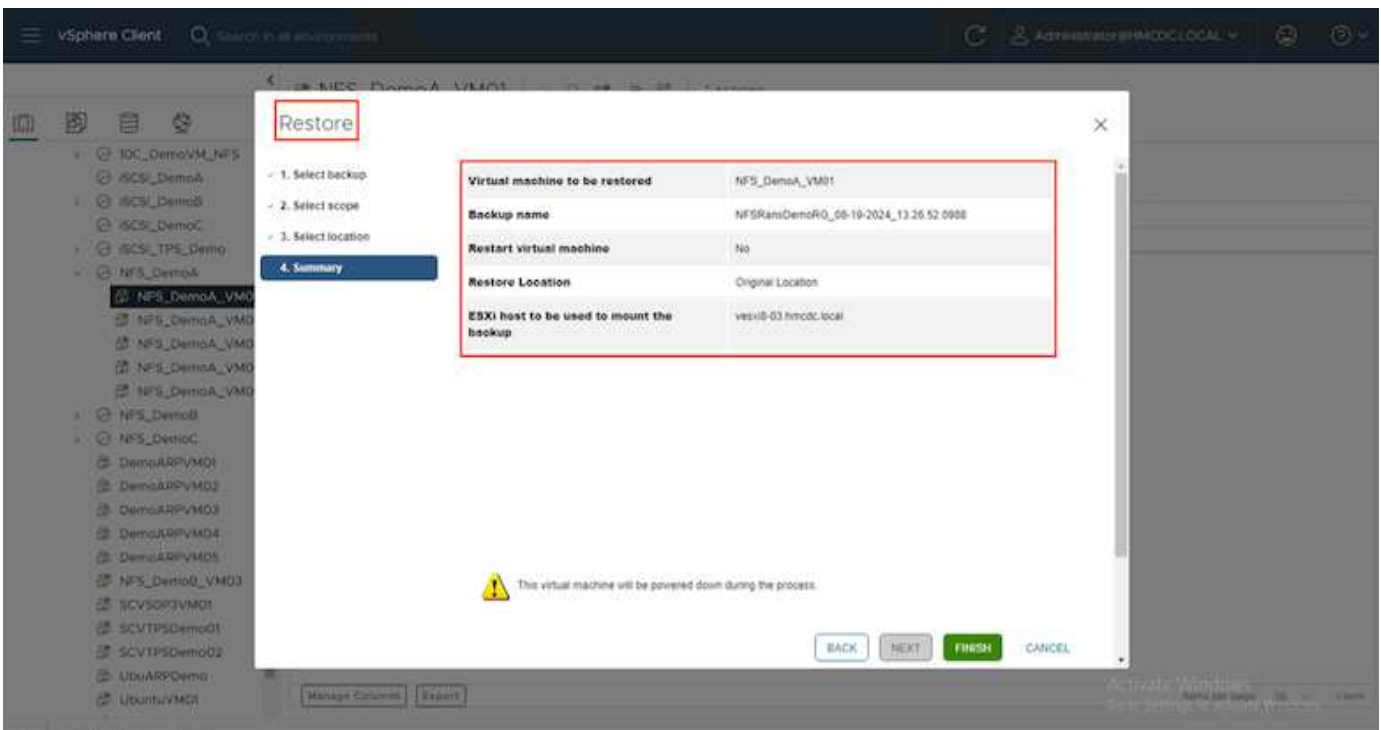
Wenn ein Ransomware-Angriff auf die virtuelle Maschine (VM) zielt und Dateien innerhalb der VM verändert, ohne Änderungen außerhalb der VM vorzunehmen, erkennt der Advanced Ransomware Protection (ARP) immer noch die Bedrohung, wenn die Standard-Entropie der VM niedrig ist, z. B. für Dateitypen wie .txt, .docx oder .mp4-Dateien. Obwohl ARP in diesem Szenario einen schützenden Snapshot erstellt, erzeugt es keine Bedrohungswarnung, da die Dateierweiterungen außerhalb der VM nicht manipuliert wurden. In solchen Szenarien würden die anfänglichen Verteidigungsschichten die Anomalie identifizieren, ARP hilft jedoch bei der Erstellung eines Snapshots basierend auf der Entropie.

Ausführliche Informationen finden Sie im Abschnitt „ARP und virtuelle Maschinen“ in ["ARP-Nutzungen und Überlegungen"](#).

Das Verlagern von Dateien zu Backup-Daten führt bei Ransomware-Angriffen zunehmend zu Backup- und Snapshot-Wiederherstellungspunkten, da versucht wird, diese zu löschen, bevor die Dateien verschlüsselt werden. Mit ONTAP lässt sich dies jedoch verhindern, indem mit manipulationssichere Snapshots auf primären oder sekundären Systemen erstellt ["NetApp Snapshot™ Sperren von Kopien"](#) werden.



Diese Snapshot Kopien können von Angreifern oder betrügerischen Administratoren nicht gelöscht oder geändert werden. Die Kopien sind also auch nach einem Angriff verfügbar. Wenn der Datastore oder bestimmte Virtual Machines betroffen sind, kann SnapCenter die Daten von Virtual Machines innerhalb von Sekunden wiederherstellen und so die Ausfallzeiten des Unternehmens minimieren.



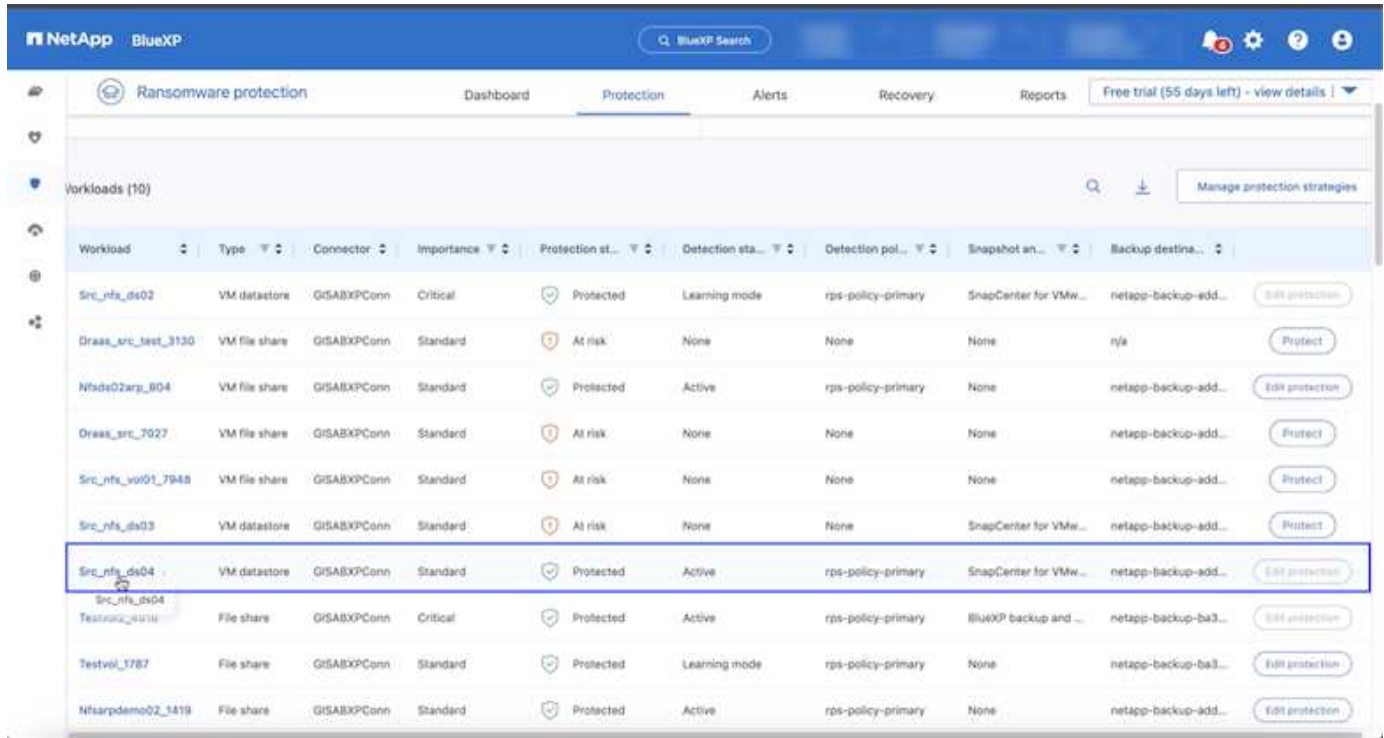
In der obigen Abbildung wird gezeigt, wie ONTAP Storage Locking die vorhandenen Techniken um eine zusätzliche Schicht erweitert und so die Zukunftssicherheit der Umgebung verbessert.

Weitere Informationen finden Sie in der Anleitung für ["NetApp Lösungen für Ransomware"](#).

Wenn all dies nun orchestriert und in SIEM-Tools integriert werden muss, kann OFFTAP-Service wie BlueXP Ransomware-Schutz verwendet werden. Dieser Service ist darauf ausgelegt, Daten vor Ransomware zu

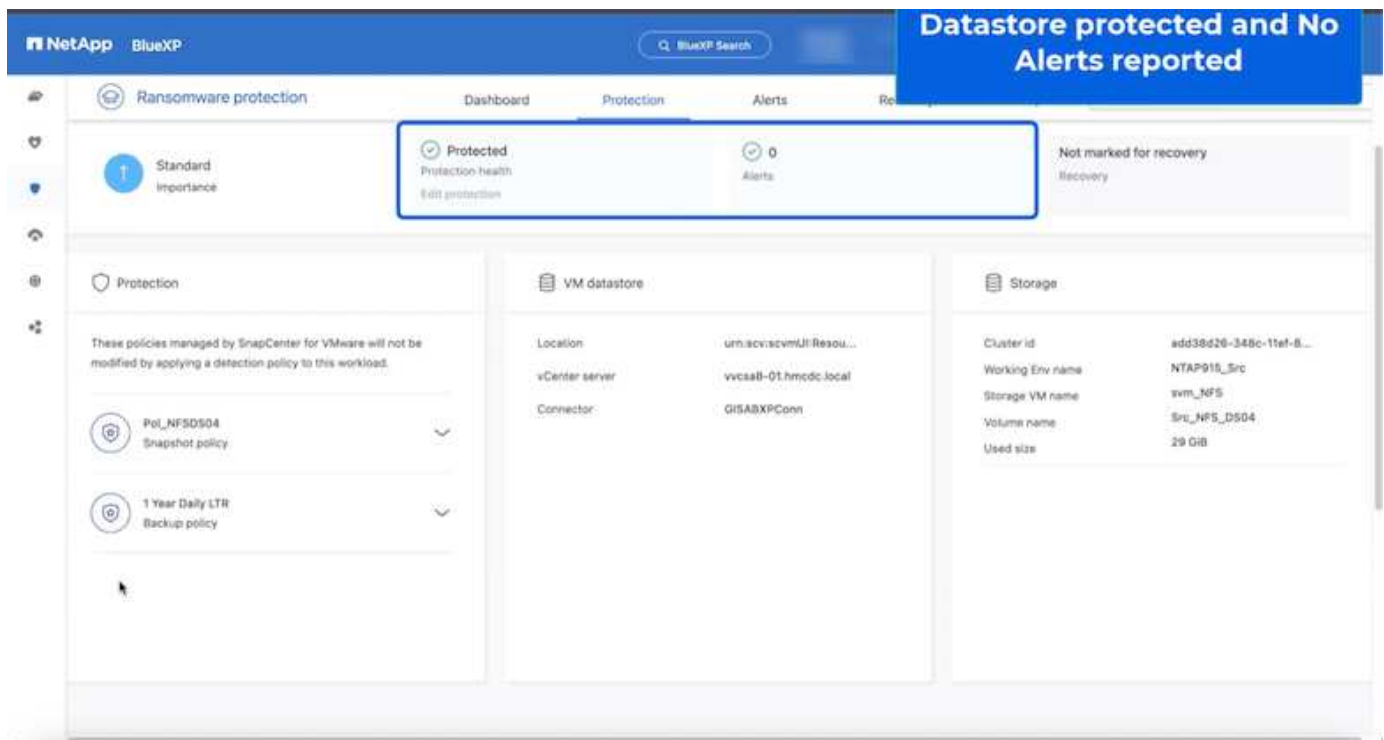
schützen. Dieser Service sichert applikationsbasierte Workloads wie Oracle, MySQL, VM-Datstores und File Shares in lokalem NFS-Storage.

In diesem Beispiel ist der NFS-Datstore „SRC_NFS_DS04“ durch BlueXP Ransomware-Schutz geschützt.



The screenshot shows the NetApp BlueXP Ransomware protection dashboard. The 'Protection' tab is active, displaying a table of workloads. The workload 'Src_nfs_ds04' is highlighted in blue, indicating it is protected. The table columns include Workload, Type, Connector, Importance, Protection status, Detection status, Detection policy, Snapshot agent, and Backup destination.

Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destina...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_src_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsds02arj_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vu01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_ds04	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsarpdemo02_1419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection



The screenshot shows the detailed protection configuration for the workload 'Src_nfs_ds04'. A blue banner at the top right states 'Datastore protected and No Alerts reported'. The 'Protection' section shows the workload is 'Protected' with 'Standard' importance and '0' alerts. The 'VM datastore' section provides details: Location (urn:scv:scvm:ll:Resou...), vCenter server (vccsa8-01.hmc:dc.local), and Connector (GISABXPConn). The 'Storage' section shows Cluster id (add38626-348c-11ef-8...), Working Env name (NTAP915_Src), Storage VM name (svm_nfs), Volume name (Src_NFS_DS04), and Used size (29 GiB). Two policies are listed: 'Pol_NFS0504 Snapshot policy' and '1 Year Daily LTR Backup policy'.

Ausführliche Informationen zum Konfigurieren von BlueXP -Ransomware-Schutz finden Sie unter "Einrichten des BlueXP Ransomware-Schutzes" und "Konfigurieren Sie BlueXP Ransomware-Schutzeinstellungen".

Es ist an der Zeit, dies anhand eines Beispiels zu erläutern. In dieser Anleitung ist der Datstore

„SRC_NFS_DS04“ betroffen.

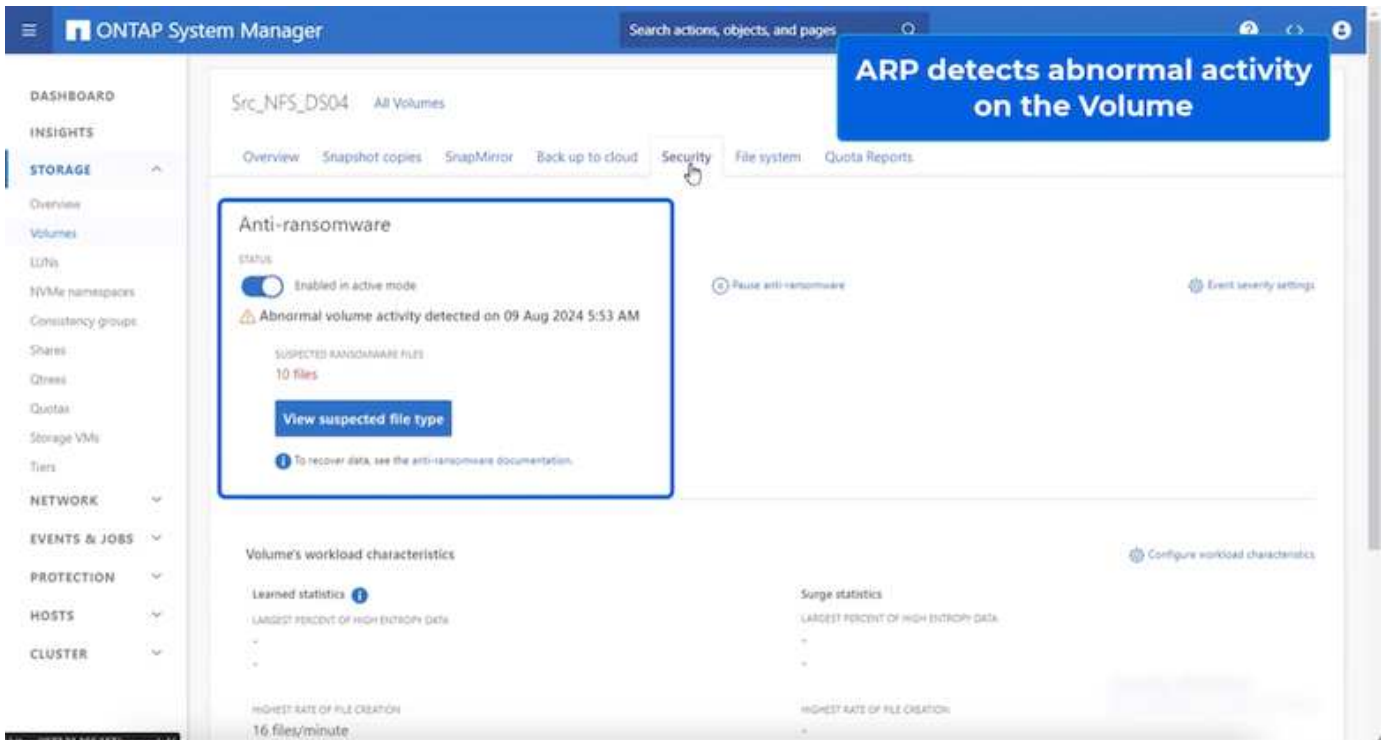
VM Disk files under Ransomware Attack and VM affected

Name	Size	Modified	Type	Path
SO_DemoVM1 scoreboard	8 KB	08/05/2024, 1:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\SO_DemoVM1\scoreboard
SO_DemoVM1 scoreboard	8 KB	08/09/2024, 9:33:11 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\SO_DemoVM1\scoreboard
NFS_DemoB_VMO1-362a6f7b.vswp	4.994.204 KB	07/22/2024, 5:53:48 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-362a6f7b.vswp
NFS_DemoB_VMO1-29f5a0b5.Hlog	0.09 KB	08/05/2024, 1:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-29f5a0b5.Hlog
NFS_DemoB_VMO1-362a6f7b.vswp	0.01 KB	08/09/2024, 5:08:46 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-362a6f7b.vswp
NFS_DemoB_VMO1-nvram	8.48 KB	07/22/2024, 5:02:56 AM	Non-volatile Memory File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-nvram
NFS_DemoB_VMO1-vmad	0.04 KB	08/09/2024, 5:08:46 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-vmad
NFS_DemoB_VMO1-vmx	3.4 KB	08/09/2024, 5:08:46 AM	Virtual Machine	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-vmx
NFS_DemoB_VMO1-vmx.klk	0 KB	08/05/2024, 1:02:39 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-vmx.klk
NFS_DemoB_VMO1-vmx1.arg	0.07 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1-vmx1.arg
NFS_DemoB_VMO1_3-13k-vmxk.arg	640,54 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1_3-13k-vmxk.arg
NFS_DemoB_VMO1_3-16k-vmxk.arg	12.485.160 KB	08/09/2024, 5:31:11 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1_3-16k-vmxk.arg
NFS_DemoB_VMO1_3-vmxk.arg	0.84 KB	08/09/2024, 5:31:22 AM	File	[Src_NFS_DS04] NFS_DemoB_VMO1\NFS_DemoB_VMO1_3-vmxk.arg

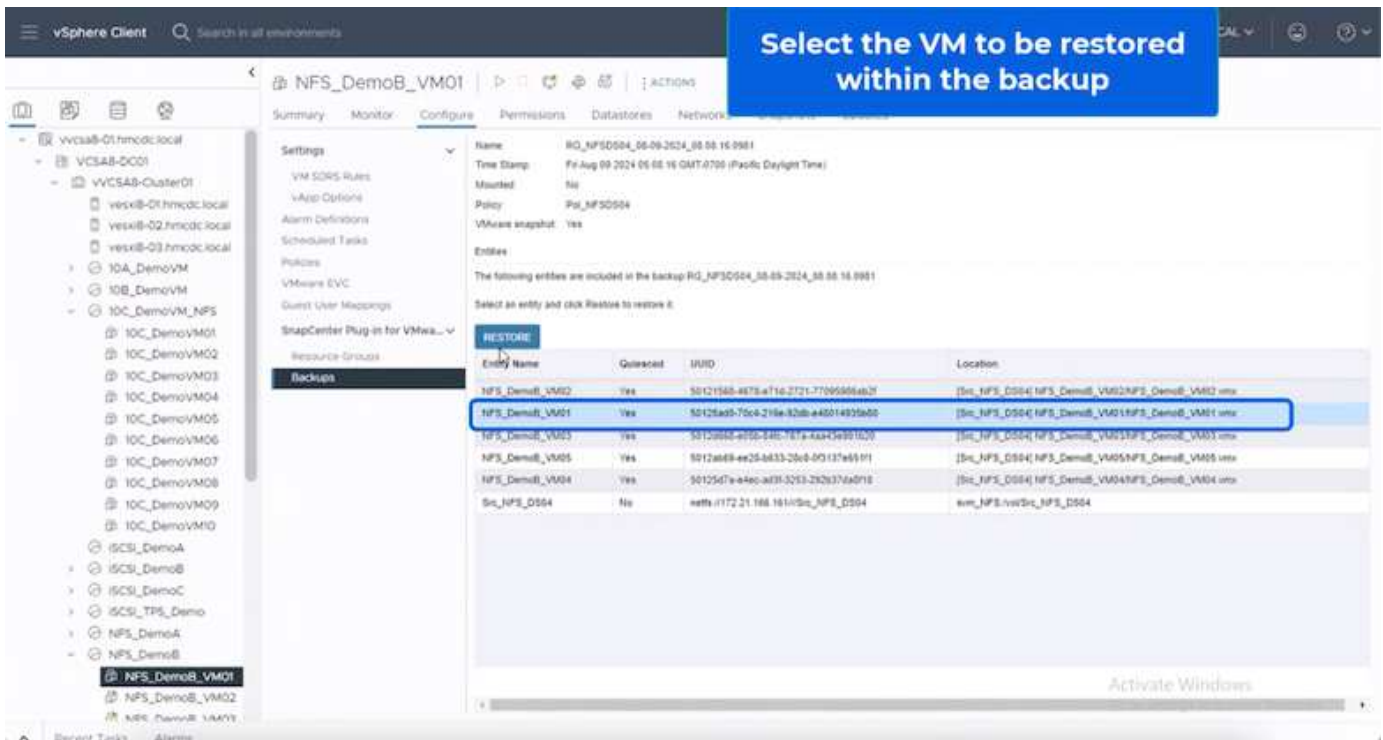
ARP hat bei der Erkennung sofort einen Snapshot auf dem Volume ausgelöst.

NetApp Snapshot triggered during suspected abnormal activity

Name	Snapshot copy creation time	Snapshot restore size
snappmirror.a2a05432-3537-11ef-bd57-00a0b86d346_21 59491296.2024-08-09_160500	Aug/9/2024 9:05 AM	50.5 GiB
Anti_ransomware_backup.2024-08-09_1326	Aug/9/2024 6:26 AM	44.5 GiB
RG_NFS_DS04_08-09-2024_08.08.16.0961	Aug/9/2024 5:08 AM	27.8 GiB
RG_NFS_DS04_08-09-2024_07.54.40.0205	Aug/9/2024 4:55 AM	27.7 GiB
[REDACTED]	Aug/9/2024 3:27 AM	27.6 GiB
RG_NFS_DS04_08-09-2024_06.27.18.0190	Aug/9/2024 3:27 AM	27.8 GiB
RG_NFS_DS04_08-09-2024_05.00.28.0747	Aug/9/2024 2:00 AM	37.7 GiB



Sobald die forensische Analyse abgeschlossen ist, können die Wiederherstellungen mithilfe von SnapCenter oder BlueXP Ransomware-Schutz schnell und nahtlos durchgeführt werden. Wechseln Sie bei SnapCenter zu den betroffenen Virtual Machines, und wählen Sie den entsprechenden wiederherzustellenden Snapshot aus.

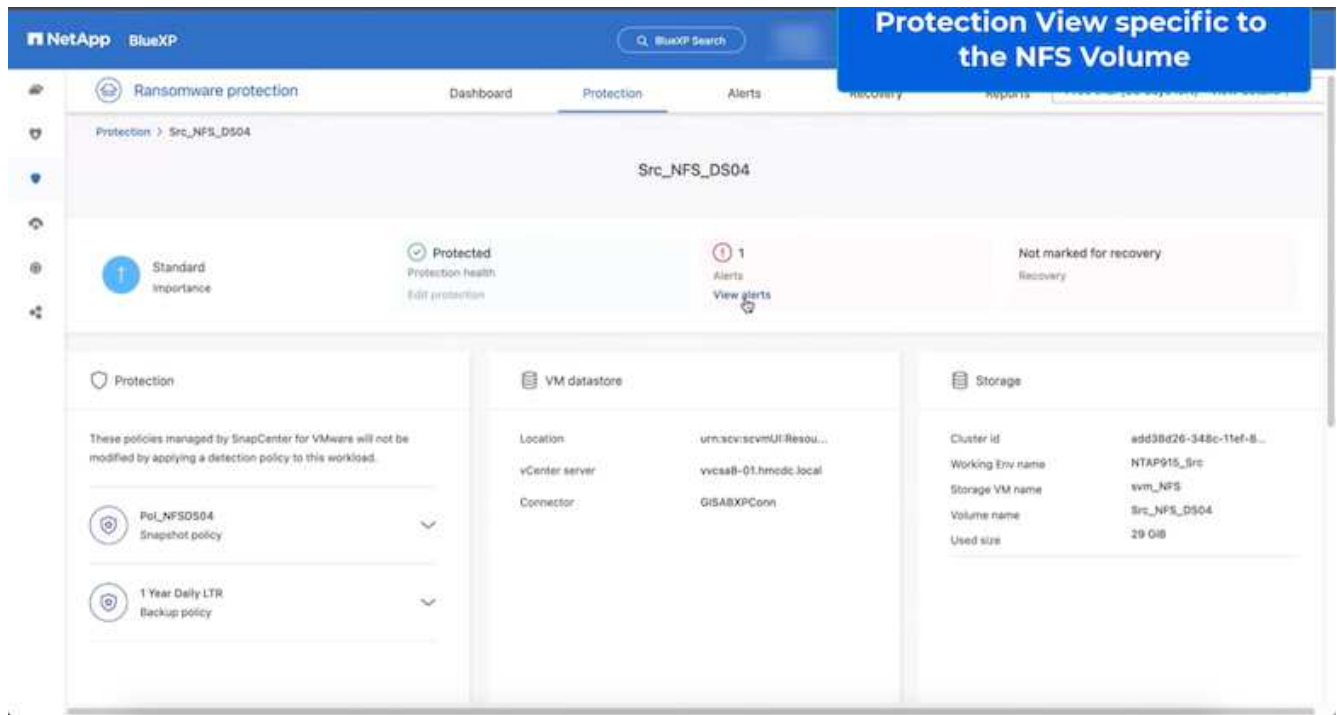


Dieser Abschnitt beschäftigt sich damit, wie der BlueXP Ransomware-Schutz die Recovery nach einem Ransomware-Vorfall orchestriert, bei dem die VM-Dateien verschlüsselt sind.

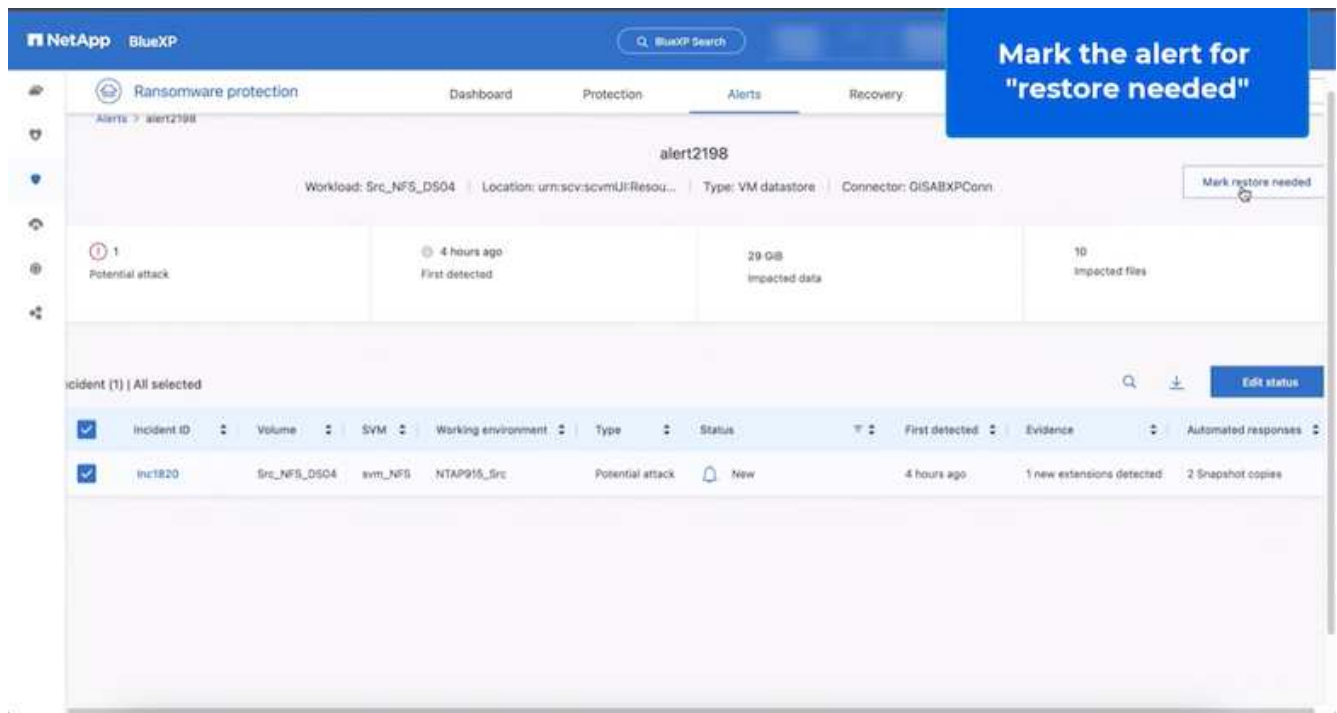


Wenn die VM durch SnapCenter gemanagt wird, stellt der BlueXP Ransomware-Schutz die VM mithilfe des VM-konsistenten Prozesses wieder in ihren vorherigen Zustand zurück.

1. Auf den BlueXP Ransomware-Schutz zugreifen und eine Warnmeldung im BlueXP Dashboard für Ransomware-Schutz erscheint.
2. Klicken Sie auf die Warnmeldung, um die Vorfälle auf diesem bestimmten Volume für die generierte Warnmeldung zu überprüfen

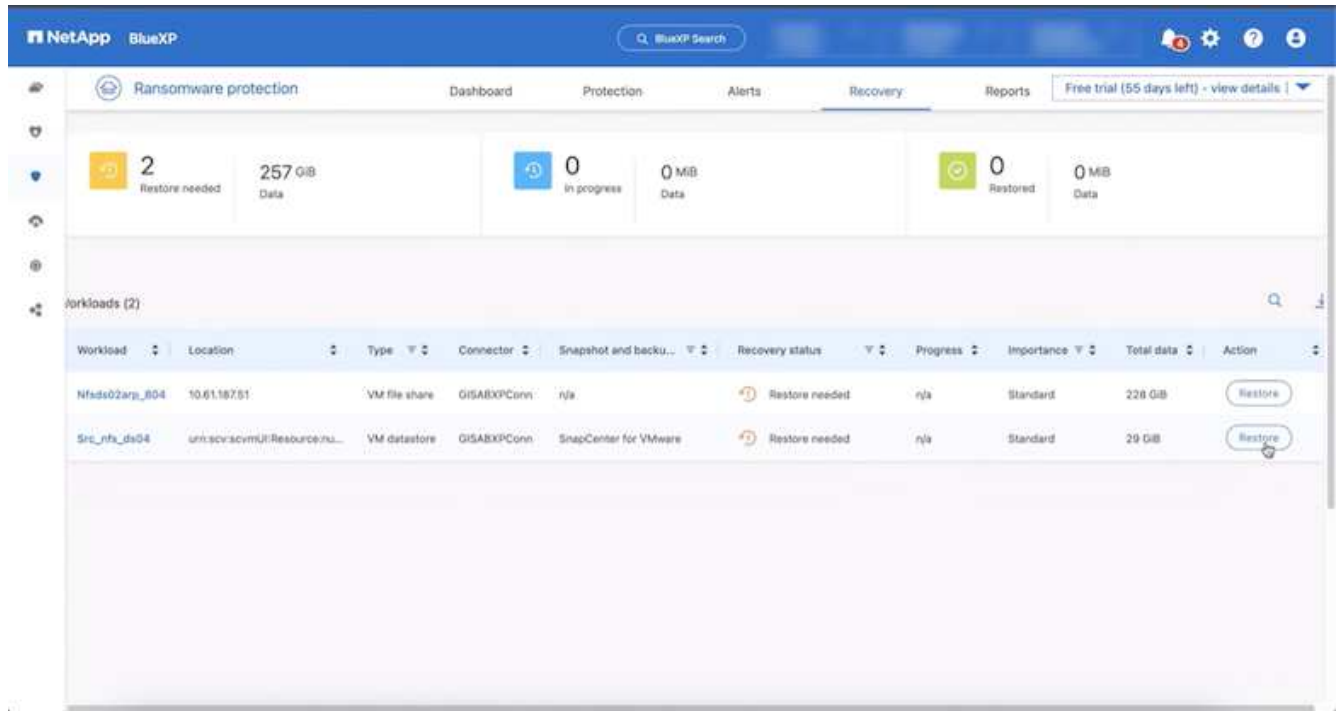


3. Markieren Sie den Ransomware-Vorfall als bereit für die Wiederherstellung (nach dem Neutralisieren von Vorfällen), indem Sie „Wiederherstellung erforderlich markieren“ auswählen.

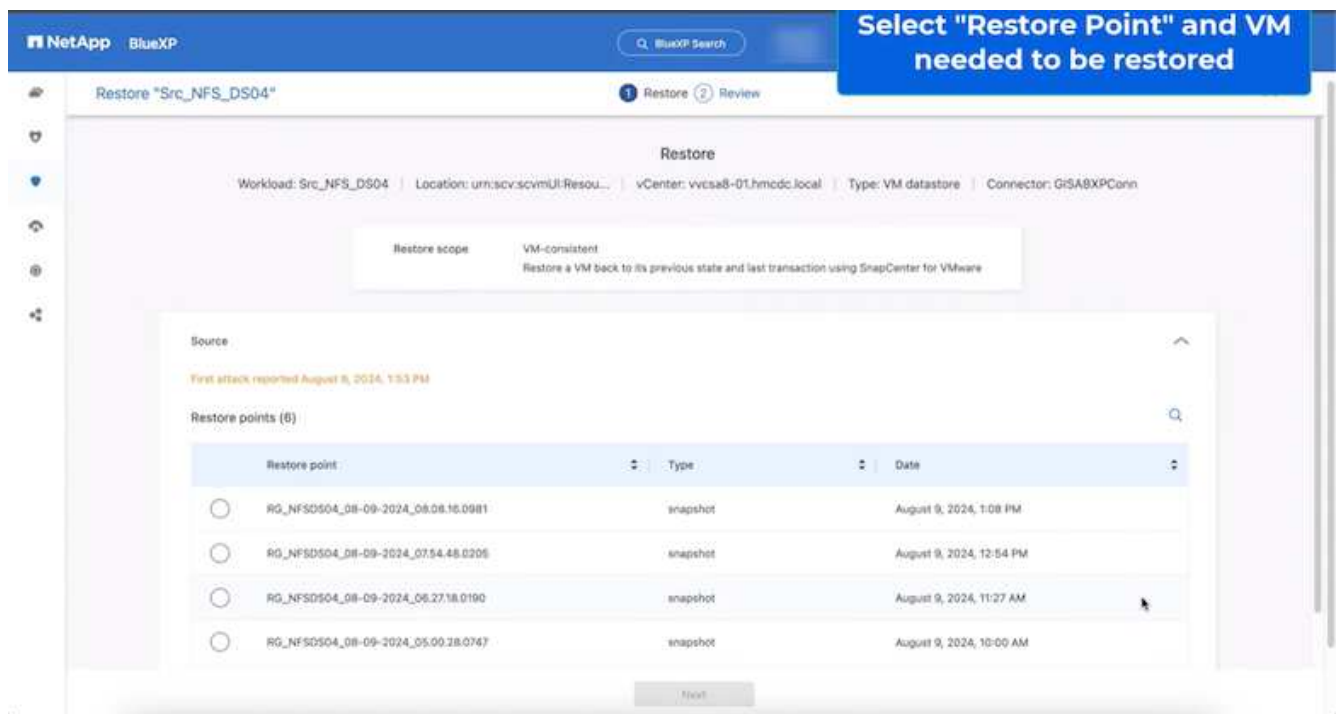


Die Warnung kann abgewiesen werden, wenn sich der Vorfall als falsch positiv herausstellt.

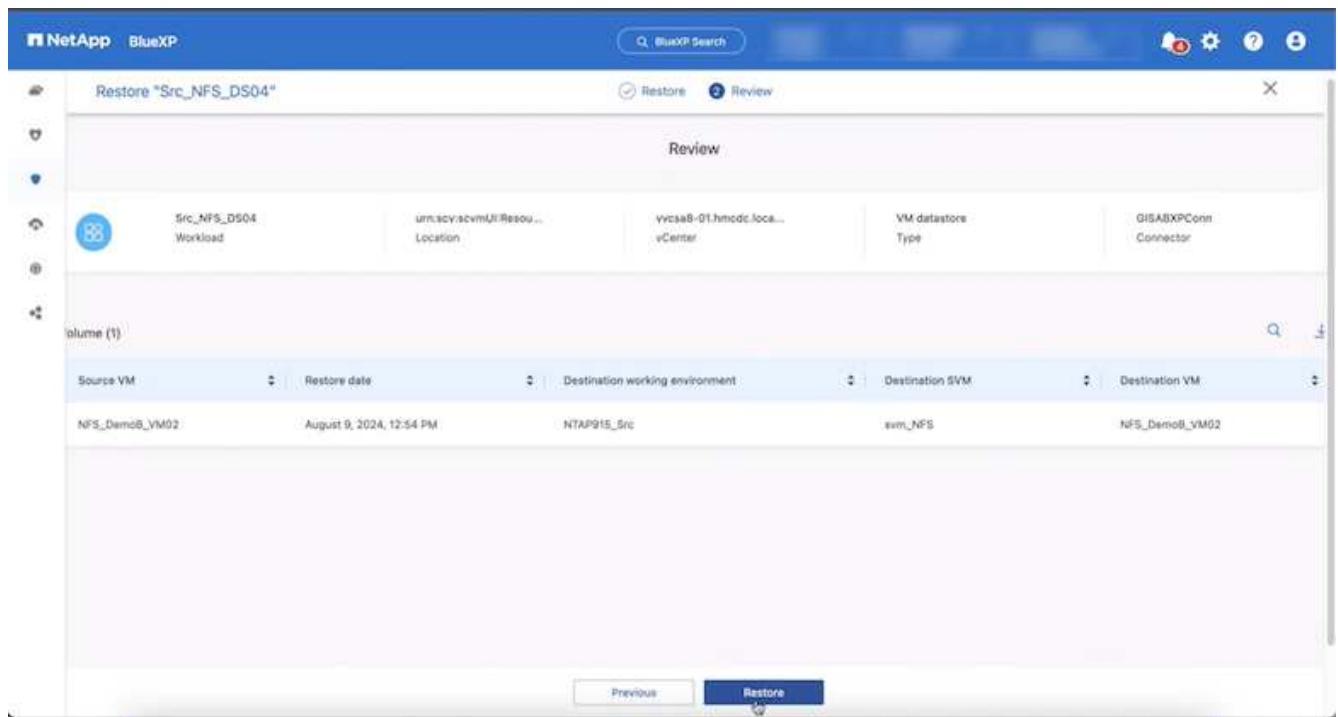
- Ging zur Registerkarte Recovery und überprüfe die Workload-Informationen auf der Recovery Seite und wähle das Datastore-Volumen aus, das sich im Status „Restore needed“ befindet, und wähle Restore aus.



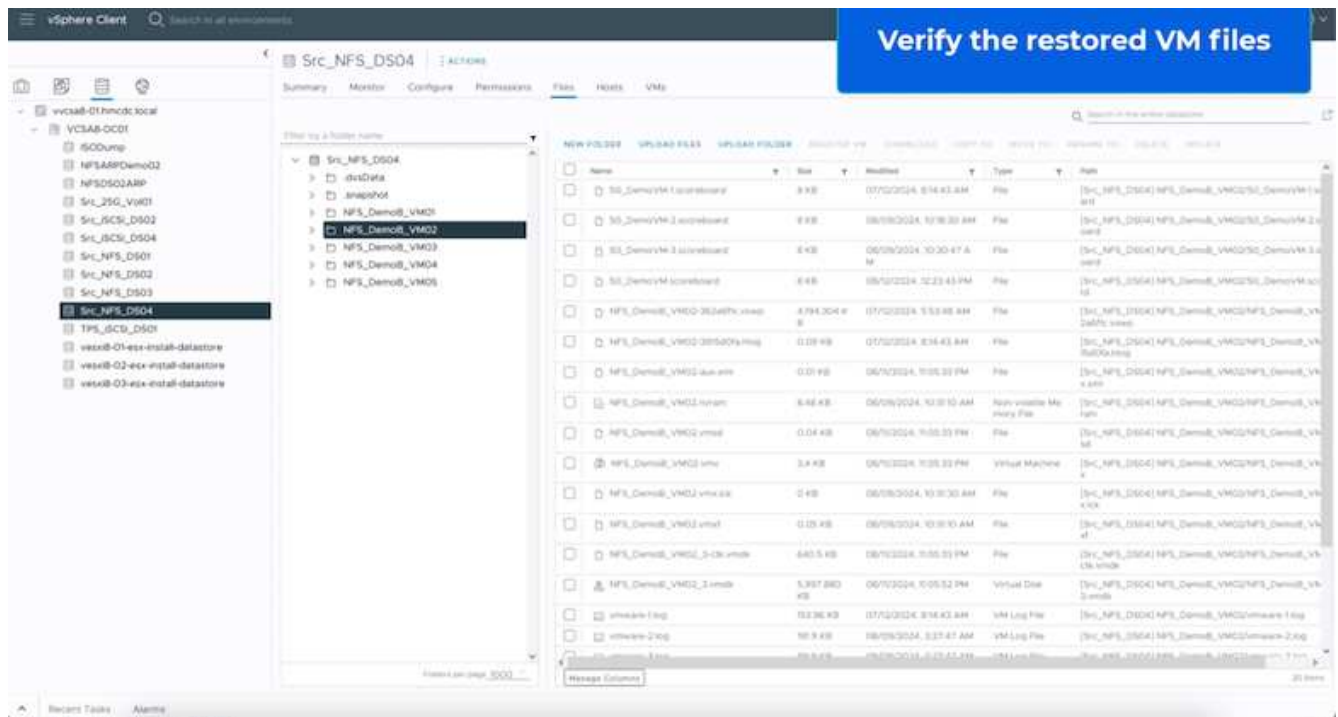
- In diesem Fall ist der Umfang der Wiederherstellung „durch VM“ (für SnapCenter für VMs ist der Umfang der Wiederherstellung „durch VM“)



- Wählen Sie den Wiederherstellungspunkt aus, mit dem die Daten wiederhergestellt werden sollen, und wählen Sie Ziel aus, und klicken Sie auf Wiederherstellen.



- Wählen Sie im oberen Menü die Option Recovery, um die Arbeitslast auf der Seite Recovery zu überprüfen, auf der sich der Status des Vorgangs durch die Zustände bewegt. Sobald die Wiederherstellung abgeschlossen ist, werden die VM-Dateien wie unten gezeigt wiederhergestellt.



Die Wiederherstellung kann von SnapCenter für VMware oder SnapCenter Plugin, je nach Anwendung durchgeführt werden.

Die NetApp Lösung bietet verschiedene effektive Tools für das Einsehen, Erkennen und Beheben von Bedrohungen. So können Sie Ransomware frühzeitig erkennen, diese Ausbreitung verhindern und bei Bedarf schnell eine Wiederherstellung durchführen, um kostspielige Ausfallzeiten zu vermeiden. Traditionelle

mehrschichtige Verteidigungslösungen sind nach wie vor weit verbreitet, ebenso wie Lösungen von Drittanbietern und Partnern für Transparenz und Erkennung. Eine effektive Gegenmaßnahmen sind nach wie vor ein wichtiger Teil der Reaktion auf Bedrohungen.

VMware Virtual Volumes mit ONTAP

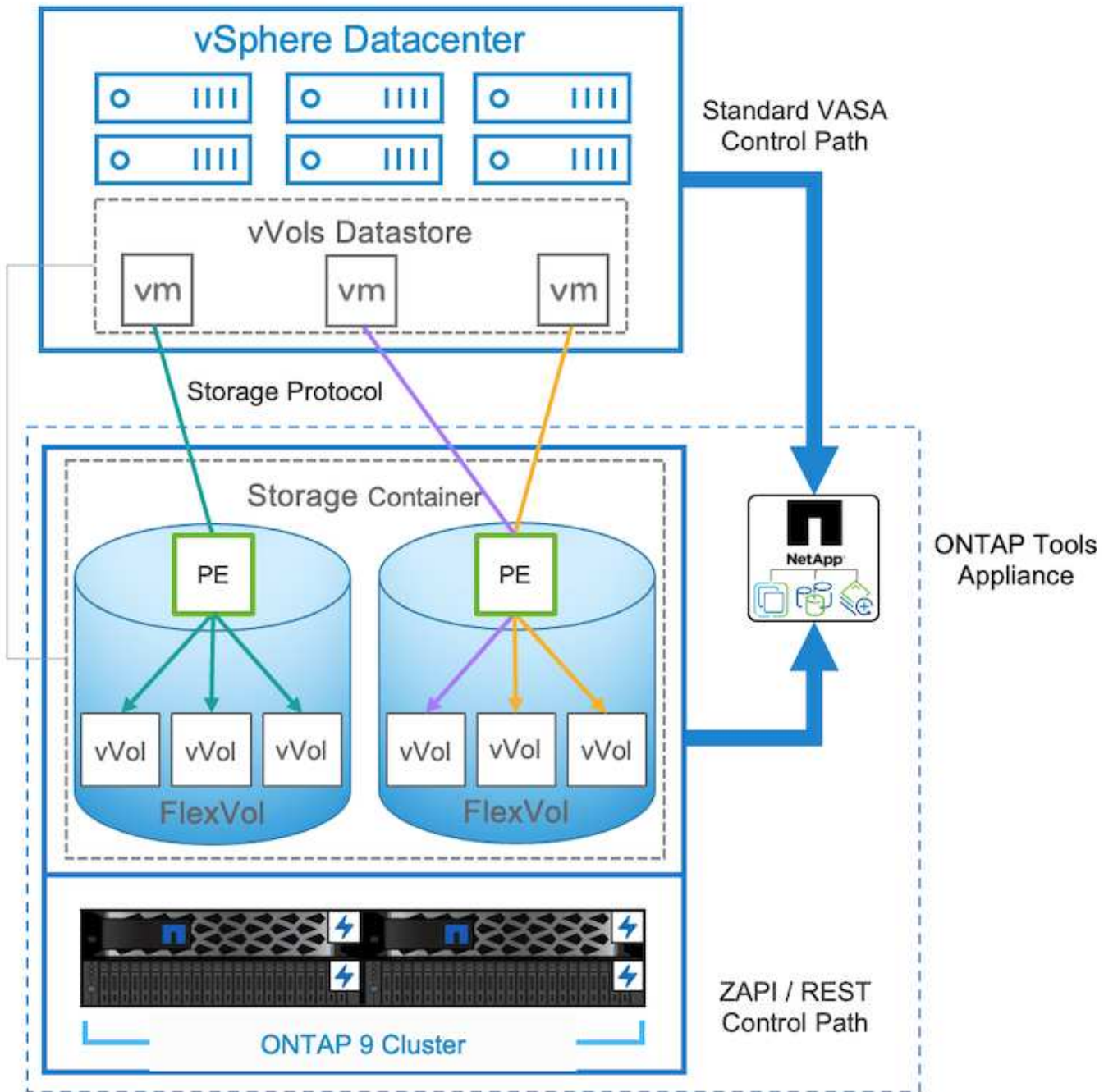
VMware Virtual Volumes (VVols) ermöglichen die Erfüllung applikationsspezifischer Anforderungen zur Grundlage von Entscheidungen für die Storage-Bereitstellung, während gleichzeitig die umfassenden Funktionen der Storage-Arrays genutzt werden können. Mit der vSphere API for Storage Awareness (VASA) können VM-Administratoren leicht alle benötigten Storage-Funktionen 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. Der VASA Provider für ONTAP ist im Rahmen von ONTAP Tools für VMware vSphere enthalten.

Vorteile von VASA Provider aus dem Storage Array:

- Eine einzelne Instanz kann mehrere Speicher-Arrays managen.
- Release-Zyklus muss nicht von der Storage OS Version abhängen.
- Ressourcen auf dem Storage Array sind sehr teuer.

Jeder vVol Datastore wird durch den Storage Container gesichert, einem logischen Eintrag im VASA Provider zur Definition der Storage-Kapazität. Der Storage Container mit ONTAP Tools wird mit ONTAP Volumes erstellt. Der Storage-Container kann durch Hinzufügen von ONTAP Volumes innerhalb derselben SVM erweitert werden.

Der Protokollendpunkt (PE) wird hauptsächlich von ONTAP-Tools verwaltet. Bei iSCSI-basierten VVols wird für jedes ONTAP Volume, das Teil dieses Storage Containers oder vVol Datastores ist, ein PE erstellt. Der PE für iSCSI ist eine kleine LUN (4 MiB für 9.x und 2 gib für 10.x), die dem vSphere-Host präsentiert wird und Multipathing-Richtlinien auf den PE angewendet werden.



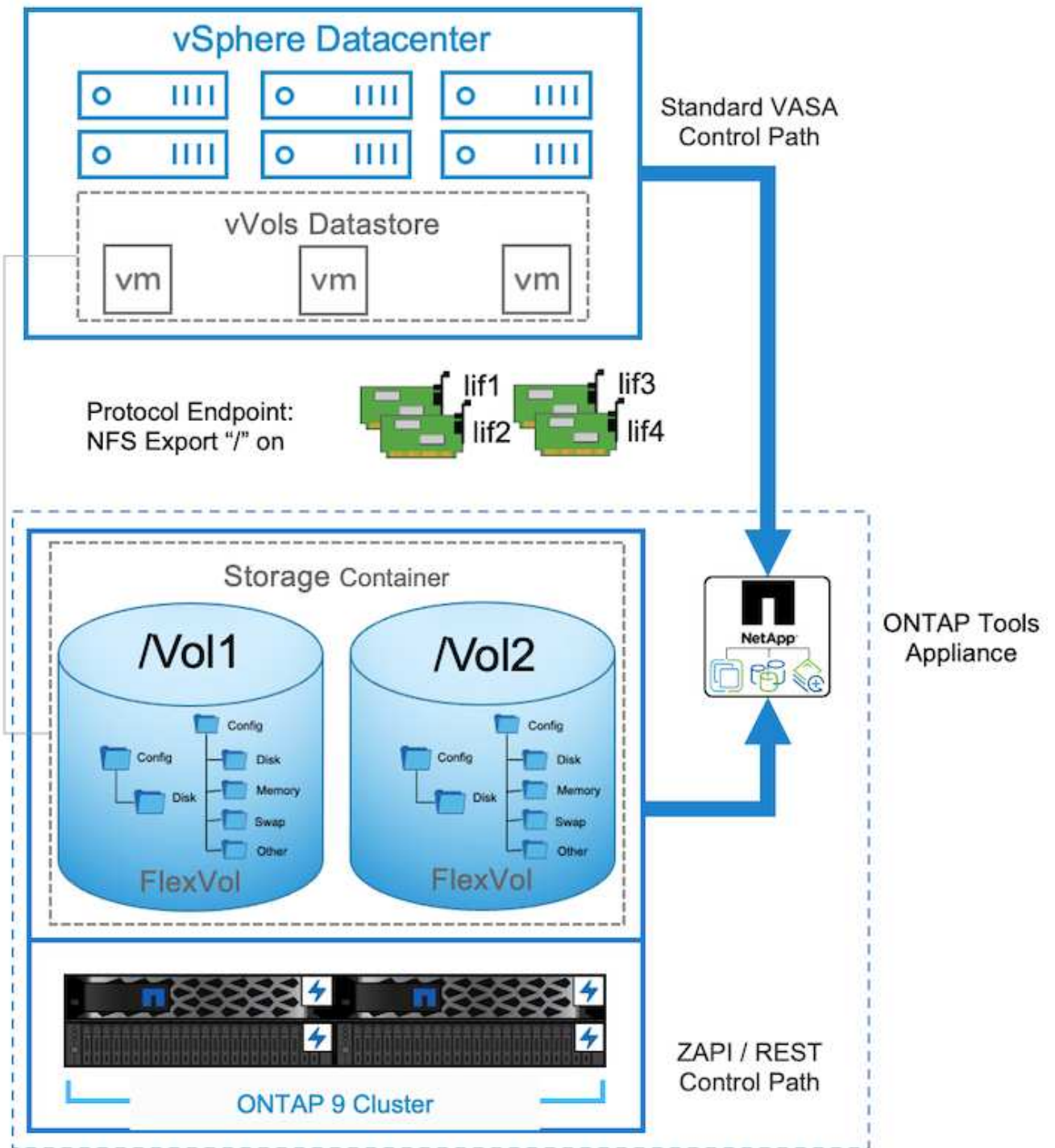
```

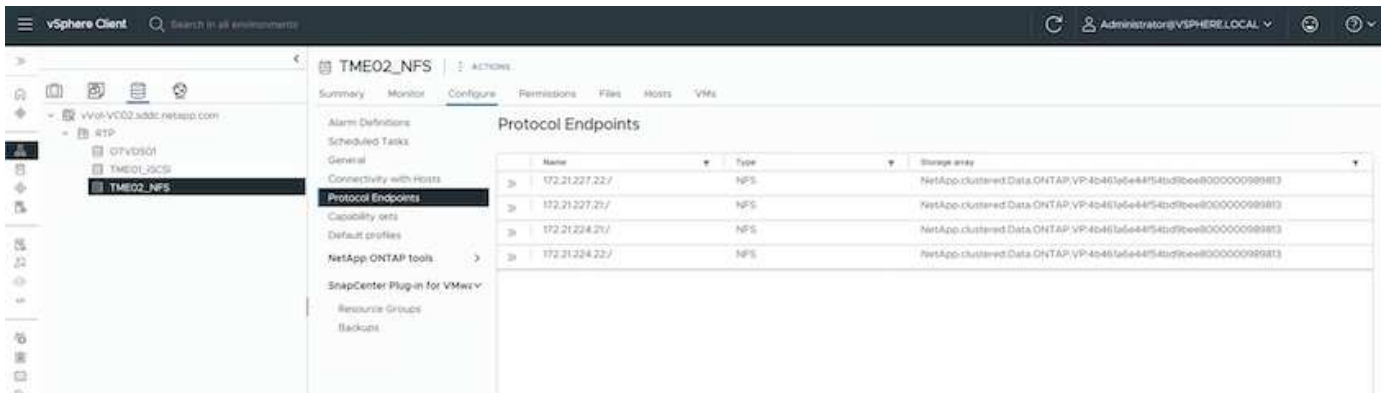
ntaphci-a300e9u25::> lun show -vserver zoneb -class protocol-endpoint -fields size
vserver path size
-----
zoneb /vol/Demo01_fv01/Demo01_fv01-vvolPE-1723681460207 2GB
zoneb /vol/Demo01_fv02/Demo01_fv02-vvolPE-1723681460217 2GB
zoneb /vol/TME01_iSCSI_01/vvolPE-1723727751956 4MB
zoneb /vol/TME01_iSCSI_02/vvolPE-1723727751970 4MB
4 entries were displayed.

```

Für NFS wird ein PE für den Export des Root-Dateisystems mit jedem NFS-Daten-LIF auf der SVM erstellt, auf

der sich der Storage-Container oder vVol-Datstore befindet.





ONTAP Tools managen den Lebenszyklus von PE und auch für die vSphere Host-Kommunikation mit vSphere-Cluster-Erweiterung und -Verkleinerung. Die ONTAP-Tools-API lässt sich in vorhandene Automatisierungs-Tools integrieren.

ONTAP Tools für VMware vSphere sind derzeit in zwei Versionen erhältlich.

ONTAP-Tools 9.x

- Wenn vVol Unterstützung für NVMe/FC erforderlich ist
- US-Bundesbehörden oder EU-Vorschriften
- Weitere Anwendungsfälle sind mit dem SnapCenter Plug-in für VMware vSphere integriert

ONTAP-Tools 10.x

- Hohe Verfügbarkeit
- Mandantenfähigkeit
- In Großem Umfang
- Unterstützung von SnapMirror Active Sync für VMFS Datastore
- Kommende Integration für bestimmte Anwendungsfälle mit dem SnapCenter Plug-in für VMware vSphere

Warum VVols?

VMware Virtual Volumes (VVols) bietet die folgenden Vorteile:

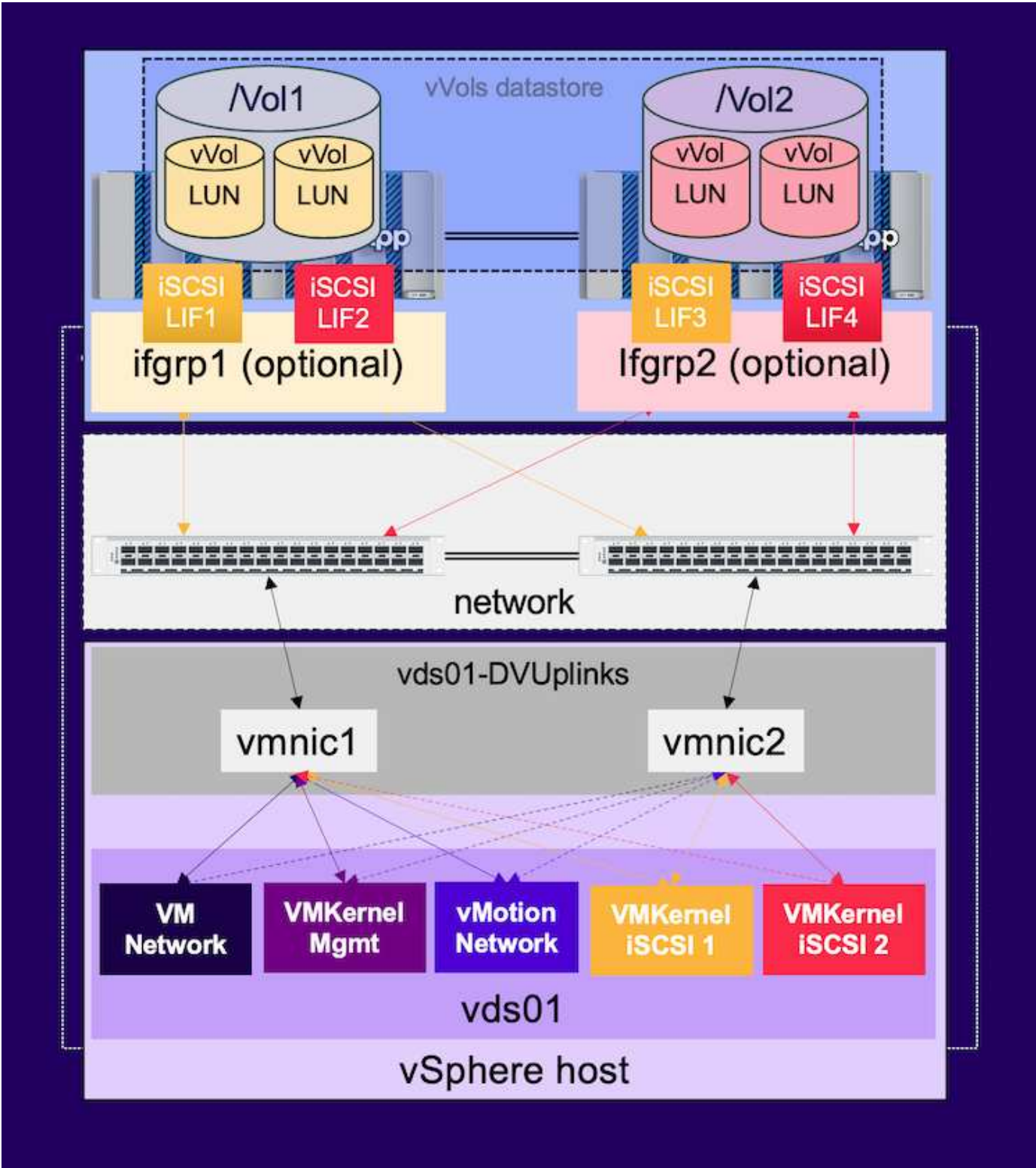
- Vereinfachte Bereitstellung (keine Sorge wegen maximaler LUN-Limits pro vSphere Host oder Erstellung der NFS-Exporte für jedes Volume erforderlich)
- Minimiert die Anzahl der iSCSI-/FC-Pfade (für blockbasiertes SCSI-basiertes vVol)
- Snapshots, Klone und andere Storage-Prozesse werden in der Regel auf das Storage-Array verlagert und liefern wesentlich schnellere Performance.
- Vereinfachte Datenmigrationen für die VMs (keine Koordinierung mit anderen VM-Inhabern in derselben LUN erforderlich)
- QoS-Richtlinien werden auf VM-Festplattenebene statt auf Volume-Ebene angewendet.
- Benutzerfreundlichkeit (Storage-Anbieter bieten unterschiedliche Funktionen im VASA Provider)
- Unterstützung einer großen VM-Skalierung.
- VVol-Replikationsunterstützung für die Migration zwischen vCenter.

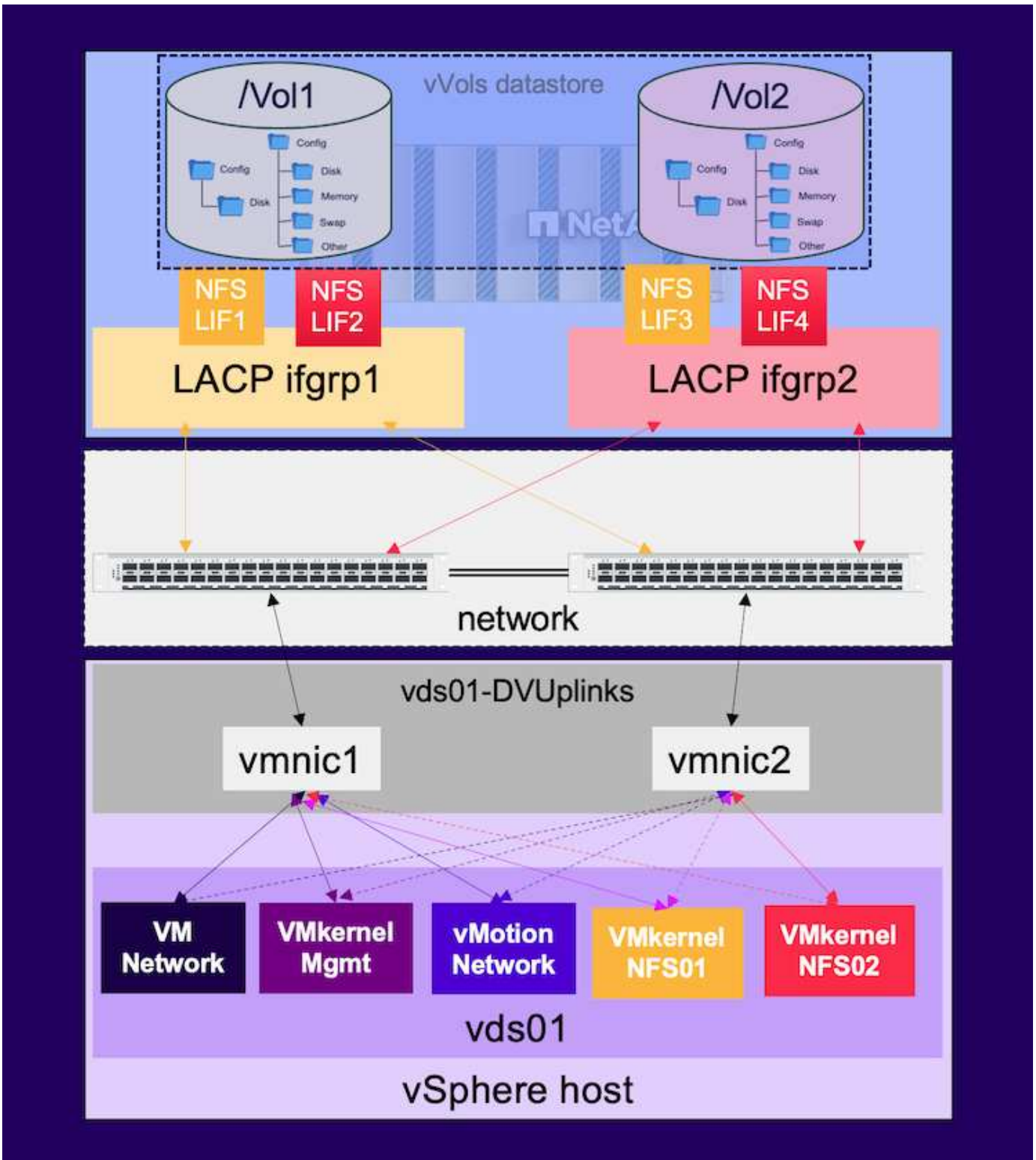
- Speicheradministratoren haben die Möglichkeit, auf VM-Festplattenebene zu überwachen.

Konnektivitätsoptionen

Eine Dual-Fabric-Umgebung wird in der Regel für Storage-Netzwerke empfohlen, um Hochverfügbarkeit, Performance und Fehlertoleranz zu gewährleisten. Die VVols werden mit iSCSI, FC, NFSv3 und NVMe/FC unterstützt. HINWEIS: Weitere "[Interoperabilitäts-Matrix-Tool \(IMT\)](#)" Informationen finden Sie unter Unterstützte Version des ONTAP-Tools

Die Konnektivitätsoption bleibt konsistent mit den Optionen für VMFS-Datastore oder NFS-Datastore. Im Folgenden ist ein Beispiel für ein vSphere-Referenznetzwerk für iSCSI und NFS aufgeführt.





Bereitstellung mit ONTAP Tools für VMware vSphere

Der vVol Datastore kann mithilfe von ONTAP Tools ähnlich wie VMFS oder NFS Datastore bereitgestellt werden. Wenn das Plug-in für ONTAP-Tools auf der vSphere Client-Benutzeroberfläche nicht verfügbar ist, lesen Sie den Abschnitt „erste Schritte“ weiter unten.

Mit ONTAP-Tools 9.13

1. Klicken Sie mit der rechten Maustaste auf vSphere Cluster oder Host und wählen Sie unter NetApp ONTAP Tools die Option Provisioning Datastore aus.
2. Behalten Sie den Typ als VVols bei, geben Sie einen Namen für den Datastore ein und wählen Sie das gewünschte Protokoll aus

The screenshot shows the 'New Datastore' wizard in NetApp ONTAP Tools. The left sidebar contains a navigation menu with four items: '1 General' (selected), '2 Storage system', '3 Storage attributes', and '4 Summary'. The main area is titled 'General' and contains the following fields:

- Provisioning destination:** Cluster01 (with a BROWSE button to the right)
- Type:** Radio buttons for NFS, VMFS, and vVols (vVols is selected).
- Name:** TME01_ISCSI
- Description:** An empty text box.
- Protocol:** Radio buttons for NFS, ISCSI (selected), FC / FCoE, and NVMe/FC.

At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

The screenshot shows the 'New Datastore' wizard in NetApp ONTAP Tools. The left sidebar contains a navigation menu with four items: '1 General' (selected), '2 Storage system', '3 Storage attributes', and '4 Summary'. The main area is titled 'General' and contains the following fields:

- Provisioning destination:** Cluster01 (with a BROWSE button to the right)
- Type:** Radio buttons for NFS, VMFS, and vVols (vVols is selected).
- Name:** TME02_NFS
- Description:** An empty text box.
- Protocol:** Radio buttons for NFS (selected), ISCSI, FC / FCoE, and NVMe/FC.

At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

3. Wählen Sie das gewünschte Storage-Funktionsprofil aus und wählen Sie das Storage-System und die SVM aus.

New Datastore

- 1 General
- 2 Storage system**
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles: **Default profiles**

- Platinum_AFF_A
- Platinum_AFF_C
- Platinum_ASA_A
- Platinum_ASA_C

[Create storage capability profile](#)

Storage system:

Storage VM:

[CANCEL](#) [BACK](#) [NEXT](#)

4. Erstellen Sie neue ONTAP Volumes oder wählen Sie vorhandene für den vVol Datastore aus.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes**
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
TME01_ISCSI_01	250 GB	Platinum_AFF_A	EHCAGgr01
TME01_ISCSI_02	250 GB	Platinum_AFF_A	EHCAGgr02

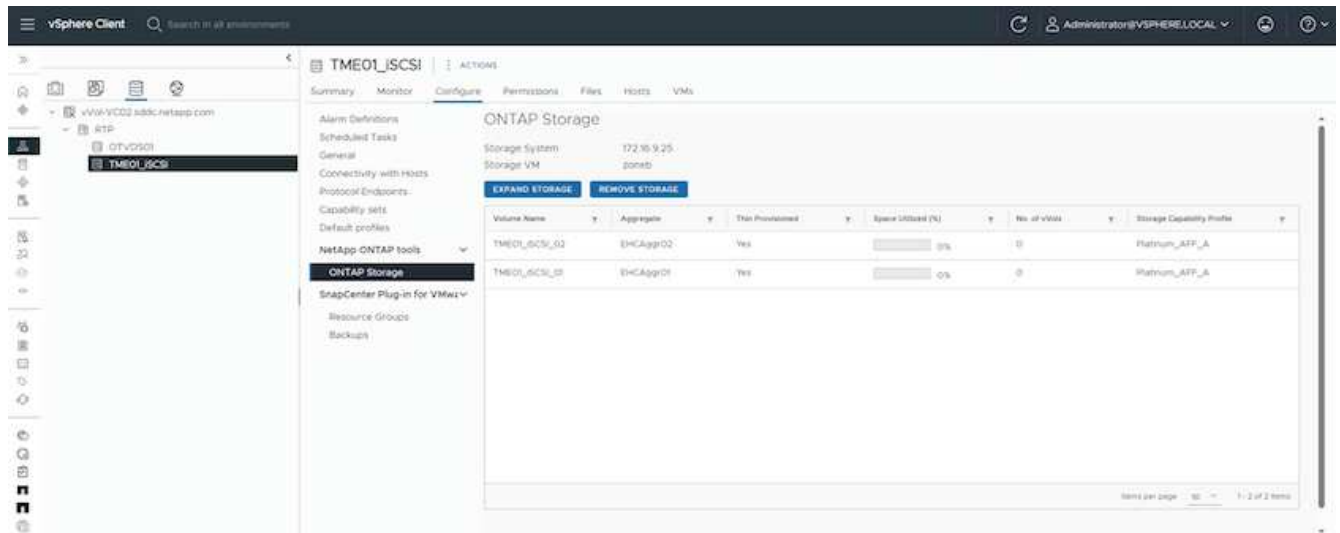
1 - 2 of 2 items

Name	Size(GB)	Storage capability profile	Aggregates	Space reserve
<input type="text"/>	<input type="text"/>	<input type="text" value="Platinum_AFF_A"/>	<input type="text" value="EHCAGgr02 - (17109.63 Gi)"/>	<input type="text" value="Thin"/>

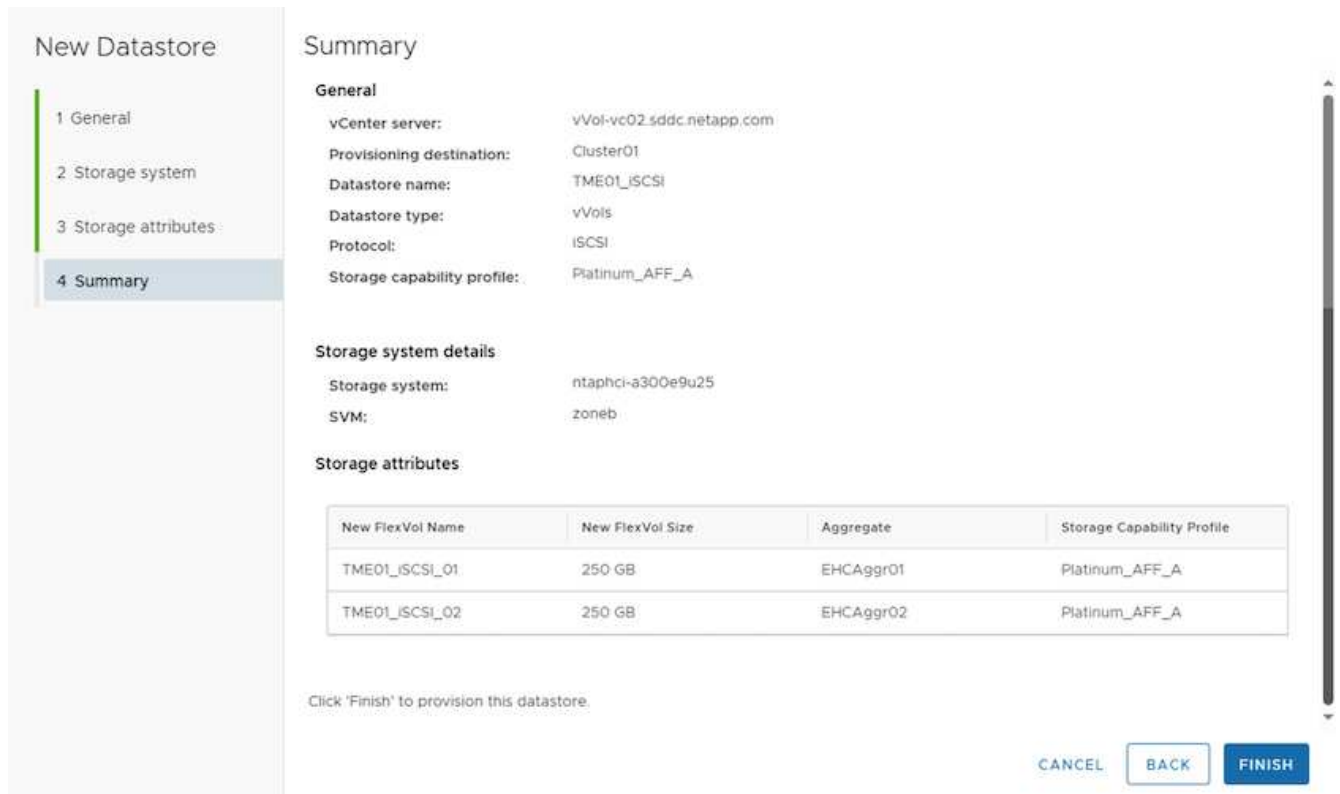
[ADD](#)

[CANCEL](#) [BACK](#) [NEXT](#)

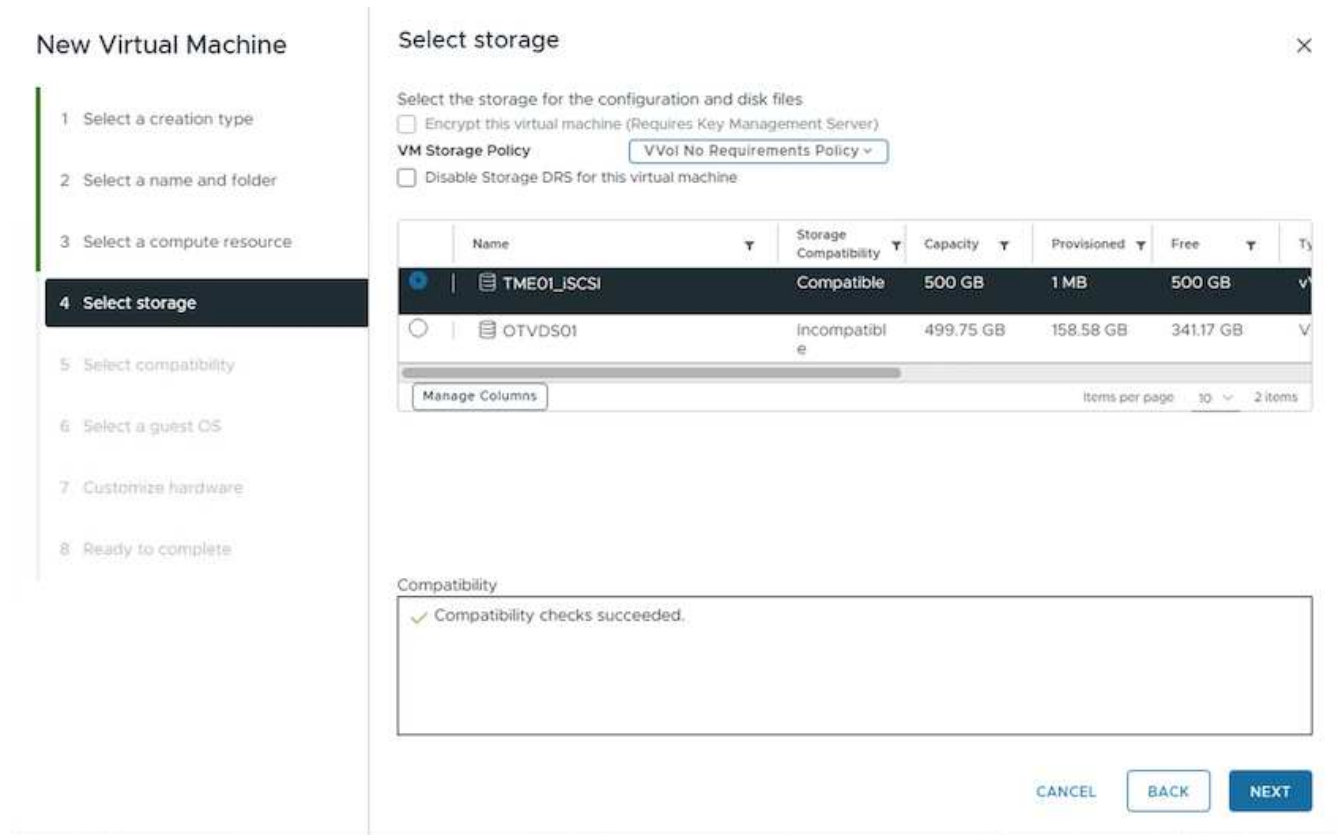
ONTAP Volumes können über die Datastore-Option angezeigt oder später geändert werden.



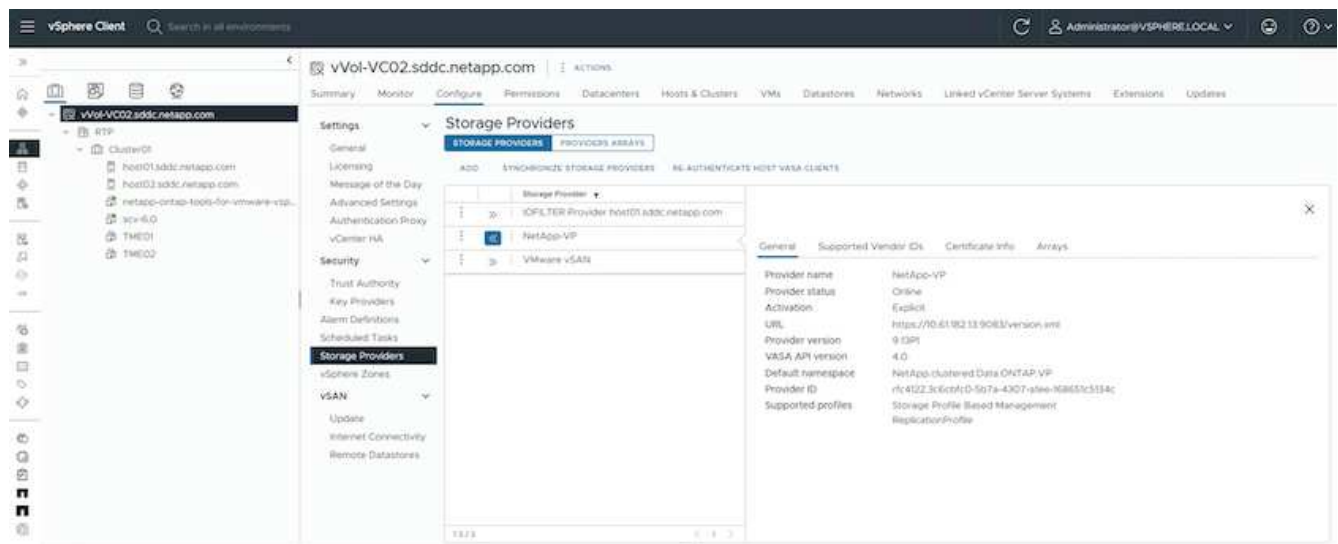
5. Überprüfen Sie die Zusammenfassung, und klicken Sie auf Fertig stellen, um den vVol-Datstore zu erstellen.



6. Sobald ein vVol Datastore erstellt wurde, kann dieser wie jeder andere Datastore verwendet werden. Dies ist ein Beispiel für die Zuweisung von Datastores auf Basis der VM-Storage-Richtlinie zu einer VM, die erstellt wird.



7. VVol-Details können über eine webbasierte CLI-Schnittstelle abgerufen werden. Die URL des Portals ist identisch mit der URL des VASA-Providers ohne den Dateinamen Version.XML.



Die Anmeldeinformationen sollten mit den Informationen übereinstimmen, die bei der Bereitstellung von ONTAP-Tools verwendet werden

← ↻ Not secure | https://10.61.182.13:9083/jsp/login.jsp

- Welcome to VASA Client Login
- Username* administrator
- Password *
- Token *
-

▼ Where can I find Token

You can generate Token by logging into maint console.
In main menu
Select option 1) **Application Configuration**
Select option 12) **Generate Web-Cli Authentication token**

Oder verwenden Sie das aktualisierte Passwort mit der Wartungskonsole der ONTAP Tools.

Application Configuration Menu:

- 1) Display server status summary
 - 2) Start Virtual Storage Console service
 - 3) Stop Virtual Storage Console service
 - 4) Start VASA Provider and SRA service
 - 5) Stop VASA Provider and SRA service
 - 6) Change 'administrator' user password
 - 7) Re-generate certificates
 - 8) Hard reset database
 - 9) Change LOG level for Virtual Storage Console service
 - 10) Change LOG level for VASA Provider and SRA service
 - 11) Display TLS configuration
 - 12) Generate Web-CLI Authentication token
 - 13) Start ONTAP tools plug-in service
 - 14) Stop ONTAP tools plug-in service
 - 15) Start Log Integrity service
 - 16) Stop Log Integrity service
 - 17) Change database password
-
- b) Back
 - x) Exit

Enter your choice: 12

Starting token creation
Your webcli auth token is :668826

This token is for one time use only. Its valid for 20 minutes.

Press ENTER to continue.

Wählen Sie die webbasierte CLI-Schnittstelle aus.

NetApp ONTAP tools for VMware vSphere - Control Panel:

Operation	Description
Web based CLI interface	Web based access to the command line interface for administrative tasks
Inventory	Listing of all objects and information currently known in Unified Virtual Appliance database
Statistics	Listing of all counters and information regarding internal state
Right Now	See what operations are in flight right now
Logout	Logout

Build Release 9.13P1
Build Timestamp 03/08/2024 11:11:42 AM
System up since Thu Aug 15 02:23:18 UTC 2024
Current time Thu Aug 15 17:59:26 UTC 2024

Geben Sie den gewünschten Befehl aus der Liste der verfügbaren Befehle ein. Um Details zu vVol und Informationen zum zugrunde liegenden Storage aufzulisten, versuchen Sie es mit `vvol list -verbose=true`

```

Command: vvol list --verbose=true [Execute]
Executed:
vvol list --verbose=true
Returned:
[{"id":"naa.600a0980383043595a2b506b67783041", "metadta": {"StorageLocation": "172.18.9.25[zoneb] TME01_iSCSI_01", "Path": "/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk", "BindInformation": {"KeyValuePair": [{"Key": "VolumeName", "Value": "vvol1"}, {"Key": "VolumePath", "Value": "/vol/naa.600a0980383043595a2b506b67783041"}]}}, "size": 255, "comment": "TME01.vmdk - DATA"}, {"id":"naa.600a0980383043595a2b506b67783042", "metadta": {"StorageLocation": "172.18.9.25[zoneb] TME01_iSCSI_01", "Path": "/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk", "BindInformation": {"KeyValuePair": [{"Key": "VolumeName", "Value": "vvol2"}, {"Key": "VolumePath", "Value": "/vol/naa.600a0980383043595a2b506b67783042"}]}}, "size": 16, "comment": "TME01.vmdk - METADATA"}, {"id":"naa.600a0980383043595a2b506b67783043", "metadta": {"StorageLocation": "172.18.9.25[zoneb] TME01_iSCSI_01", "Path": "/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk", "BindInformation": {"KeyValuePair": [{"Key": "VolumeName", "Value": "vvol3"}, {"Key": "VolumePath", "Value": "/vol/naa.600a0980383043595a2b506b67783043"}]}}, "size": 16, "comment": "TME01.vmdk - DATA"}, {"id":"naa.600a0980383043595a2b506b67783044", "metadta": {"StorageLocation": "172.18.9.25[zoneb] TME01_iSCSI_01", "Path": "/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783044.vmdk", "BindInformation": {"KeyValuePair": [{"Key": "VolumeName", "Value": "vvol4"}, {"Key": "VolumePath", "Value": "/vol/naa.600a0980383043595a2b506b67783044"}]}}, "size": 16, "comment": "TME01.vmdk - DATA"}, {"id":"naa.600a0980383043595a2b506b67783045", "metadta": {"StorageLocation": "172.18.9.25[zoneb] TME01_iSCSI_01", "Path": "/vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783045.vmdk", "BindInformation": {"KeyValuePair": [{"Key": "VolumeName", "Value": "vvol5"}, {"Key": "VolumePath", "Value": "/vol/naa.600a0980383043595a2b506b67783045"}]}}, "size": 255, "comment": "TME01 - METADATA"}]

```

für LUN-basiert. Es können auch die ONTAP cli oder System Manager verwendet werden.

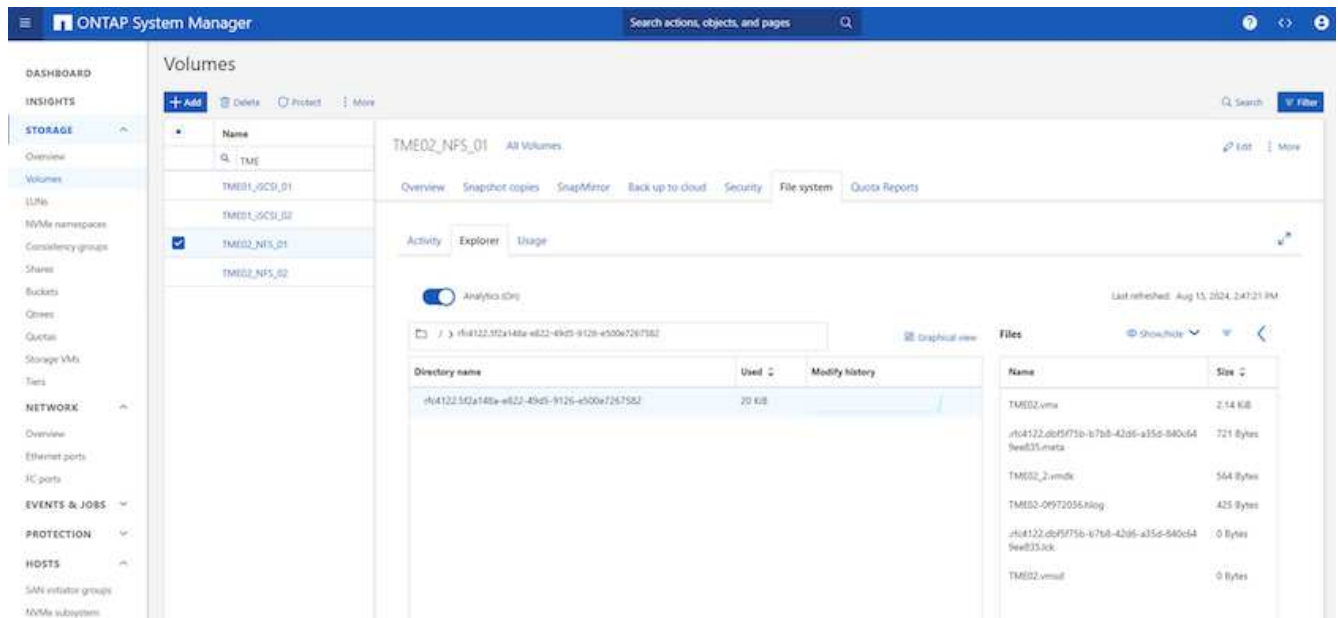
```

vserver path
-----
zoneb /vol/Demo01_fv01/naa.600a0980383043595a2b506b67783038.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683735.vmdk 255GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683736.vmdk 16GB
zoneb /vol/Demo01_fv02/naa.600a098038304359463f515057683737.vmdk 16GB
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783041.vmdk
255GB TME01 - METADATA
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783042.vmdk
16GB TME01.vmdk - DATA
zoneb /vol/TME01_iSCSI_01/naa.600a0980383043595a2b506b67783043.vmdk
16GB TME01.vmdk - DATA

```

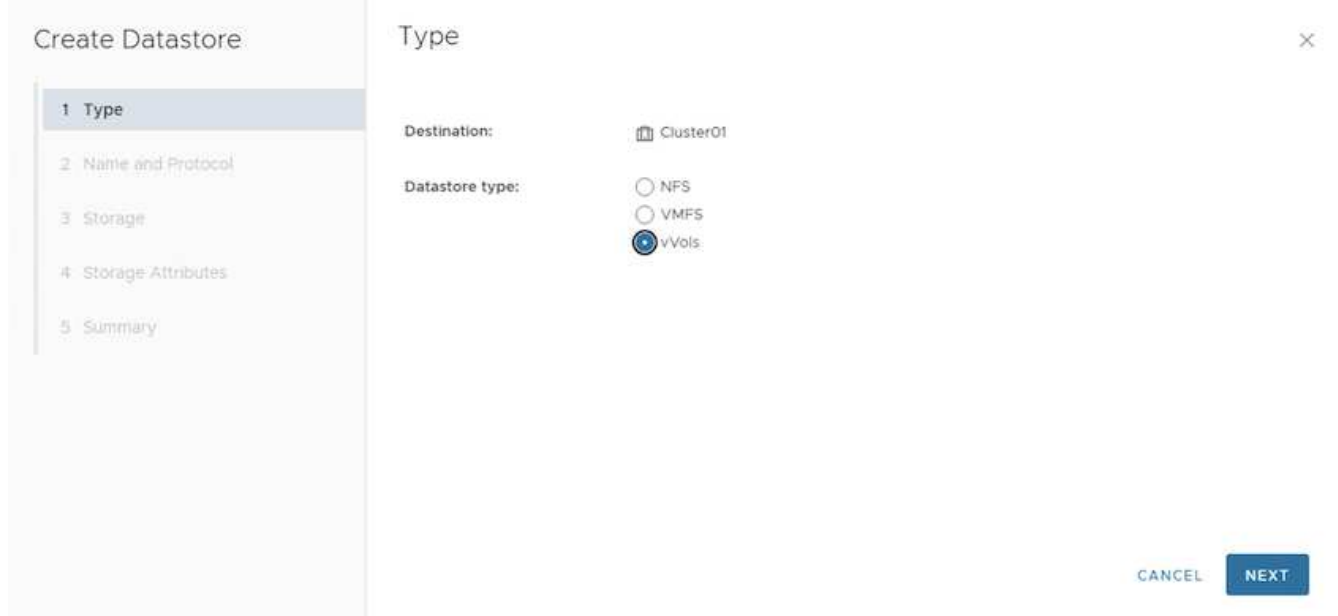
Name	Storage VM	Volume	Size	IOPS	Latency (ms)	Throughput (MB/s)
naa.600a0980383043595a2b506b67783041.vmdk	zoneb	TME01_iSCSI_01	255 GB	0	0	0
naa.600a0980383043595a2b506b67783042.vmdk	zoneb	TME01_iSCSI_01	16 GB	-	-	-
naa.600a0980383043595a2b506b67783043.vmdk	zoneb	TME01_iSCSI_01	16 GB	0	0	0
naa.600a0980383043595a2b506b67783044.vmdk	zoneb	TME01_iSCSI_01	16 GB	0	0	0
naa.600a0980383043595a2b506b67783045.vmdk	zoneb	TME01_iSCSI_01	255 GB	0	0	0

Bei NFS-basiertem System Manager kann der Datenspeicher durchsucht werden.

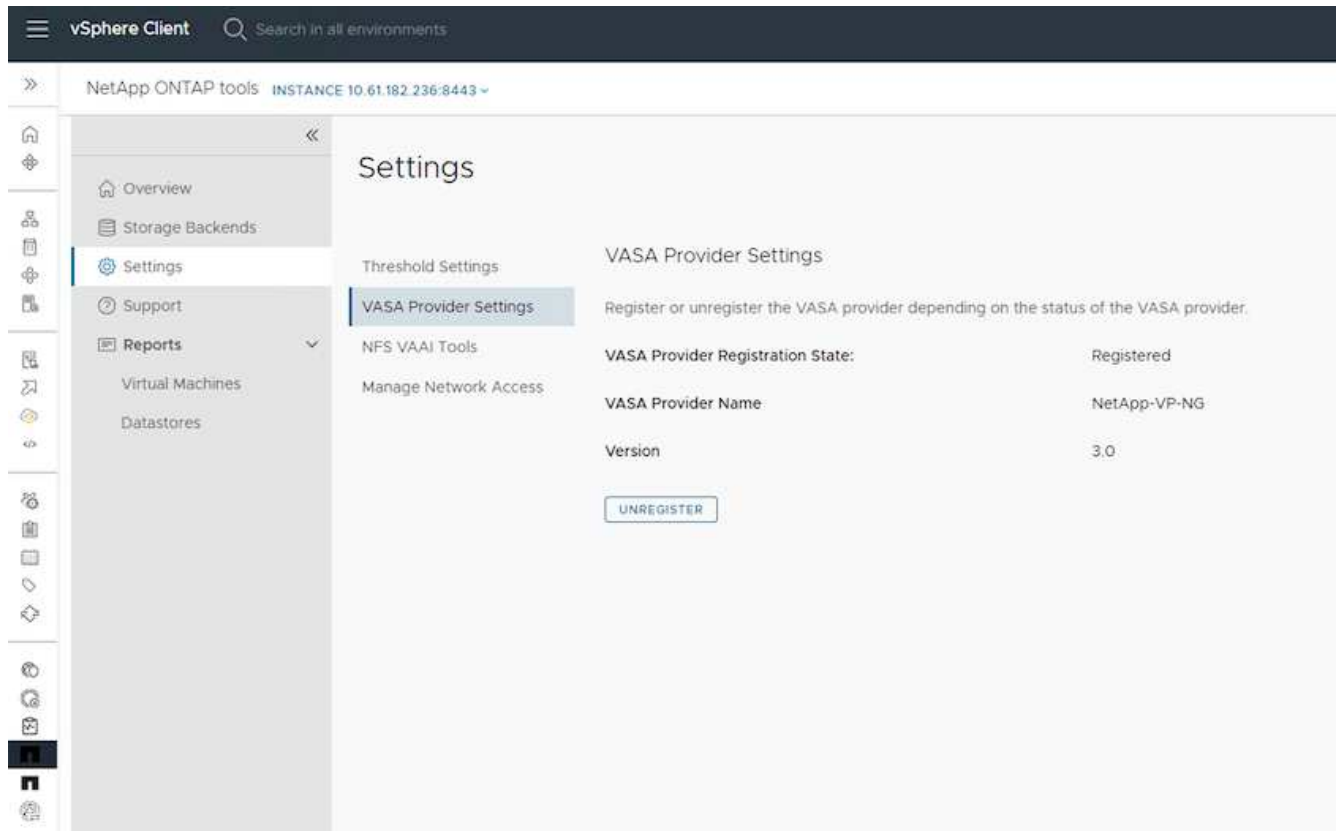


Mit ONTAP-Tools 10.1

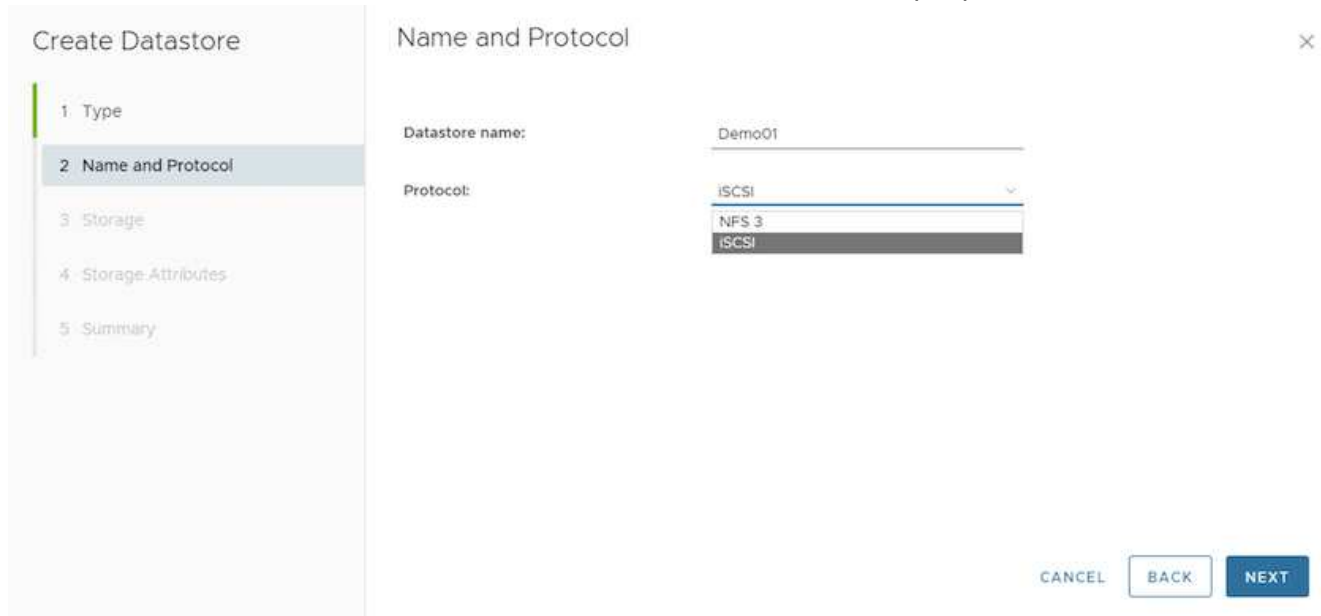
1. Klicken Sie mit der rechten Maustaste auf vSphere Cluster oder Host und wählen Sie unter NetApp ONTAP Tools Create Datastore (10.1) aus.
2. Wählen Sie den Datastore-Typ als VVols aus.



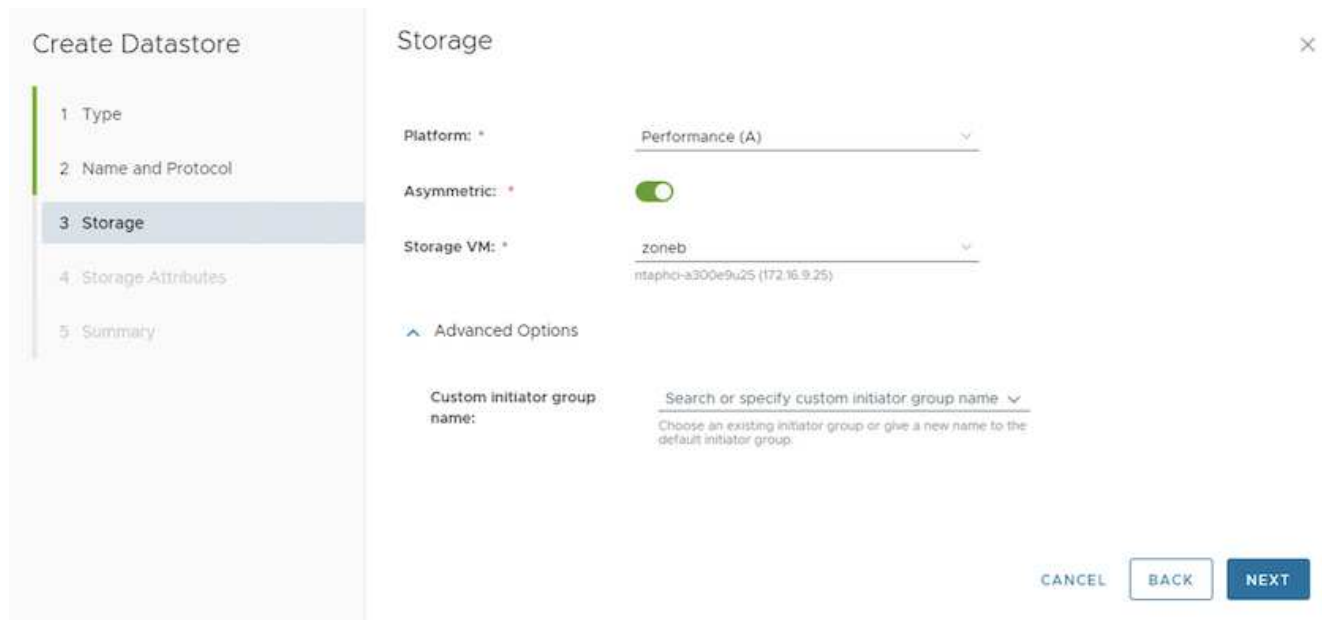
Wenn die VVols-Option nicht verfügbar ist, vergewissern Sie sich, dass der VASA-Provider registriert ist.



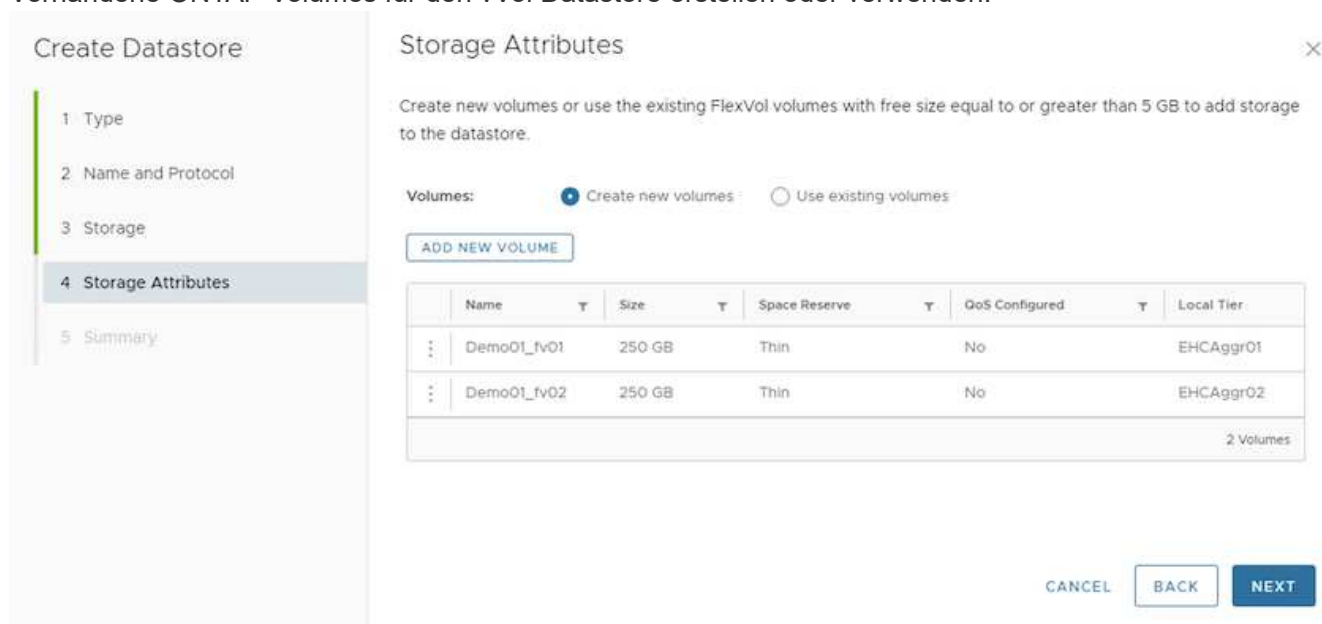
3. Geben Sie den Namen des vVol-Datastore an, und wählen Sie das Transportprotokoll aus.



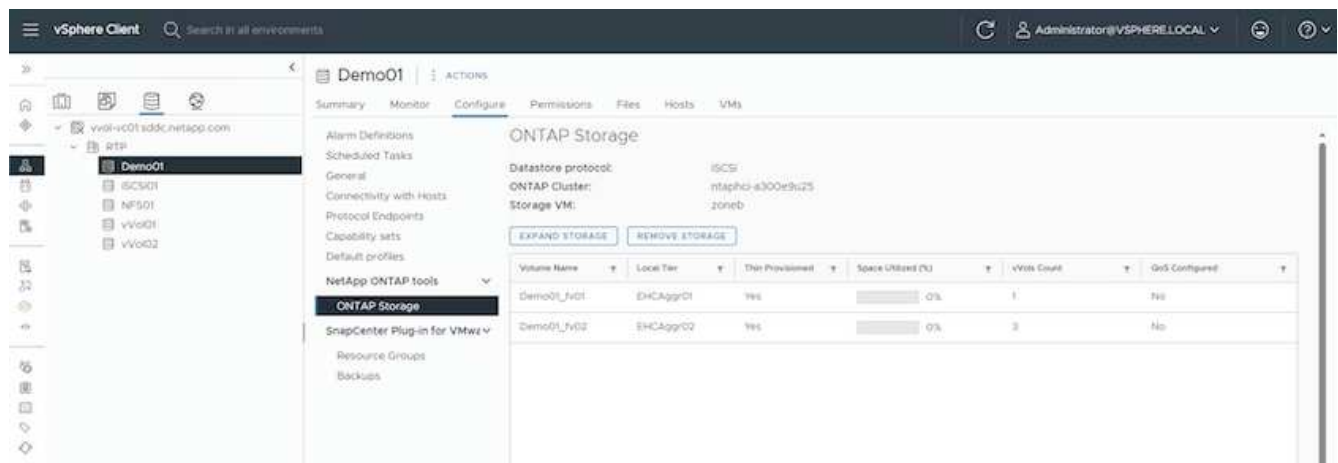
4. Wählen Sie Plattform und Storage VM aus.



5. Vorhandene ONTAP Volumes für den vVol Datastore erstellen oder verwenden.



ONTAP Volumes können zu einem späteren Zeitpunkt aus der Datastore-Konfiguration angezeigt oder aktualisiert werden.



6. Nachdem der vVol Datastore bereitgestellt wurde, kann er ähnlich wie jeder andere Datastore verwendet

werden.

7. ONTAP Tools stellen den Bericht zu VM und Datenspeicher bereit.

The first screenshot shows the 'Virtual Machines' report. The table lists three VMs: 'scv', 'Demo01', and 'Demo02'. The 'scv' VM is running on VMFS storage, while 'Demo01' and 'Demo02' are on vVols. The 'scv' VM has a high disk latency of 189 µs and a throughput of 10.89 KB/s. The 'Demo01' VM has a latency of 53 µs and a throughput of 86 Bytes/s. The 'Demo02' VM has a latency of 0 µs and a throughput of 0 Bytes/s.

VM Name	Primary Datastore Type	Primary Datastore Name	vCenter VM Latency	Max Datastore Latency	Total Datastore IOPS	Average Datastore Throughput	Total Datastore Capacity	Uptime	Power State	vCenter VM Committed Capacity
scv	VMFS	scv001	0 ms	189 µs	3	10.89 KB/s	37.27%	16 hours	On	96 GB OS
Demo01	vVol	Demo01	-	53 µs	1	86 Bytes/s	0.03%	-	Off	287 GB
Demo02	vVol	vVol02	-	0 µs	0	0 Bytes/s	0.01%	-	Off	271 GB

The second screenshot shows the 'Datastores' report. The table lists five datastores: 'scv001', 'NF001', 'vVol01', 'vVol02', and 'Demo01'. The 'scv001' datastore is VMFS and is 37.21% full. The 'NF001' datastore is NFS and is 0.01% full. The 'vVol01' and 'vVol02' datastores are vVols and are 3.02% and 5.01% full, respectively. The 'Demo01' datastore is vVol and is 5.03% full.

Name	Space Utilized (%)	Type	IOPS	Latency	Throughput	Storage VM	Storage Controller
scv001	37.21%	VMFS	3	189 µs	10.89 KB/s	scv	ntaprci-4300w9u25
NF001	0.01%	NFS	0	297 µs	21 Bytes/s	demo	ntaprci-4300w9u25
vVol01	3.02%	vVol	2	48 µs	81 Bytes/s	demo	ntaprci-4300w9u25
vVol02	5.01%	vVol	0	0 µs	0 Bytes/s	demo	ntaprci-4300w9u25
Demo01	5.03%	vVol	1	53 µs	86 Bytes/s	demo	ntaprci-4300w9u25

Datensicherheit von VMs auf vVol Datastore

Überblick über die Datensicherheit von VMs auf vVol Datastore finden Sie unter "[Sicherung von vVols](#)".

1. Registrieren Sie das Speichersystem, das den vVol-Datastore und alle Replikationspartner hostet.

vSphere Client Search in all environments Administrator@VSPHERE.LOCAL

SnapCenter Plug-in for VMware vSphere INSTANCE 10.10.102.12-8144

Dashboard Settings Resource Groups Policies **Storage Systems** Guest File Restore

Storage Systems

Beginning with SnapCenter Plug-in for VMware vSphere (SCV) 5.0, you need to add applications of type HTTP and ONTAP as user login methods for any ONTAP users with customized role-based access to the SCV. Without access to these applications, backups will fail. You need to restart the SCV service to recognize changes to ONTAP user login methods. Click here to know more.

Name	Display Name	Type	Protocol	Port	Username	SYNs	TimeOutSec	Certificate
B:RTH-C503-5403-orig-1	nasadm-4300e9a25	ONTAP Cluster	HTTPS	443	admin	0	60	No
VCF_SCSI	VCF_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
isur0	isur0	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.228.20	isur0	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_SCSI_3510	HMC_SCSI_3510	ONTAP SVM	HTTPS	443	-	-	60	No
JL_SHC_SCSI	JL_SHC_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
0301102.217	psdadm-symb-SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_M7	HMC_M7	ONTAP SVM	HTTPS	443	-	-	60	No
VCF_3422	VCF_3422	ONTAP SVM	HTTPS	443	-	-	60	No
VCF_NVM	VCF_NVM	ONTAP SVM	HTTPS	443	-	-	60	No
demo	demo	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.254.100	Temp_3510_N1	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.30.10	HYPERV-SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
EHC_NFS	EHC_NFS	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.18.203	EHC_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
02.21.18.10	VCF_NFS	ONTAP SVM	HTTPS	443	-	-	60	No
HMC_3510	HMC_3510	ONTAP SVM	HTTPS	443	-	-	60	No
00fa_symb_4300	00fa_symb_4300	ONTAP SVM	HTTPS	443	-	-	60	No
B:ontap-destination-443c-1e...	ontap-destination	ONTAP Cluster	HTTPS	443	admin	1	90	No
0301102.147	symb2	ONTAP SVM	HTTPS	443	-	-	90	No

2. Erstellen Sie eine Richtlinie mit den erforderlichen Attributen.

New Backup Policy



Name

Description

Frequency

Locking Period Enable Snapshot Locking

Retention

Replication Update SnapMirror after backup
 Update SnapVault after backup

Snapshot label

Advanced

VM consistency

Include datastores with independent disks

Scripts

CANCEL

ADD

3. Erstellen Sie eine Ressourcengruppe und verknüpfen Sie sie mit der Richtlinie (oder den Richtlinien).

Create Resource Group



1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

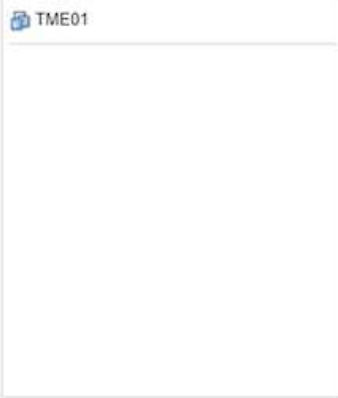
Scope:

Virtual Machines

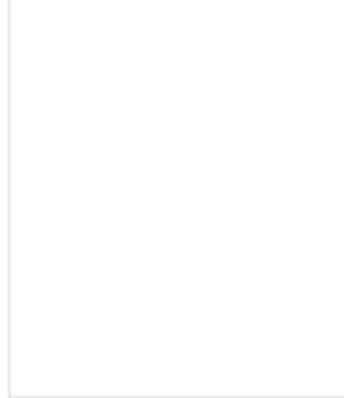
Parent entity:

Datstores
Virtual Machines
Tags
Folders
Enter available entity name

Available entities



Selected entities



BACK

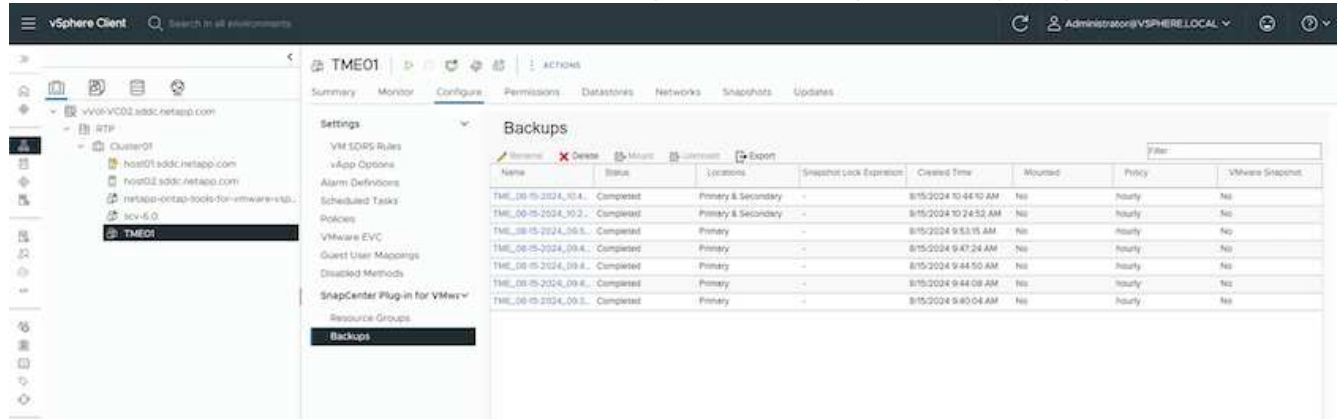
NEXT

FINISH

CANCEL

HINWEIS: Für vVol Datstore muss mit VM, Tag oder Ordner geschützt werden. VVol Datstore kann nicht in die Ressourcengruppe aufgenommen werden.

4. Der spezifische VM-Backup-Status kann auf der Registerkarte Konfigurieren angezeigt werden.



5. VM kann vom primären oder sekundären Standort aus wiederhergestellt werden.

"[SnapCenter Plug-in-Dokumentation](#)" Weitere Anwendungsfälle finden Sie in.

VM-Migration von herkömmlichen Datstores zu vVol Datstore

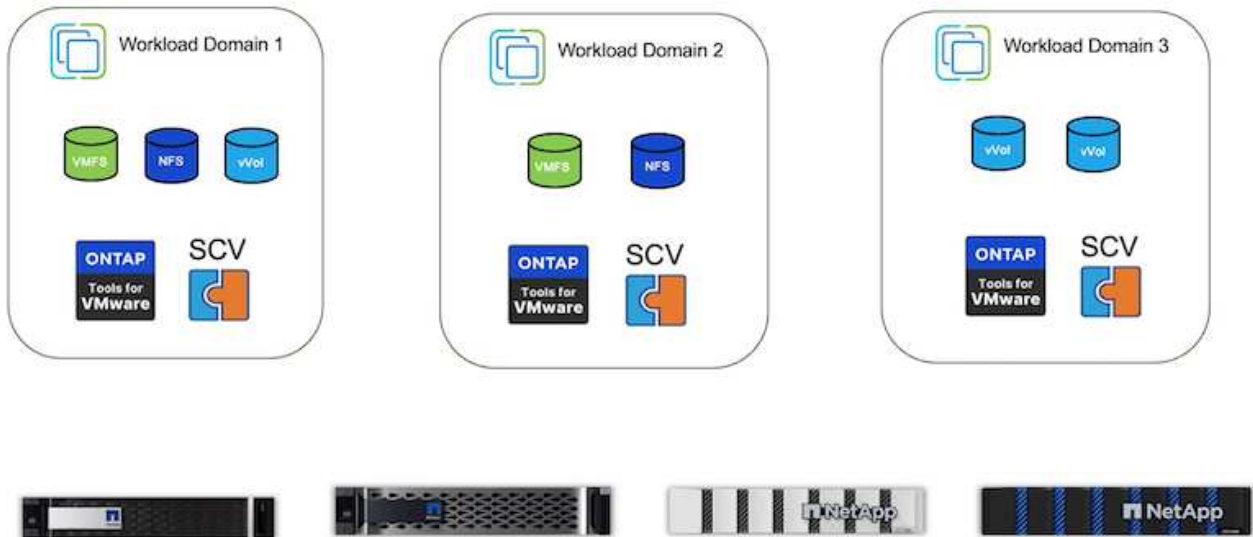
Um VMs von anderen Datstores auf einen vVol Datstore zu migrieren, sind verschiedene Optionen auf der Grundlage des Szenarios verfügbar. Die Migration kann von einem einfachen Storage vMotion Vorgang bis hin zur Migration mit HCX variieren. "[Migrieren Sie vms zu ONTAP Datstore](#)" Weitere Informationen finden Sie unter.

VM-Migration zwischen vVol Datastores

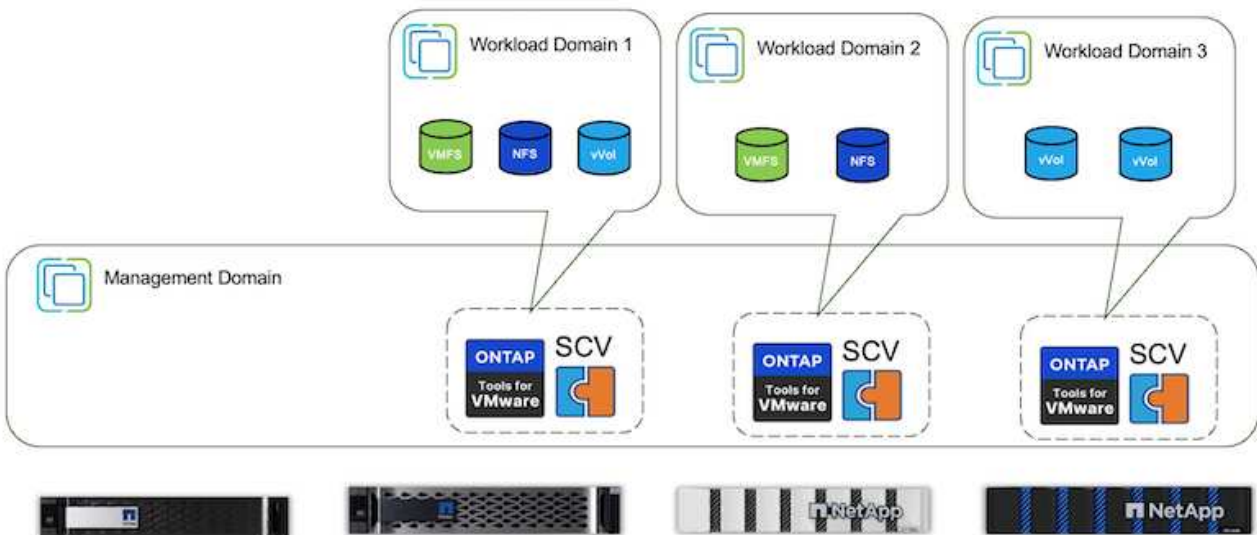
Für die Massenmigration von VMs zwischen vVol Datastores, überprüfen Sie bitte ["Migrieren Sie vms zu ONTAP Datastore"](#).

Beispiel für eine Referenzarchitektur

ONTAP Tools für VMware vSphere und SCV können auf demselben vCenter installiert werden, das es selbst managt, oder auf einem anderen vCenter Server. Es ist besser, zu vermeiden, auf vVol Datastore zu hosten, den es managt.

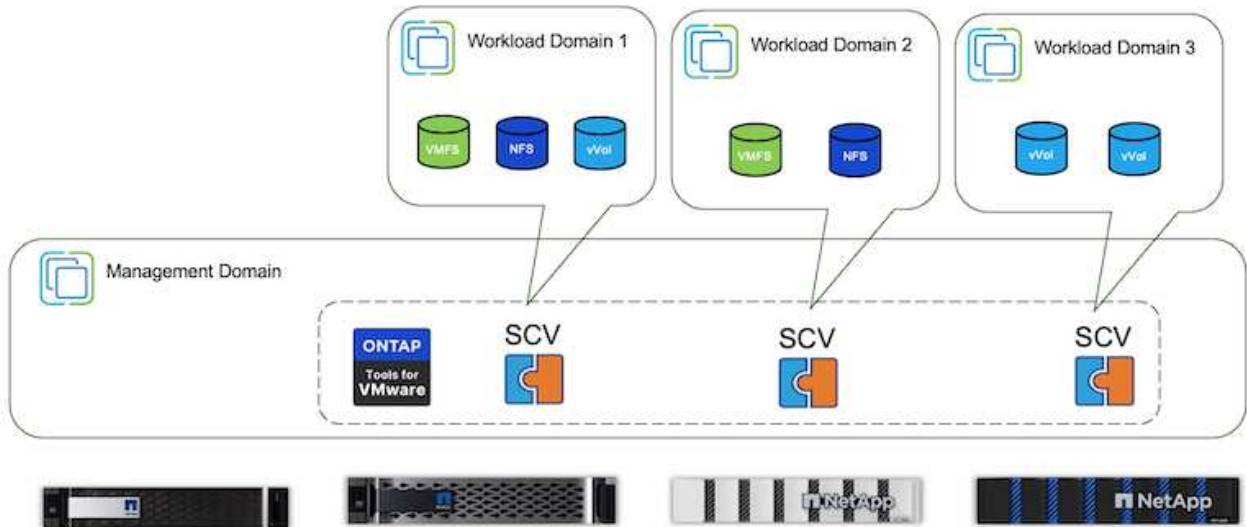


Da viele Kunden ihre vCenter Server auf verschiedenen Hosten, statt sie zu managen, wird ein ähnlicher Ansatz auch für ONTAP Tools und SCV rät.

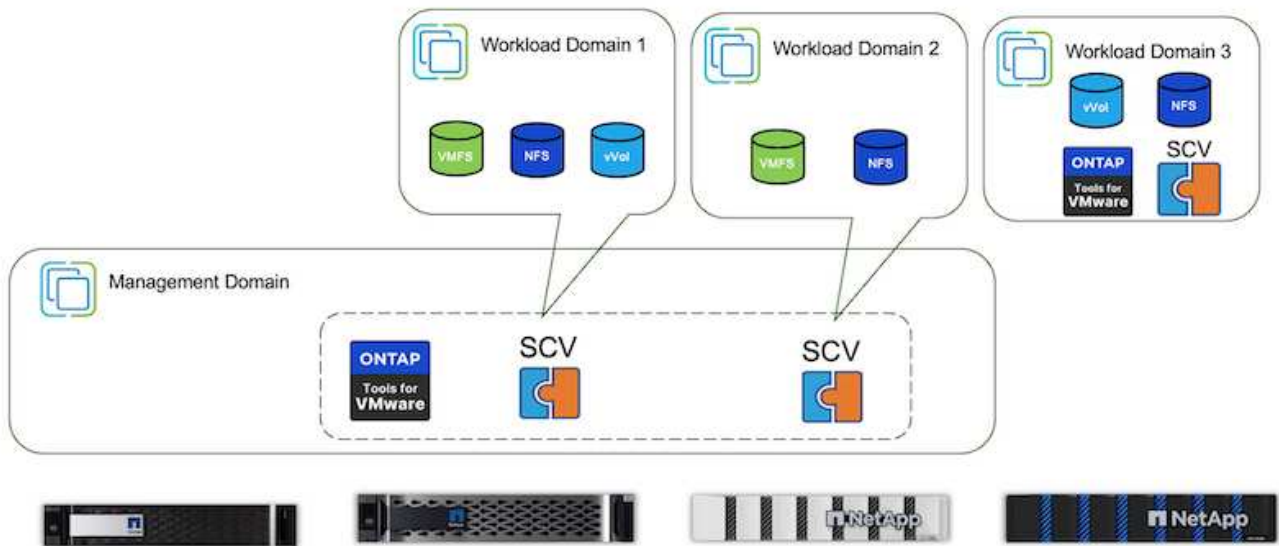


Mit den ONTAP Tools 10.x kann eine einzelne Instanz mehrere vCenter Umgebungen managen. Die Storage-Systeme sind weltweit mit Cluster-Anmeldedaten registriert und SVMs werden jedem vCenter Mandanten-

Server zugewiesen.



Auch die Mischung aus dediziertem und Shared Modell wird unterstützt.



Erste Schritte

Wenn ONTAP-Tools nicht in Ihrer Umgebung installiert sind, laden Sie sie bitte von [herunter](#) "NetApp Support-Website" und folgen Sie den Anweisungen unter "Verwendung von VVols mit ONTAP".

Implementierungsleitfaden für VMFS

Mit den Storage-Lösungen und -Angeboten von NetApp können Kunden die Vorteile einer virtualisierten Infrastruktur voll ausschöpfen. Mit NetApp Lösungen können Kunden umfassende Datenmanagement-Software effizient implementieren und so Automatisierung, Effizienz, Datensicherung und Sicherheitsfunktionen gewährleisten, um

anspruchsvolle Performance-Anforderungen effektiv zu erfüllen. Durch Kombination der ONTAP Software mit VMware vSphere können Sie die Kosten für die Host-Hardware und die VMware Lizenzierung senken, Daten kostengünstiger schützen und eine durchgängig hohe Performance bereitstellen.

Einführung

Virtualisierte Workloads sind mobil. Daher verwenden Administratoren VMware Storage vMotion, um VMs über VMware Virtual Machine File System (VMFS), NFS oder VVols Datastores zu verschieben, die sich alle auf demselben Storage-System befinden. Daher werden verschiedene Storage-Ansätze bei Nutzung eines All-Flash-Systems untersucht oder die neuesten ASA Modelle mit SAN-Innovation verwendet, um die Kosteneffizienz zu steigern.

Zentrale Aussage ist, dass die Migration zu ONTAP die Benutzerfreundlichkeit und die Applikations-Performance verbessert und gleichzeitig die Flexibilität bietet, Daten und Applikationen zwischen FCP, iSCSI, NVMe/FC und NVMe/TCP zu migrieren. Für Unternehmen, die tief in VMware vSphere investiert haben, ist die Verwendung von ONTAP Storage angesichts der aktuellen Marktbedingungen eine kostengünstige Option, die einzigartige Geschäftschance bietet. Unternehmen stehen heute vor neuen Anforderungen, die ein moderner SAN-Ansatz einfach und schnell erfüllen kann. Nachfolgend werden einige Möglichkeiten beschrieben, wie bestehende und neue NetApp Kunden mit ONTAP Mehrwert schaffen.

- **Kosteneffizienz:** Dank integrierter Storage-Effizienz senkt ONTAP die Storage-Kosten deutlich. NetApp ASA Systeme können alle Storage-Effizienzfunktionen ohne Auswirkung auf die Performance in Produktionsumgebungen ausführen. NetApp erleichtert die Planung dieser Effizienzvorteile mit der effektivsten Garantie.
- **Datensicherung:** SnapCenter Software mithilfe von Snapshots bietet erweiterte Datensicherung auf VM- und Applikationsebene für verschiedene Enterprise-Applikationen, die in einer VM-Konfiguration implementiert sind.
- **Sicherheit – Schutz vor Malware und Ransomware mit Snapshot Kopien** Verbesserte Sicherung durch die unveränderliche Erstellung von Snapshot Kopien mit Snapshot Sperrung und NetApp SnapLock Software
- **Cloud – ONTAP bietet eine Vielzahl von Hybrid Cloud-Optionen, mit denen Unternehmen Public und Private Clouds kombinieren können.** Dadurch bieten sie Flexibilität und verringern den Overhead des Infrastrukturmanagements. Zusätzliche Datastore-Unterstützung auf Basis von ONTAP-Angeboten ermöglicht die Nutzung von VMware Cloud on Azure, AWS und Google, um für die TCO optimierte Implementierung, Datensicherung und Business Continuity zu sorgen und gleichzeitig die Festlegung auf einen Anbieter zu vermeiden.
- **Flexibilität:** ONTAP ist gut gerüstet, um die sich schnell ändernden Anforderungen moderner Unternehmen zu erfüllen. Bei ONTAP One sind alle diese Funktionen standardmäßig mit einem ONTAP System ohne Zusatzkosten enthalten.

Größe anpassen und optimieren

Angesichts der bevorstehenden Lizenzierungsänderungen gehen Unternehmen proaktiv auf die potenzielle Erhöhung der Gesamtbetriebskosten (TCO) ein. Sie optimieren ihre VMware-Infrastruktur durch offensives Ressourcenmanagement und richtiges Sizing strategisch, um die Ressourcenauslastung zu verbessern und die Kapazitätsplanung zu optimieren. Durch den effektiven Einsatz spezialisierter Tools können Unternehmen verschwendete Ressourcen effizient identifizieren und wieder nutzbar machen, wodurch die Anzahl der Kerne und die Lizenzierungskosten insgesamt reduziert werden. Viele Unternehmen integrieren diese Verfahren bereits in ihre Cloud-Bewertungen. Sie zeigen auf, wie mit diesen Prozessen und Tools Kostenbedenken in On-Premises-Umgebungen wirksam entschärft und unnötige Migrationskosten für alternative Hypervisoren vermieden werden.

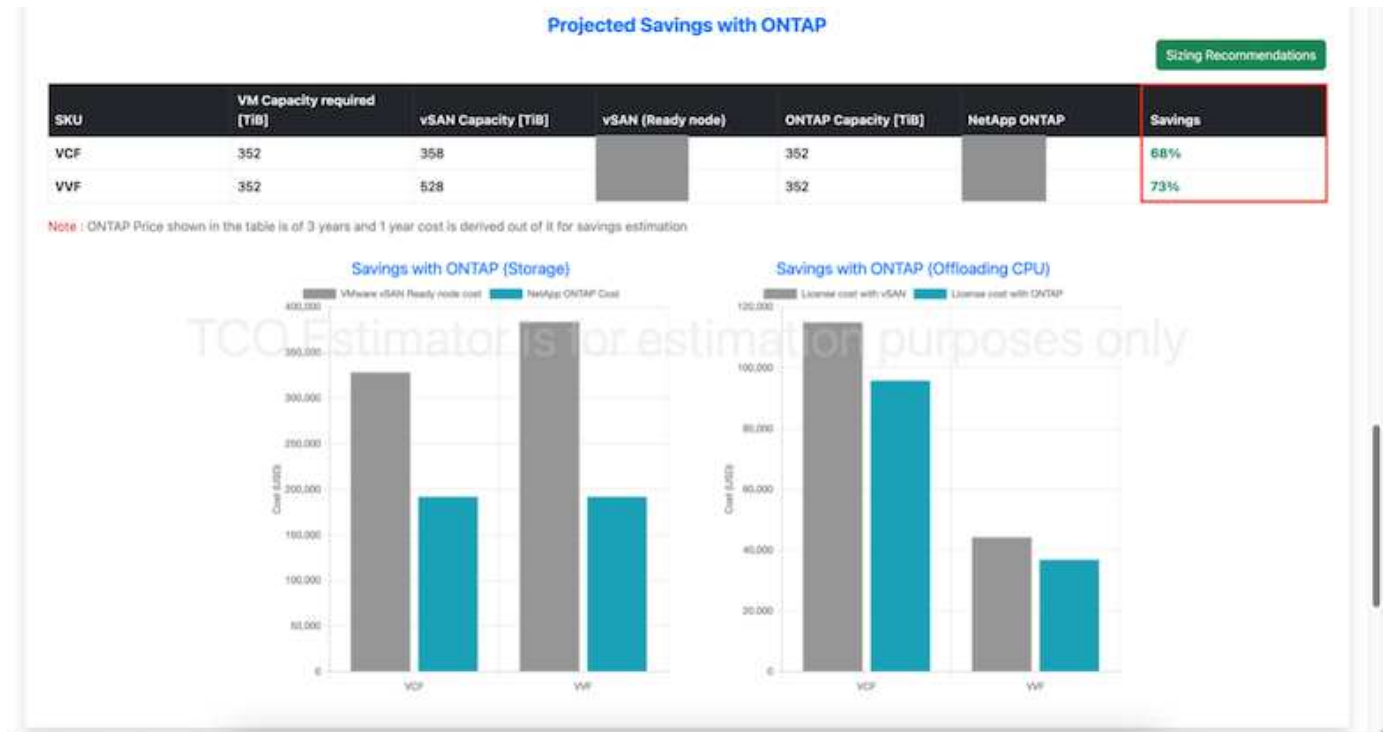
TCO-Kalkulator

NetApp hat eine einfache TCO-Kalkulator entwickelt, der als Sprungbrett für diesen Optimierungsschritt fungiert. Der TCO-Kalkulator verwendet RVTools oder manuelle Eingabemethoden, um auf einfache Weise zu ermitteln, wie viele Hosts für die jeweilige Implementierung benötigt werden, und die Einsparungen zur Optimierung der Bereitstellung mit NetApp ONTAP Storage-Systemen zu berechnen. Denken Sie daran, dies ist der Sprungbrett.



Der TCO-Kalkulator ist nur für NetApp Teams und Partner vor Ort verfügbar. Bewerten Sie gemeinsam mit den NetApp Account Teams die vorhandene Umgebung.

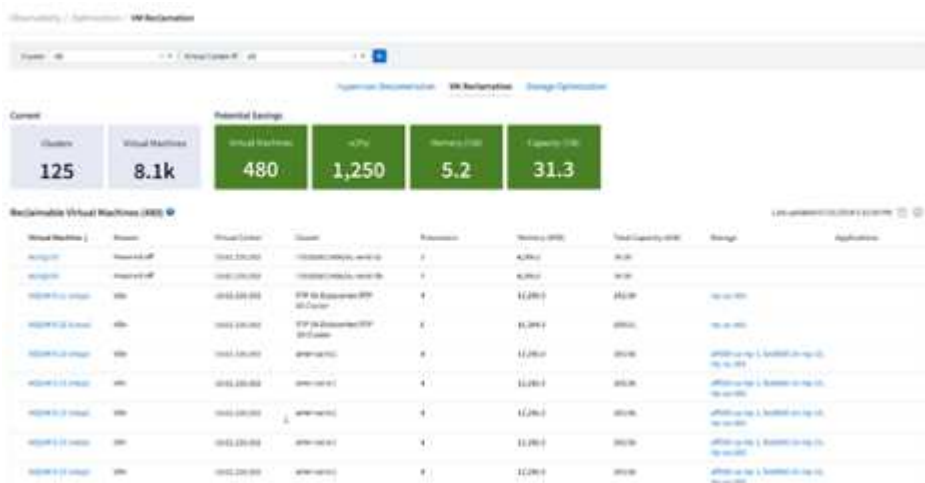
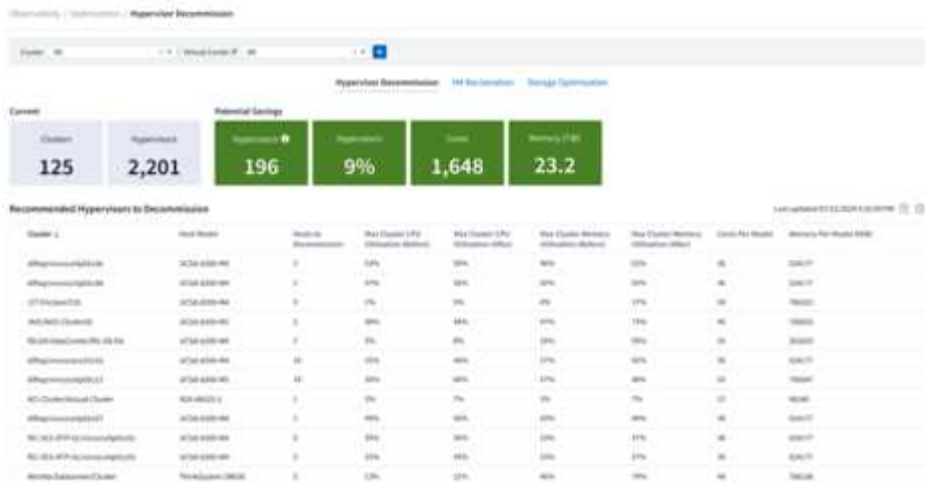
Hier ist ein Screenshot aus der TCO-Kalkulation.



Einblicke in die Cloud

Sobald der Schätzer die möglichen Einsparungen zeigt (was für jede Organisation der Fall sein wird), ist es an der Zeit, tief in die Analyse der Workload-IO-Profile auf virtuellen Maschinen unter Verwendung von Echtzeit-Metriken einzutauchen. Hierzu stellt NetApp Cloud Insights bereit. Durch detaillierte Analysen und Empfehlungen zur Rückgewinnung von VMs unterstützt Cloud Insights Unternehmen bei der Optimierung ihrer VM-Umgebung und hilft ihnen, fundierte Entscheidungen zu treffen. Die Lösung kann ermitteln, wo Ressourcen zurückgewonnen oder Hosts stillgelegt werden können, ohne dass sich dies auf die Produktion auswirkt. So können Unternehmen die durch die Übernahme von VMware durch Broadcom vorgenommenen Änderungen auf durchdachte und strategische Weise bewältigen. Mit anderen Worten: Cloud Insight hilft Unternehmen, die Entscheidung ohne Emotionen zu treffen. Anstatt in Panik oder Frustration auf Änderungen zu reagieren, können sie die Einblicke des Cloud Insights Tools nutzen, um rationale, strategische Entscheidungen zu treffen, die ein ausgewogenes Verhältnis zwischen Kostenoptimierung und betrieblicher Effizienz und Produktivität bieten.

Unten sind die Screenshots von Cloud Insights.



Führen Sie regelmäßige Analysen durch, um nicht ausgelastete Ressourcen zu ermitteln, die Dichte virtueller Maschinen zu erhöhen und die Auslastung innerhalb von VMware-Clustern zu erhöhen, um die steigenden Kosten im Zusammenhang mit neuen Abonnementlizenzen zu kontrollieren. Bei Neuanschaffungen von Servern sollte die Anzahl der Kerne pro CPU auf 16 reduziert werden, um sie an Änderungen der VMware-Lizenzierungsmodelle anzupassen.

Mit NetApp passen Sie die Größe Ihrer virtualisierten Umgebungen an und führen kostengünstige Flash-Storage-Performance ein sowie vereinfachtes Datenmanagement und Ransomware-Lösungen. So können Sie sicherstellen, dass Unternehmen auf ein neues Abonnementmodell vorbereitet sind und gleichzeitig die aktuellen IT-Ressourcen optimieren.

NetApp ONTAP Tools für VMware vSphere

Zur weiteren Verbesserung und Vereinfachung der VMware Integration bietet NetApp verschiedene OFFTAP Tools, die sich mit NetApp ONTAP und VMware vSphere für das effiziente Management virtualisierter Umgebungen verwenden lassen. Dieser Abschnitt widmet sich den ONTAP Tools für VMware. ONTAP Tools für VMware vSphere 10 bieten eine umfangreiche Palette an Tools für das Lifecycle Management von Virtual Machines, die das Storage Management vereinfachen, Effizienzfunktionen verbessern, die Verfügbarkeit verbessern und Storage-Kosten und Betriebsaufwand senken. Diese Tools lassen sich nahtlos in das VMware Ecosystem integrieren und erleichtern so die Bereitstellung von Datastores und bieten grundlegende Sicherung für Virtual Machines. Die 10.x-Version der ONTAP Tools für VMware vSphere umfasst horizontal skalierbare, ereignisgesteuerte Microservices, die als Open Virtual Appliance (OVA) implementiert werden. Sie folgt Best Practices für die Bereitstellung von Datastores und die Optimierung der ESXi-Hosteinstellungen für

Block- und NFS-Speicherumgebungen. Angesichts dieser Vorteile wird OTV als Best Practice für Systeme mit ONTAP-Software empfohlen.

Erste Schritte

Stellen Sie vor der Bereitstellung und Konfiguration von ONTAP-Tools für VMware sicher, dass die Voraussetzungen erfüllt sind. Implementieren Sie anschließend eine Konfiguration mit einem einzelnen Node.



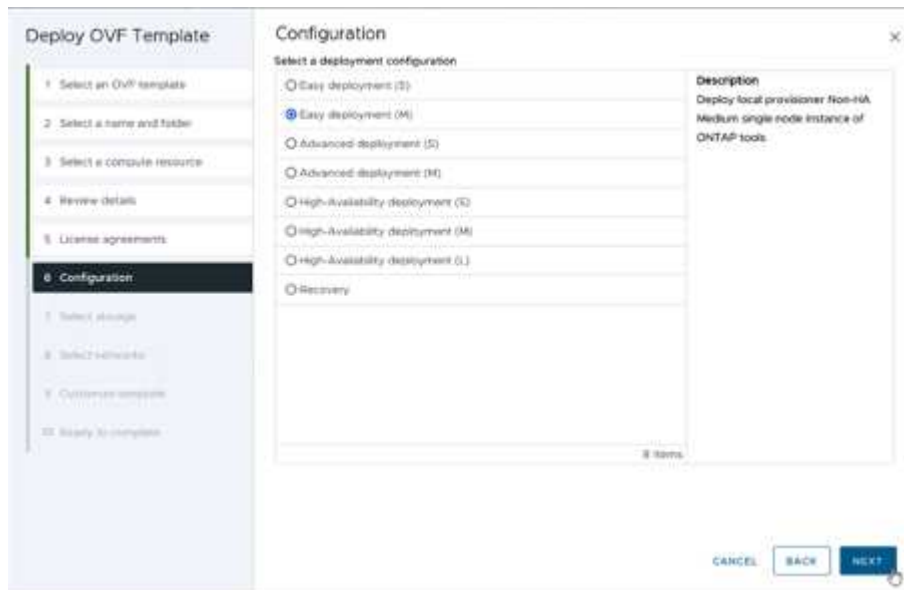
Für die Implementierung sind drei IP-Adressen erforderlich: Eine IP-Adresse für den Load Balancer, eine IP-Adresse für die Kubernetes-Kontrollebene und eine für den Node.

Schritte

1. Melden Sie sich beim vSphere-Server an.
2. Navigieren Sie zum Cluster oder Host, auf dem Sie die OVA bereitstellen möchten.
3. Klicken Sie mit der rechten Maustaste auf den gewünschten Speicherort, und wählen Sie OVF-Vorlage bereitstellen.
 - a. Geben Sie die URL für die .ova-Datei ein, oder navigieren Sie zu dem Ordner, in dem die .ova-Datei gespeichert wird, und wählen Sie dann Weiter.
4. Wählen Sie einen Namen, Ordner, Cluster/Host für die virtuelle Maschine aus, und wählen Sie Weiter.
5. Wählen Sie im Fenster Konfiguration die Option Einfache Bereitstellung(S), Einfache Bereitstellung(M), erweiterte Bereitstellung(S) oder erweiterte Bereitstellung(M)-Konfiguration aus.



Die einfache Bereitstellungsoption wird bei dieser Einführung verwendet.



6. Wählen Sie den Datastore für die OVA-Implementierung sowie das Quell- und Zielnetzwerk aus. Wählen Sie anschließend Weiter.
7. Es ist an der Zeit, die Vorlage anzupassen > Fenster Systemkonfiguration.

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 Configuration
- 7 Select storage
- 8 Select networks
- 9 Customize template
- 10 Ready to complete

Customize template

Administrator username(*)	Username to assign to the Administrator. Please use only a letter as the beginning. And only [a-z, 0-9, -, _] special characters are supported. <input type="text" value="admin"/>
Administrator password(*)	Password to assign to the Administrator. Password <input type="password" value="*****"/> 👁 Confirm Password <input type="password" value="*****"/> 👁
NTP servers	A comma-separated list of hostnames or IP addresses of NTP servers. If left blank, VMware Tools based time synchronization will be used. <input type="text" value="172.21.166.1"/>
Maintenance user password(*)	Password to assign to maint user account. Password <input type="password" value="*****"/> 👁 Confirm Password <input type="password" value="*****"/> 👁

CANCEL BACK NEXT

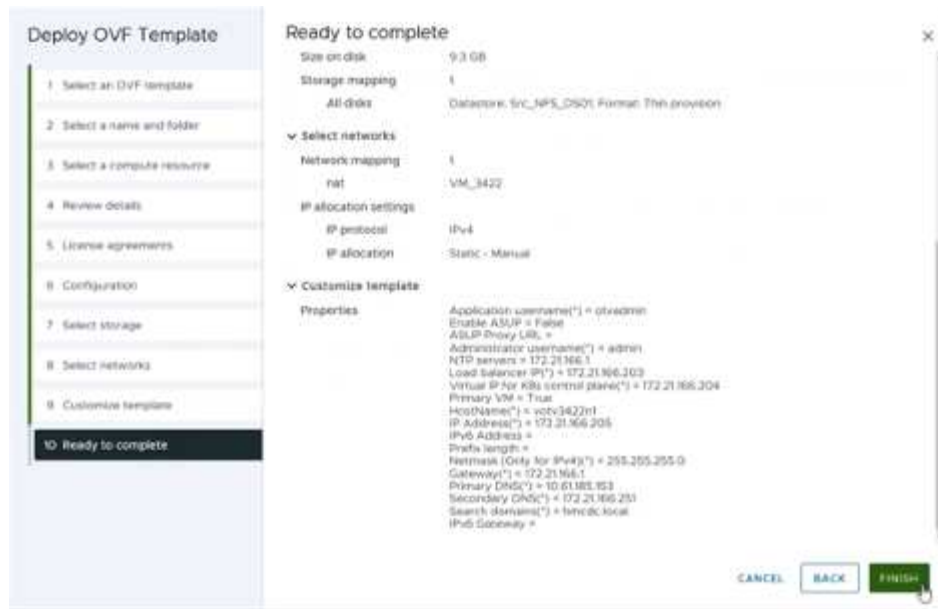
Deploy OVF Template

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

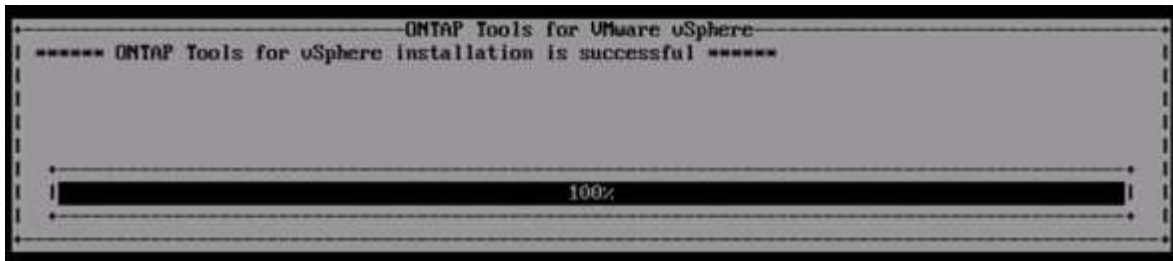
Customize template

Deployment Configuration	3 settings
Load balancer IP(*)	Load balancer IP (*) <input type="text" value="172.21.166.203"/>
Virtual IP for K8s control plane(*)	Provides the virtual IP address for K8s control plane. <input type="text" value="172.21.166.204"/>
Primary VM	Maintain this field as selected to set the current VM as primary and install the ONTAP tools. <input checked="" type="checkbox"/>
Node Configuration	10 settings
HostName(*)	Specify the hostname for the VM. <input type="text" value="vst-0422r1"/>
IP Address(*)	Specify the IP address for the appliance. <input type="text" value="172.21.166.205"/>
IPv6 Address	Specify the IPv6 address on the deployed network only when you need dual stack. <input type="text"/>
Prefix length	Specify the prefix length. <input type="text"/>

CANCEL BACK NEXT



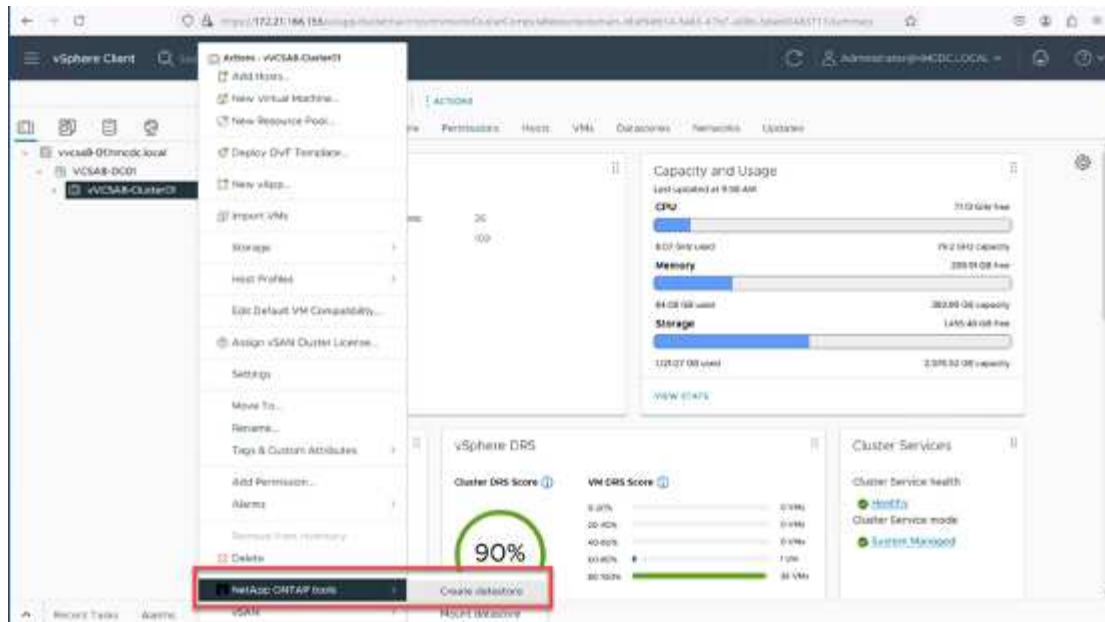
Nach der erfolgreichen Installation zeigt die Webkonsole den Status der ONTAP Tools für VMware vSphere an.



Der Assistent für die Datastore-Erstellung unterstützt die Bereitstellung von VMFS, NFS und VVols Datastores.

Es ist an der Zeit, ISCSI-basierte VMFS-Datenspeicher für diese Anleitung bereitzustellen.

1. Melden Sie sich mit beim vSphere-Client an <https://<vcenterip>/ui>
2. Klicken Sie mit der rechten Maustaste auf einen Host oder einen Hostcluster oder einen Datenspeicher, und wählen Sie dann NetApp ONTAP Tools > Create Datastore aus.



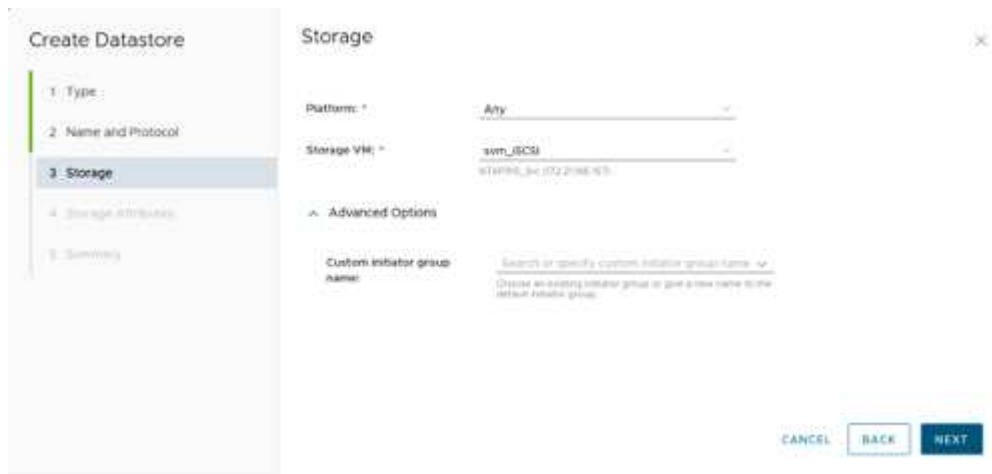
3. Wählen Sie im Fensterbereich Typ die Option VMFS im Datenspeichertyp aus.



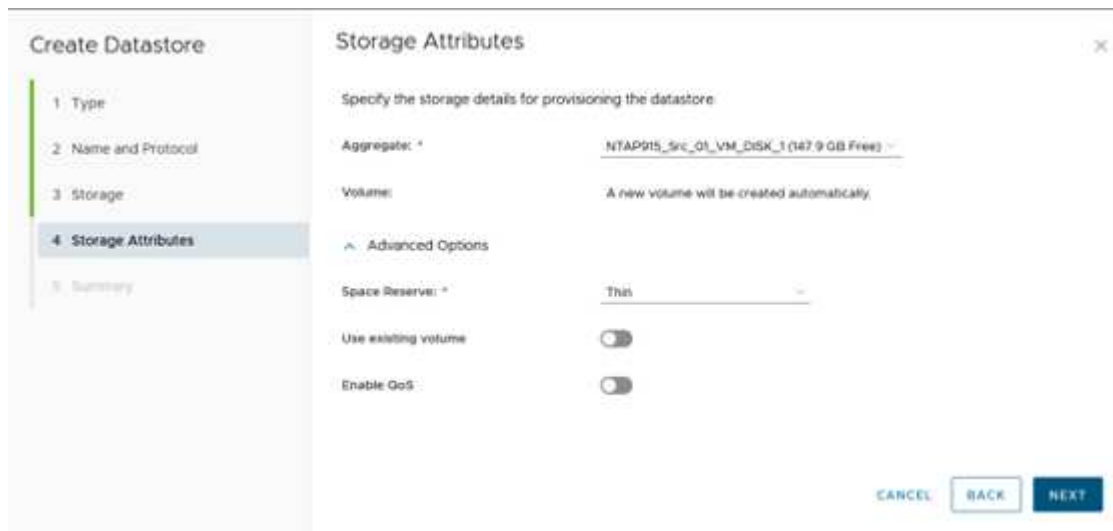
4. Geben Sie im Teilfenster Name und Protokoll den Namen, die Größe und die Protokollinformationen des Datastore ein. Wählen Sie im Bereich Erweiterte Optionen des Teilfensters den Datastore-Cluster aus, wenn Sie diesen Datastore hinzufügen möchten.



5. Wählen Sie im Fensterbereich Storage die Option Platform and Storage VM aus. Geben Sie im Abschnitt „Erweiterte Optionen“ des Teilfensters den Namen der benutzerdefinierten Initiatorgruppe an (optional). Sie können entweder eine vorhandene Initiatorgruppe für den Datastore auswählen oder eine neue Initiatorgruppe mit einem benutzerdefinierten Namen erstellen.



6. Wählen Sie im Fensterbereich Storage-Attribute aus dem Dropdown-Menü die Option Aggregat aus. Wählen Sie im Abschnitt Erweiterte Optionen die Option Speicherplatzreserve, Volume und aktivieren Sie QoS-Optionen nach Bedarf.



7. Überprüfen Sie die Datastore-Details im Fenster Zusammenfassung, und klicken Sie auf Fertig stellen. Der VMFS Datastore wird auf allen Hosts erstellt und gemountet.



Mithilfe dieser Links erhalten Sie weitere Informationen zur Bereitstellung von vVol, FC, NVMe/TCP-Datstores.

VAAI-Auslagerung

VAAI-Primitive werden in vSphere Routineaufgaben verwendet, wie beispielsweise das Erstellen, Klonen, Migrieren, Starten und Stoppen von VMs. Diese Vorgänge können aus Vereinfachen über den vSphere Client oder über die Befehlszeile für Skripting oder für genauere Timing ausgeführt werden. VAAI für SAN wird nativ von ESX unterstützt. VAAI ist auf unterstützten NetApp Storage-Systemen immer aktiviert und bietet nativen Support für die folgenden VAAI Operationen auf SAN-Speicher:

- Copy-Offload
- Atomic Test & Set (ATS) Verriegelung
- Schreiben Sie Gleich
- Umgang mit Bedingungen, die nicht genügend Platz bieten
- Speicherplatzrückgewinnung

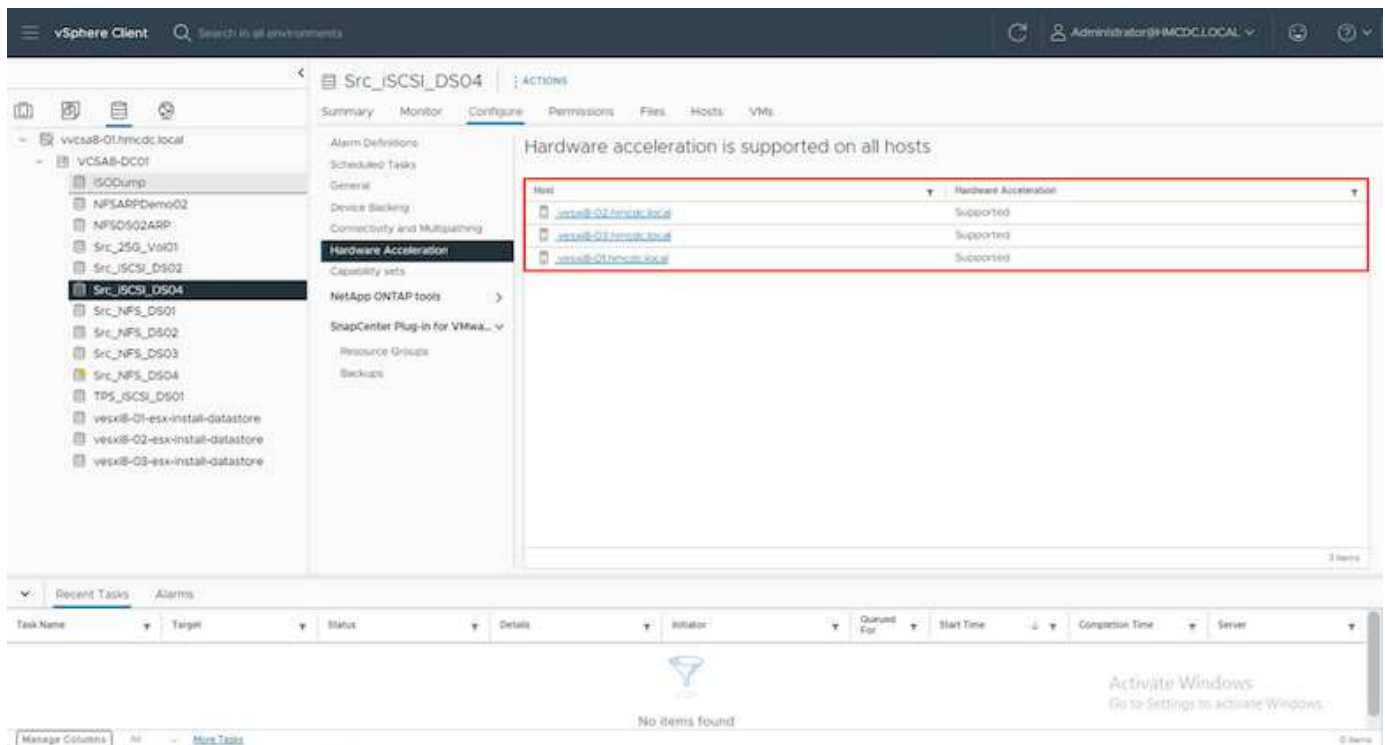
```
[root@vesxi8-02:~] esxcli storage core device vaai status get -d=naa.600a09805a506576495d576a57553455
naa.600a09805a506576495d576a57553455
VAAI Plugin Name: VMW_VAAIP_NETAPP
ATS Status: supported
Clone Status: supported
Zero Status: supported
Delete Status: supported
```



Stellen Sie sicher, dass HardwareAcceleratedMove über die erweiterten ESX-Konfigurationsoptionen aktiviert ist.



Stellen Sie sicher, dass die „Speicherplatzzuweisung“ auf der LUN aktiviert ist. Wenn diese Option nicht aktiviert ist, aktivieren Sie die Option und scannen Sie alle HBAs erneut.





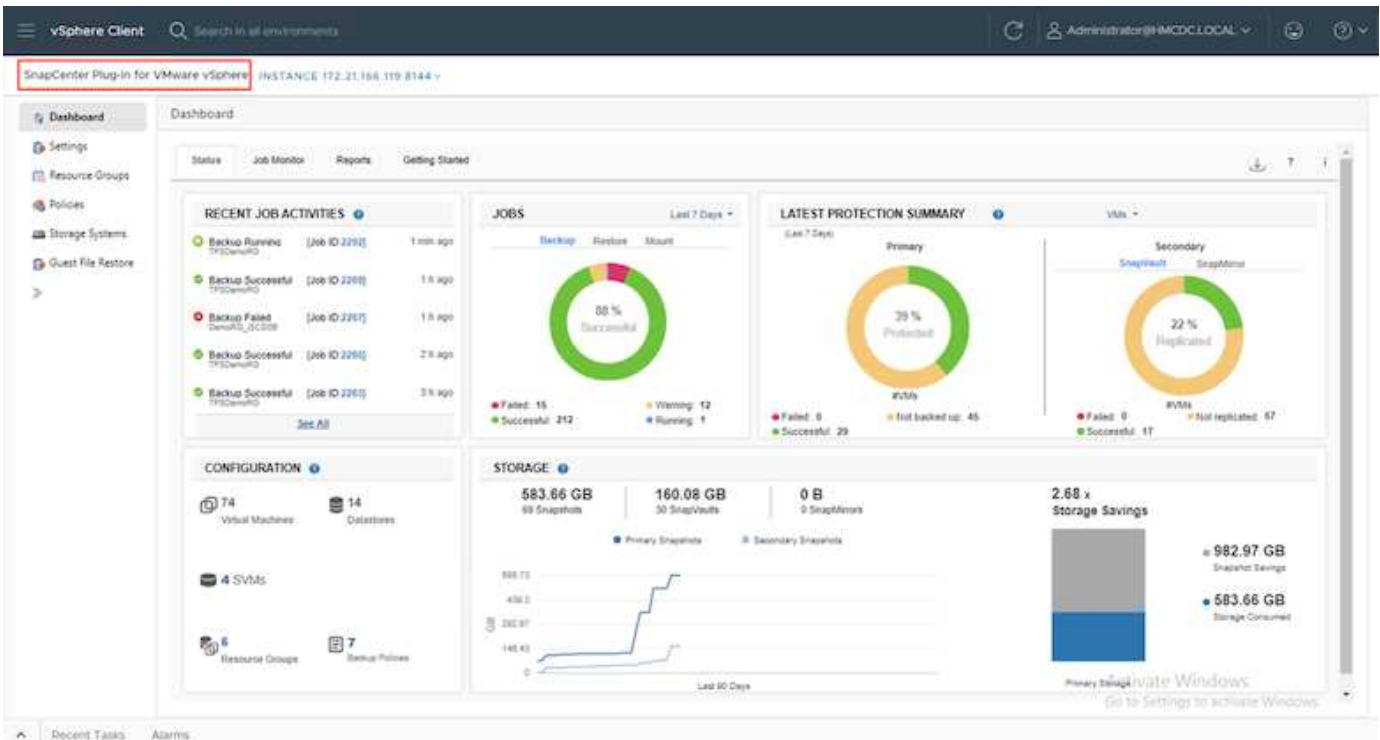
Diese Werte lassen sich mit den ONTAP Tools für VMware vSphere problemlos festlegen. Wechseln Sie im Dashboard „Übersicht“ zur ESXi-Host-Compliance-Karte, und wählen Sie die Option „Empfohlene Einstellungen anwenden“. Wählen Sie im Fenster Empfohlene Host-Einstellungen anwenden die Hosts aus, und klicken Sie auf Weiter, um die von NetApp empfohlenen Host-Einstellungen anzuwenden.



Ausführliche Anleitungen anzeigen für "Empfohlene ESXi Host-Einstellungen und andere ONTAP Einstellungen".

Datensicherung

Zu den wichtigsten Vorteilen von ONTAP für vSphere gehören die effiziente Sicherung und Wiederherstellung von VMs auf VMFS Datenspeichern. Durch die Integration in vCenter bietet die NetApp SnapCenter® Software eine Vielzahl von Backup- und Recovery-Funktionen für VMs. Sie ermöglicht schnelle, platzsparende, absturzkonsistente und VM-konsistente Backup- und Restore-Prozesse für VMs, Datastores und VMDKs. Es funktioniert auch mit SnapCenter Server, um applikationsbasierte Backup- und Restore-Vorgänge in VMware Umgebungen mithilfe von applikationsspezifischen SnapCenter Plug-ins zu unterstützen. Durch die Nutzung von Snapshot Kopien können schnelle Kopien der VM oder des Datastore ohne Auswirkungen auf die Performance erstellt werden. Außerdem wird die NetApp SnapMirror®- oder NetApp SnapVault®-Technologie für langfristige externe Datensicherung verwendet.



Der Workflow ist einfach. Fügen Sie primäre Storage-Systeme und SVMs (und sekundäre Storage-Systeme

bei Bedarf für SnapMirror/SnapVault) hinzu.

Übergeordnete Schritte für Implementierung und Konfiguration:

1. Laden Sie das SnapCenter für VMware Plug-in OVA herunter
2. Melden Sie sich mit den vSphere Client-Anmeldeinformationen an
3. Stellen Sie die OVF-Vorlage bereit, um den VMware Deploy Wizard zu starten und die Installation abzuschließen
4. Um auf das Plug-in zuzugreifen, wählen Sie im Menü SnapCenter Plug-in für VMware vSphere aus
5. Speicher Hinzufügen
6. Backup-Richtlinien erstellen
7. Erstellen von Ressourcengruppen
8. Backup-Ressourcengruppen
9. Stellen Sie die gesamte virtuelle Maschine oder ein bestimmtes virtuelles Laufwerk wieder her

Einrichten des SnapCenter Plug-in für VMware für VMs

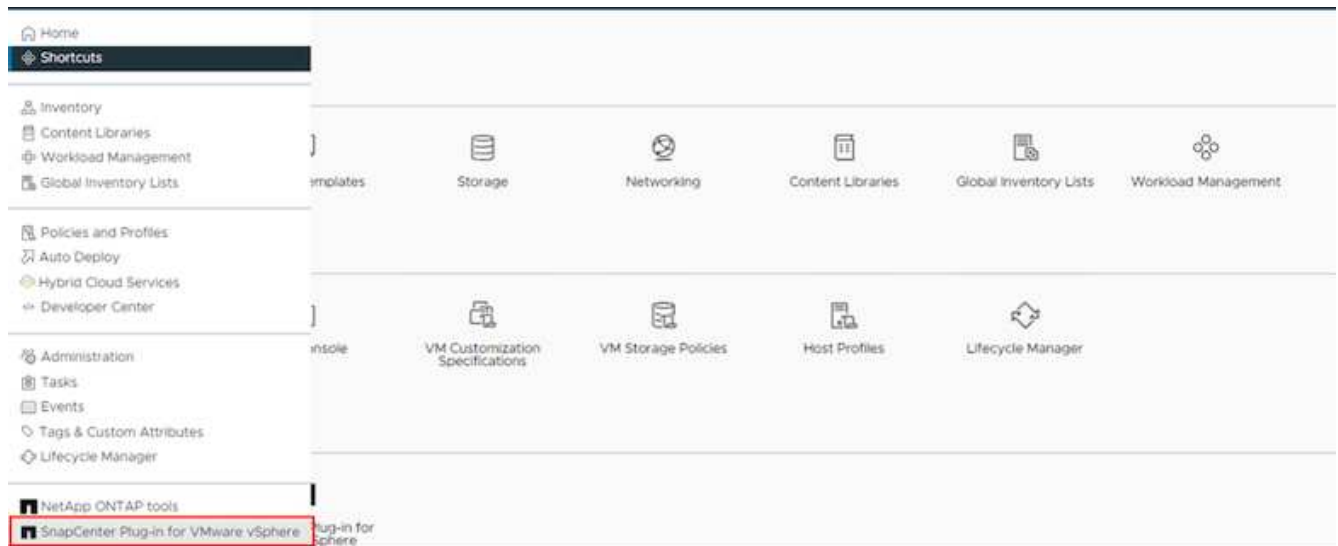
Um VMs und iSCSI-Datstores, die sie hosten, zu sichern, muss das SnapCenter Plug-in für VMware implementiert werden. Es handelt sich um einen einfachen OVF-Import.

Die Implementierung erfolgt wie folgt:

1. Laden Sie die offene virtuelle Appliance (OVA) von der NetApp Support-Website herunter.
2. Melden Sie sich beim vCenter an.
3. Klicken Sie in vCenter mit der rechten Maustaste auf ein beliebiges Bestandsobjekt, z. B. ein Rechenzentrum, einen Ordner, ein Cluster oder einen Host, und wählen Sie OVF-Vorlage bereitstellen aus.
4. Wählen Sie die richtigen Einstellungen für Storage und Netzwerk aus und passen Sie die Vorlage an, um vCenter und seine Zugangsdaten zu aktualisieren. Klicken Sie nach der Überprüfung auf Fertig stellen.
5. Warten Sie, bis der OVF-Import und die Bereitstellungsaufgaben abgeschlossen sind.
6. Sobald das SnapCenter Plug-in für VMware erfolgreich bereitgestellt wurde, wird es innerhalb von vCenter registriert. Das gleiche kann durch den Zugriff auf Administration > Client Plugins überprüft werden



7. Um auf das Plug-in zuzugreifen, navigieren Sie zum linken Seitenrand der vCenter-Webclientseite, und wählen Sie SnapCenter-Plug-in für VMware aus.



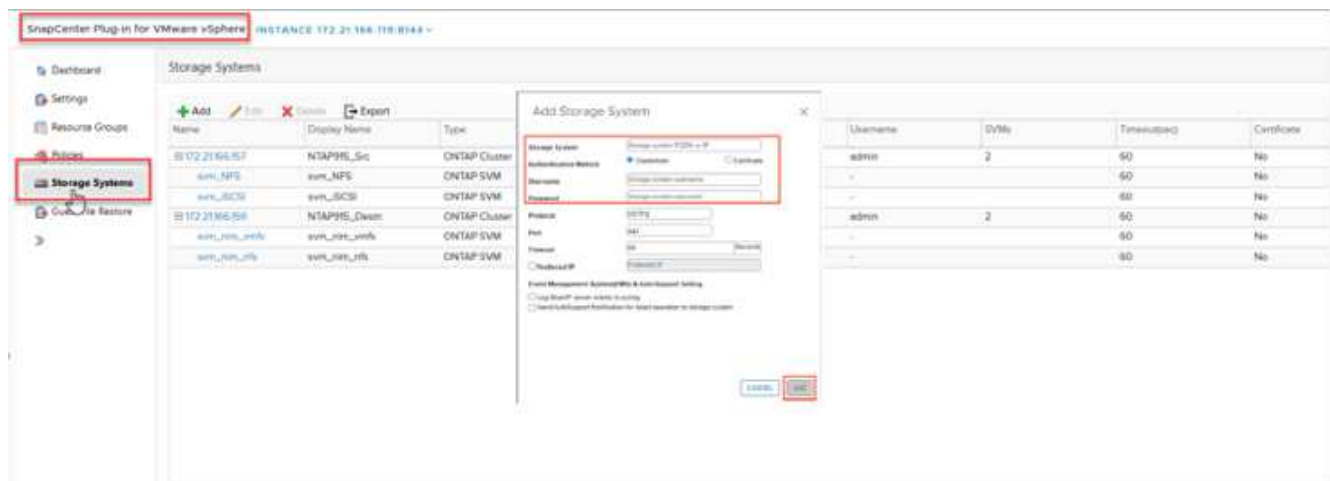
Fügen Sie Speicher hinzu, erstellen Sie Richtlinien und Ressourcengruppen

Storage-System hinzugefügt

Im nächsten Schritt fügen Sie das Storage-System hinzu. Der Clustermanagementendpunkt oder die SVM (Storage Virtual Machine)-Administrationsendpunkt-IP sollte als Storage-System zum Backup und zur Wiederherstellung der VMs hinzugefügt werden. Durch das Hinzufügen von Speicher kann das SnapCenter Plug-in für VMware Backup- und Restore-Vorgänge in vCenter erkennen und managen.

Der Prozess ist einfach.

1. Wählen Sie in der linken Navigation das SnapCenter Plug-in für VMware aus.
2. Wählen Sie Storage Systems Aus.
3. Wählen Sie Hinzufügen, um die „Storage“-Details hinzuzufügen.
4. Verwenden Sie als Authentifizierungsmethode Anmeldedaten, geben Sie den Benutzernamen und das zugehörige Kennwort ein, und klicken Sie dann auf Hinzufügen, um die Einstellungen zu speichern.



SnapCenter Plug-in for VMware vSphere - INSTANCE 172.21.166.119.8144

Dashboard Settings Resource Groups Policies Storage Systems Guest File Restore

Storage Systems

Name	Display Name	Type	Protocol	Port	Username	DNAs	Timeout	Certificate
E: 02.21.166.119	NTAPSE_Sn	ONTAP Cluster	HTTPS	443	admin	2	60	No
svm_nfs	svm_nfs	ONTAP SVM	HTTPS	443	-	-	60	No
svm_SCSI	svm_SCSI	ONTAP SVM	HTTPS	443	-	-	60	No
E: 172.21.166.119	NDAPSE_Sn	ONTAP Cluster	HTTPS	443	admin	2	60	No
svm_nfs_1	svm_nfs_1	ONTAP SVM	HTTPS	443	-	-	60	No
svm_nfs_2	svm_nfs_2	ONTAP SVM	HTTPS	443	-	-	60	No

Backup-Richtlinie erstellen

Eine umfassende Backup-Strategie umfasst Faktoren wie wann, was zu sichern ist und wie lange Backups aufbewahrt werden müssen. Snapshots können auf stündlicher oder täglicher Basis ausgelöst werden, um ganze Datenspeicher zu sichern. Dieser Ansatz erfasst nicht nur die Datenspeicher, sondern ermöglicht auch Backup und Restore der VMs und VMDKs innerhalb dieser Datenspeicher.

Vor dem Backup der VMs und Datastores müssen eine Backup-Richtlinie und eine Ressourcengruppe erstellt werden. Eine Backup-Richtlinie schließt Einstellungen wie den Zeitplan und die Aufbewahrungsrichtlinie ein. Führen Sie die folgenden Schritte aus, um eine Sicherungsrichtlinie zu erstellen.

1. Klicken Sie im linken Navigationsbereich des SnapCenter Plug-ins für VMware auf Richtlinien.
2. Klicken Sie auf der Seite Richtlinien auf Erstellen, um den Assistenten zu starten.

SnapCenter Plug-in for VMware vSphere - INSTANCE 172.21.166.119.8144

Dashboard Settings Resource Groups Policies Storage Systems Guest File Restore

Policies

VM Consistency	Include Independent Disks	Signature Type	Snap/Alert	Snap/Mirror	Snapshot Locking Period
DemoSCSI_TPS	Yes	No	Daily	Yes	7 Days
DemoNFSv1TPS	Yes	No	Daily	No	1 Day
DemoFol	No	No	Hourly	No	1 Day
DemoFull1	No	No	Daily	Yes	7 Days
TempSCSI	Yes	No	Daily	Yes	7 Days

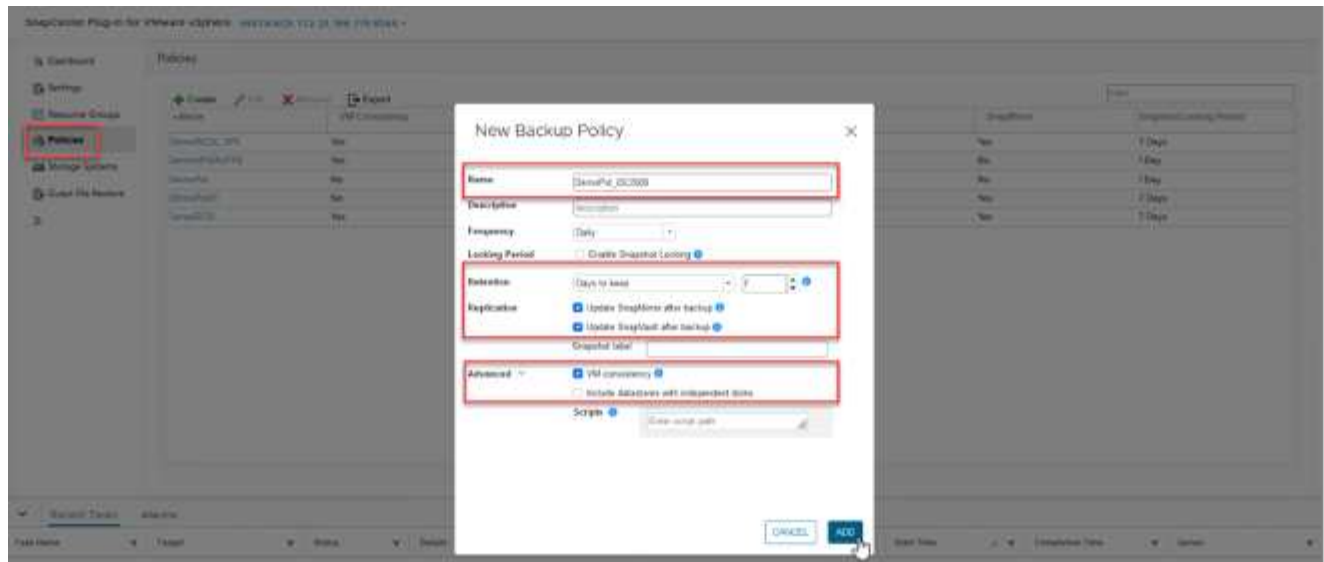
3. Geben Sie auf der Seite Neue Sicherungsrichtlinie den Richtliniennamen ein.
4. Geben Sie die Aufbewahrung, die Frequenzeinstellungen und die Replikation an.



Um Snapshot-Kopien auf ein sekundäres Spiegelungs- oder Vault-Storage-System zu replizieren, müssen die Beziehungen vorab konfiguriert werden.



Um VM-konsistente Backups zu ermöglichen, müssen VMware Tools installiert und ausgeführt werden. Wenn das Kontrollkästchen VM Consistency aktiviert ist, werden die VMs zunächst stillgelegt, dann führt VMware einen VM-konsistenten Snapshot (ohne Arbeitsspeicher) aus, und dann führt das SnapCenter Plug-in für VMware den Backup-Vorgang durch, und anschließend werden die VM-Vorgänge wieder aufgenommen.



Nach Erstellung der Richtlinie wird im nächsten Schritt die Ressourcengruppe erstellt, die die geeigneten iSCSI-Datenspeicher und VMs definiert, die gesichert werden sollen. Nach der Erstellung der Ressourcengruppe ist es Zeit, Backups auszulösen.

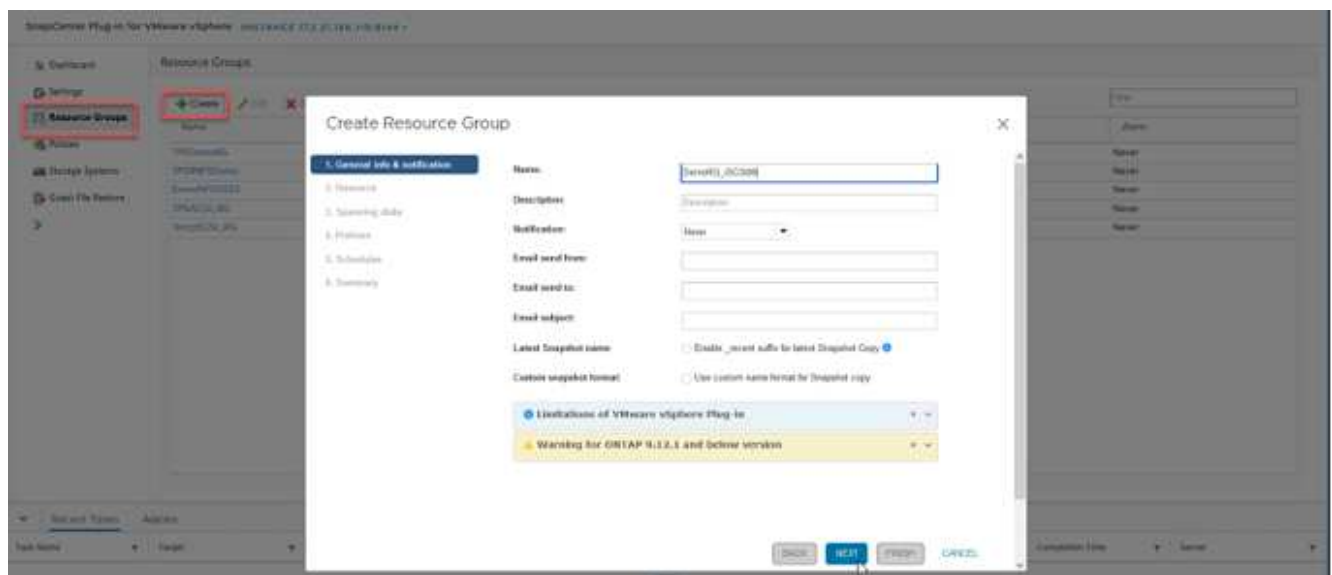
Ressourcengruppe erstellen

Eine Ressourcengruppe ist der Container für VMs und Datastores, der gesichert werden muss. Die Ressourcen können jederzeit zu Ressourcengruppen hinzugefügt oder entfernt werden.

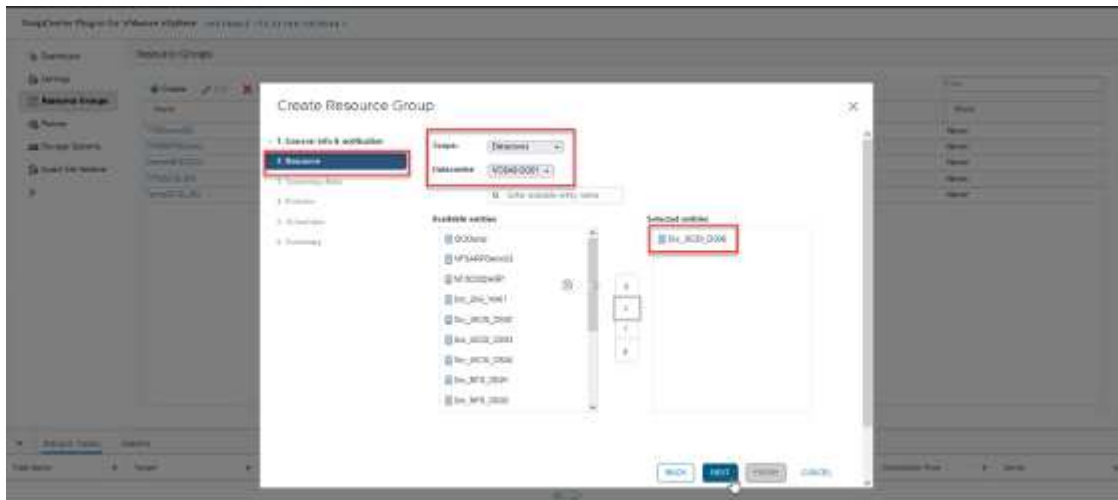
Führen Sie die folgenden Schritte aus, um eine Ressourcengruppe zu erstellen.

1. Klicken Sie im linken Navigationsbereich des SnapCenter-Plug-ins für VMware auf Ressourcengruppen.
2. Klicken Sie auf der Seite Ressourcengruppen auf Erstellen, um den Assistenten zu starten.

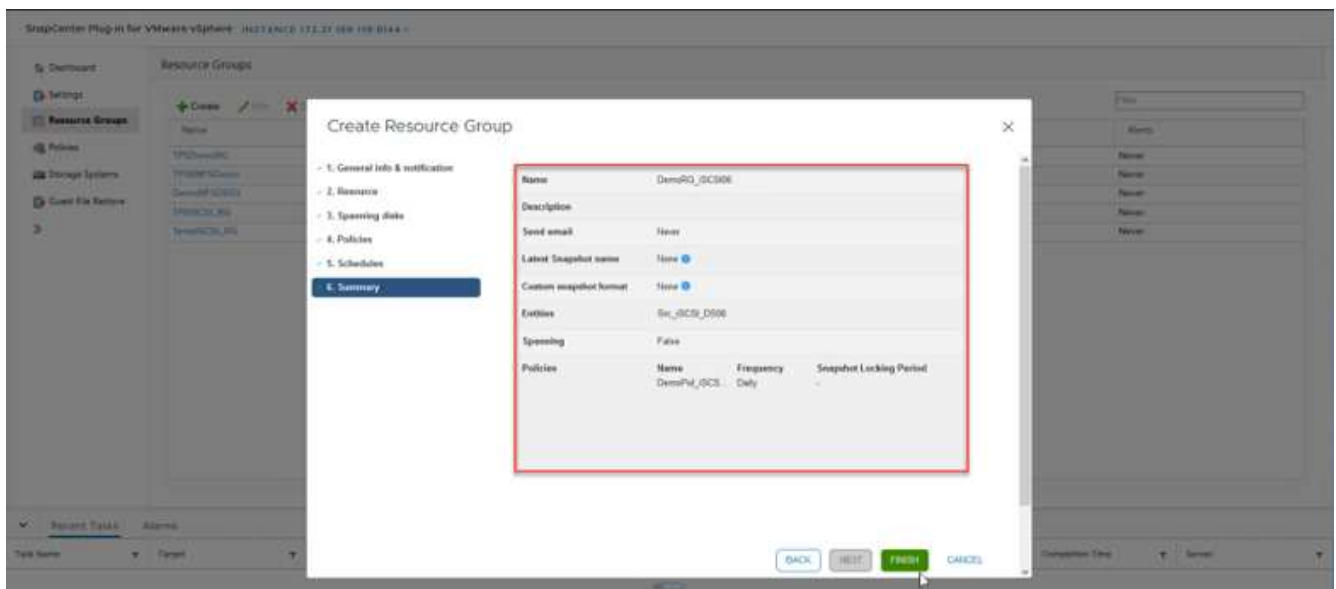
Eine weitere Option zum Erstellen von Ressourcengruppen ist die Auswahl der einzelnen VM oder des Datastores und die Erstellung einer Ressourcengruppe.



3. Wählen Sie auf der Seite Ressourcen den Umfang (virtuelle Maschinen oder Datastores) und das Rechenzentrum aus.

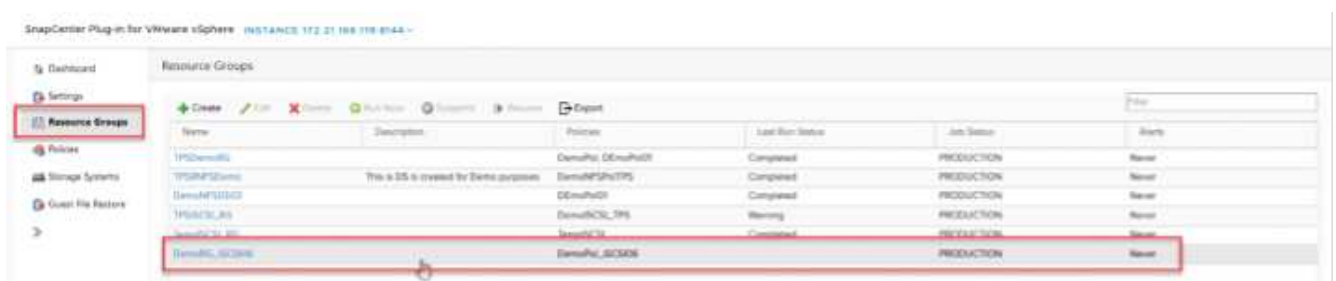


4. Wählen Sie auf der Seite Spanning Disks eine Option für Virtual Machines mit mehreren VMDKs über mehrere Datastores aus
5. Im nächsten Schritt wird eine Sicherungsrichtlinie zugeordnet. Wählen Sie eine vorhandene Richtlinie aus, oder erstellen Sie eine neue Backup-Richtlinie.
6. Konfigurieren Sie auf der Seite Zeitpläne den Backup-Zeitplan für jede ausgewählte Richtlinie.



7. Klicken Sie nach der Auswahl auf Fertig stellen.

Dadurch wird eine neue Ressourcengruppe erstellt und zur Liste der Ressourcengruppen hinzugefügt.



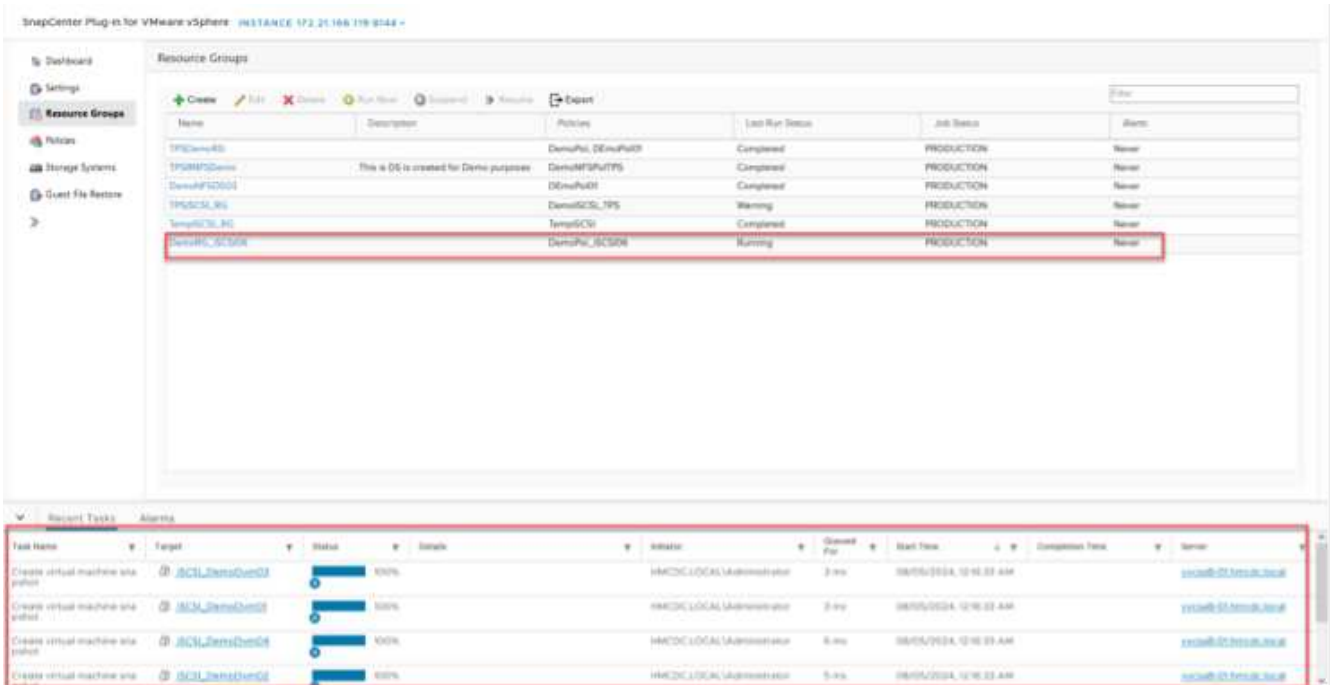
Sichern von Ressourcengruppen

Jetzt ist es an der Zeit, ein Backup auszulösen. Die Backup-Vorgänge werden für alle Ressourcen durchgeführt, die in einer Ressourcengruppe definiert sind. Wenn einer Ressourcengruppe eine Richtlinie angehängt und ein Zeitplan konfiguriert ist, werden die Backups automatisch gemäß dem Zeitplan durchgeführt.

1. Wählen Sie im linken Navigationsbereich der vCenter Web Client-Seite SnapCenter-Plug-in für VMware > Ressourcengruppen aus, und wählen Sie dann die entsprechende Ressourcengruppe aus. Wählen Sie Jetzt ausführen, um das Ad-hoc-Backup zu starten.



2. Wenn für die Ressourcengruppe mehrere Richtlinien konfiguriert sind, wählen Sie im Dialogfeld Jetzt sichern die Richtlinie für den Backup-Vorgang aus.
3. Wählen Sie OK, um die Sicherung zu starten.



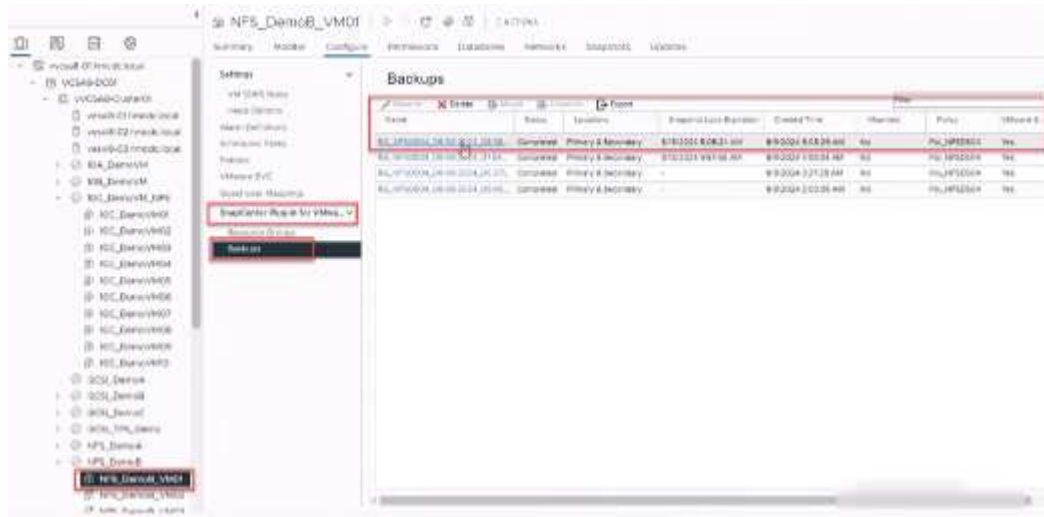
Überwachen Sie den Vorgangsfortschritt, indem Sie im unteren Bereich des Fensters die Option Letzte Aufgaben oder im Dashboard Job Monitor für weitere Details auswählen.

Wiederherstellung von VMs aus Backup

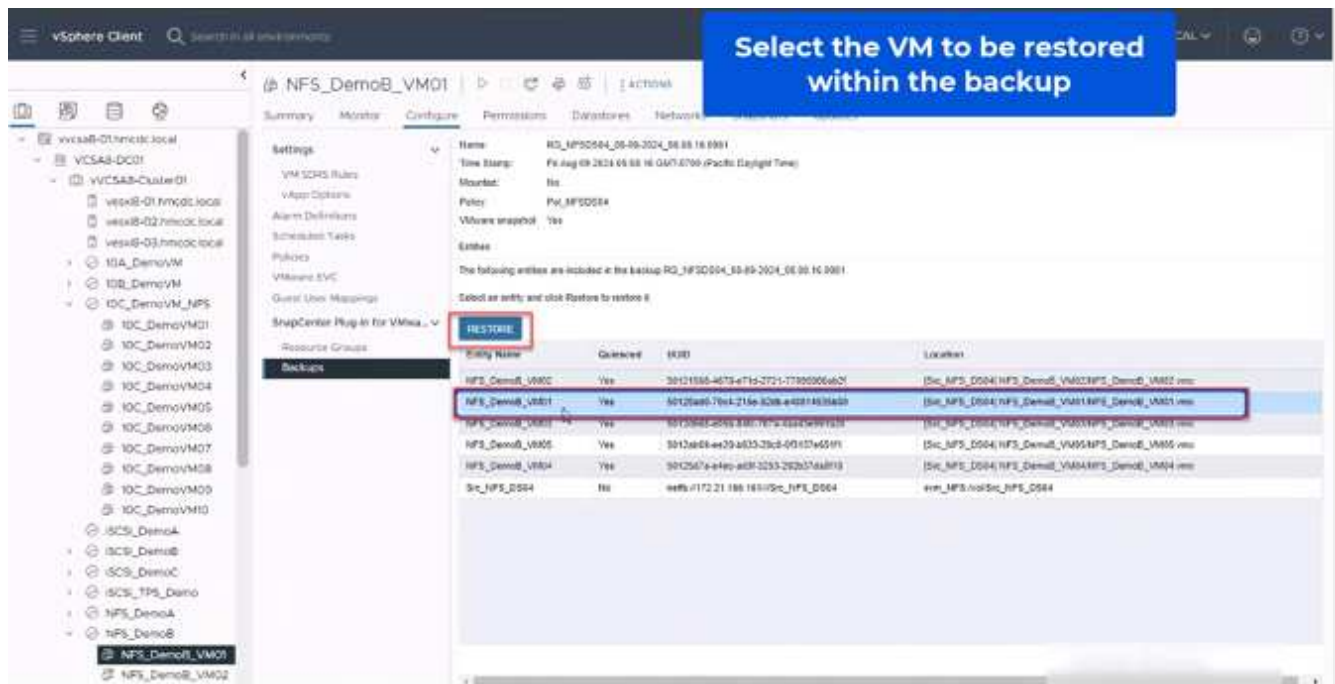
Mit dem SnapCenter Plug-in für VMware können Virtual Machines (VMs) in vCenter wiederhergestellt werden. Während der Wiederherstellung einer VM kann sie auf dem ursprünglichen Datastore wiederhergestellt werden, der auf dem ursprünglichen ESXi-Host gemountet ist. Dabei wird der vorhandene Inhalt mit der ausgewählten Sicherungskopie überschrieben oder eine gelöschte/umbenannte VM kann aus einer

Sicherungskopie wiederhergestellt werden (Vorgang überschreibt die Daten in den ursprünglichen virtuellen Laufwerken). Führen Sie die folgenden Schritte aus, um die Wiederherstellung durchzuführen:

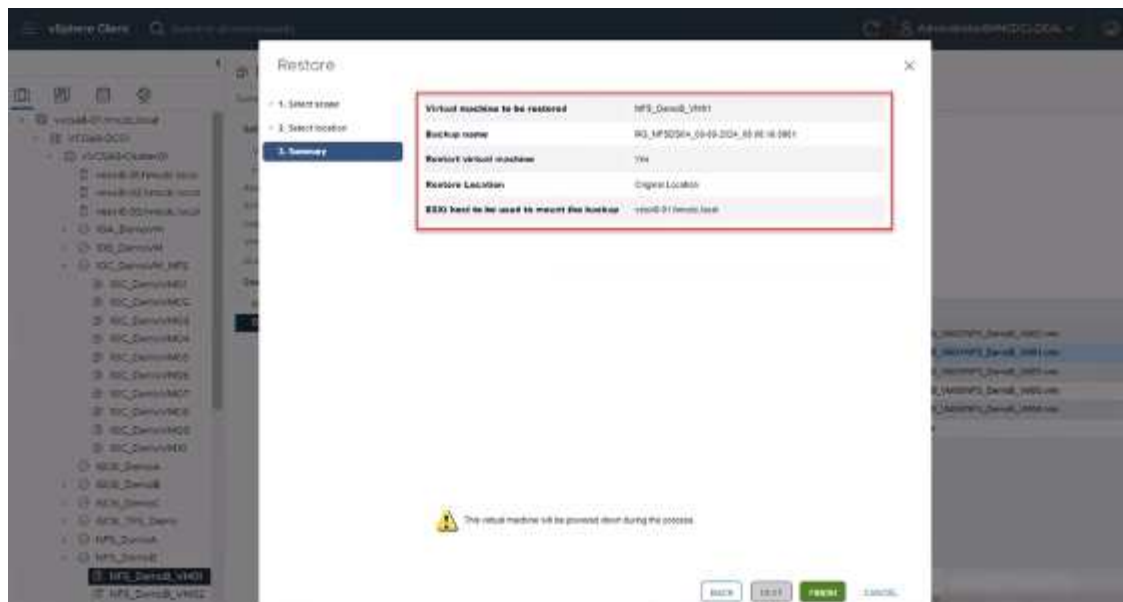
1. Wählen Sie in der VMware vSphere Web Client GUI in der Symbolleiste die Option Menü aus. Wählen Sie Inventar und dann Virtuelle Maschinen und Vorlagen.
2. Wählen Sie in der linken Navigation die virtuelle Maschine aus, und wählen Sie dann die Registerkarte Konfigurieren und unter SnapCenter-Plug-in für VMware die Option Backups auswählen aus. Klicken Sie auf den Backupjob, von dem die VM wiederhergestellt werden muss.



3. Wählen Sie die VM aus, die aus dem Backup wiederhergestellt werden soll.



4. Wählen Sie auf der Seite Bereich auswählen im Feld Bereich Wiederherstellen die Option gesamte virtuelle Maschine aus, wählen Sie Speicherort wiederherstellen aus, und geben Sie dann die ESXi-Zielinformationen ein, auf die das Backup gemountet werden soll. Aktivieren Sie das Kontrollkästchen VM neu starten, wenn die VM nach dem Wiederherstellungsvorgang eingeschaltet werden muss.

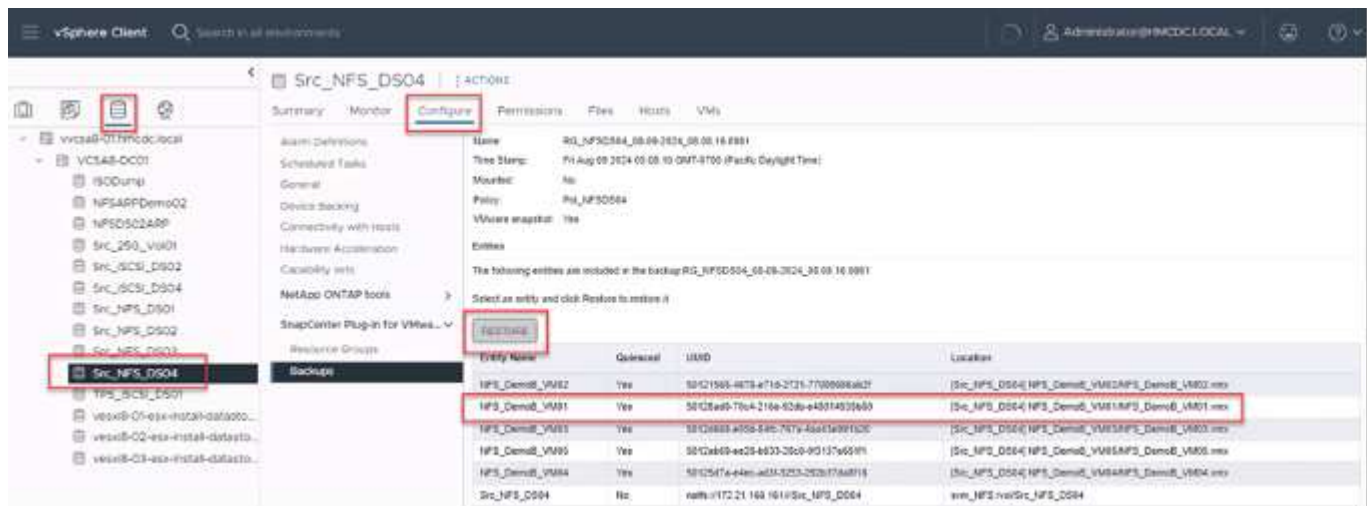


Überwachen Sie den Fortschritt des Vorgangs, indem Sie am unteren Bildschirmrand die Option Letzte Aufgaben auswählen.



Obwohl die VMs wiederhergestellt sind, werden sie nicht automatisch ihren früheren Ressourcengruppen hinzugefügt. Fügen Sie daher die wiederhergestellten VMs manuell den entsprechenden Ressourcengruppen hinzu, wenn ein Schutz dieser VMs erforderlich ist.

Was wäre, wenn die ursprüngliche VM gelöscht würde? Mit dem SnapCenter Plug-in für VMware ist die Aufgabe ganz einfach. Der Wiederherstellungsvorgang für eine gelöschte VM kann von der Datastore-Ebene aus durchgeführt werden. Wechseln Sie zu „jeweiliges Datastore“ > „Configure“ > „Backups“, wählen Sie die gelöschte VM aus und wählen Sie „Restore“ aus.

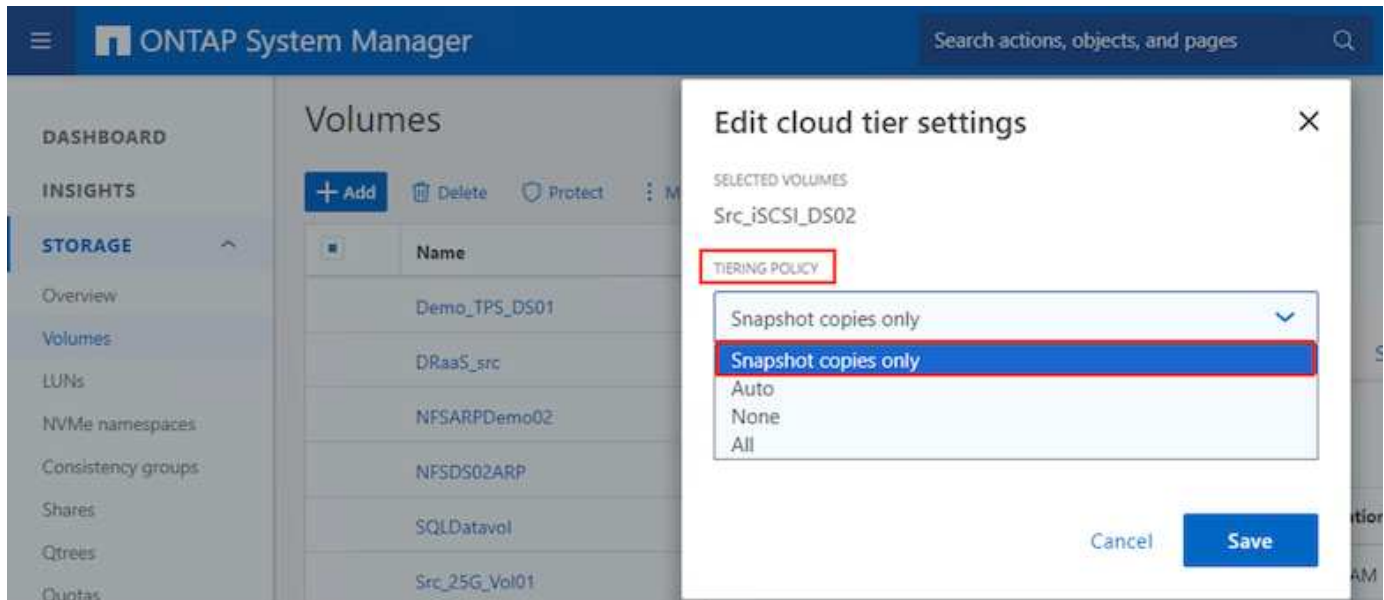


Zusammenfassend lässt sich sagen, dass Sie beim Einsatz von ONTAP ASA Storage zur Optimierung der TCO für eine VMware Implementierung das SnapCenter Plug-in für VMware als einfache und effiziente Methode für Backups von VMs verwenden. Sie ermöglicht es, VMs nahtlos und schnell zu sichern und wiederherzustellen, da Snapshot-Backups in nur wenigen Sekunden abgeschlossen sind.

Sehen Sie sich dies "[Lösungsleitfaden](#)" an und "[Produktdokumentation](#)" erfahren Sie mehr über SnapCenter Konfigurationen, Backups und Restores vom primären oder sekundären Storage-System oder sogar von

Backups, die auf Objekt-Storage zur langfristigen Aufbewahrung gespeichert sind.

Um Storage-Kosten zu senken, kann FabricPool Volume Tiering aktiviert werden, um Daten für Snapshot Kopien automatisch auf eine kostengünstigere Storage Tier zu verschieben. Snapshot-Kopien nutzen in der Regel mehr als 10 % des zugewiesenen Storage. Obwohl sie für Datensicherung und Disaster Recovery wichtig sind, werden diese zeitpunktgenauen Kopien nur selten verwendet und können keinen effizienten High-Performance Storage verwenden. Durch die „nur Snapshots“-Richtlinie für FabricPool wird auf einfache Weise Speicherplatz auf hochperformantem Storage freigesetzt. Wenn diese Richtlinie aktiviert ist, werden inaktive Blöcke von Snapshot-Kopien des Volume, die nicht vom aktiven Filesystem verwendet werden, in die Objektebene verschoben. Nach dem Lesen wird die Snapshot-Kopie auf die lokale Tier verschoben, um eine VM oder einen gesamten Datastore wiederherzustellen. Diese Objekt-Tier kann in Form einer Private Cloud (z. B. NetApp StorageGRID) oder einer Public Cloud (z. B. AWS oder Azure) vorliegen.

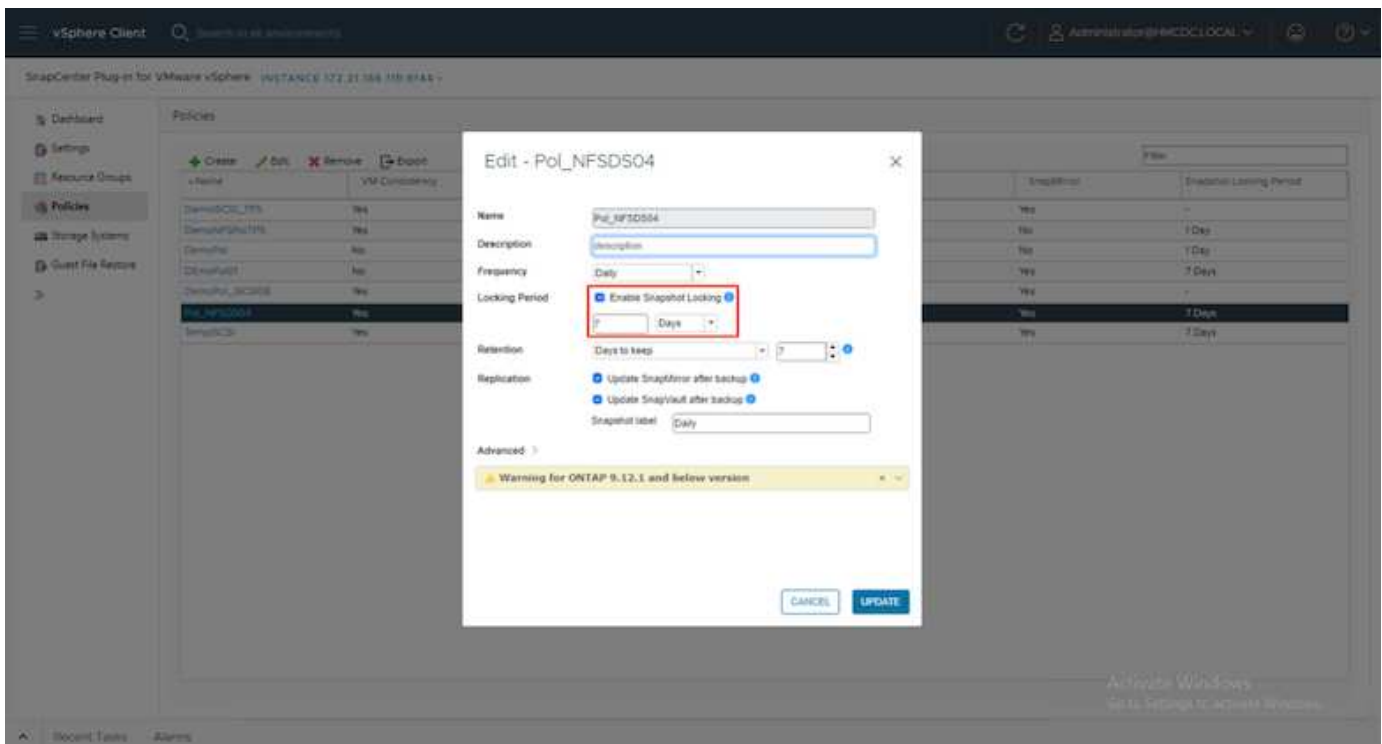


Ausführliche Anleitungen anzeigen für "VMware vSphere mit ONTAP –".

Schutz Vor Ransomware

Eine der effektivsten Methoden zum Schutz vor Ransomware-Angriffen ist die Implementierung mehrschichtiger Sicherheitsmaßnahmen. Jede virtuelle Maschine auf einem Datastore hostet ein Standard-Betriebssystem. Stellen Sie sicher, dass die Produktsuiten für Anti-Malware-Produkte von Unternehmensservern installiert und regelmäßig aktualisiert werden, was ein wesentlicher Bestandteil einer mehrschichtigen Ransomware-Schutzstrategie ist. Gleichzeitig können Sie mit der NetApp Snapshot Technologie eine Datensicherung implementieren, um nach einem Ransomware-Angriff eine schnelle und zuverlässige Recovery zu gewährleisten.

Ransomware-Angriffe zielen zunehmend auf Backups und Wiederherstellungspunkte von Snapshots ab, indem sie sie zu löschen versuchen, bevor sie Dateien verschlüsseln. Mit ONTAP lässt sich dies jedoch verhindern, indem manipulationssichere Snapshots auf primären oder sekundären Systemen mit "[NetApp Snapshot™ Sperren von Kopien](#)" in ONTAP erstellt werden. Diese Snapshot Kopien können von Angreifern oder betrügerischen Administratoren nicht gelöscht oder geändert werden. Die Kopien sind also auch nach einem Angriff verfügbar. Sie können Virtual Machine-Daten in Sekundenschnelle wiederherstellen und so die Ausfallzeiten Ihres Unternehmens minimieren. Zudem haben Sie die Flexibilität, den für Ihr Unternehmen passenden Snapshot-Zeitplan und die Sperrdauer auszuwählen.



Es besteht auch eine native integrierte ONTAP-Lösung zum Schutz vor dem unbefugten Löschen von Backup-Snapshot-Kopien. Sie wird als Multiadmin-Verifizierung oder MAV bezeichnet, die in ONTAP 9.11.1 und höher verfügbar ist. Der ideale Ansatz ist die Verwendung von Abfragen für MAV-spezifische Operationen.

Weitere Informationen zum MAV und zur Konfiguration der Schutzfunktionen finden Sie im ["Übersicht über die Verifizierung mit mehreren Administratoren"](#).

Migration

Viele IT-Abteilungen setzen im Zuge einer Transformationsphase auf den Hybrid-Cloud-First-Ansatz. Die Kunden bewerten ihre aktuelle IT-Infrastruktur und verschieben ihre Workloads auf der Grundlage dieser Bewertung und Analyse in die Cloud. Die Gründe für die Migration zur Cloud sind unterschiedlich. Es können Faktoren wie Elastizität und Burst-Kapazität, Datacenter-Ausstieg, Datacenter-Konsolidierung, Szenarien, Auslaufen des Lebenszyklus, Fusionen, Übernahmen und vieles mehr sein. Das Migrationsdenken jedes Unternehmens hängt von seinen spezifischen geschäftlichen Prioritäten ab, wobei die Kostenoptimierung die höchste Priorität hat. Die Auswahl des richtigen Cloud-Storage ist für den Wechsel zur Hybrid Cloud von entscheidender Bedeutung, da dadurch das Potenzial der Cloud-Implementierung und Flexibilität ausgeschöpft wird.

Durch die Integration in 1P-Services, die von NetApp bei jedem Hyperscaler unterstützt werden, können Unternehmen eine auf vSphere basierende Cloud-Lösung mit einem einfachen Migrationsansatz realisieren – ohne erneute Plattform, ohne IP-Änderungen oder ohne Änderungen an der Architektur. Zudem ermöglicht diese Optimierung eine Skalierung des Storage-Platzbedarfs, während die Host-Anzahl auf die geringste Menge in vSphere beschränkt wird, jedoch keine Änderung der Storage-Hierarchie, der Sicherheit oder der verfügbaren Dateien vorgenommen werden muss.

- Ausführliche Anleitungen anzeigen für ["Migrieren Sie Workloads in FSX ONTAP-Datastore"](#).
- Ausführliche Anleitungen anzeigen für ["Migrieren Sie Workloads in den Azure NetApp Files Datastore"](#).
- Ausführliche Anleitungen anzeigen für ["Migrieren Sie Workloads in den Google Cloud NetApp Volumes Datastore"](#).

Disaster Recovery

Disaster Recovery zwischen lokalen Standorten

Weitere Informationen finden Sie unter ["DR, die BlueXP DRaaS für VMFS-Datstores verwendet"](#)

Disaster Recovery zwischen On-Premises-Lösung und VMware Cloud in jedem Hyperscaler

Für Kunden, die VMware Cloud bei jedem Hyperscaler als Disaster-Recovery-Ziel verwenden möchten, können Datstores mit ONTAP Storage-Unterstützung (Azure NetApp Files, FSX ONTAP, Google Cloud NetApp Volumes) verwendet werden, um Daten aus der On-Premises-Umgebung mit einer validierten Drittanbieterlösung zu replizieren, die eine VM-Replizierungsfunktion bietet. Durch das Hinzufügen von Datstores, die über ONTAP Storage bereitgestellt werden, wird eine kostenoptimierte Disaster Recovery auf dem Ziel mit einer geringeren Anzahl an ESXi Hosts ermöglicht. Auf diese Weise können sekundäre Standorte in der On-Premises-Umgebung außer Betrieb gesetzt werden und dadurch erhebliche Kosteneinsparungen erzielt werden.

- Ausführliche Anleitungen anzeigen für ["Disaster Recovery für FSX ONTAP-Datstore"](#).
- Ausführliche Anleitungen anzeigen für ["Disaster Recovery für Azure NetApp Files Datstore"](#).
- Ausführliche Anleitungen anzeigen für ["Disaster Recovery für Google Cloud NetApp Volumes Datstore"](#).

Schlussfolgerung

Diese Lösung stellt den optimalen Ansatz für den Einsatz von ONTAP SAN-Technologien und OFFTAP Tools dar, um wichtige IT-Services für Unternehmen jetzt und in Zukunft bereitzustellen. Diese Vorteile sind insbesondere für virtualisierte Umgebungen von denen VMware vSphere in einem SAN ausgeführt wird, von Vorteil. Mit der Flexibilität und Skalierbarkeit der NetApp Storage-Systeme schaffen Unternehmen die Grundlage für die Aktualisierung und Anpassung ihrer Infrastruktur, damit sie den sich ändernden geschäftlichen Anforderungen über die Zeit gerecht werden können. Das System ist für aktuelle Workloads gerüstet und steigert die Infrastruktureffizienz, senkt die Betriebskosten und bereitet sich auf zukünftige Workloads vor.

NetApp All-Flash SAN-Array mit VMware vSphere 8

NetApp All-Flash SAN-Array mit VMware vSphere 8

Seit fast zwei Jahrzehnten hat sich die NetApp ONTAP Software als eine der führenden Storage-Lösungen für VMware vSphere Umgebungen etabliert und führt kontinuierlich innovative Funktionen ein, die das Management vereinfachen und Kosten senken. NetApp ist führend in der Entwicklung von NAS und Unified Storage-Plattformen, die eine Vielzahl von Protokollen und Konnektivitätsunterstützung bieten. Neben diesem Marktsegment gibt es viele Kunden, die die Einfachheit und die Kostenvorteile von blockbasierten SAN-Storage-Plattformen bevorzugen, die sich nur um eine gute Arbeit bewerben möchten. Die All-Flash SAN-Arrays (ASA) von NetApp werden diesem Versprechen gerecht: Sie profitieren von einfacher Skalierbarkeit sowie von konsistenten Management- und Automatisierungsfunktionen für alle Applikationen und Cloud-Provider.

Autor: Josh Powell – NetApp Solutions Engineering

Lösungsüberblick

Zweck dieses Dokuments

In diesem Dokument behandeln wir den besonderen Nutzen aus der Nutzung von NetApp ASA Storage-Systemen mit VMware vSphere und stellen einen Technologieüberblick über das rein Flash-basierte SAN-Array von NetApp zur Verfügung. Darüber hinaus sehen wir uns zusätzliche Tools zur Vereinfachung der Storage-Bereitstellung, der Datensicherung und des Monitoring Ihrer VMware und ONTAP Datacenter an.

Im Abschnitt zur Implementierung dieses Dokuments wird das Erstellen von vVol Datastores mit ONTAP Tools für VMware vSphere sowie Observability für das moderne Datacenter mit NetApp Cloud Insights behandelt.

Technologischer Überblick

Diese Lösung umfasst innovative Technologien von VMware und NetApp.

VMware vSphere 8.0

VMware vSphere ist eine Virtualisierungsplattform, mit der physische Ressourcen in Computing-, Netzwerk- und Storage-Pools umgewandelt werden, die zur Erfüllung der Workload- und Applikationsanforderungen von Kunden genutzt werden können. Zu den wichtigsten Komponenten von VMware vSphere gehören:

- **ESXi** - der Hypervisor von VMware, der die Abstraktion von Rechenprozessoren, Arbeitsspeicher, Netzwerk und anderen Ressourcen ermöglicht und diese virtuellen Maschinen und Container-Workloads zur Verfügung stellt.
- **VCenter** - VMware vCenter ist eine zentrale Management-Plattform für die Interaktion mit Computing-Ressourcen, Netzwerk und Speicher als Teil einer virtuellen Infrastruktur. VCenter spielt bei der Vereinfachung der Administration der virtualisierten Infrastruktur eine entscheidende Rolle.

Neue Verbesserungen in vSphere 8.0

vSphere 8.0 bringt einige neue Verbesserungen mit sich, darunter:

Skalierbarkeit - vSphere 8.0 unterstützt die neuesten Intel- und AMD-CPU's und hat erweiterte Limits für vGPU-Geräte, ESXi-Hosts, VMs pro Cluster und VM DirectPath-I/O-Geräte.

Distributed Services Engine - Netzwerkableitung mit NSX zu Data Processing Units (DPUs).

Verbesserte Geräteeffizienz - vSphere 8.0 verbessert die Geräteverwaltungsfunktionen mit Funktionen wie Gerätegruppen und Device Virtualization Extensions (DVX).

Verbesserte Sicherheit - die Einbindung einer SSH Timeout und TPM-Bereitstellungsrichtlinie stärkt das Sicherheitsframework.

Integration mit Hybrid Cloud Services – Diese Funktion ermöglicht einen nahtlosen Übergang zwischen On-Premises- und Cloud-Workloads.

Integrated Kubernetes Runtime - vSphere 8.0 vereinfacht mit Tanzu die Container-Orchestrierung.

Weitere Informationen finden Sie im Blog, ["Neuerungen in vSphere 8"](#).

VMware Virtual Volumes (VVols)

VVols stellen eine revolutionäre neue Herangehensweise an das Storage-Management in vSphere Clustern dar, die ein vereinfachtes Management und eine granularere Kontrolle der Storage-Ressourcen bietet. In

einem VVols Datastore ist jede virtuelle Festplatte ein vVol und wird zu einem nativen LUN-Objekt auf dem Storage-System. Die Integration des Storage-Systems mit vSphere erfolgt über den Provider **VMware API's for Storage Awareness (VASA)** und ermöglicht es dem Storage-System, die VM-Daten zu erkennen und entsprechend zu managen. Storage-Richtlinien, die im vCenter Client definiert werden, werden zur Zuweisung und Verwaltung von Speicherressourcen verwendet.

VVols bieten einen vereinfachten Ansatz für das Storage-Management und werden in einigen Anwendungsfällen bevorzugt.

Weitere Informationen zu VVols finden Sie im "[VVols Getting Started Guide](#)".

NVMe over Fabric

Mit der Veröffentlichung von vSphere 8.0 wird NVMe jetzt durchgängig unterstützt mit voller Unterstützung für VVols mit NVMe-TCP und NVMe-FC.

Detaillierte Informationen zur Verwendung von NVMe mit vSphere finden Sie unter "[VMware NVMe Storage](#)" In der vSphere Storage-Dokumentation.

NetApp ONTAP

Seit fast zwei Jahrzehnten ist die NetApp ONTAP Software 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. Die Kombination von ONTAP und vSphere ermöglicht Kosteneinsparungen für Host-Hardware und VMware Software. Sichern Sie Ihre Daten außerdem zu niedrigeren Kosten durch eine konstant hohe Performance und profitieren Sie gleichzeitig von der nativen Storage-Effizienz.

Basis-ONTAP-Funktionen

NetApp Snapshot Kopien: Snapshot Kopien einer VM oder eines Datastores. So wird die Performance bei der Erstellung oder Nutzung eines Snapshots nicht beeinträchtigt. Diese Replikat können als Wiederherstellungspunkte für VMs oder als einfache Datensicherung dienen. Diese Array-basierten Snapshots unterscheiden sich von den VMware (Konsistenz-)Snapshots. Die geradlinigste Methode zum Generieren einer ONTAP Snapshot Kopie ist das SnapCenter Plug-in für VMware vSphere für das Backup von VMs und Datastores.

- **Storage-Effizienz** – ONTAP bietet Deduplizierung und Komprimierung im Hintergrund in Echtzeit, Zero-Block-Deduplizierung und Data-Compaction.
- **Volume- und LUN-Verschiebung** - ermöglicht unterbrechungsfreies Verschieben von Volumes und LUNs, die vSphere Datastores und VVols im ONTAP-Cluster unterstützen, um Performance und Kapazität auszubalancieren oder unterbrechungsfreie Wartung und Upgrades zu ermöglichen.
- **Relocation von Volume und LUN** - ONTAP ermöglicht die unterbrechungsfreie Verschiebung von Volumes und LUNs auf denen vSphere Datastores und VVols im ONTAP Cluster gehostet werden. Dadurch können Performance und Kapazität besser ausbalanciert und unterbrechungsfreie Upgrades ermöglicht werden.
- **Quality of Service** - QoS ist eine Funktion, die das Management der Performance auf einer einzelnen LUN, einem Volume oder einer Datei ermöglicht. Mit dieser Lösung kann eine aggressive VM begrenzt oder sichergestellt werden, dass eine kritische VM ausreichend Performance-Ressourcen erhält.
- **Verschlüsselung** - NetApp-Volume-Verschlüsselung und NetApp-Aggregat-Verschlüsselung. Diese Optionen bieten einen einfachen, softwarebasierten Ansatz zur Verschlüsselung von Daten im

Ruhezustand und gewährleisten somit ihren Schutz.

- **Fabric Pool** - bei dieser Funktion werden Daten, auf die weniger häufig zugegriffen wird, in einen separaten Objektspeicher verlagert, wodurch wertvoller Flash-Speicher freigegeben wird. Auf Block-Ebene werden kältere Daten effizient erkannt und verschoben. So lassen sich Storage-Ressourcen optimieren und Kosten senken.
- **Automatisierung** – vereinfacht Storage- und Datenmanagementaufgaben durch den Einsatz von ONTAP REST-APIs zur Automatisierung und durch die Nutzung von Ansible-Modulen für ein nahtloses Konfigurationsmanagement von ONTAP-Systemen. Ansible-Module bieten eine praktische Lösung zum effizienten Management der Konfigurationen von ONTAP-Systemen. Durch die Kombination dieser leistungsstarken Tools werden die Workflows optimiert und das gesamte Management der Storage-Infrastruktur verbessert.

ONTAP Funktionen für die Disaster Recovery

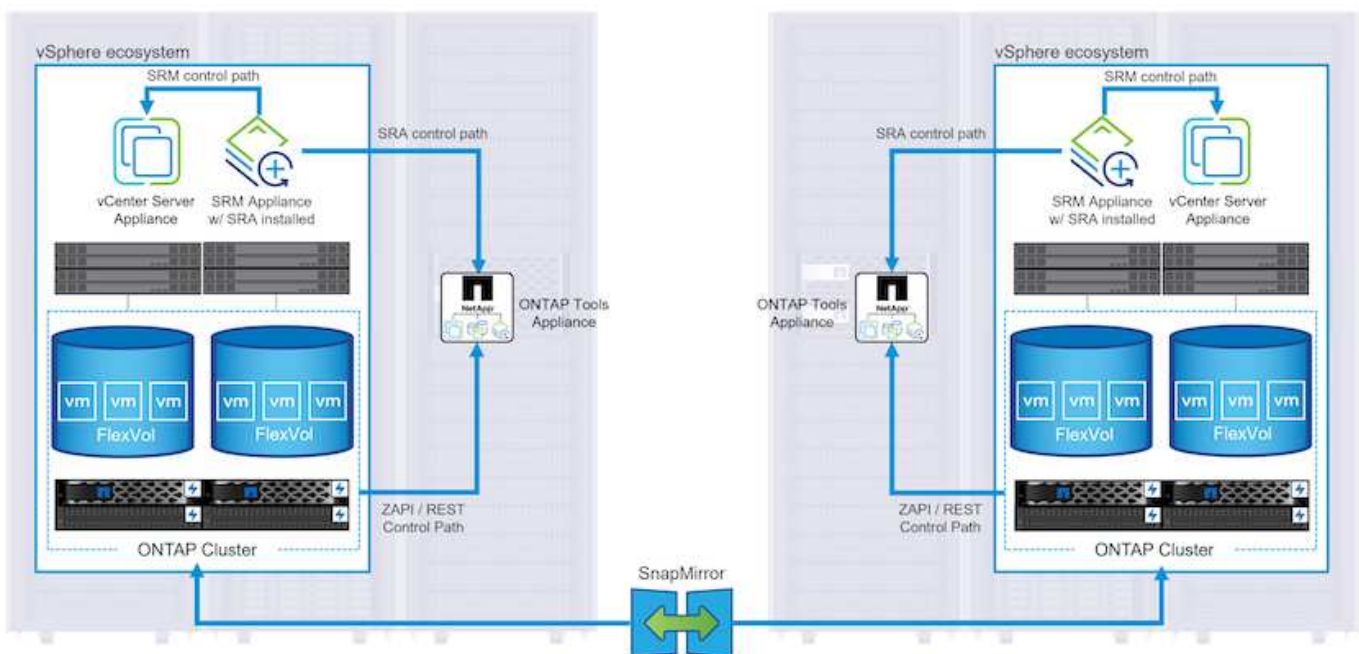
NetApp ONTAP bietet robuste Disaster Recovery-Lösungen für VMware Umgebungen. Diese Lösungen nutzen die SnapMirror Replizierungstechnologien zwischen primären und sekundären Storage-Systemen, um bei Ausfällen Failover und schnelle Recoverys zu ermöglichen.

Storage Replication Adapter:

Der NetApp Storage Replication Adapter (SRA) ist eine Softwarekomponente, die die Integration von NetApp Storage-Systemen mit VMware Site Recovery Manager (SRM) ermöglicht. Sie ermöglicht die Replizierung von VM-Daten (Virtual Machine) über NetApp Storage Arrays hinweg und liefert somit robuste Datensicherungs- und Disaster Recovery-Funktionen. SRA verwendet SnapMirror und SnapVault, um VM-Daten über heterogene Storage-Systeme oder geografische Standorte hinweg zu replizieren.

Der Adapter bietet mithilfe der SnapMirror Technologie asynchrone Replizierung auf SVM-Ebene (Storage Virtual Machine) und erweitert die Unterstützung von VMFS in SAN-Storage-Umgebungen (iSCSI und FC) und NFS in NAS-Storage-Umgebungen.

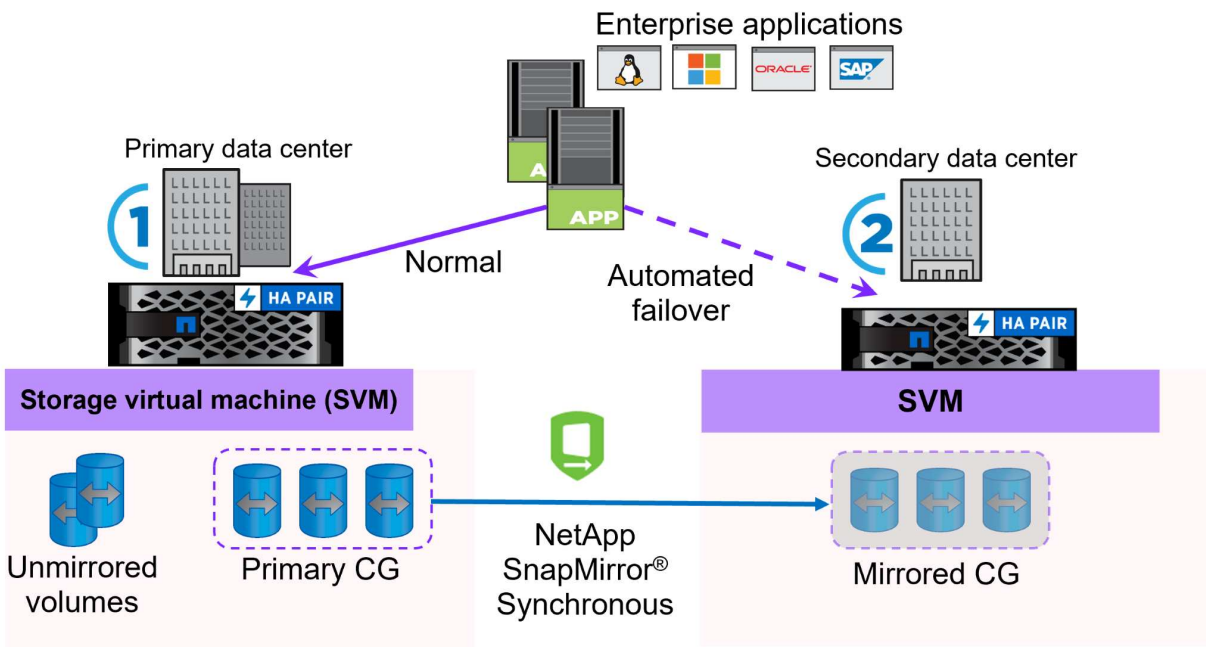
NetApp SRA wird im Rahmen der ONTAP-Tools für VMware vSphere installiert.



Weitere Informationen zum NetApp-Speicherreplikationsadapter für SRM finden Sie unter "[VMware Site Recovery Manager mit NetApp ONTAP](#)".

SnapMirror Business Continuity:

SnapMirror ist eine NetApp Technologie zur Datenreplizierung, mit der Daten zwischen Storage-Systemen synchron repliziert werden können. Sie ermöglicht die Erstellung mehrerer Datenkopien an verschiedenen Standorten, um Daten im Falle eines Ausfalls oder einer Datenverlust wiederherzustellen. SnapMirror bietet Flexibilität in Bezug auf die Replizierungshäufigkeit und ermöglicht die Erstellung zeitpunktgenauer Datenkopien für Backup- und Recovery-Zwecke. SM-BC repliziert Daten auf Konsistenzgruppenebene.



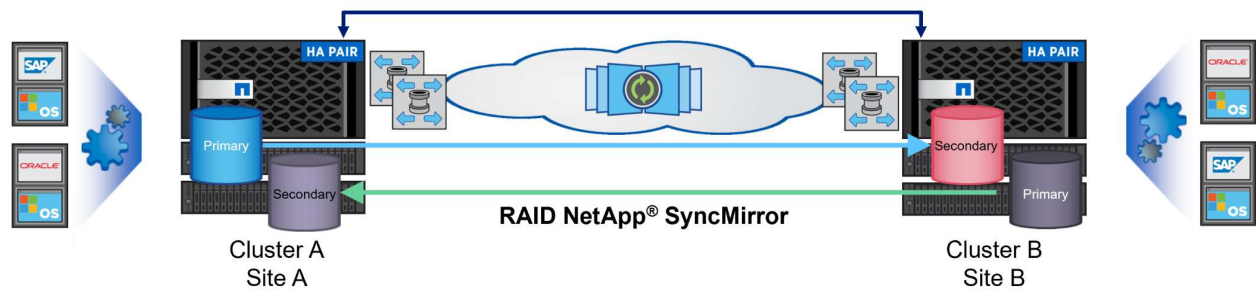
Weitere Informationen finden Sie unter SnapMirror "[Business Continuity im Überblick](#)".

NetApp MetroCluster:

NetApp MetroCluster ist eine Hochverfügbarkeits- und Disaster Recovery-Lösung mit synchroner Datenreplizierung zwischen zwei geografisch verteilten NetApp Storage-Systemen. Es wurde entwickelt, um kontinuierliche Datenverfügbarkeit und Datensicherheit bei einem standortweiten Ausfall zu gewährleisten.

MetroCluster verwendet SyncMirror, um Daten direkt über dem RAID-Level synchron zu replizieren. SyncMirror ist für die effiziente Migration zwischen synchronem und asynchronem Modus konzipiert. Dadurch kann das primäre Speicher-Cluster in Situationen, in denen vorübergehend nicht mehr auf den sekundären Standort zugegriffen werden kann, weiterhin in einem nicht replizierten Zustand betrieben werden. Bei der Wiederherstellung der Konnektivität repliziert SyncMirror auch zurück in den Zustand RPO = 0.

MetroCluster kann über IP-basierte Netzwerke oder über Fibre Channel betrieben werden.



Detaillierte Informationen zur Architektur und Konfiguration von MetroCluster finden Sie im "[MetroCluster Dokumentations-Website](#)".

ONTAP One Lizenzmodell

Bei ONTAP One handelt es sich um ein umfassendes Lizenzmodell, das den Zugriff auf alle Funktionen von ONTAP ohne zusätzliche Lizenzen ermöglicht. Dazu gehören Datensicherung, Disaster Recovery, Hochverfügbarkeit, Cloud-Integration, Storage-Effizienz, Performance und Sicherheit. Kunden mit NetApp Storage-Systemen, die mit Flash, Core PLUS Data Protection oder Premium lizenziert sind, haben Anspruch auf ONTAP One Lizenzierung und können so die Nutzung ihrer Storage-Systeme maximieren.

Die Lizenzierung von ONTAP One umfasst alle folgenden Funktionen:

NVMeoF – ermöglicht den Einsatz von NVMe over Fabrics für Front-End-Client-I/O, sowohl NVMe/FC als auch NVMe/TCP.

FlexClone – ermöglicht die schnelle Erstellung von platzsparendem Klonen von Daten auf Basis von Snapshots.

S3 – aktiviert das S3-Protokoll für Front-End-Client-I/O.

SnapRestore – ermöglicht schnelle Wiederherstellung von Daten aus Snapshots.

Autonomous Ransomware Protection - aktiviert den automatischen Schutz von NAS-Dateifreigaben, wenn abnormale Dateisystemaktivitäten erkannt werden.

Multi Tenant Key Manager - ermöglicht die Möglichkeit, mehrere Schlüsselmanager für verschiedene Mandanten im System zu haben.

SnapLock – ermöglicht den Schutz von Daten vor Veränderung, Löschung oder Beschädigung des Systems.

SnapMirror Cloud – ermöglicht die Replizierung von System-Volumes auf Objektziele.

S3 SnapMirror – ermöglicht die Replizierung von ONTAP S3 Objekten auf alternative S3-kompatible Ziele.

NetApp All-Flash-SAN-Array

Das rein Flash-basierte SAN-Array NetApp (ASA) ist eine hochperformante Storage-Lösung, die auf die hohen Anforderungen moderner Datacenter ausgerichtet ist. Sie kombiniert die Geschwindigkeit und Zuverlässigkeit von Flash Storage mit den erweiterten Datenmanagement-Funktionen von NetApp und bietet dadurch herausragende Performance, Skalierbarkeit und Datensicherung.

Die Produktpalette von ASA umfasst sowohl Die Modelle Der A-Serie als auch der C-Serie.

All-NVMe-Flash-Arrays der NetApp A-Serie wurden für hochperformante Workloads entwickelt und bieten eine äußerst niedrige Latenz und hohe Ausfallsicherheit. Dadurch sind sie für geschäftskritische Applikationen geeignet.



QLC Flash-Arrays der C-Serie richten sich an Anwendungsfälle mit höherer Kapazität, die die Geschwindigkeit von Flash mit der Wirtschaftlichkeit von Hybrid Flash bieten.



Ausführliche Informationen finden Sie im ["NetApp ASA Landing Page"](#).

Funktionen von NetApp ASA

Das rein Flash-basierte NetApp SAN-Array bietet folgende Funktionen:

Performance – das All-Flash-SAN-Array nutzt SSD-Laufwerke (Solid-State Drives) mit einer End-to-End-NVMe-Architektur, um eine blitzschnelle Performance bereitzustellen, die Latenz erheblich zu reduzieren und die Reaktionszeiten von Applikationen zu verbessern. Sie bietet konsistent hohe IOPS bei niedriger Latenz und ist somit für latenzkritische Workloads wie Datenbanken, Virtualisierung und Analysen geeignet.

Skalierbarkeit - NetApp All-Flash-SAN-Arrays verfügen über eine Scale-out-Architektur, mit der Unternehmen ihre Storage-Infrastruktur bei wachsenden Anforderungen nahtlos skalieren können. Mit der Möglichkeit, zusätzliche Storage-Nodes hinzuzufügen, können Unternehmen ihre Kapazität und Performance unterbrechungsfrei erhöhen und so sicherstellen, dass ihr Storage mit den steigenden Datenanforderungen Schritt halten kann.

Datenmanagement - das NetApp Betriebssystem Data ONTAP unterstützt das All-Flash SAN Array und bietet eine umfassende Suite an Datenmanagement-Funktionen. Dazu gehören Thin Provisioning, Deduplizierung, Komprimierung und Data-Compaction, mit denen die Storage-Auslastung optimiert und die Kosten gesenkt werden. Erweiterte Datensicherungsfunktionen wie Snapshots, Replizierung und Verschlüsselung stellen die

Integrität und Sicherheit der gespeicherten Daten sicher.

Integration und Flexibilität – das All-Flash SAN-Array lässt sich in das umfassendere Ecosystem von NetApp integrieren und ermöglicht so eine nahtlose Integration in andere NetApp Storage-Lösungen, wie z. B. Hybrid-Cloud-Implementierungen mit NetApp Cloud Volumes ONTAP. Außerdem werden Standardprotokolle wie Fibre Channel (FC) und iSCSI unterstützt, was eine einfache Integration in vorhandene SAN-Infrastrukturen ermöglicht.

Analyse und Automatisierung: Die Managementsoftware von NetApp, einschließlich NetApp Cloud Insights, bietet umfassende Monitoring-, Analyse- und Automatisierungsfunktionen. Mit diesen Tools erhalten Administratoren Einblicke in ihre Storage-Umgebung, optimieren die Performance und automatisieren Routineaufgaben, vereinfachen das Storage Management und verbessern die betriebliche Effizienz.

Datensicherung und Business Continuity – das All-Flash SAN Array bietet integrierte Funktionen zur Datensicherung wie Point-in-Time-Snapshots, Replikation und Disaster Recovery. Diese Funktionen sorgen für die Datenverfügbarkeit und ermöglichen im Falle von Datenverlusten oder Systemausfällen eine schnelle Recovery.

Unterstützte Protokolle

Das ASA unterstützt alle standardmäßigen SAN-Protokolle, einschließlich iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) und NVMe over Fabrics.

iSCSI - NetApp ASA bietet robuste Unterstützung für iSCSI und ermöglicht den Zugriff auf Speichergeräte auf Blockebene über IP-Netzwerke. Die nahtlose Integration mit iSCSI-Initiatoren ermöglicht eine effiziente Bereitstellung und Verwaltung von iSCSI-LUNs. Die erweiterten Funktionen von ONTAP wie Multi-Pathing, CHAP-Authentifizierung und ALUA-Unterstützung

Designanleitungen zu iSCSI-Konfigurationen finden Sie unter .

Fibre Channel - NetApp ASA bietet umfassende Unterstützung für Fibre Channel (FC), eine Hochgeschwindigkeits-Netzwerktechnologie, die häufig in Storage Area Networks (SANs) verwendet wird. ONTAP lässt sich nahtlos in FC-Infrastrukturen integrieren und bietet zuverlässigen und effizienten Zugriff auf Storage-Geräte auf Blockebene. Mit Funktionen wie Zoning, Multi-Pathing und Fabric Login (FLOGI) wird die Performance optimiert, die Sicherheit erhöht und die nahtlose Konnektivität in FC-Umgebungen sichergestellt.

Anleitungen zum Design von Fibre Channel-Konfigurationen finden Sie im "[Referenzdokumentation zur SAN-Konfiguration](#)".

NVMe over Fabrics: NetApp ONTAP und ASA unterstützen NVMe over Fabrics. NVMe/FC ermöglicht die Verwendung von NVMe-Storage-Geräten über Fibre-Channel-Infrastruktur und NVMe/TCP über Storage-IP-Netzwerke.

Eine Anleitung zum Design für NVMe finden Sie unter "[Konfiguration, Support und Einschränkungen von NVMe](#)".

Aktiv/aktiv-Technologie

NetApp All-Flash SAN Arrays ermöglichen aktiv/aktiv-Pfade durch beide Controller. Dadurch muss das Host-Betriebssystem nicht auf einen Ausfall eines aktiven Pfads warten, bevor der alternative Pfad aktiviert wird. Das bedeutet, dass der Host alle verfügbaren Pfade auf allen Controllern nutzen kann und sicherstellen kann, dass immer aktive Pfade vorhanden sind, unabhängig davon, ob sich das System in einem stabilen Zustand befindet oder ob ein Controller Failover durchgeführt wird.

Darüber hinaus bietet die NetApp ASA eine herausragende Funktion, die die Geschwindigkeit des SAN-

Failover enorm erhöht. Jeder Controller repliziert kontinuierlich wichtige LUN-Metadaten an seinen Partner. So ist jeder Controller bereit, bei einem plötzlichen Ausfall des Partners die Verantwortung für die Datenüberlassung zu übernehmen. Diese Bereitschaft ist möglich, da der Controller bereits über die notwendigen Informationen verfügt, um die Laufwerke zu nutzen, die zuvor vom ausgefallenen Controller verwaltet wurden.

Beim aktiv/aktiv-Pathing haben sowohl geplante als auch ungeplante Takeovers I/O-Wiederaufnahme-Zeiten von 2-3 Sekunden.

Weitere Informationen finden Sie unter ["TR-4968: NetApp All-SAS-Array – Datenverfügbarkeit und Datenintegrität mit der NetApp ASA"](#).

Storage-Garantien

NetApp bietet mit All-Flash-SAN-Arrays von NetApp einzigartige Storage-Garantien. Einzigartige Vorteile:

Storage-Effizienz-Garantie: mit der Storage-Effizienz-Garantie erzielen Sie eine hohe Performance bei gleichzeitiger Minimierung der Storage-Kosten. 4:1 für SAN-Workloads.

6 Nines (99.9999%) Data Availability guarantee: garantiert die Behebung von ungeplanten Ausfallzeiten in mehr als 31.56 Sekunden pro Jahr.

Ransomware Recovery-Garantie: Garantierte Datenwiederherstellung im Falle eines Ransomware-Angriffs.

Siehe ["NetApp ASA Produktportal"](#) Finden Sie weitere Informationen.

NetApp Plug-ins für VMware vSphere

NetApp Storage-Services sind mithilfe der folgenden Plug-ins eng in VMware vSphere integriert:

ONTAP Tools für VMware vSphere

Mit den ONTAP Tools für VMware können Administratoren NetApp Storage direkt innerhalb des vSphere Clients managen. Mit den ONTAP Tools können Sie Datastores implementieren und managen und vVol Datastores bereitstellen.

Mit ONTAP Tools können Datenspeicher Storage-Funktionsprofilen zugeordnet werden, die eine Reihe von Attributen des Storage-Systems bestimmen. Dadurch können Datastores mit bestimmten Attributen wie Storage-Performance oder QoS erstellt werden.

ONTAP-Tools enthält die folgenden Komponenten:

Virtual Storage Console (VSC): die VSC umfasst die in den vSphere-Client integrierte Schnittstelle, über die Sie Speicher-Controller hinzufügen, Datenspeicher bereitstellen, die Performance von Datastores überwachen und ESXi-Hosteinstellungen anzeigen und aktualisieren können.

VASA Provider: der VMware vSphere APIs for Storage Awareness (VASA) Provider für ONTAP sendet Informationen über den von VMware vSphere verwendeten Storage an den vCenter Server, wodurch die Bereitstellung von VMware Virtual Volumes (VVols)-Datastores, die Erstellung und Nutzung von Storage-Funktionsprofilen, Compliance-Überprüfung und Performance-Monitoring ermöglicht werden.

Storage Replication Adapter (SRA): Wenn SRA aktiviert ist und mit VMware Site Recovery Manager (SRM) verwendet wird, erleichtert SRA die Wiederherstellung von vCenter Server-Datastores und virtuellen Maschinen im Falle eines Ausfalls und ermöglicht so die Konfiguration geschützter Standorte und Recovery-

Standorte für die Disaster Recovery.

Weitere Informationen zu NetApp ONTAP-Tools für VMware finden Sie unter ["ONTAP-Tools für VMware vSphere - Dokumentation"](#).

SnapCenter Plug-in für VMware vSphere

Das SnapCenter Plug-in für VMware vSphere (SCV) ist eine Softwarelösung von NetApp, die umfassende Datensicherung für VMware vSphere Umgebungen bietet. Er vereinfacht und optimiert den Prozess des Schutzes und des Managements von Virtual Machines (VMs) und Datastores.

Das SnapCenter Plug-in für VMware vSphere bietet folgende Funktionen in einer einheitlichen Oberfläche, die in den vSphere Client integriert ist:

Policy-basierte Snapshots - mit SnapCenter können Sie Richtlinien für die Erstellung und Verwaltung von anwendungskonsistenten Snapshots von virtuellen Maschinen (VMs) in VMware vSphere definieren.

Automatisierung - automatisierte Snapshot-Erstellung und -Verwaltung auf Basis definierter Richtlinien unterstützen einen konsistenten und effizienten Datenschutz.

Schutz auf VM-Ebene - granularer Schutz auf VM-Ebene ermöglicht effizientes Management und Recovery einzelner virtueller Maschinen.

Funktionen zur Storage-Effizienz - durch die Integration in NetApp Storage-Technologien können Storage-Effizienz-Funktionen wie Deduplizierung und Komprimierung für Snapshots erzielt werden, was die Speicheranforderungen minimiert.

Das SnapCenter-Plug-in orchestriert die Stilllegung von Virtual Machines in Verbindung mit hardwarebasierten Snapshots auf NetApp Storage-Arrays. Die SnapMirror Technologie wird eingesetzt, um Backup-Kopien auf sekundäre Storage-Systeme einschließlich in der Cloud zu replizieren.

Weitere Informationen finden Sie im ["Dokumentation zum SnapCenter Plug-in für VMware vSphere"](#).

Die Integration von BlueXP ermöglicht 3-2-1-1-Backup-Strategien zur Erweiterung von Datenkopien auf Objekt-Storage in der Cloud.

Weitere Informationen zu 3-2-1-1-Backup-Strategien mit BlueXP finden Sie unter ["3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs"](#).

NetApp Cloud Insights

NetApp Cloud Insights vereinfacht die Beobachtung der On-Premises- und Cloud-Infrastruktur und bietet Analyse- und Fehlerbehebungsfunktionen, um komplexe Probleme zu lösen. Cloud Insights erfasst Daten aus einer Datacenter-Umgebung und sendet sie in die Cloud. Dies geschieht mit lokal installierter Software, der sogenannten Acquisition Unit, und mit spezifischen Sammlern, die für die Assets im Rechenzentrum aktiviert sind.

Die Assets in Cloud Insights können mit Annotationen versehen werden, die eine Methode zum Organisieren und Klassifizieren von Daten bieten. Dashboard kann mit einer Vielzahl von Widgets für die Anzeige der Daten erstellt werden, und Metric Abfragen können für detaillierte tabellarische Datenansichten erstellt werden.

Im Lieferumfang von Cloud Insights sind zahlreiche fertige Dashboards enthalten, mit denen sich bestimmte Arten von Problembereichen und Datenkategorien genau herausstellen lassen.

Cloud Insights ist ein heterogenes Tool, mit dem Daten von einer Vielzahl von Geräten erfasst werden können. Es gibt jedoch eine Bibliothek mit Vorlagen mit dem Namen „ONTAP Essentials“, mit der NetApp-Kunden den Einstieg leicht machen können.

Detaillierte Informationen zum Einstieg in Cloud Insights finden Sie im ["Landing Page von NetApp BlueXP und Cloud Insights"](#).

NetApp All-Flash SAN-Array mit VMware vSphere 8

Mit den ONTAP Tools für VMware können Administratoren NetApp Storage direkt innerhalb des vSphere Clients managen. Mit den ONTAP Tools können Sie Datastores implementieren und managen und vVol Datastores bereitstellen.

Mit ONTAP Tools können Datenspeicher Storage-Funktionsprofilen zugeordnet werden, die eine Reihe von Attributen des Storage-Systems bestimmen. Dadurch können Datastores mit bestimmten Attributen wie Storage-Performance oder QoS erstellt werden.

Autor: Josh Powell – NetApp Solutions Engineering

Managen von Blockspeicher mit ONTAP-Tools für VMware vSphere

ONTAP-Tools enthält die folgenden Komponenten:

Virtual Storage Console (VSC): die VSC umfasst die in den vSphere-Client integrierte Schnittstelle, über die Sie Speicher-Controller hinzufügen, Datenspeicher bereitstellen, die Performance von Datastores überwachen und ESXi-Hosteinstellungen anzeigen und aktualisieren können.

VASA Provider: der VMware vSphere APIs for Storage Awareness (VASA) Provider für ONTAP sendet Informationen über den von VMware vSphere verwendeten Storage an den vCenter Server, wodurch die Bereitstellung von VMware Virtual Volumes (VVols)-Datastores, die Erstellung und Nutzung von Storage-Funktionsprofilen, Compliance-Überprüfung und Performance-Monitoring ermöglicht werden.

Storage Replication Adapter (SRA): Wenn SRA aktiviert ist und mit VMware Site Recovery Manager (SRM) verwendet wird, erleichtert SRA die Wiederherstellung von vCenter Server-Datastores und virtuellen Maschinen im Falle eines Ausfalls und ermöglicht so die Konfiguration geschützter Standorte und Recovery-Standorte für die Disaster Recovery.

Weitere Informationen zu NetApp ONTAP-Tools für VMware finden Sie unter ["ONTAP-Tools für VMware vSphere - Dokumentation"](#).

Übersicht Zur Lösungsimplementierung

In dieser Lösung demonstrieren wir die Verwendung der ONTAP Tools für VMware vSphere zur Bereitstellung eines VMware Virtual Volumes (vVol)-Datastores und erstellen eine virtuelle Maschine auf einem vVol-Datastore.

In einem VVols Datastore ist jede virtuelle Festplatte ein vVol und wird zu einem nativen LUN-Objekt auf dem Storage-System. Die Integration des Storage-Systems und vSphere erfolgt über den VASA Provider (VMware API's for Storage Awareness) (installiert mit ONTAP Tools), mit dem das Storage-System die VM-Daten erkennen und entsprechend managen kann. Storage-Richtlinien, die im vCenter Client definiert werden, werden zur Zuweisung und Verwaltung von Speicherressourcen verwendet.

Detaillierte Informationen zu VVols mit ONTAP finden Sie unter ["Virtual Volumes VVols\) mit ONTAP"](#).

Diese Lösung deckt die folgenden grundlegenden Schritte ab:

1. Fügen Sie in den ONTAP-Tools ein Storage-System hinzu.
2. Erstellen Sie in ONTAP-Tools ein Storage-Funktionsprofil.
3. Erstellen Sie einen VVols-Datastore in ONTAP Tools.
4. Erstellen Sie eine VM-Storage-Richtlinie im vSphere Client.
5. Erstellen Sie eine neue virtuelle Maschine auf dem vVol-Datastore.

Voraussetzungen

Folgende Komponenten wurden in dieser Lösung verwendet:

1. NetApp All-Flash SAN-Array A400 mit ONTAP 9.13
2. Auf dem ASA erstellte iSCSI-SVM mit Netzwerkverbindung zu den ESXi-Hosts
3. ONTAP Tools für VMware vSphere 9.13 (VASA Provider ist standardmäßig aktiviert).
4. vSphere 8.0-Cluster (vCenter-Appliance und ESXi-Hosts).

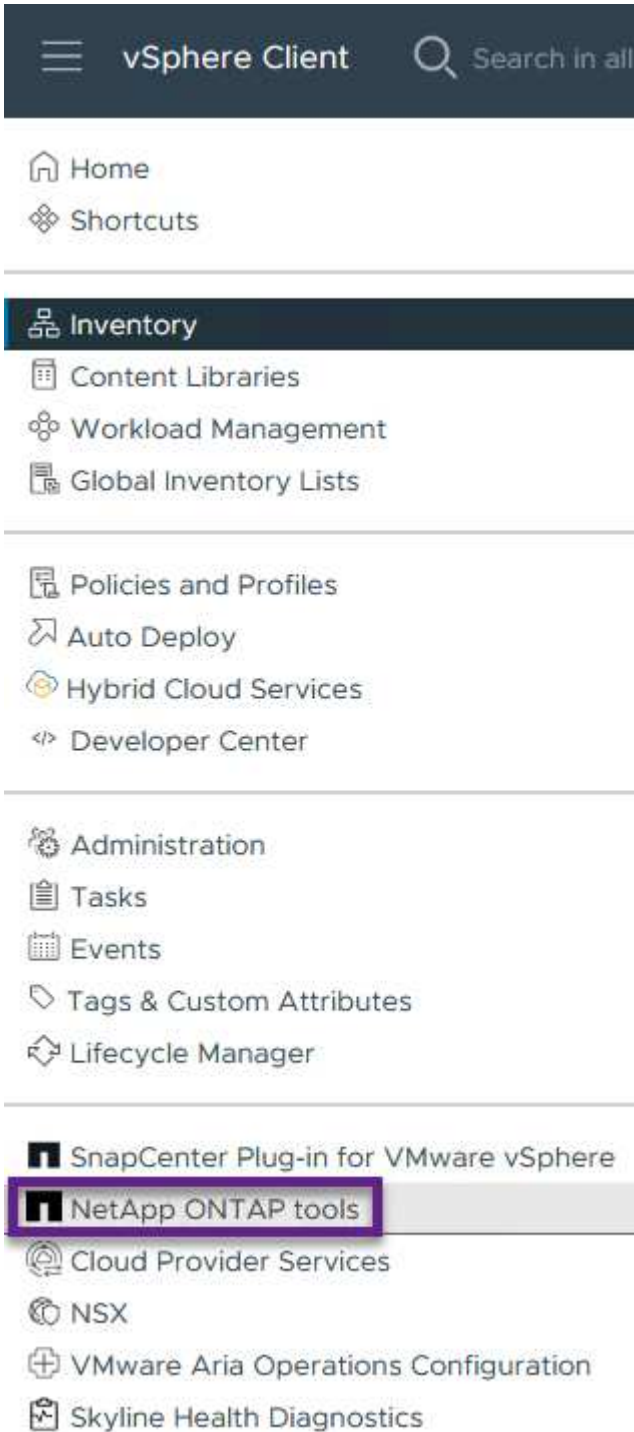
Lösungsimplementierung

Erstellen Sie einen VVols-Datastore in ONTAP Tools

Führen Sie die folgenden Schritte aus, um einen VVols-Datastore in ONTAP Tools zu erstellen:

Fügen Sie ONTAP Tools ein Storage-System hinzu.

1. Greifen Sie auf die NetApp ONTAP-Tools zu, indem Sie sie im Hauptmenü des vSphere-Clients auswählen.



2. Wählen Sie in den ONTAP-Tools im linken Menü **Speichersysteme** aus, und drücken Sie dann **Hinzufügen**.



NetApp ONTAP tools INSTANCE 10.61.181.154:8443 ▾

Overview

Storage Systems

Storage capability profile

ADD **REDISCOVER ALL**

3. Geben Sie die IP-Adresse, die Anmeldeinformationen des Speichersystems und die Portnummer ein. Klicken Sie auf **Add**, um den Ermittlungsvorgang zu starten.

Add Storage System



Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

10.61.181.205 ▾

Name or IP address:

10.192.102.103

Username:

admin

Password:

●●●●●●●●

Port:

443

Advanced options ^

ONTAP Cluster Certificate:



Automatically fetch



Manually upload

CANCEL

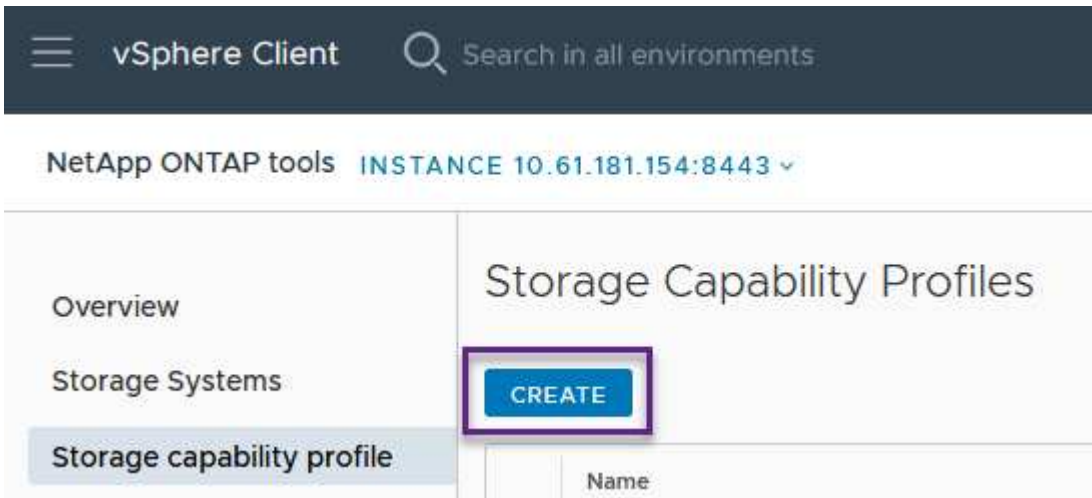
ADD

Erstellen Sie in ONTAP-Tools ein Storage-Funktionsprofil

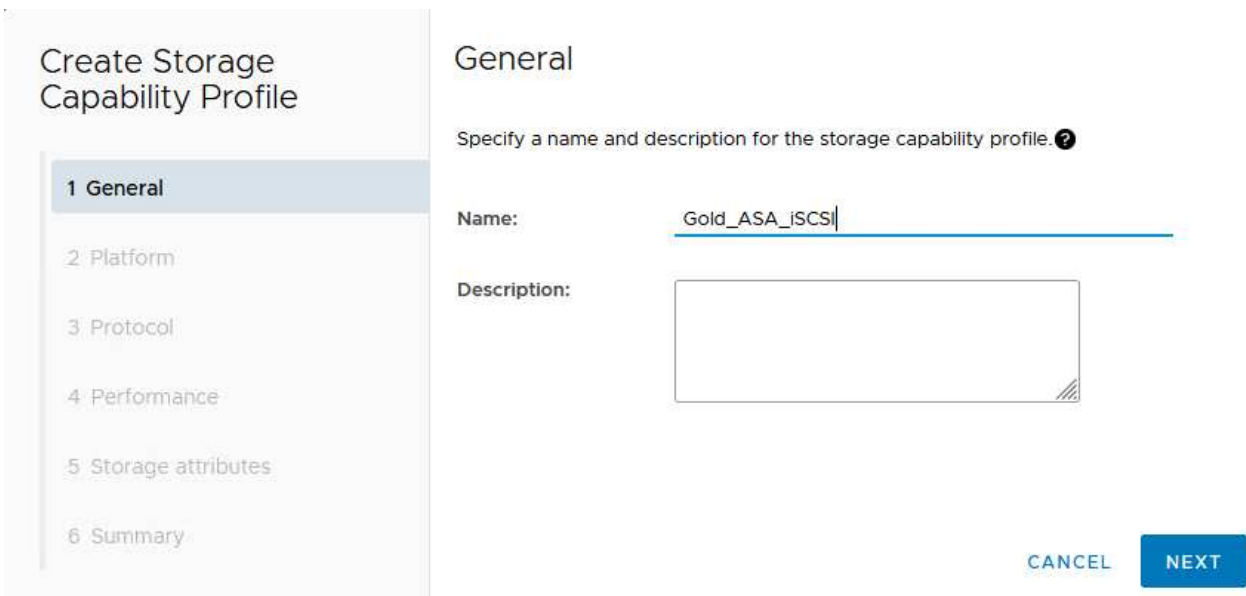
Storage-Funktionsprofile beschreiben die Funktionen eines Storage-Arrays oder Storage-Systems. Sie umfassen Definitionen zur Servicequalität und werden zur Auswahl von Storage-Systemen verwendet, die die im Profil definierten Parameter erfüllen.

Führen Sie die folgenden Schritte aus, um ein Storage-Funktionsprofil in ONTAP Tools zu erstellen:

1. Wählen Sie in den ONTAP-Tools im linken Menü **Speicherfähigkeitsprofil** aus und drücken Sie dann **Erstellen**.



2. Geben Sie im Assistenten **Create Storage Capability Profile** einen Namen und eine Beschreibung des Profils ein und klicken Sie auf **Weiter**.



3. Wählen Sie den Plattfortmtyp aus und geben Sie an, dass das Speichersystem ein All-Flash-SAN-Array sein soll. Setzen Sie **Asymmetric** auf FALSE.

Create Storage Capability Profile

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

Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. Wählen Sie als nächstes das gewünschte Protokoll oder **any** aus, um alle möglichen Protokolle zuzulassen. Klicken Sie auf **Weiter**, um fortzufahren.

Create Storage Capability Profile

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

Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. Die Seite **Performance** ermöglicht die Einstellung der Servicequalität in Form von erlaubten Mindest- und Höchstwerten.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

6. Füllen Sie die Seite **Storage-Attribute** aus und wählen Sie nach Bedarf Storage-Effizienz, Speicherplatzreservierung, Verschlüsselung und beliebige Tiering-Richtlinien aus.

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:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

7. Überprüfen Sie abschließend die Zusammenfassung, und klicken Sie auf Fertig stellen, um das Profil zu erstellen.

Create Storage Capability Profile

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

Summary

Name:	ASA_Gold
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	No
Tiering policy (FabricPool):	None

CANCEL

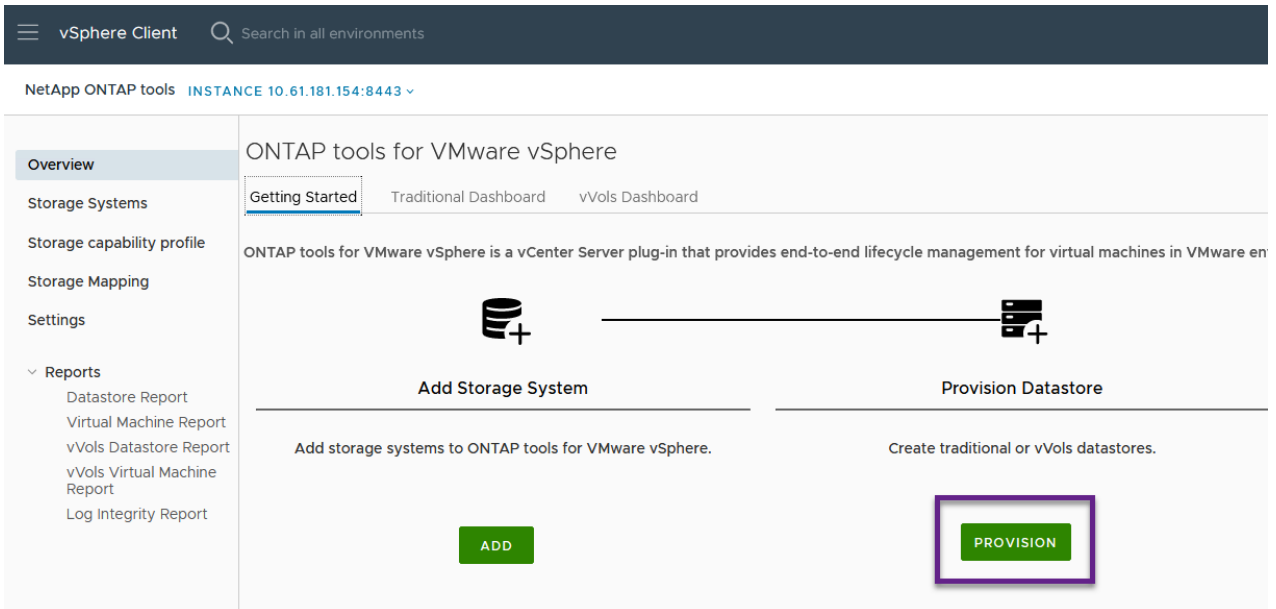
BACK

FINISH

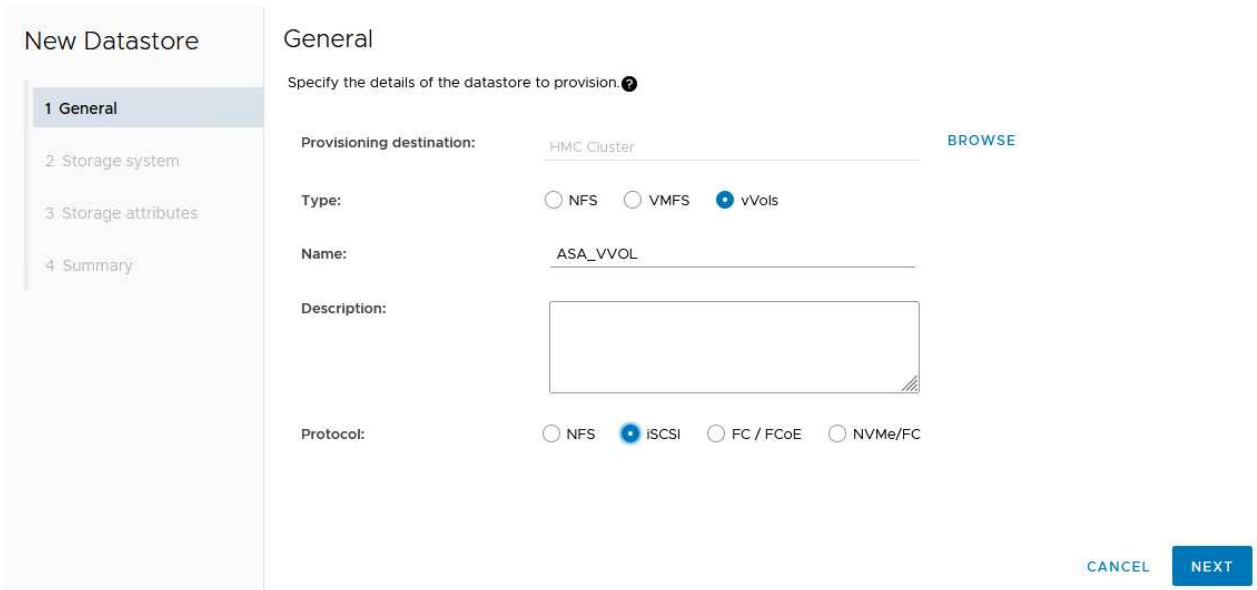
Erstellen Sie einen VVols-Datstore in ONTAP Tools

Führen Sie die folgenden Schritte aus, um einen VVols-Datstore in ONTAP Tools zu erstellen:

1. Wählen Sie in den ONTAP-Tools **Übersicht** und klicken Sie im Register **erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.



2. Wählen Sie auf der Seite **Allgemein** des Assistenten für neue Datenspeicher das vSphere Datacenter- oder Cluster-Ziel aus. Wählen Sie **VVols** als Typ dastore aus, geben Sie einen Namen für den Datenspeicher ein und wählen Sie das Protokoll aus.



3. Wählen Sie auf der Seite **Storage System** das Speicherfähigkeitsprofil, das Speichersystem und die SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

FAS_Default
FAS_Max20
Custom profiles
Gold_ASA_JSCSI
Gold_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svm1

CANCEL

BACK

NEXT

4. Wählen Sie auf der Seite **Speicherattribute** aus, um ein neues Volume für den Datenspeicher zu erstellen und die Speicherattribute des zu erstellenden Volumes auszufüllen. Klicken Sie auf **Add**, um das Volume zu erstellen, und dann auf **Next**, um fortzufahren.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
ASA_VVOL	2000	Gold_ASA	HCG_A400_E3u3b_NVMe	Thin

ADD

CANCEL

BACK

NEXT

5. Überprüfen Sie abschließend die Zusammenfassung und klicken Sie auf **Finish**, um den vVol Datastore-Erstellungsprozess zu starten.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

General

vCenter server: 10.61.181.205

Provisioning destination: HMC Cluster

Datastore name: ASA_VVOL

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: Gold_ASA

Storage system details

Storage system: HCG-NetApp-A400-E3U03

SVM: svm1

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

Erstellen Sie eine VM-Storage-Richtlinie im vSphere Client

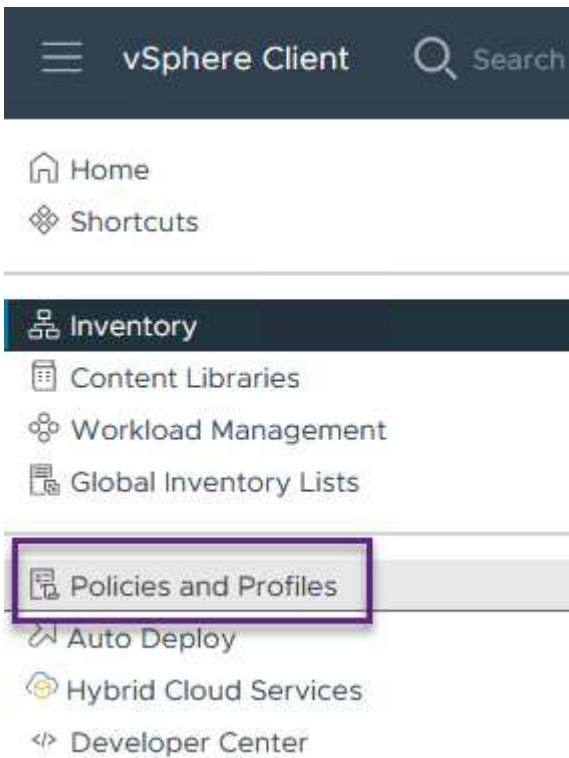
Eine VM Storage-Richtlinie ist eine Reihe von Regeln und Anforderungen, die festlegen, wie Daten für Virtual Machines (VM) gespeichert und gemanagt werden sollen. Er gibt die gewünschten Storage-Merkmale wie Performance, Verfügbarkeit und Datenservices für eine bestimmte VM an.

In diesem Fall umfasst die Aufgabe das Erstellen einer VM-Speicherrichtlinie, um anzugeben, dass eine virtuelle Maschine auf vVol-Datstores generiert wird, und um eine 1:1-Zuordnung mit dem zuvor generierten Storage-Funktionsprofil zu erstellen.

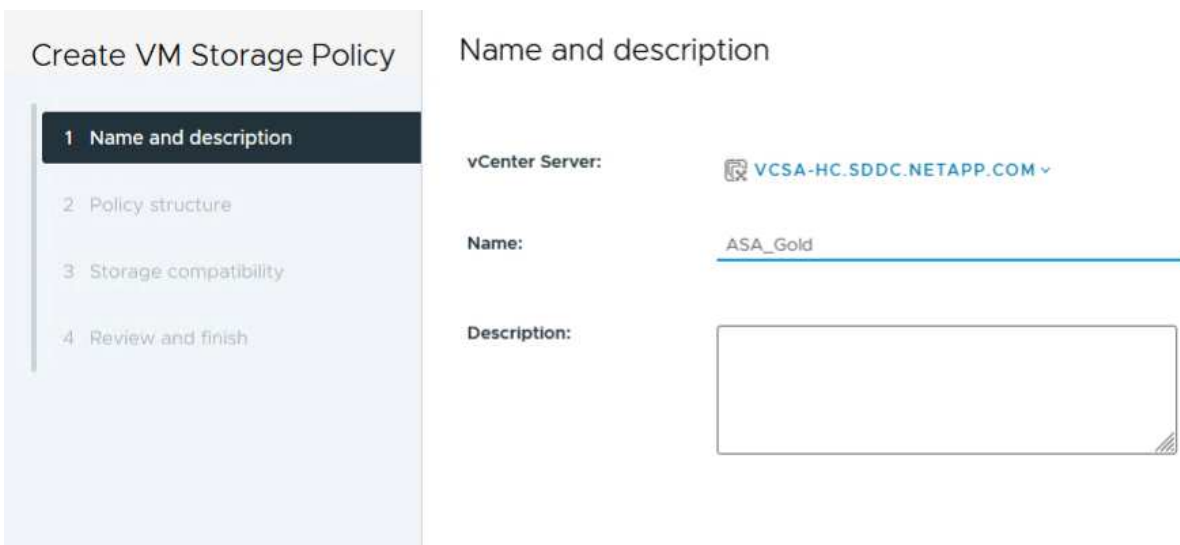
Erstellen einer VM-Storage-Richtlinie

Führen Sie die folgenden Schritte aus, um eine VM-Storage-Richtlinie zu erstellen:

1. Wählen Sie im vSphere Clients Hauptmenü **Policies und Profile**.



2. Geben Sie im Assistenten **Create VM Storage Policy** zunächst einen Namen und eine Beschreibung für die Richtlinie ein und klicken Sie auf **Weiter**, um fortzufahren.

The image shows the 'Create VM Storage Policy' wizard. On the left, there is a sidebar with four steps: '1 Name and description' (highlighted), '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The main area is titled 'Name and description' and contains three fields: 'vCenter Server' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name' with a text input field containing 'ASA_Gold', and 'Description' with a large empty text area.

3. Wählen Sie auf der Seite **Richtlinienstruktur** die Option aus, um Regeln für NetApp Clustered Data ONTAP vVol-Speicher zu aktivieren, und klicken Sie auf **Weiter**.

Create VM Storage Policy

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

Policy structure ✕

Host based services

Create rules for data services provided by hosts. Available data services could include encryption, I/O control, caching, etc. Host based services will be applied in addition to any datastore specific rules.

Enable host based rules

Datastore specific rules

Create rules for a specific storage type to configure data services provided by the datastores. The rules will be applied when VMs are placed on the specific storage type.

Enable rules for "vSAN" storage
 Enable rules for "vSANDirect" storage
 Enable rules for "VMFS" storage
 Enable rules for "NetApp.clustered.Data.ONTAP.VP.VASA10" storage
 Enable rules for "NetApp.clustered.Data.ONTAP.VP.vvol" storage
 Enable tag based placement rules

Storage topology

Create rules for storage consumption domain topology. The storage topology will be applied to all datastore specific rules.

Enable consumption domain

CANCEL
BACK
NEXT

4. Wählen Sie auf der nächsten Seite im Hinblick auf die ausgewählte Richtlinienstruktur das Storage-Funktionsprofil aus, das die Speichersysteme beschreibt, die in der VM-Speicherrichtlinie verwendet werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.

Create VM Storage Policy

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

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

Placement	Replication	Tags
ProfileName ⓘ Gold_ASA		

5. Überprüfen Sie auf der Seite **Storage Compatibility** die Liste der vSAN-Datstores, die dieser Richtlinie entsprechen, und klicken Sie auf **Weiter**.
6. Überprüfen Sie abschließend die Richtlinie, die implementiert werden soll, und klicken Sie auf **Fertig stellen**, um die Richtlinie zu erstellen.

Erstellen Sie eine VM-Storage-Richtlinie im vSphere Client

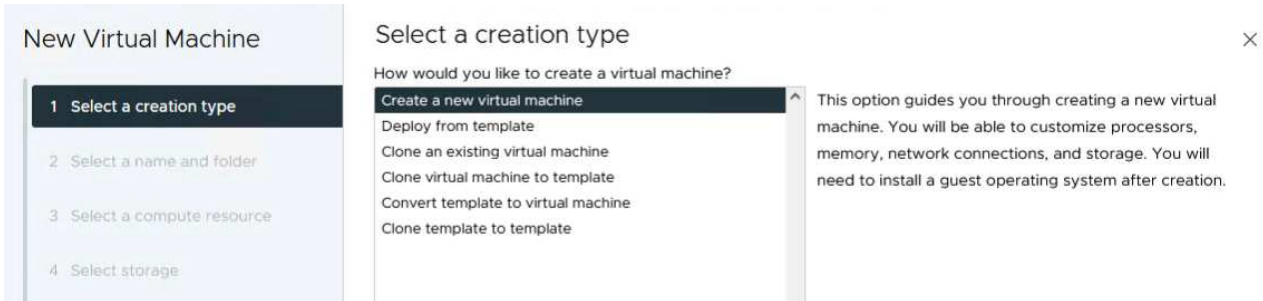
Eine VM Storage-Richtlinie ist eine Reihe von Regeln und Anforderungen, die festlegen, wie Daten für Virtual Machines (VM) gespeichert und gemanagt werden sollen. Er gibt die gewünschten Storage-Merkmale wie Performance, Verfügbarkeit und Datenservices für eine bestimmte VM an.

In diesem Fall umfasst die Aufgabe das Erstellen einer VM-Speicherrichtlinie, um anzugeben, dass eine virtuelle Maschine auf vVol-Datastores generiert wird, und um eine 1:1-Zuordnung mit dem zuvor generierten Storage-Funktionsprofil zu erstellen.

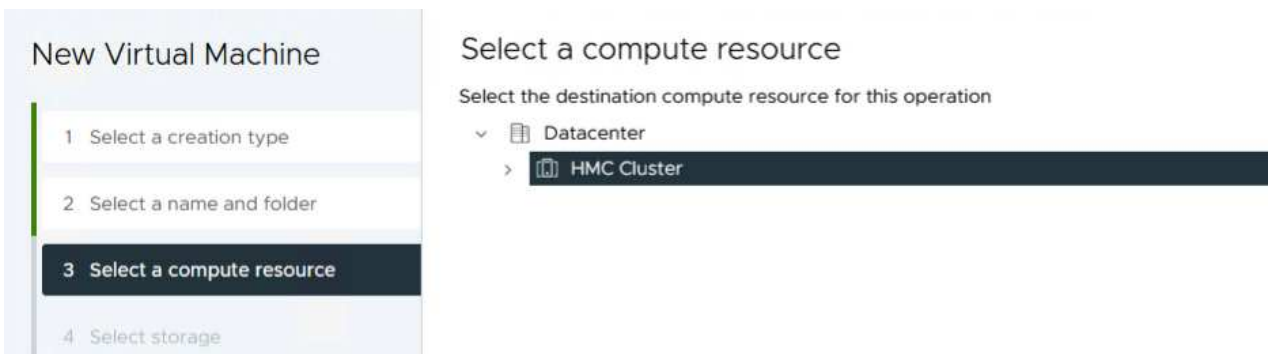
Erstellen Sie eine virtuelle Maschine auf einem vVol-Datastore

Der letzte Schritt besteht darin, mithilfe der zuvor erstellten VM-Storage-Richtlinien eine Virtual Machine zu erstellen:

1. Wählen Sie im Assistenten **Neue virtuelle Maschine Neue virtuelle Maschine erstellen** und wählen Sie **Weiter**, um fortzufahren.



2. Geben Sie einen Namen ein und wählen Sie einen Speicherort für die virtuelle Maschine aus und klicken Sie auf **Weiter**.
3. Wählen Sie auf der Seite **Select a Compute Resource** ein Ziel aus und klicken Sie auf **Next**.



4. Wählen Sie auf der Seite **Storage auswählen** eine VM-Speicherrichtlinie und den VVols-Datastore aus, der das Ziel für die VM sein soll. Klicken Sie auf **Weiter**.

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

Customize hardware

Configure the virtual machine hardware

Virtual Hardware VM Options Advanced Parameters

ADD NEW DEVICE ▾

> CPU *	4	i
> Memory *	32	GB ▾
> New Hard disk *	150	GB ▾

Maximum Size	1.95 TB
VM storage policy	ASA_Gold ▾
Location	Store with the virtual machine ▾
Disk Provisioning	Thin Provision ▾
Sharing	Unspecified ▾
Disk Mode	Dependent ▾
Virtual Device Node	New SCSI controller ▾ SCSI(0:0) New Hard disk ▾

> New SCSI controller	LSI Logic SAS	⋮
> New Network	VM Network ▾ <input checked="" type="checkbox"/> Connected	⋮

CANCEL
BACK
NEXT

8. Überprüfen Sie abschließend die Übersichtsseite und klicken Sie auf **Fertig stellen**, um die VM zu erstellen.

Zusammenfassend lässt sich sagen, dass NetApp ONTAP Tools die Erstellung von vVol Datastores auf ONTAP Storage-Systemen automatisiert. Storage-Funktionsprofile definieren nicht nur die Storage-Systeme, die für die Erstellung von Datenspeichern verwendet werden sollen, sondern diktieren auch QoS-Richtlinien, die auf individueller VMDK-Basis implementiert werden können. VVols bieten ein vereinfachtes Storage-Management-Paradigma und eine enge Integration zwischen NetApp und VMware. Dies macht sie zu einer praktischen Lösung für eine optimierte, effiziente und granulare Steuerung virtualisierter Umgebungen.

NetApp All-Flash SAN-Array mit VMware vSphere 8

NetApp Cloud Insights ist eine Cloud-basierte Plattform für Monitoring und Analyse der Infrastruktur, die sowohl vor Ort als auch in der Cloud einen umfassenden Einblick in Performance, Zustand und Kosten von IT-Infrastrukturen bietet. Zu den wichtigsten Funktionen von NetApp Cloud Insights gehören Echtzeitüberwachung, anpassbare Dashboards, prädiktive Analysen und Tools zur Kostenoptimierung, sodass Unternehmen ihre On-Premises- und Cloud-Umgebungen effektiv managen und optimieren können.

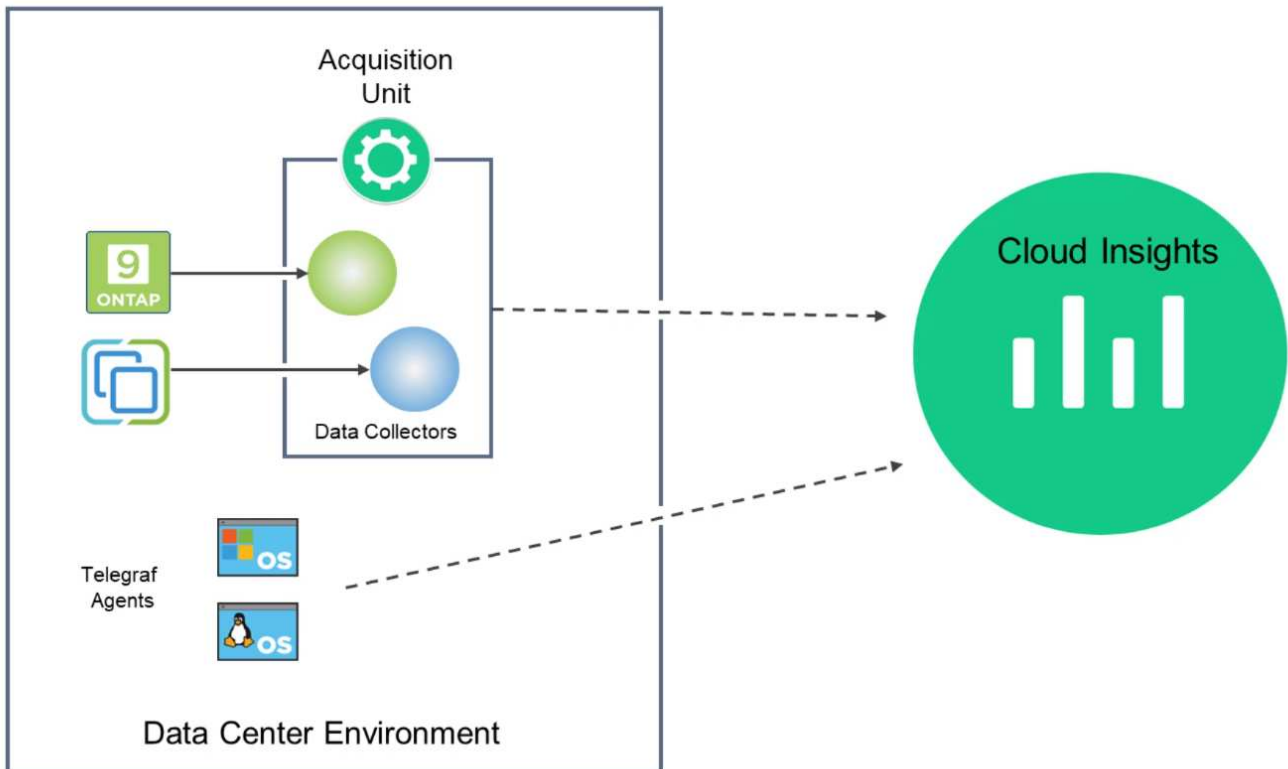
Autor: Josh Powell – NetApp Solutions Engineering

Überwachen Sie Ihre lokalen Storage-Systeme mit NetApp Cloud Insights

NetApp Cloud Insights wird über die Acquisition Unit-Software ausgeführt, die mit Datensammlern für Assets wie VMware vSphere und NetApp ONTAP Storage-Systemen eingerichtet wird. Diese Sammler sammeln

Daten und übermitteln sie an Cloud Insights. Die Plattform verwendet dann eine Vielzahl von Dashboards, Widgets und metrischen Abfragen, um die Daten in aufschlussreichen Analysen zu organisieren, die Benutzer interpretieren können.

Architekturdiagramm von Cloud Insights:



Übersicht Zur Lösungsimplementierung

Diese Lösung bietet eine Einführung zum Monitoring von lokalen VMware vSphere und ONTAP Storage-Systemen mithilfe von NetApp Cloud Insights.

Diese Liste enthält die allgemeinen Schritte, die in dieser Lösung behandelt werden:

1. Konfigurieren Sie Data Collector für einen vSphere-Cluster.
2. Konfigurieren Sie den Data Collector für ein ONTAP-Speichersystem.
3. Verwenden Sie Anmerksungsregeln, um Assets zu kennzeichnen.
4. Analysieren und Korrelieren von Ressourcen
5. Isolieren Sie das „Noisy Neighbor“-Problem mithilfe eines Dashboards der Top-VM-Latenz.
6. Identifizieren Sie Chancen für die optimale Dimensionierung von VMs.
7. Nutzen Sie Abfragen zum Isolieren und Sortieren von Kennzahlen.

Voraussetzungen

Diese Lösung nutzt die folgenden Komponenten:

1. NetApp All-Flash SAN-Array A400 mit ONTAP 9.13

2. VMware vSphere 8.0-Cluster
3. NetApp Cloud Insights Konto.
4. NetApp Cloud Insights Acquisition Unit-Software auf einer lokalen VM mit Netzwerkverbindung zu Ressourcen zur Datenerfassung.

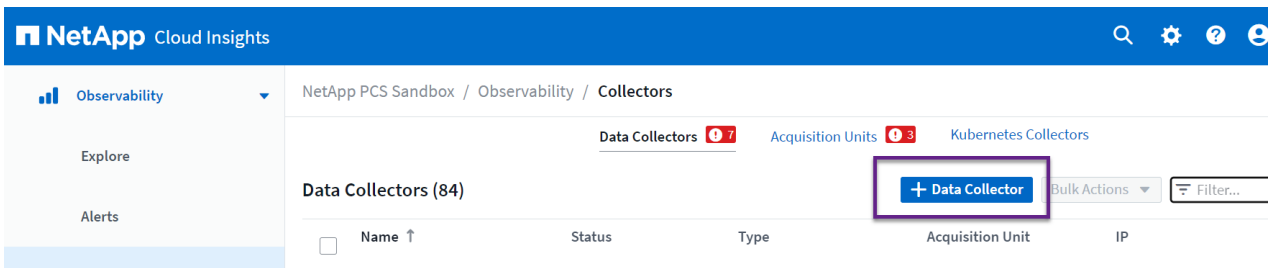
Lösungsimplementierung

Konfigurieren Sie Datensammler

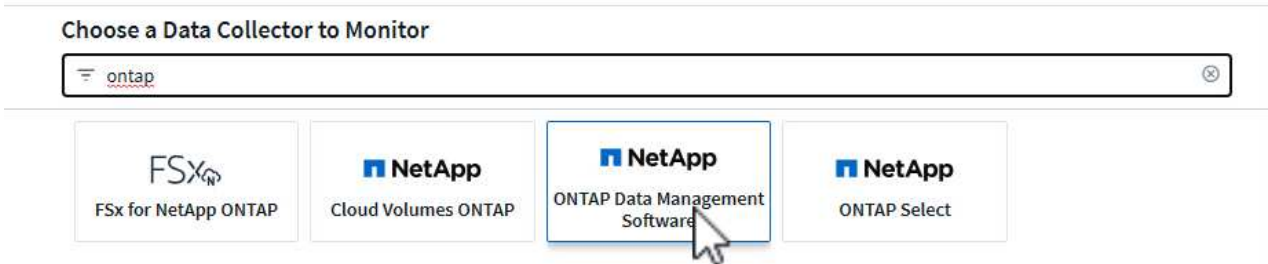
So konfigurieren Sie Data Collectors für VMware vSphere- und ONTAP-Speichersysteme:

Fügen Sie einen Data Collector für ein ONTAP-Speichersystem hinzu

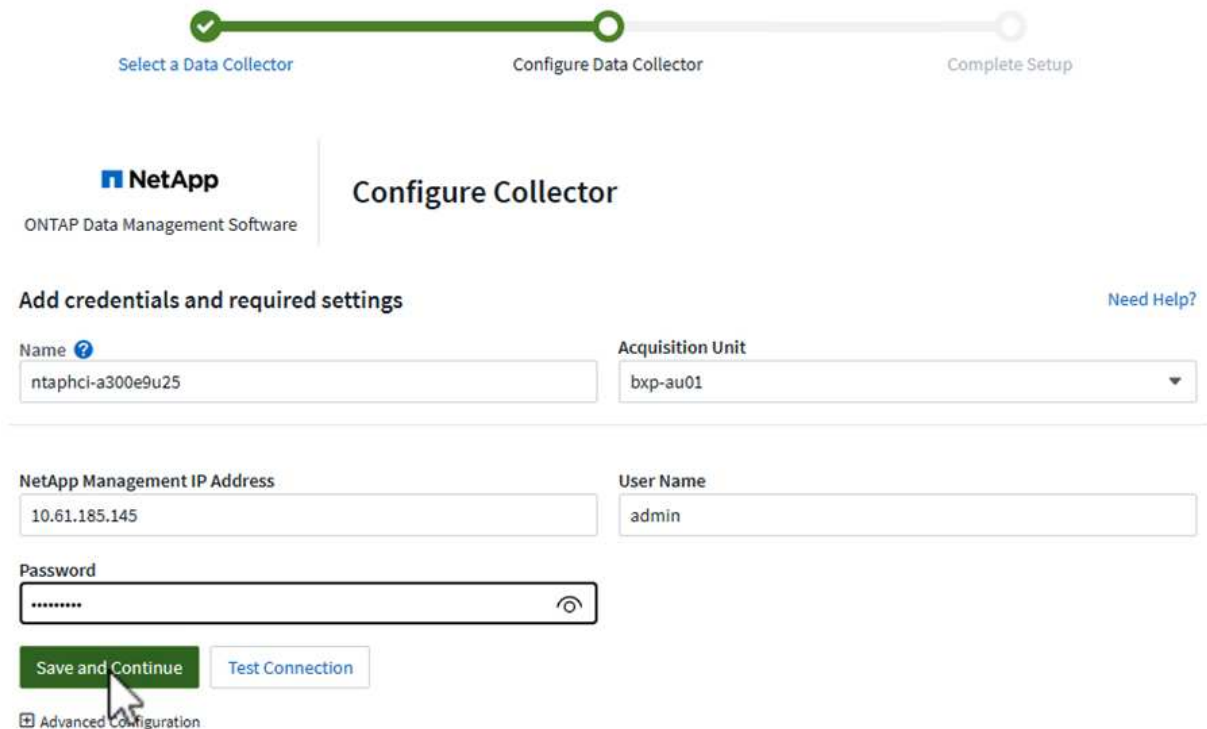
1. Sobald Sie sich bei Cloud Insights angemeldet haben, navigieren Sie zu **Observability > Collectors > Data Collectors**, und drücken Sie die Taste, um einen neuen Data Collector zu installieren.



2. Suchen Sie hier nach **ONTAP** und klicken Sie auf **ONTAP Datenmanagement Software**.

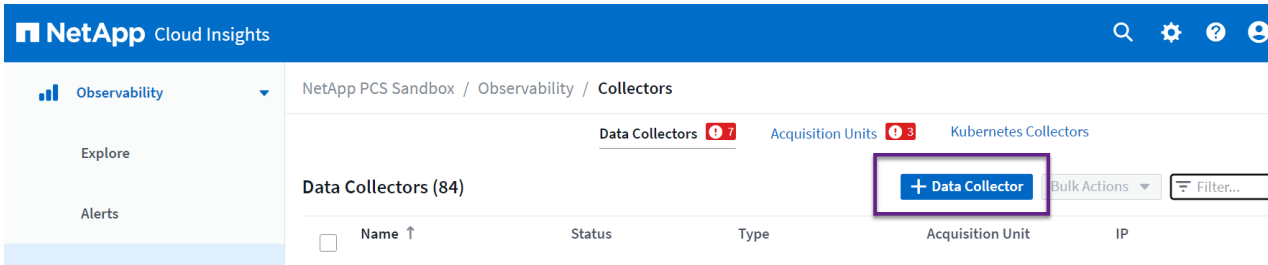


3. Geben Sie auf der Seite **Collector konfigurieren** einen Namen für den Collector ein, geben Sie die richtige **Acquisition Unit** an und geben Sie die Anmeldeinformationen für das ONTAP-Speichersystem an. Klicken Sie unten auf der Seite auf **Speichern und fortfahren** und dann auf **Setup abschließen**, um die Konfiguration abzuschließen.

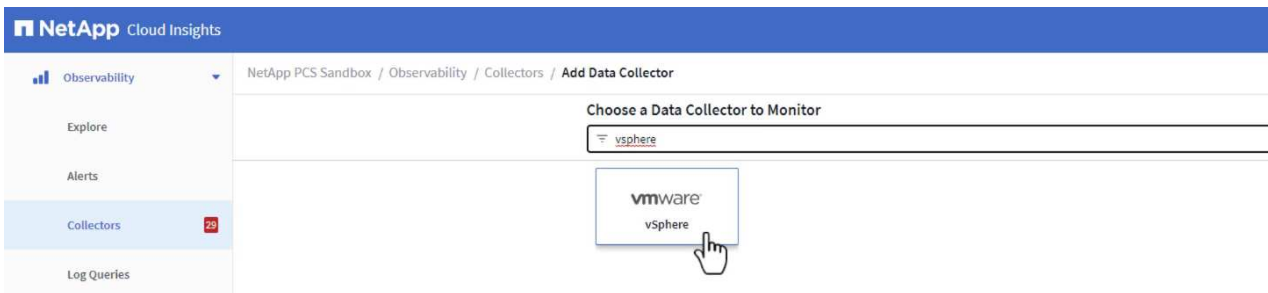


Fügen Sie einen Data Collector für einen VMware vSphere-Cluster hinzu

1. Navigieren Sie erneut zu **Observability > Collectors > Data Collectors**, und drücken Sie die Taste, um einen neuen Data Collector zu installieren.



2. Suchen Sie hier nach **vSphere** und klicken Sie auf **VMware vSphere**.



3. Geben Sie auf der Seite **Configure Collector** einen Namen für den Collector ein, geben Sie die richtige **Acquisition Unit** an und geben Sie die Anmeldeinformationen für den vCenter-Server an. Klicken Sie unten auf der Seite auf **Speichern und fortfahren** und dann auf **Setup abschließen**, um die Konfiguration abzuschließen.



Configure Collector

Add credentials and required settings

[Need Help?](#)

Name [?]	Acquisition Unit
<input type="text" value="VCSA7"/>	<input type="text" value="bxp-au01"/>

Virtual Center IP Address	User Name
<input type="text" value="10.61.181.210"/>	<input type="text" value="administrator@vsphere.local"/>

Password
<input type="password" value="*****"/>

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
---	--

Advanced Configuration

Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min)	Communication Port
<input type="text" value="20"/>	<input type="text" value="443"/>

Filter VMs by	Choose 'Exclude' or 'Include' to Specify a List
<input type="text" value="ESX_HOST"/>	<input type="text" value="Exclude"/>

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)	Performance Poll Interval (sec)
<input type="text"/>	<input type="text" value="300"/>

 Collect basic performance metrics only

<input type="button" value="Complete Setup"/>	<input type="button" value="Test Connection"/>
---	--

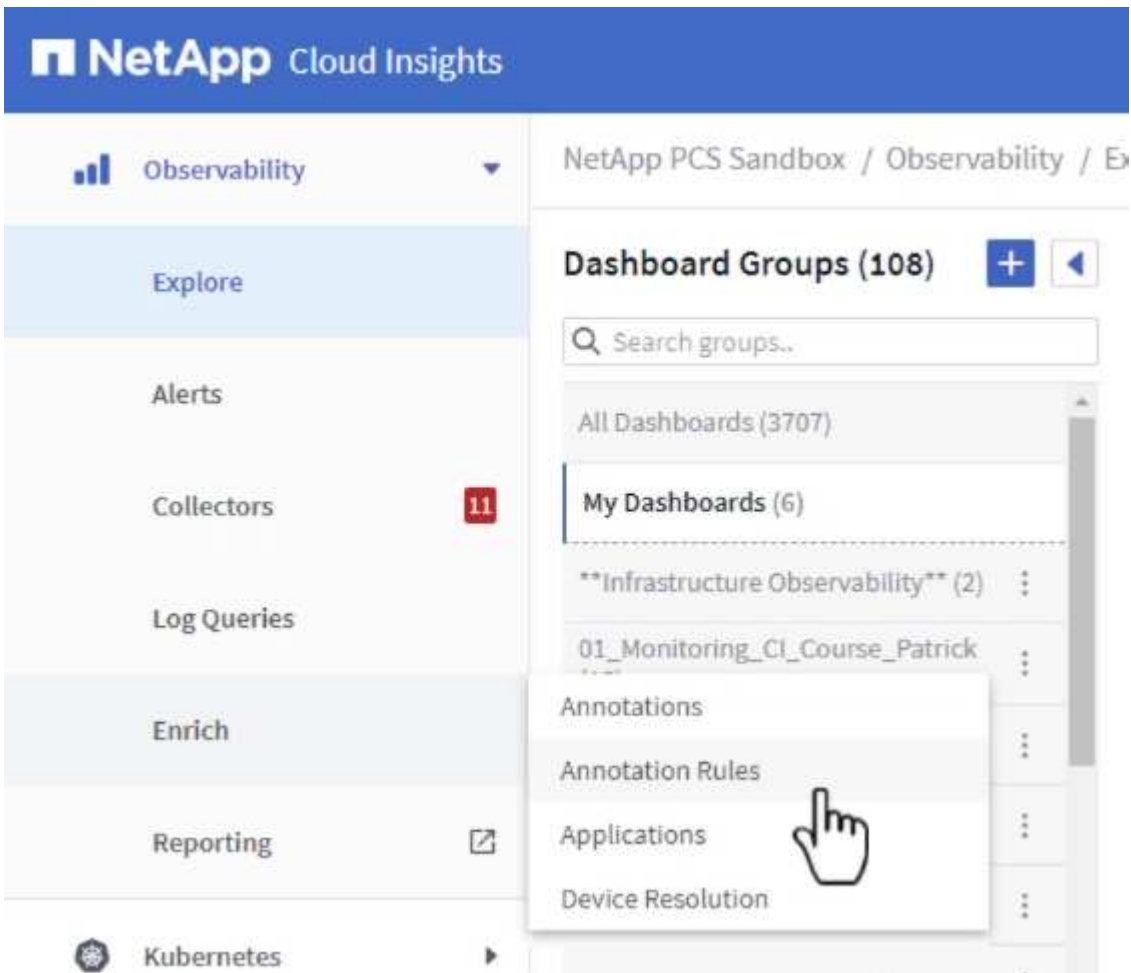
Anmerkungen zu Assets hinzufügen

Annotationen sind eine nützliche Methode zum Tagging von Assets, sodass sie in den verschiedenen Ansichten und metrischen Abfragen, die in Cloud Insights verfügbar sind, gefiltert und anderweitig identifiziert werden können.

In diesem Abschnitt werden Anmerkungen zu virtuellen Maschinen-Assets hinzugefügt, um nach **Rechenzentrum** zu filtern.

Verwenden Sie Anmerksungsregeln, um Assets zu kennzeichnen

1. Navigieren Sie im linken Menü zu **Observability > Enrich > Anmerksungsregeln** und klicken Sie auf die Schaltfläche **+ Regel** oben rechts, um eine neue Regel hinzuzufügen.



2. Geben Sie im Dialogfeld **Regel hinzufügen** einen Namen für die Regel ein, suchen Sie eine Abfrage, auf die die Regel angewendet wird, das betroffene Anmerkungsfeld und den einzufüllenden Wert.

Add Rule
✕

Name

Query

Annotation

Value

3. Klicken Sie in der oberen rechten Ecke der Seite **Anmerksungsregeln** auf **Alle Regeln ausführen**, um die Regel auszuführen und die Anmerkung auf die Assets anzuwenden.

NetApp PCS Sandbox / Observability / Enrich / **Annotation Rules**

Annotation rules (217)

Name	Resource Type	Query	Annotation	Value
Annotate Tier 1 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 1
Annotate Tier 2 Storage Pools	Storage Pool	Find Storage Pools (no aggro) for Tier...	Tier	Tier 2

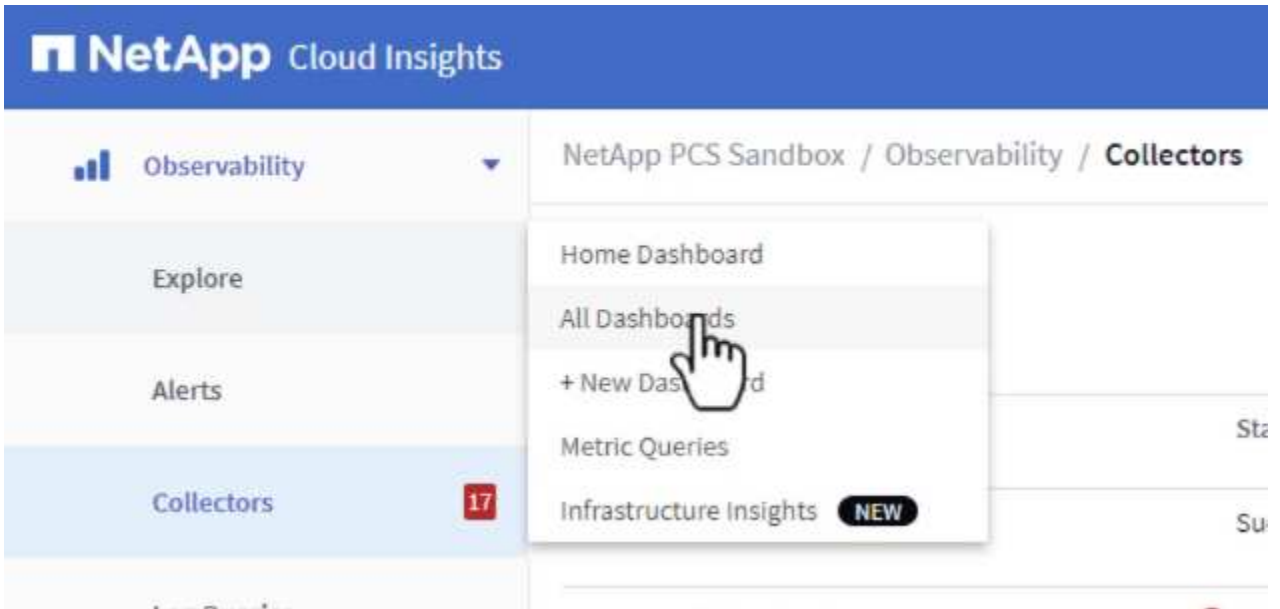
Analysieren und Korrelieren von Ressourcen

Cloud Insights zieht logische Schlüsse über die Ressourcen, die in Ihren Storage-Systemen und vsphere Clustern gemeinsam ausgeführt werden.

In diesen Abschnitten wird die Verwendung von Dashboards zur Korrelation von Assets erläutert.

Korrelation von Assets aus einem Storage Performance Dashboard

1. Navigieren Sie im linken Menü zu **Observability > Explore > All Dashboards**.



2. Klicken Sie auf die Schaltfläche **+ von Galerie**, um eine Liste der fertigen Dashboards anzuzeigen, die importiert werden können.



3. Wählen Sie aus der Liste ein Dashboard für die FlexVol-Performance aus und klicken Sie unten auf der Seite auf die Schaltfläche **Dashboards hinzufügen**.

- ONTAP FAS/AFF - Cluster Capacity
- ONTAP FAS/AFF - Efficiency
- ONTAP FAS/AFF - FlexVol Performance
- ONTAP FAS/AFF - Node Operational/Optimal Points
- ONTAP FAS/AFF - PrePost Capacity Efficiencies
- Storage Admin - Which nodes are in high demand?
- Storage Admin - Which pools are in high demand?
- StorageGRID - Capacity Summary
- StorageGRID - ILM Performance Monitoring
- StorageGRID - MetaData Usage
- StorageGRID - S3 Performance Monitoring
- VMware Admin - ESX Hosts Overview
- VMware Admin - Overview
- VMware Admin - VM Performance
- VMware Admin - Where are opportunities to right size?
- VMware Admin - Where can I potentially reclaim waste?
- VMware Admin - Where do I have VM Latency?

+ Additional Dashboards (13)
These dashboards require additional data collectors to be installed. [Add More](#)

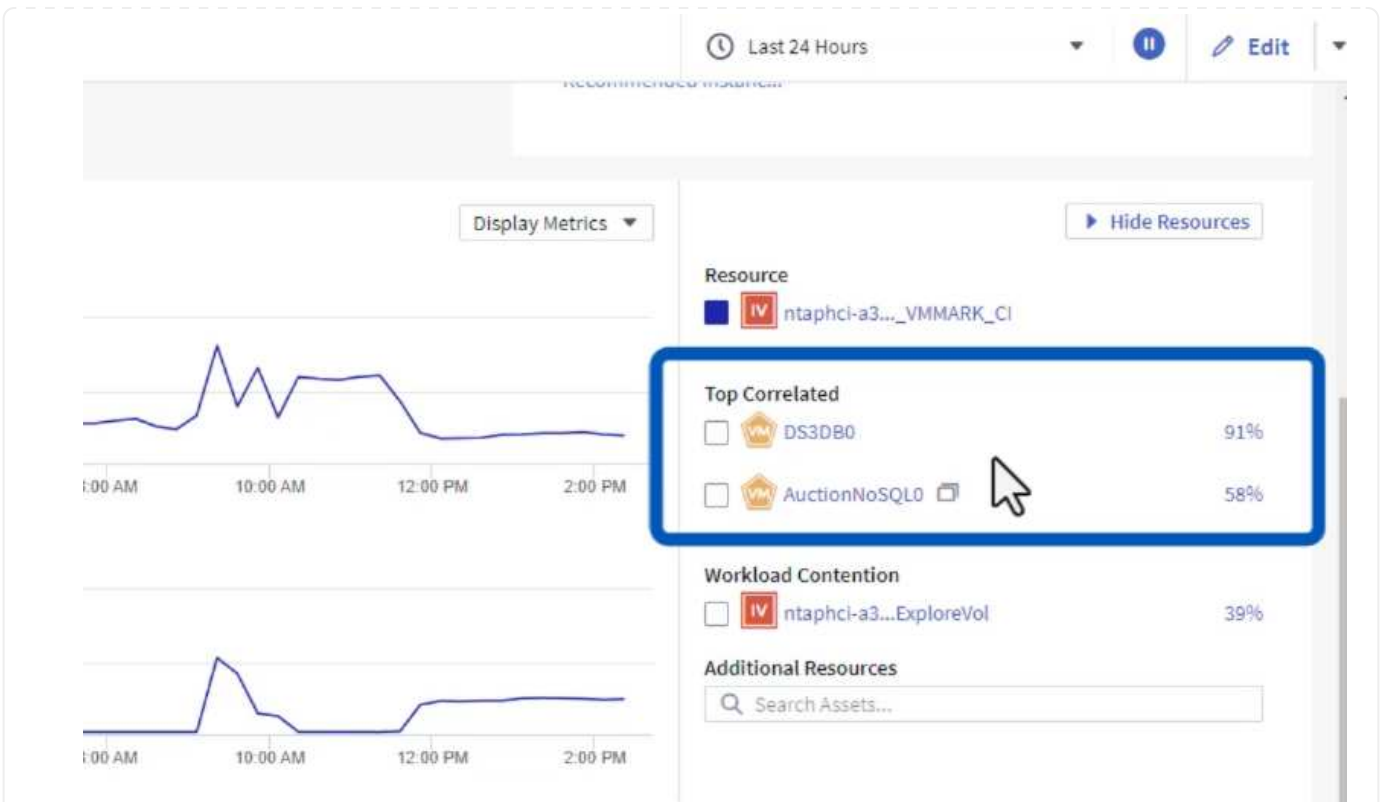
[Add Dashboards](#) [Go Back](#)

4. Öffnen Sie nach dem Import das Dashboard. Von hier aus können Sie verschiedene Widgets mit detaillierten Leistungsdaten sehen. Fügen Sie einen Filter hinzu, um ein einzelnes Storage-System anzuzeigen, und wählen Sie ein Storage-Volume aus, um detaillierte Informationen zu erhalten.

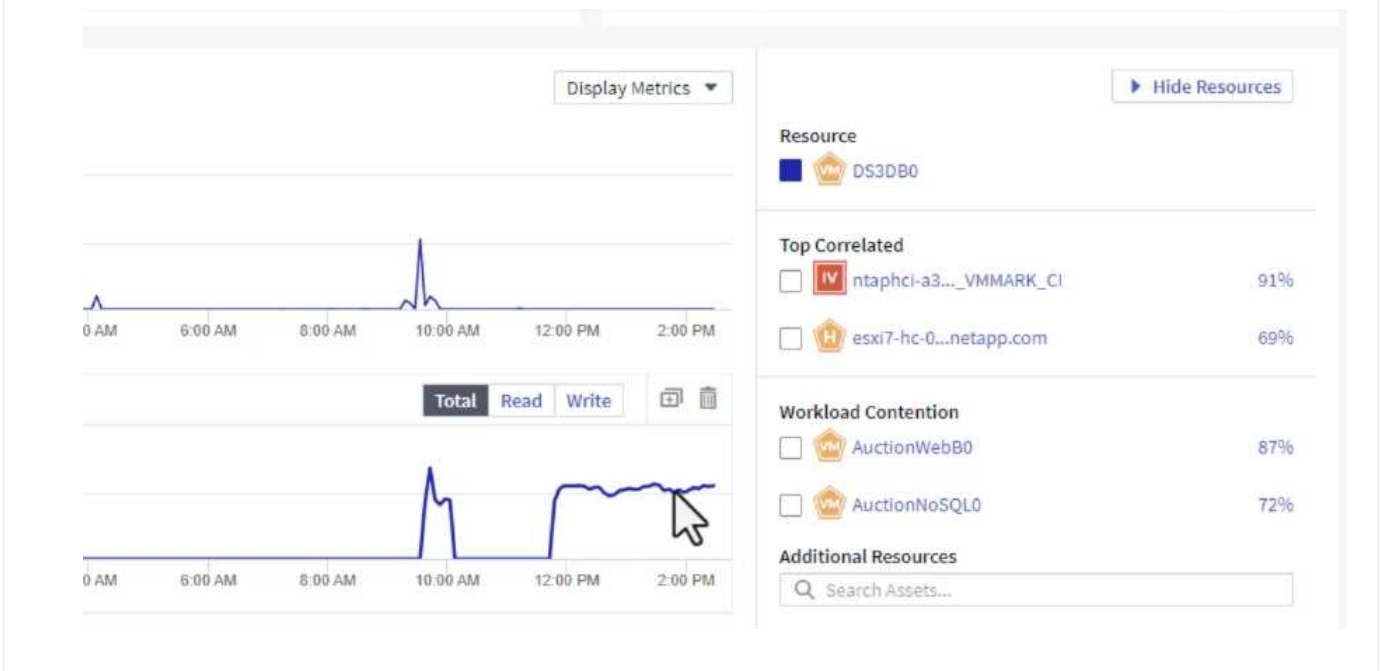
The screenshot shows the NetApp Cloud Insights interface. The breadcrumb trail is: NetApp PCS Sandbox / Observability / Dashboards / ONTAP FAS/AFF - FlexVol Performance (10). The dashboard is filtered for 'Storage' and 'ntaphci-a300e9u25'. Two charts are visible: 'FlexVol IOPS Max Trend - Top 10' and 'Avg FlexVol Latency'. The IOPS chart shows a peak around 7:40 PM. The latency chart shows a peak around 1:13 AM. Below the charts is a table of top 10 storage volumes and their associated VMs.

Storage Volume	VM
ntaphci-a300e9u25-E	ntaphci-a300e9u25-n
HC_NFS:8a6hjd	taphci-a300-01v0l0
DEST_TEST_01	MC_3510>Select_N1
ntaphci-a300e9u25-H	ntaphci-a300e9u25-H
MC_3510>Select_N2	ntaphci-a300e9u25-E
HC_NFS:DRO_Mini	HC_NFS:NFSmountTe
ntaphci-a300e9u25-E	ntaphci-a300e9u25-E
ntaphci-a300e9u25-E	HC_NFS:NFS_VMMAR
ntaphci-a300e9u25-E	K_CI
ntaphci-a300e9u25-E	ntaphci-a300e9u25-H

5. In dieser Ansicht werden verschiedene Kennzahlen zu diesem Storage-Volume sowie die am häufigsten genutzten und korrelierten Virtual Machines angezeigt, die auf dem Volume ausgeführt werden.



6. Wenn Sie auf die VM mit der höchsten Auslastung klicken, werden die Metriken der VM angezeigt, um mögliche Probleme anzuzeigen.

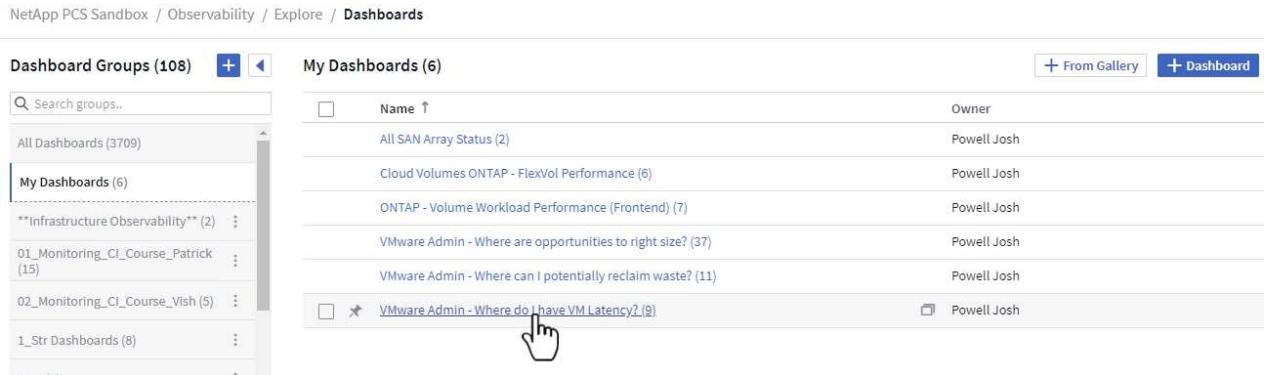


Erkennen von „Noisy Neighbors“ mit Cloud Insights

Cloud Insights verfügt über Dashboards, die sich problemlos Peer-VMs isolieren lassen, die sich negativ auf andere VMs auswirken, die auf demselben Storage Volume ausgeführt werden.

Isolieren Sie das „Noisy Neighbor“-Problem mithilfe eines Dashboards der Top-VM-Latenz

1. In diesem Beispiel greifen Sie auf ein Dashboard zu, das in der **Galerie** mit der Bezeichnung **VMware Admin - wo habe ich VM-Latenz?** verfügbar ist



2. Als Nächstes filtern Sie nach der Anmerkung **Data Center**, die in einem vorherigen Schritt erstellt wurde, um eine Teilmenge von Assets anzuzeigen.



3. Dieses Dashboard zeigt eine Liste der 10 wichtigsten VMs nach der durchschnittlichen Latenz. Klicken Sie hier auf die entsprechende VM, um die Details anzuzeigen.

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

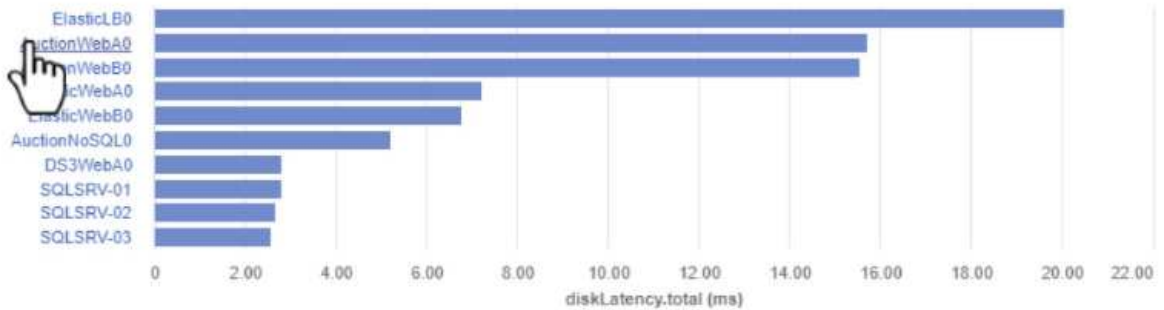
5m

1.55 ms

diskLatency.total

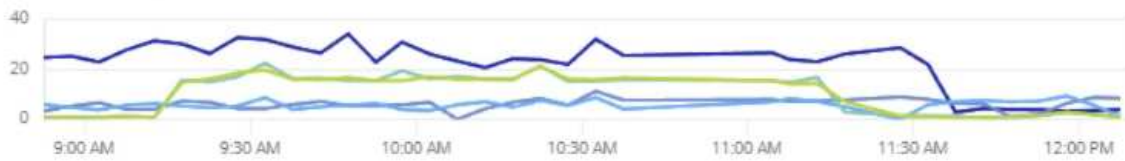
Avg VM Latency - Top 10

5m

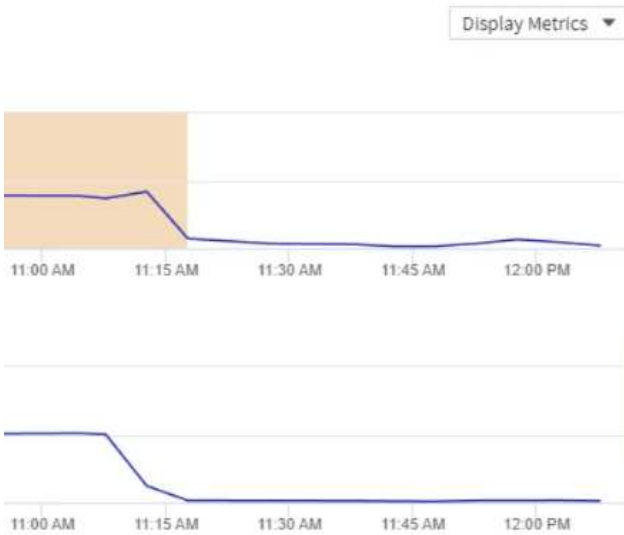


Top 5 Avg VM Latency Trend

30s



4. Die VMs, die möglicherweise zu Workload-Engpässen führen, werden aufgelistet und verfügbar sein. Zeigen Sie diese VM-Performance-Kennzahlen auf, um mögliche Probleme zu untersuchen.



Resource

VM AuctionWebA0

Top Correlated

esxi7-hc-0...netapp.com 91%

ntaphci-a3..._VMMARK_CI 84%

Workload Contention

AuctionNoSQL0 92%

AuctionWebB0 57%

Additional Resources

Search Assets...

Übersicht über und zu wenig genutzte Ressourcen in Cloud Insights

Indem VM-Ressourcen den tatsächlichen Workload-Anforderungen entsprechen, kann die Ressourcenauslastung optimiert werden, was zu Kosteneinsparungen bei Infrastruktur- und Cloud-Services führt. Daten in Cloud Insights können so angepasst werden, dass sie sich problemlos über oder unter ausgelastete VMs anzeigen lassen.

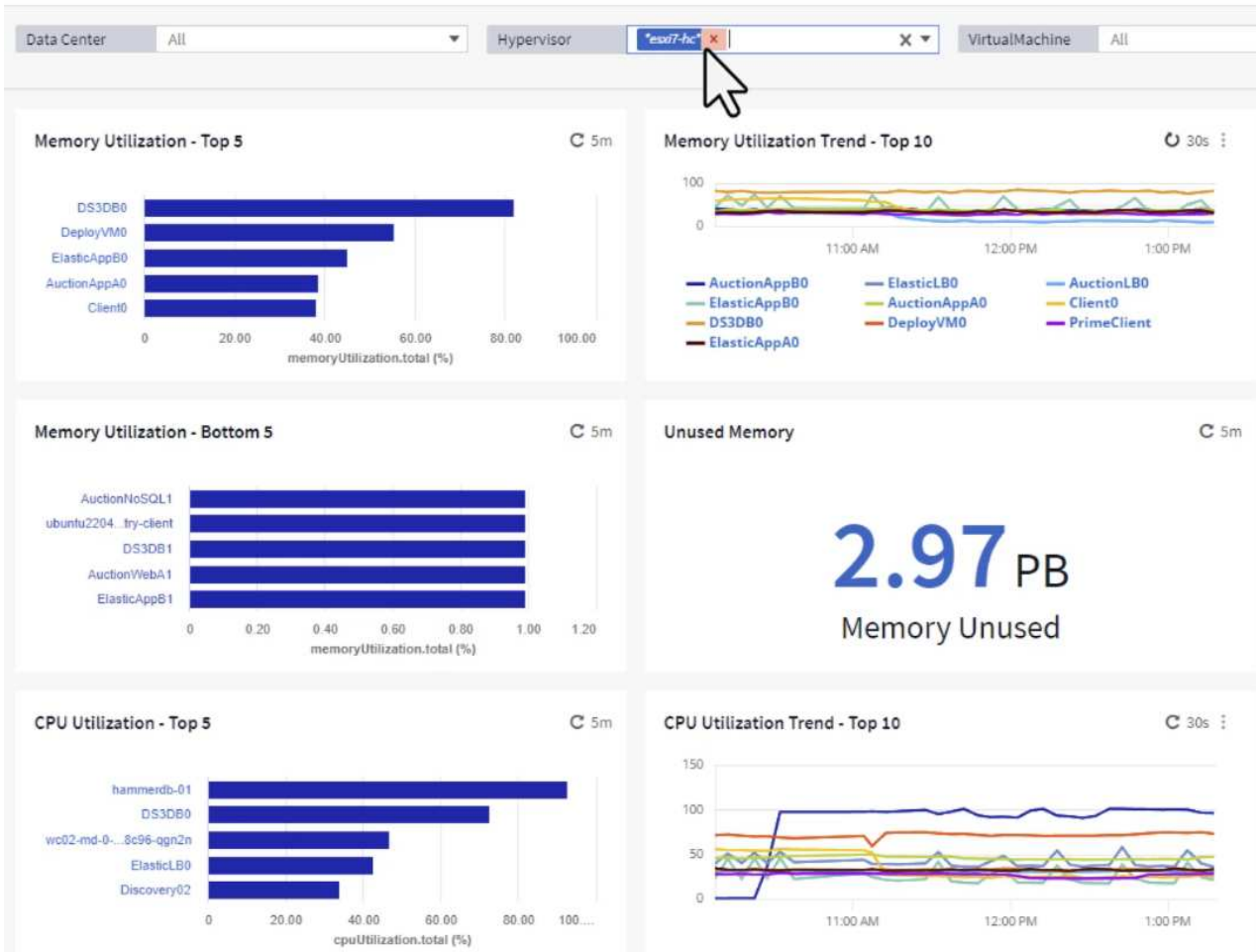
Ermittlung von Möglichkeiten zur optimalen Dimensionierung von VMs

1. In diesem Beispiel greifen Sie auf ein Dashboard zu, das in der **Galerie** unter dem Namen **VMware Admin - wo gibt es Möglichkeiten, die richtige Größe zu haben?** verfügbar ist

My Dashboards (6)

<input type="checkbox"/>	Name ↑
	All SAN Array Status (2)
	Cloud Volumes ONTAP - FlexVol Performance (6)
	ONTAP - Volume Workload Performance (Frontend) (7)
<input type="checkbox"/>	★ <u>VMware Admin - Where are opportunities to right size? (37)</u>
	VMware Admin - Where do I have VMs that potentially reclaim waste? (11)
	VMware Admin - Where do I have VM Latency? (9)

2. Zuerst Filter durch alle ESXi-Hosts im Cluster. Anschließend wird eine Rangfolge der VMs oben und unten nach Arbeitsspeicher und CPU-Auslastung angezeigt.



3. Tabellen ermöglichen die Sortierung und bieten mehr Details auf der Grundlage der ausgewählten Datenspalten.

Memory Usage

5m

121 items found

Virtual Machine	memory (MiB)	memoryUt... ↓
DS3DB0	768.0	81.64
DeployVM0	92.0	55.06
ElasticAppB0	92.0	44.91
AuctionAppA0	336.0	38.42
Client0	480.0	37.98
AuctionAppB0	336.0	37.83
ElasticAppA0	92.0	35.63
ElasticLB0	96.0	35.13
user-cluster1-8872k-78c65dd794...	92.0	32.47
PrimeClient	48.0	30.30

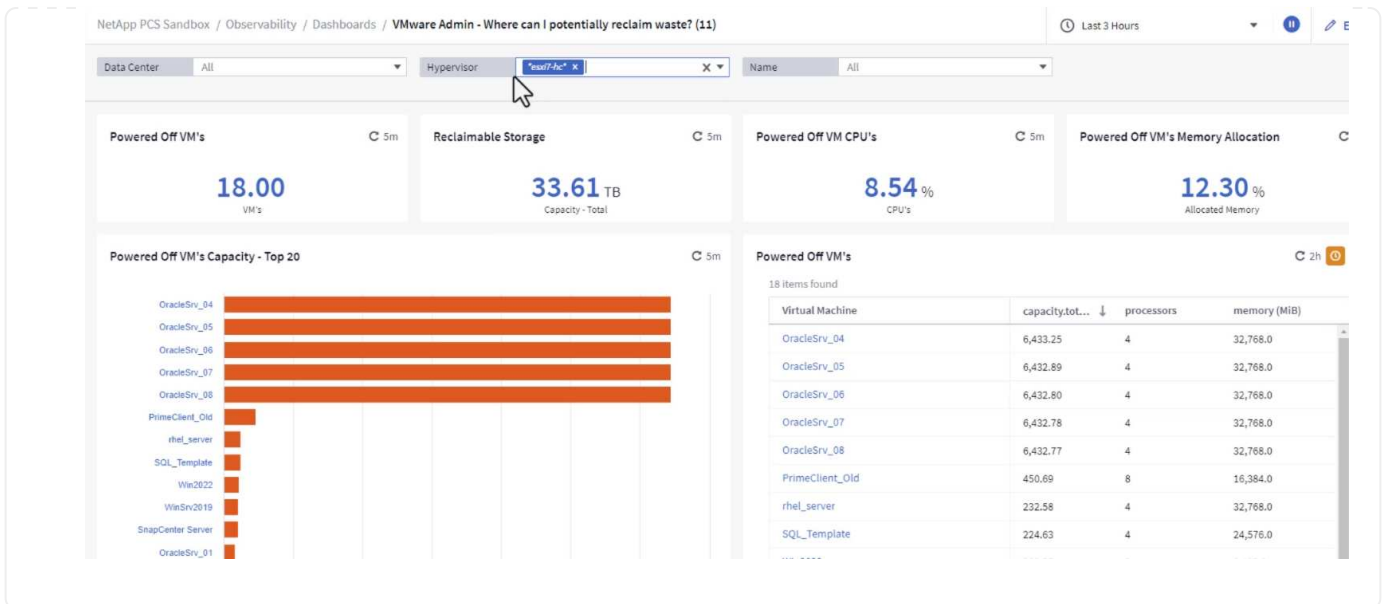
CPU Utilization

5m

121 items found

Virtual Machine	name
hammerdb-01	hammerdb-01
DS3DB0	DS3DB0
wc02-md-0-xwdgb-8cf48c96-qgn...	wc02-md-0-xwdgb-8cf48c96-qg...
ElasticLB0	ElasticLB0

4. Ein anderes Dashboard namens **VMware Admin** - wo kann ich potenziell Abfälle zurückfordern? zeigt ausgeschalteten VMs sortiert nach ihrer Kapazitätsnutzung.

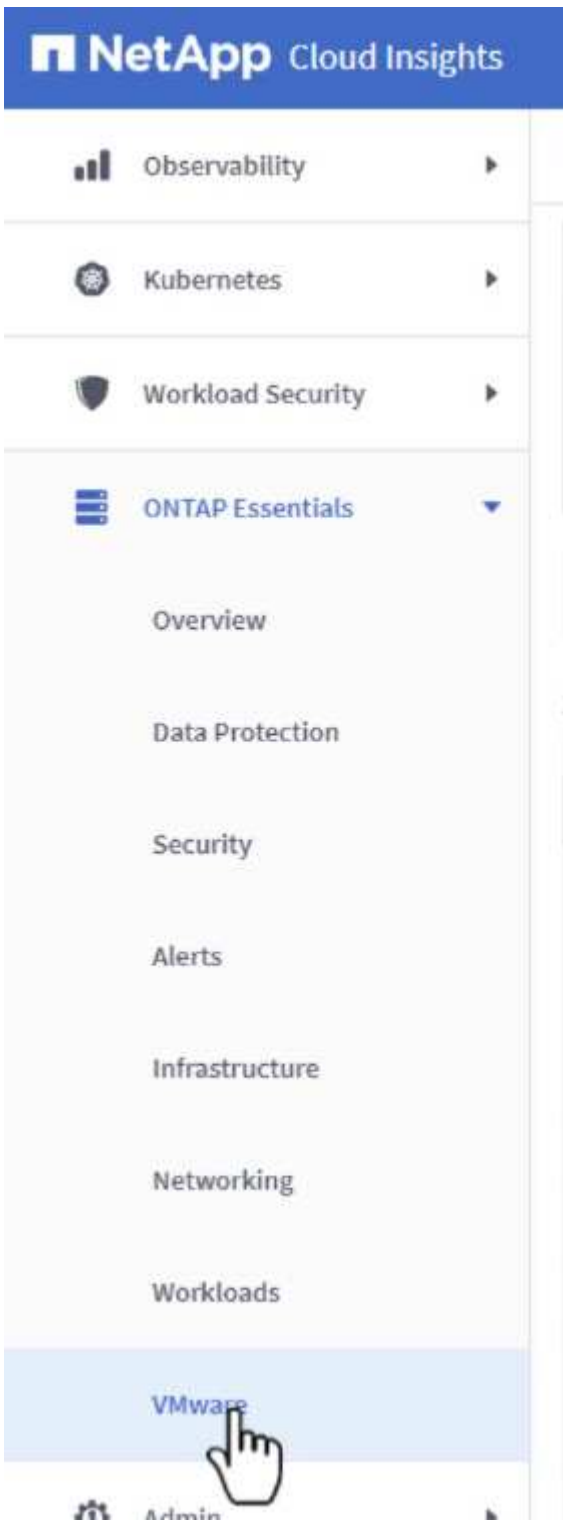


Nutzen Sie Abfragen zum Isolieren und Sortieren von Kennzahlen

Die von Cloud Insights erfassten Daten sind recht umfangreich. Metrische Abfragen bieten eine leistungsstarke Möglichkeit, große Datenmengen auf nützliche Weise zu sortieren und zu organisieren.

Zeigen Sie eine detaillierte VMware-Abfrage unter ONTAP Essentials an

1. Navigieren Sie zu **ONTAP Essentials > VMware**, um auf eine umfassende VMware-Metrikenabfrage zuzugreifen.



2. In dieser Ansicht werden Ihnen mehrere Optionen zum Filtern und Gruppieren der Daten am oberen Rand angezeigt. Alle Datenspalten können angepasst werden, und zusätzliche Spalten können problemlos hinzugefügt werden.

VirtualMachine | All Virtual Machines

Filter by Attribute: storageResources.storage.vendor: NetApp | host.Los: VMware

Filter by Metric: +

Group By: Virtual Machine

Formatting: Show Expanded Details | Conditional Formatting: Background Color | Show In Range as green

281 Items found

Virtual Machine	name ↑	powerState	capacity.used (GiB)	capacity.total (GiB)	capacityRatio.us...	diskIops.total (I/O/s)	diskLatency.total...	diskThroughput...
01rfk8sprodclient	01rfk8sprodclient	On	49.38	69.86	70.68	1.21	8.13	0.01
02rfk8sprodserver	02rfk8sprodserver	On	63.64	74.06	85.93	22.80	4.13	0.11
03rfk8sprodmaster01	03rfk8sprodmaster01	On	65.13	77.21	84.36	26.64	5.64	0.20
04rfk8sprodmaster02	04rfk8sprodmaster02	On	63.89	76.27	83.77	26.82	5.14	0.16
05rfk8sprodmaster03	05rfk8sprodmaster03	On	63.77	75.58	84.38	28.23	4.63	0.17
AIQUM 9.11 (vApp)	AIQUM 9.11 (vApp)	On	152.00	152.00	100.00	23.24	0.19	0.41
AIQUM 9.12 (Linux)	AIQUM 9.12 (Linux)	On	55.28	100.00	55.28	0.01	11.83	0.00
AN-JumpHost01	AN-JumpHost01	On	90.00	90.00	100.00	1.39	0.19	0.01
AuctionAppA0	AuctionAppA0	On	9.38	16.00	58.62	1.21	0.44	0.12
AuctionAppA1	AuctionAppA1	On	6.44	16.00	40.26	0.00	3.00	0.00

Schlussfolgerung

Diese Lösung wurde als Einführung entwickelt. Sie soll Ihnen den Einstieg in NetApp Cloud Insights erleichtern und Ihnen einige der leistungsstarken Funktionen zeigen, die diese Beobachtbarkeit ermöglichen kann. Das Produkt enthält Hunderte von Dashboards und metrischen Abfragen, die einen sofortigen Einstieg erleichtern. Die Vollversion von Cloud Insights ist als 30-Tage-Testversion erhältlich und die Basisversion ist für NetApp Kunden kostenlos erhältlich.

Weitere Informationen

Weitere Informationen zu den in dieser Lösung vorgestellten Technologien finden Sie in den folgenden zusätzlichen Informationen.

- ["Landing Page von NetApp BlueXP und Cloud Insights"](#)
- ["NetApp Cloud Insights Dokumentation"](#)

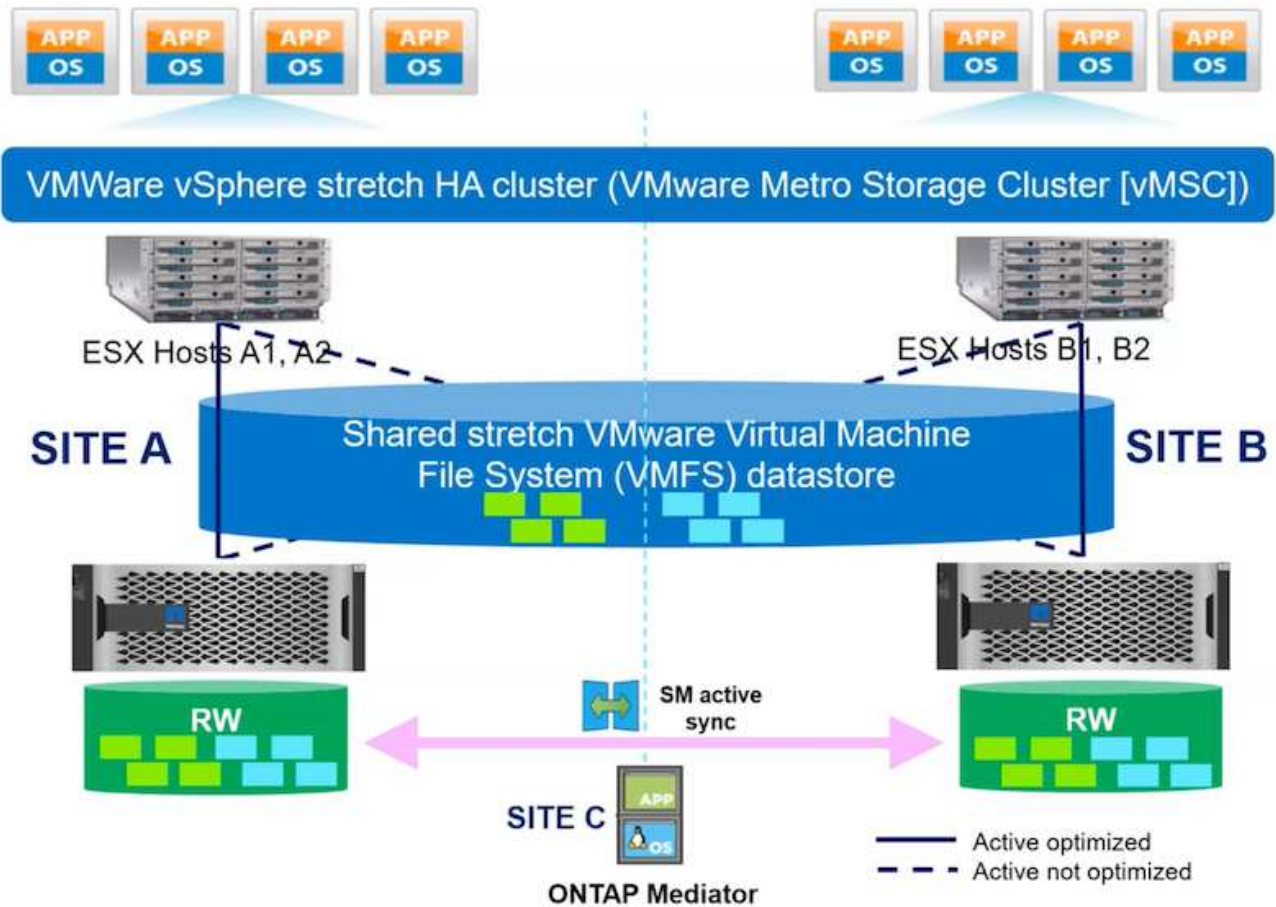
VMware vSphere Metro Storage-Cluster mit SnapMirror Active Sync

"VMware vSphere Metro Storage-Cluster (vMSC)" ist eine verteilte Cluster-Lösung über verschiedene Fehlerdomänen hinweg, um * Workload-Mobilität über Verfügbarkeitszonen oder Standorte hinweg zu ermöglichen. * Vermeidung von Ausfallzeiten * Vermeidung von Notfällen * schnelle Recovery

Dieses Dokument enthält Details zur vMSC-Implementierung "[SnapMirror Active Sync \(SM-AS\)](#)" unter Verwendung von System Manager- und ONTAP-Tools. Außerdem wird gezeigt, wie die VM durch Replizierung an einen dritten Standort gesichert und mit dem SnapCenter Plug-in für VMware vSphere gemanagt werden kann.

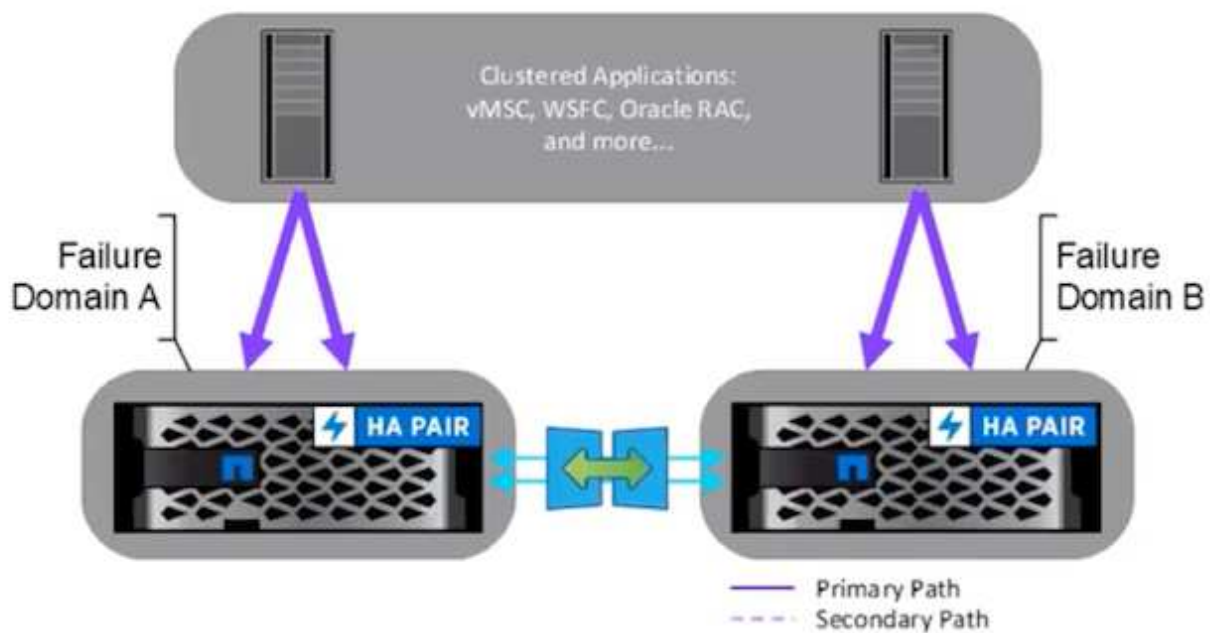
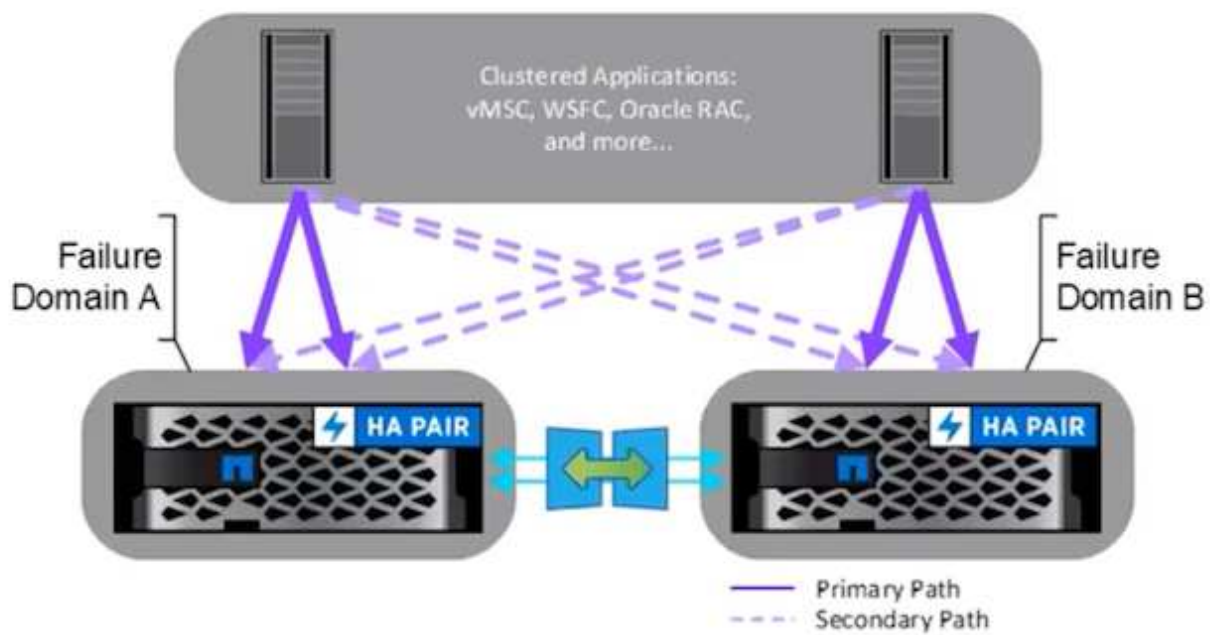
SnapMirror active sync

General availability release 9.15.1 for symmetric configuration



SnapMirror Active Sync unterstützt ASA, AFF und FAS Storage-Arrays. Es wird empfohlen, bei beiden Fehlerdomänen denselben Typ (Performance-/Kapazitätsmodelle) zu verwenden. Derzeit werden nur Blockprotokolle wie FC und iSCSI unterstützt. Weitere Support-Richtlinien finden Sie unter ["Interoperabilitäts-Matrix-Tool"](#) und ["Hardware Universe"](#)

VMSC unterstützt zwei verschiedene Implementierungsmodelle mit den Namen „einheitlicher Host-Zugriff“ und „nicht einheitlicher Host-Zugriff“. Bei einer einheitlichen Hostzugriffskonfiguration hat jeder Host auf dem Cluster auf beiden Fehlerdomänen Zugriff auf die LUN. Sie wird normalerweise in verschiedenen Verfügbarkeitszonen im selben Datacenter verwendet.



In der Konfiguration für den nicht einheitlichen Hostzugriff hat der Host nur Zugriff auf die lokale Fehlerdomäne. Es wird in der Regel an verschiedenen Standorten verwendet, wo das Ausführen mehrerer Kabel über die Fehlerdomänen restriktiv ist.



Im nicht einheitlichen Host-Zugriffsmodus werden die VMs in einer anderen Fehlerdomäne von vSphere HA neu gestartet. Die Anwendungsverfügbarkeit wird je nach Design beeinflusst. Der nicht einheitliche Host-Zugriffsmodus wird nur ab ONTAP 9.15 unterstützt.

Voraussetzungen

- "VMware vSphere-Hosts, die mit Dual-Storage Fabric (zwei HBAs oder Dual-VLAN für iSCSI) pro Host bereitgestellt werden".
- "Speicher-Arrays werden mit Link Aggregation für Daten-Ports (für iSCSI) bereitgestellt".
- "Storage VM und LIFs sind verfügbar"
- "Die Paketumlaufzeit zwischen Clustern muss weniger als 10 Millisekunden betragen".
- "ONTAP Mediator VM wird auf einer anderen Fehlerdomäne bereitgestellt"
- "Cluster Peer-Beziehung wurde hergestellt"
- "SVM-Peer-Beziehung wurde hergestellt"
- "ONTAP Mediator ist beim ONTAP Cluster registriert"



Bei Verwendung eines selbstsignierten Zertifikats kann das Zertifikat der Zertifizierungsstelle von der <installation path>/ontap_Mediator/Server_config/ca.crt auf der VM des Mediators abgerufen werden.

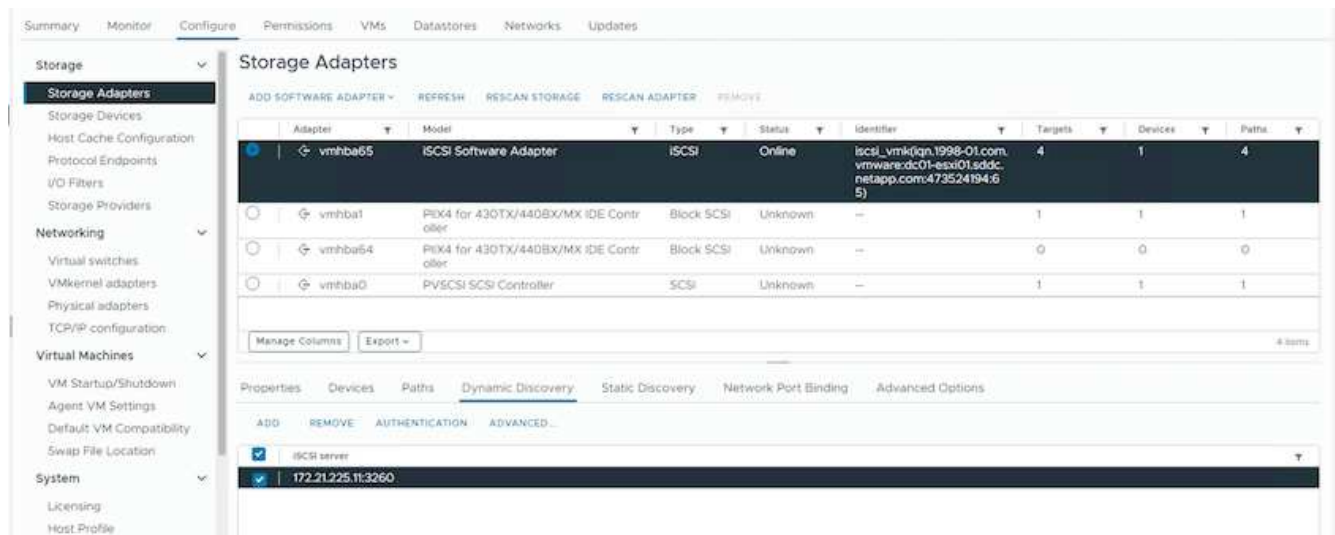
VMSC nicht einheitlicher Host-Zugriff mit der ONTAP System Manager UI.

Hinweis: Mit den ONTAP Tools 10.2 oder höher kann der erweiterte Datastore mit einem nicht-einheitlichen Host-Zugriffsmodus erstellt werden, ohne dass Sie mehrere Benutzerschnittstellen wechseln müssen. Dieser Abschnitt dient nur als Referenz, wenn ONTAP-Tools nicht verwendet werden.

1. Notieren Sie eine der iSCSI-Daten-LIF-IP-Adressen des Speicherarrays für die lokale Fehlerdomäne.

Name	Status	Storage VM	IPspace	Address	Current node	Current p...	Portset	Protocols	Ty...	Throughput
iscsi02	✔	zonea	Default	172.21.226.11	E13A300_1	a0a-3482		iSCSI	D...	0
iscsi03	✔	zonea	Default	172.21.225.12	E13A300_2	a0a-3481		iSCSI	D...	0.33
iscsi04	✔	zonea	Default	172.21.226.12	E13A300_2	a0a-3482		iSCSI	D...	0.01
iscsi01	✔	zonea	Default	172.21.225.11	E13A300_1	a0a-3481		iSCSI	D...	0

2. Fügen Sie auf dem vSphere-Host-iSCSI-Speicheradapter diese iSCSI-IP unter der Registerkarte Dynamic Discovery hinzu.



Für einen einheitlichen Zugriffsmodus müssen Sie die iSCSI-Daten-LIF-Adresse der Quell- und Zielfehlerdomäne bereitstellen.

3. Wiederholen Sie den obigen Schritt auf vSphere-Hosts für die andere Fehlerdomäne, indem Sie die lokale iSCSI-Daten-LIF-IP auf der Registerkarte Dynamic Discovery hinzufügen.
4. Mit einer ordnungsgemäßen Netzwerkverbindung sollten vier iSCSI-Verbindungen pro vSphere-Host vorhanden sein, der über zwei iSCSI VMkernel nics und zwei iSCSI-Datenlifs pro Storage Controller verfügt.

```
E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.225.71
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zonea        iscsi01      23    0 172.21.225.11 172.21.225.71 0
zonea        iscsi03      17    0 172.21.225.12 172.21.225.71 0
2 entries were displayed.

E13A300::> iscsi connection show -vserver zonea -remote-address 172.21.226.71
Vserver      Tpgroup      Conn  Local      Remote      TCP Recv
Name         Name         ID    Address    Address     Size
-----
zonea        iscsi02      24    0 172.21.226.11 172.21.226.71 0
zonea        iscsi04      16    0 172.21.226.12 172.21.226.71 0
2 entries were displayed.
```

5. LUN mit ONTAP System Manager erstellen, SnapMirror mit Replikationsrichtlinie automatisiertFailOverDuplex einrichten, Host-Initiatoren auswählen und Host-Nähe festlegen.

Add LUNs ✕

Host ID:

Storage:

Group with related LUNs ⓘ

Storage and optimization

NUMBER OF LUNS: CAPACITY PER LUN:

PERFORMANCE SERVICE LEVEL:

Not sure? [Get help selecting type](#)

Apply the performance limits enforcement to each LUN. If unchecked, these limits will be applied to the entire set of LUNs.

Protection

Enable Snapshot copies (vSAN)

Enable SnapMirror (local or remote)

RESTRICTION ADJUST: Show legacy policies ⓘ

Source

CLUSTER:

STORAGE:

COMPATIBILITY GROUP:

Destination

CLUSTER:

STORAGE:

Destination settings

ⓘ You should manually create an group by adding replicated hosts in the destination cluster and map the group to the newly created LUNs.

Host information

HOST OPERATING SYSTEM: CVM POWER:

HOST VAPOR:

Existing initiator group

New initiator group using existing initiator groups

Host initiators

INITIATOR GROUP NAME:

Name	Description	In proximity to
<input type="checkbox"/> ipn.1954-01.com.redhat.51e1788998b	-	None
<input type="checkbox"/> ipn.1954-01.com.redhat.a3435046678	-	None
<input checked="" type="checkbox"/> ipn.1958-01.com.vmware.vb01-aaa01ad...	-	Source
<input checked="" type="checkbox"/> ipn.1958-01.com.vmware.vb01-aaa0212...	-	Source
<input type="checkbox"/> ipn.1958-01.com.vmware.vb01-aaa01ad...	-	Destination

6. Erstellen Sie auf einem anderen Fehlerdomäne-Speicher-Array die SAN-Initiatorgruppe mit ihren vSphere-Hostinitiatoren und legen Sie die Host-Nähe fest.

Overview Mapped LUNs

STORAGE VM
zoneb

TYPE
VMware

PROTOCOL
Mixed (iSCSI & FC)

COMMENT
-

PORTSET
-

CONNECTION STATUS i
✔ OK

Initiators

Name	De...	Connection status i	In proximity to
iqn.1998-01.com.vmware:dc02-esxi01.sddc.netap...	-	✔ OK	zoneb
iqn.1998-01.com.vmware:dc02-esxi02.sddc.netap...	-	✔ OK	zoneb



Für einen einheitlichen Zugriffsmodus kann die Initiatorgruppe von der Quell-Fehlerdomäne repliziert werden.

7. Ordnen Sie die replizierte LUN mit derselben Zuordnungs-ID wie in der Quellfehlerdomäne zu.

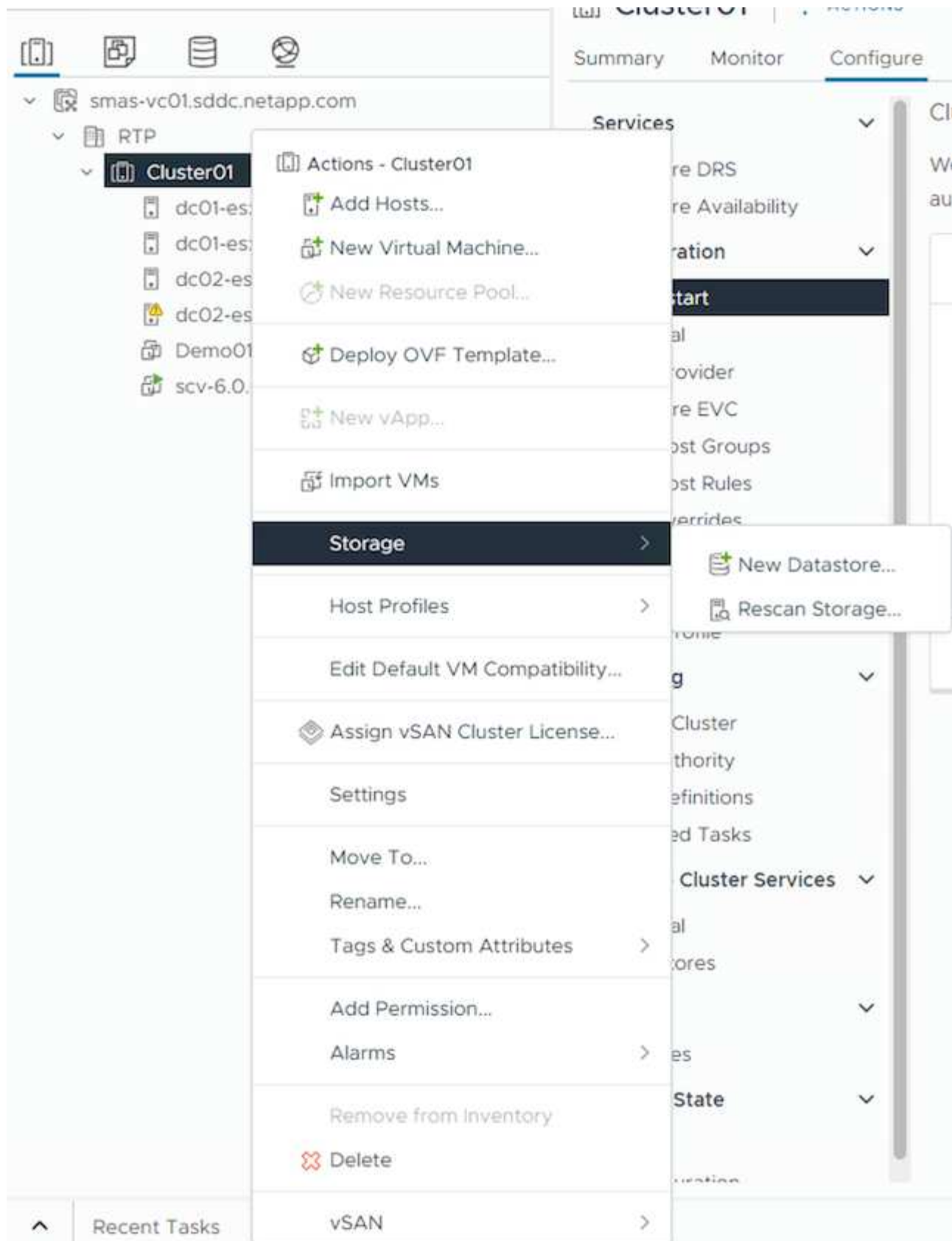
Overview Mapped LUNs

[+ Add](#) [Map LUNs](#)

[Filter](#)

<input type="checkbox"/>	Name	ID
<input type="checkbox"/>	ds02	1
<input type="checkbox"/>	ds01	0

8. Klicken Sie in vCenter mit der rechten Maustaste auf vSphere Cluster, und wählen Sie die Option Speicher erneut scannen.



9. Überprüfen Sie auf einem der vSphere-Hosts im Cluster, ob das neu erstellte Gerät mit dem Datastore angezeigt wird, der nicht verbraucht anzeigt.

dc01-esxi01.sddc.netapp.com | ACTIONS

Summary Monitor **Configure** Permissions VMs Datastores Networks Updates

Storage

- Storage Adapters**
 - Storage Devices
 - Host Cache Configuration
 - Protocol Endpoints
 - I/O Filters
 - Storage Providers
- Networking**
 - Virtual switches
 - VMkernel adapters
 - Physical adapters
 - TCP/IP configuration
- Virtual Machines**
 - VM Startup/Shutdown
 - Agent VM Settings
 - Default VM Compatibility
 - Swap File Location
- System**
 - Licensing
 - Host Profile
 - Time Configuration
 - Authentication Services

Storage Adapters

ADD SOFTWARE ADAPTER REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	ISCSI Software Adapter	ISCSI	Online	iscsi_vmk1(qn.1998-01.com,vmware:dc01-esxi01.sddc.netapp.com:473524194.65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Contr other	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Contr other	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	1	1	1

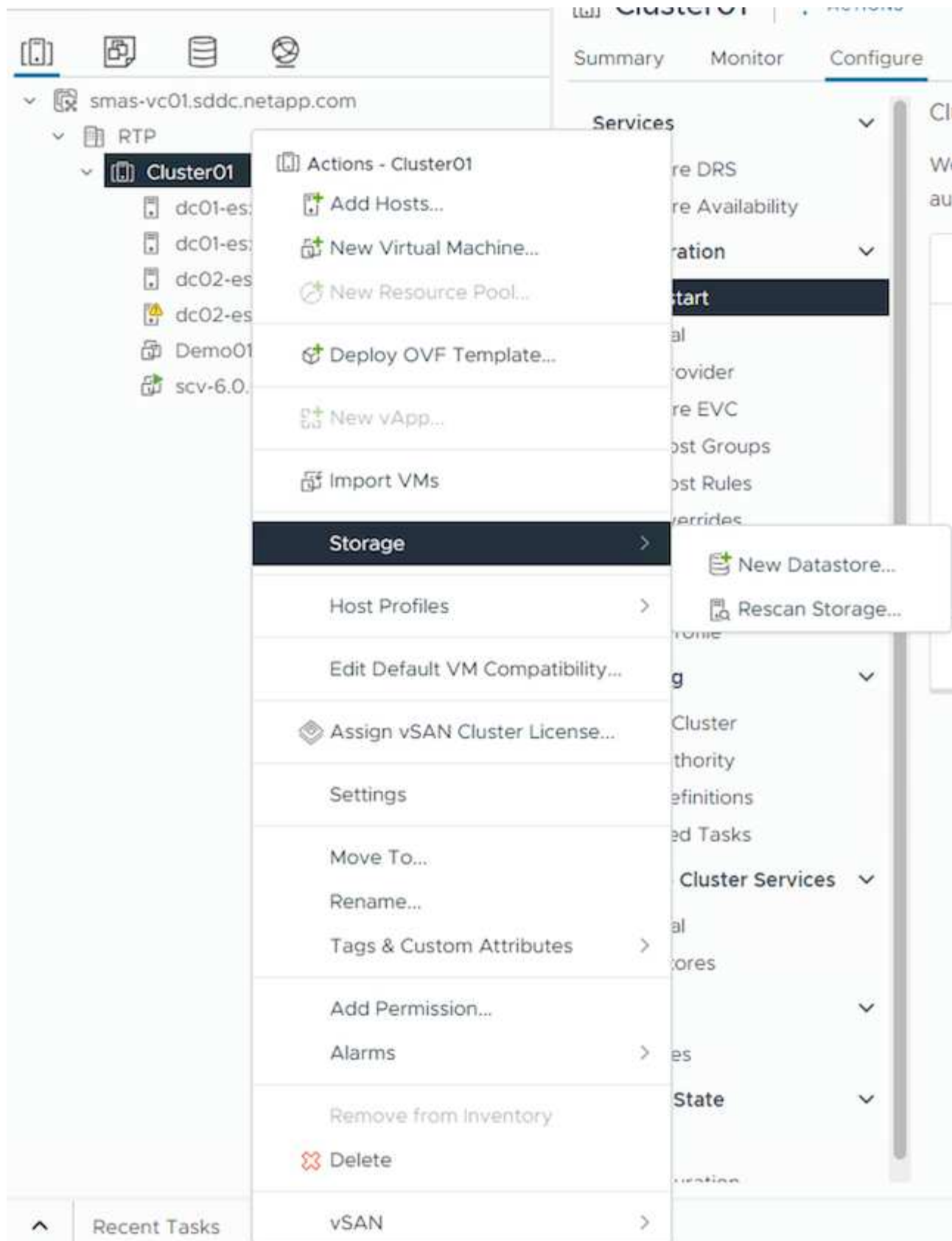
Manage Columns Export 4 items

Properties **Devices** Paths Dynamic Discovery Static Discovery Network Port Binding Advanced Options

REFRESH ATTACH DETACH RENAME

Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	0	disk	250.00 GB	DS01	Attached	Supported	Flash	iSCSI
NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	disk	300.00 GB	Not Consumed	Attached	Supported	Flash	iSCSI

10. Klicken Sie in vCenter mit der rechten Maustaste auf vSphere Cluster, und wählen Sie die Option Neuer Datenspeicher aus.



11. Denken Sie im Assistenten daran, den Datastore-Namen anzugeben und das Gerät mit der richtigen Kapazität und Geräte-ID auszuwählen.

New Datastore

- Type
- Name and device selection**
- VMFS version
- Partition configuration
- Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name:

Info: The datastore will be accessible to all the hosts that are configured with access to the selected disk/LUN. If you do not find the disk/LUN that you are interested in, it might not be accessible to that host. Try changing the host or configure accessibility of that disk/LUN.

Select a host:
Select a host to view its accessible disks/LUNs:

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Ch...
<input checked="" type="radio"/>	NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)	1	300.00 G B	Supported	Flash	512e	Nc
<input type="radio"/>	Local VMware Disk (mpx.vmhba0:CO:T:LO)	0	100.00 G B	Not support ed	HDD	512n	Nc

Manage Columns | Export v | 2 items

CANCEL | BACK | NEXT

12. Überprüfen Sie, ob der Datastore auf allen Hosts im Cluster über beide Fehlerdomänen gemountet ist.

DS02

Summary | Monitor | **Configure** | Permissions | Files | Hosts | VMs

Alarm Definitions
 Scheduled Tasks
 General
 Device Backing
Connectivity and Multipathing
 Hardware Acceleration
 Capability sets
 SnapCenter Plug-in for VMware
 Resource Groups
 Backups

Connectivity and Multipathing

Mount | Unmount

Host	Datastore Mounted	Datastore Connectivity	Mount Point
<input checked="" type="radio"/> dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/> dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/> dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
<input type="radio"/> dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Manage Columns | 4 items

Device NETAPP iSCSI Disk (naa.600a0980383038467724524975577933)

Multipathing Policies ACTIONS v

- Path Selection Policy Round Robin (VMware)
- Storage Array Type VMW_SATP_ALUA
- Owner Plugin NMP

Paths REFRESH | ENABLE | DISABLE

Runtime Name	Status	Target	LUN	Preferred
vmhba65:CO:T:LO1	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a70d56-vs.28-172.21.225.11.3260	1	No
vmhba65:C2:T:LO1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a70d56-vs.28-172.21.225.12-3260	1	No
vmhba65:C3:T:LO1	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a70d56-vs.28-172.21.226.11.3260	1	No
vmhba65:C1:T:LO1	Active (I/O)	iqn.1992-08.com.netapp:sn.3cb67894c1f1ed819200a098a70d56-vs.28-172.21.226.12-3260	1	No

DS02 ACTIONS

Summary Monitor **Configure** Permissions Files Hosts VMs

Alarm Definitions
Scheduled Tasks
General
Device Backing
Connectivity and Multipathing
Hardware Acceleration
Capability sets
SnapCenter Plug-in for VMware
Resource Groups
Backups

Connectivity and Multipathing

Mount UNMOUNT

Host	Datastore Mounted	Datastore Connectivity	Mount Point
dc01-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
dc01-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
dc02-esxi01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e
dc02-esxi02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66b2d163-cef443ad-3a67-005056b92d7e

Manage Columns 4 items

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577933) ↗

Multipathing Policies ACTIONS

- Path Selection Policy: Round Robin (VMware)
- Storage Array Type: VMW_SATP_ALUA
- Policy:
- Owner Plugin: NMP

Paths

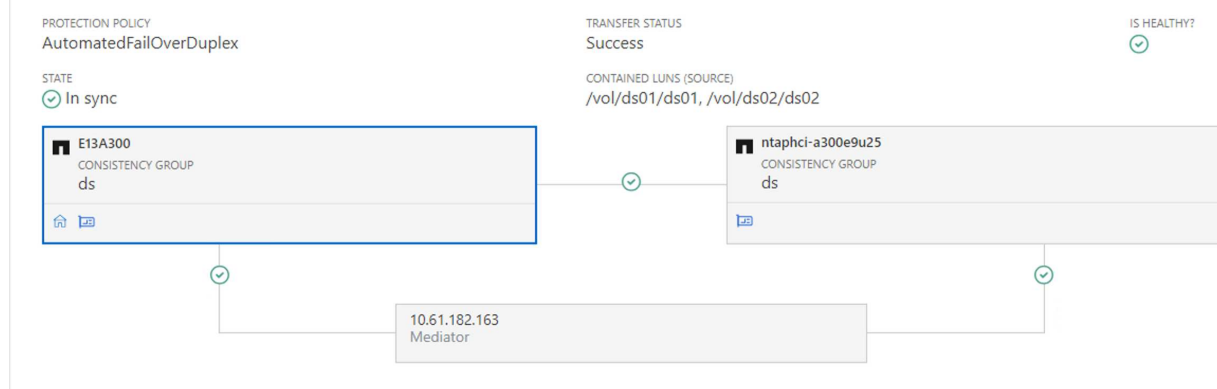
REFRESH ENABLE DISABLE

Route Name	Status	Target	LLN	Preferred
vmhba65:C2:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93efce6b1ed6b10000a098b46a21vs.12:172.21.225.21:3260	1	No
vmhba65:C0:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93efce6b1ed6b10000a098b46a21vs.12:172.21.225.22:3260	1	No
vmhba65:C3:T0:L1	Active (I/O)	iqn.1992-08.com.netapp:sn.133a93efce6b1ed6b10000a098b46a21vs.12:172.21.226.21:3260	1	No
vmhba65:C1:T0:L1	Active	iqn.1992-08.com.netapp:sn.133a93efce6b1ed6b10000a098b46a21vs.12:172.21.226.22:3260	1	No



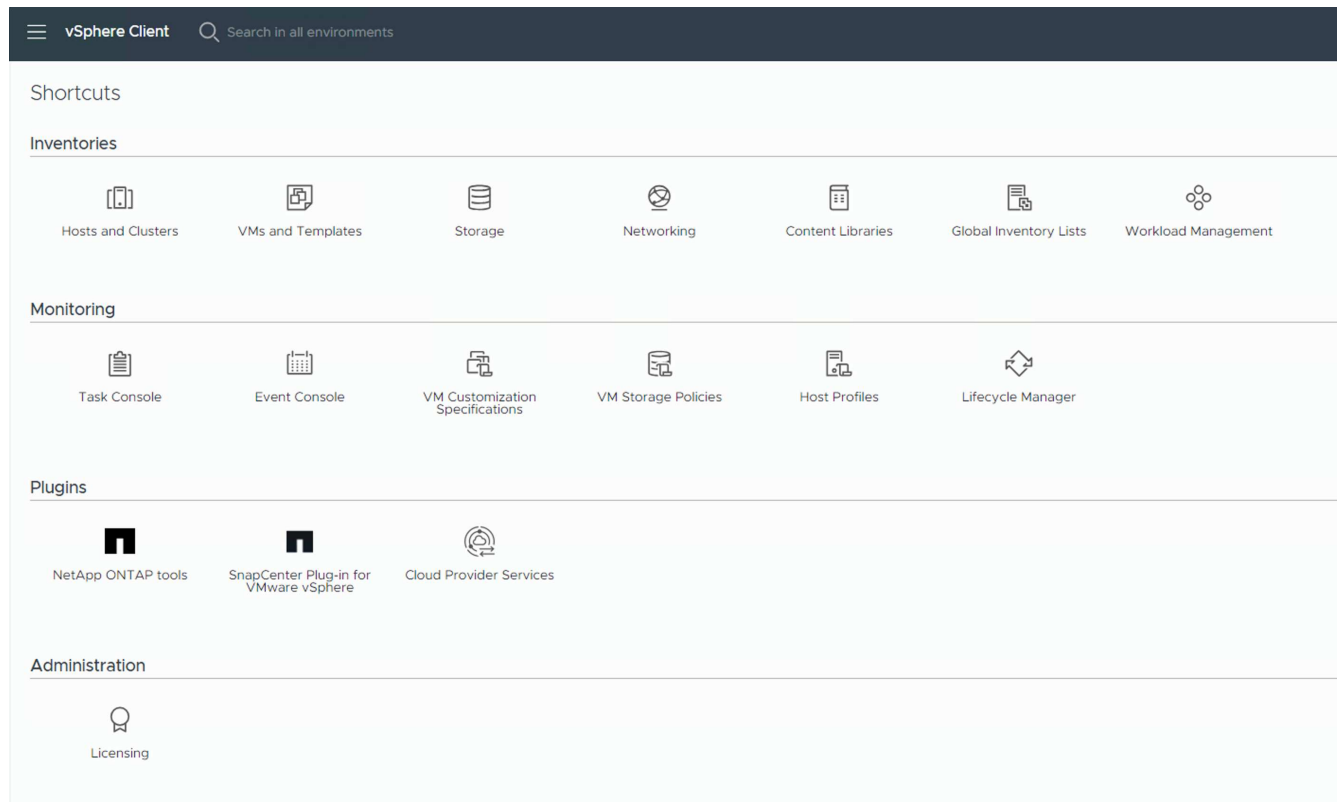
Die obigen Screenshots zeigen aktiven I/O auf dem einzelnen Controller, seit wir AFF verwendet haben. Bei ASA verfügt er über aktive IO auf allen Pfaden.

- Wenn zusätzliche Datastores hinzugefügt werden, müssen Sie daran denken, die vorhandene Consistency Group zu erweitern, damit sie im vSphere-Cluster konsistent ist.



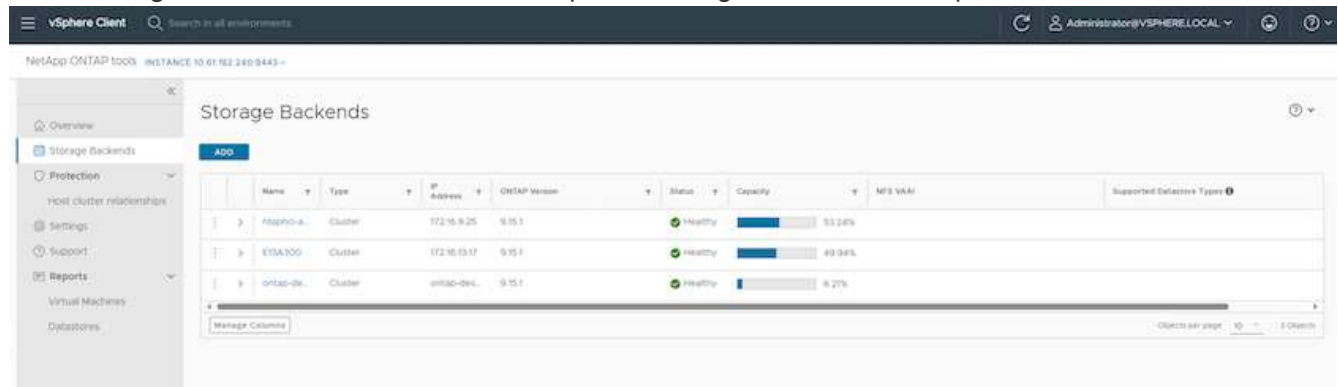
Einheitlicher vMSC Host-Zugriffsmodus mit ONTAP-Tools

- Stellen Sie sicher, dass die NetApp ONTAP-Tools in vCenter bereitgestellt und registriert sind.



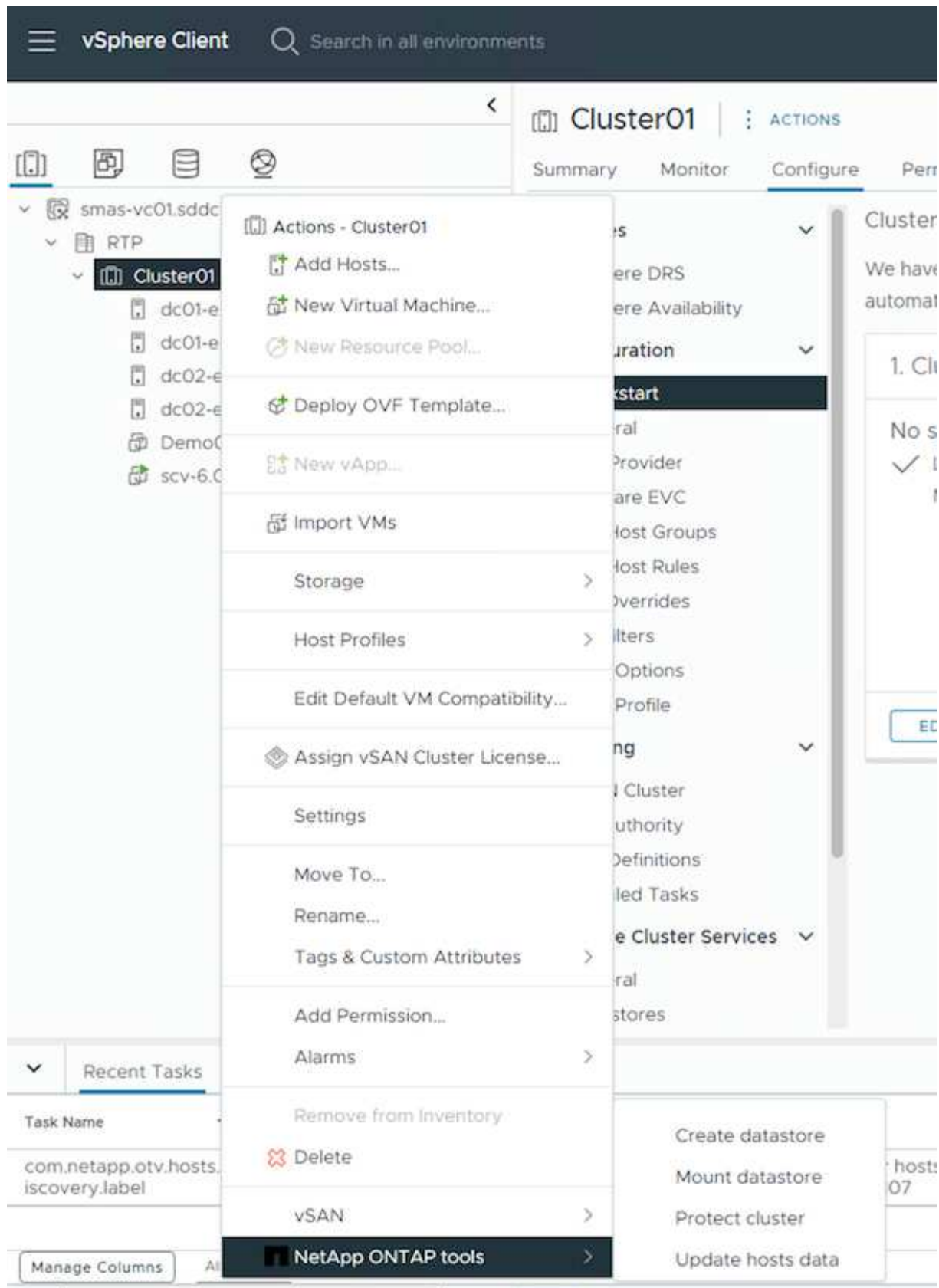
Wenn nicht, folgen Sie ["Bereitstellung von ONTAP-Tools"](#) und ["Fügen Sie eine vCenter Server-Instanz hinzu"](#)

2. Stellen Sie sicher, dass die ONTAP-Speichersysteme bei ONTAP-Tools registriert sind. Dies umfasst sowohl Fehlerdomäne-Speichersysteme als auch ein drittes für asynchrone Remote-Replikation zur Verwendung für den VM-Schutz mit dem SnapCenter Plug-in für VMware vSphere.



Wenn nicht, folgen Sie ["Fügen Sie mithilfe der vSphere Client-UI ein Storage-Back-End hinzu"](#)

3. Aktualisieren Sie die Hostdaten, um sie mit den ONTAP-Tools zu synchronisieren, und dann, ["Erstellen Sie einen Datastore"](#).



4. Um SM-AS zu aktivieren, klicken Sie mit der rechten Maustaste auf vSphere-Cluster und wählen Sie in den NetApp ONTAP-Tools den Schutz des Clusters aus (siehe Screenshot oben).
5. Es zeigt vorhandene Datastores für dieses Cluster sowie SVM-Details an. Der standardmäßige CG-Name ist <vSphere-Cluster-Name>_<SVM name>. Klicken Sie auf die Schaltfläche Beziehung hinzufügen.

Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. [Learn more](#)


Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
[2 datastores](#)

Consistency group name: * Cluster01_zonea

SnapMirror settings

[ADD RELATIONSHIP](#)

Target storage VM	Policy	Uniform Host Configuration	Host proximity
 No SnapMirror relationship found. You can protect datastores using one or more SnapMirror relationships.			
Objects per page 5 0 Object			

[CANCEL](#)

[PROTECT](#)

6. Wählen Sie die Ziel-SVM aus, und setzen Sie die Richtlinie auf AutomatedFailOverDuplex für SM-AS. Es gibt einen Kippschalter für eine einheitliche Hostkonfiguration. Legen Sie die Nähe für jeden Host fest.

Add SnapMirror Relationship

Source storage VM: * E13A300 / zonea

Target storage VM: * zoneb
Cluster: ntaphci-a300e9u25

Policy: * AutomatedFailOverDuplex

Uniform host configuration:

Host proximity settings

 As part of protection, all datastores will be mounted on all hosts.

SET PROXIMAL TO ▾

<input type="checkbox"/>	Hosts	Proximal to
<input type="checkbox"/>		
<input type="checkbox"/>	dc01-esxi02.sddc.netapp.com	Source ▾
<input type="checkbox"/>	dc02-esxi01.sddc.netapp.com	Target ▾

4 Objects

CANCEL

ADD

- Überprüfen Sie die Host-Promity-Informationen und andere Details. Fügen Sie bei Bedarf eine weitere Beziehung zum dritten Standort mit der Replikationsrichtlinie „Asynchron“ hinzu. Klicken Sie dann auf Schützen.

Protect Cluster | Cluster01

Protect the datastores of this cluster using SnapMirror replication. [Learn more](#)

Datastore type: * VMFS

Source storage VM: * zonea
Cluster: E13A300
[2 datastores](#)

Consistency group name: * Cluster01_zonea

SnapMirror settings

[ADD RELATIONSHIP](#)

Target storage VM	Policy	Uniform Host Configuration	Host proximity
⋮ ntaphci-a300e9u25 / zoneb	AutomatedFailOverDuplex	Yes	Source (2), Target (2)

Objects per page 1 Object

[CANCEL](#) [PROTECT](#)

HINWEIS: Wenn Sie das SnapCenter-Plug-in für VMware vSphere 6.0 verwenden möchten, muss die Replikation auf Volume-Ebene statt auf Konsistenzgruppenebene eingerichtet werden.

- Bei einheitlichem Hostzugriff verfügt der Host über eine iSCSI-Verbindung zu beiden Fehlerdomänenspeicher-Arrays.

Connectivity and Multipathing

Host	Datastore Mounted	Datastore Connectivity	Mount Point
dc02-esx01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc01-esx02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc02-esx02.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e
dc01-esx01.sddc.netapp.com	Mounted	Connected	/vmfs/volumes/66aaa811-71dea467-813d-005056b92d7e

Device: NETAPP iSCSI Disk (naa.600a0980383038467724524975577931) -

Multipathing Policies: ACTIONS -

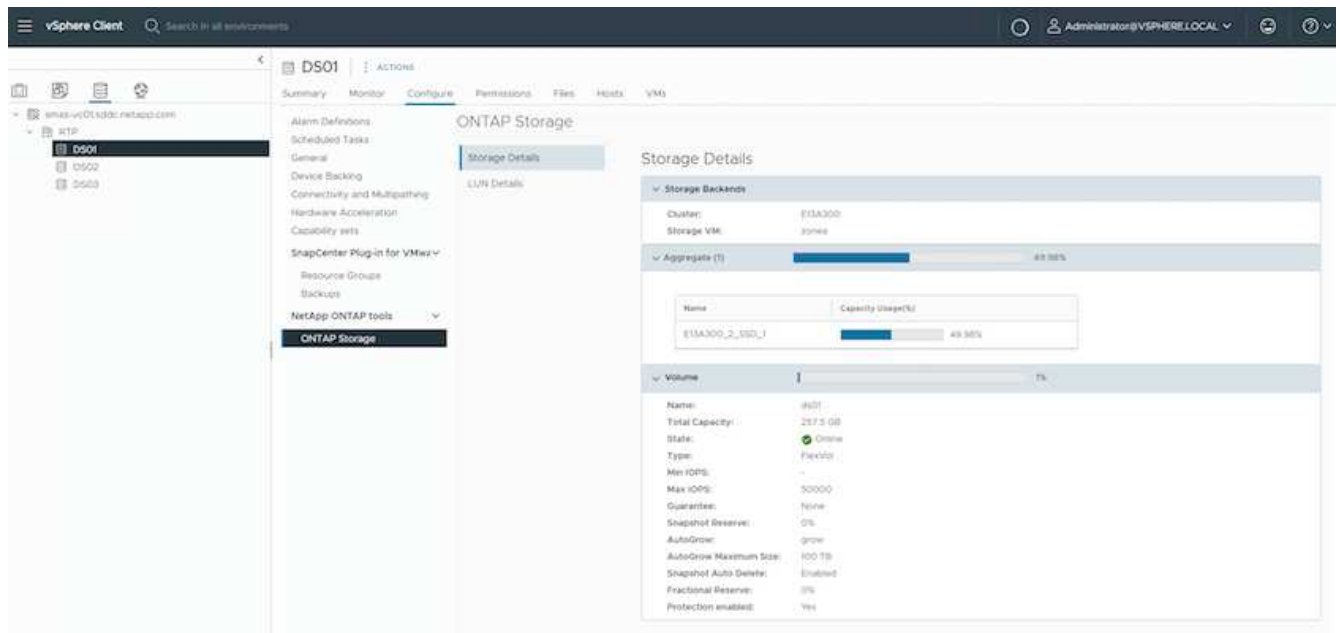
- Path Selection Policy: Round Robin (VMware)
- Storage Array Type Policy: VMW_SATP_ALUA
- Owner Plugin: NMP

Paths:

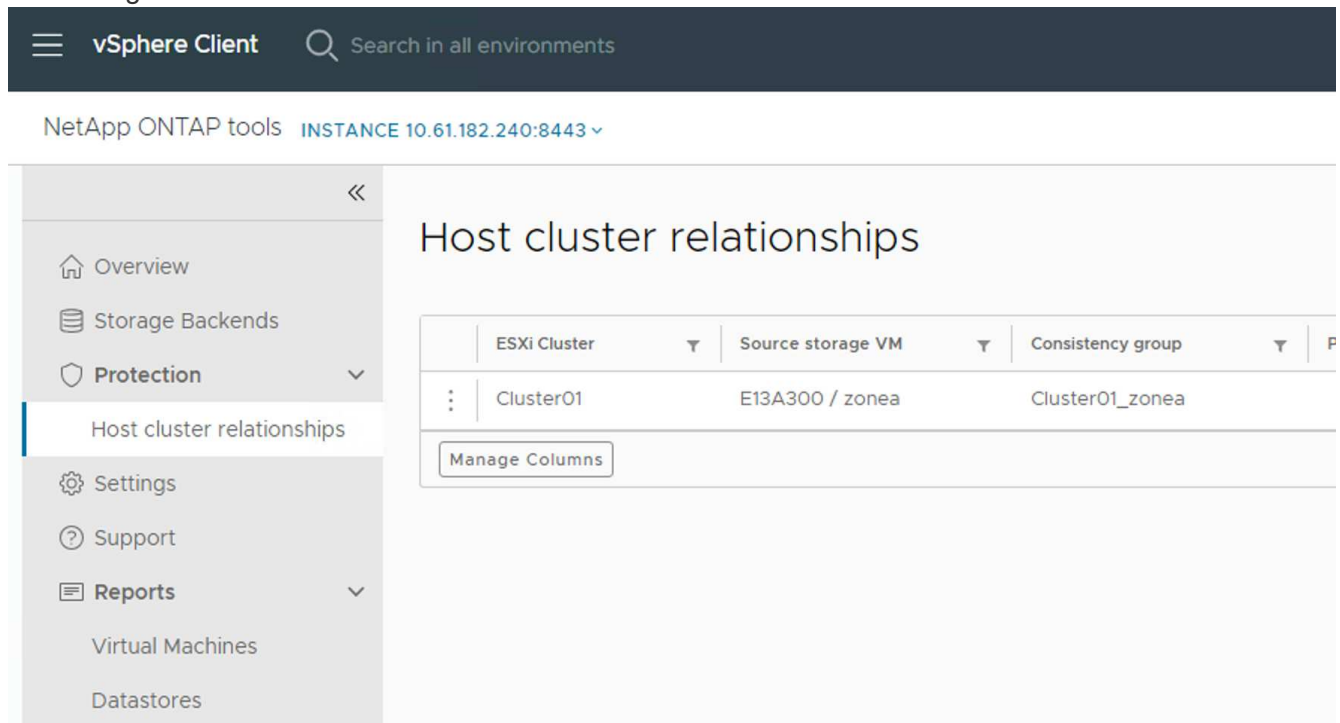
Runtime Name	Status	Target	LUN
vmhba65:C3:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.225.12.3260	0
vmhba65:C2:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.226.12.3260	0
vmhba65:C1:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.225.11.3260	0
vmhba65:C3:T0:L0	Active (VO)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.226.21.3260	0
vmhba65:C0:T1:L0	Active	iqn.1992-08.com.netapp:sn.3cb67894c1f11ed819200a098a70d56:vs.28.172.21.226.11.3260	0
vmhba65:C2:T0:L0	Active (VO)	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.225.21.3260	0
vmhba65:C1:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.226.22.3260	0
vmhba65:C0:T0:L0	Active	iqn.1992-08.com.netapp:sn.133a93e1ce6b11edb10000a098b46a21:vs.12.172.21.225.22.3260	0

HINWEIS: Der obige Screenshot stammt aus AFF. Bei ASA sollte sich DER AKTIVE I/O auf allen Pfaden mit korrekten Netzwerkverbindungen befinden.

- ONTAP Tools Plugin zeigt auch an, dass das Volume geschützt ist oder nicht.

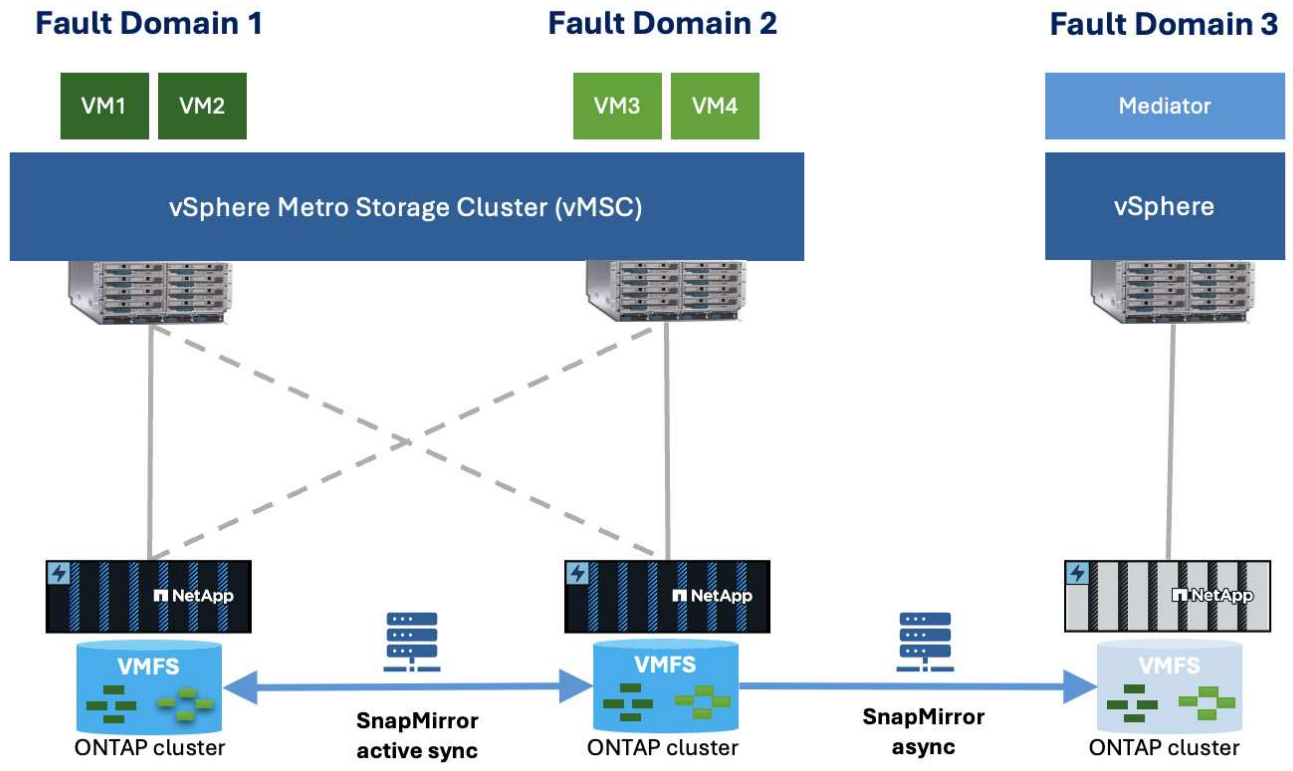


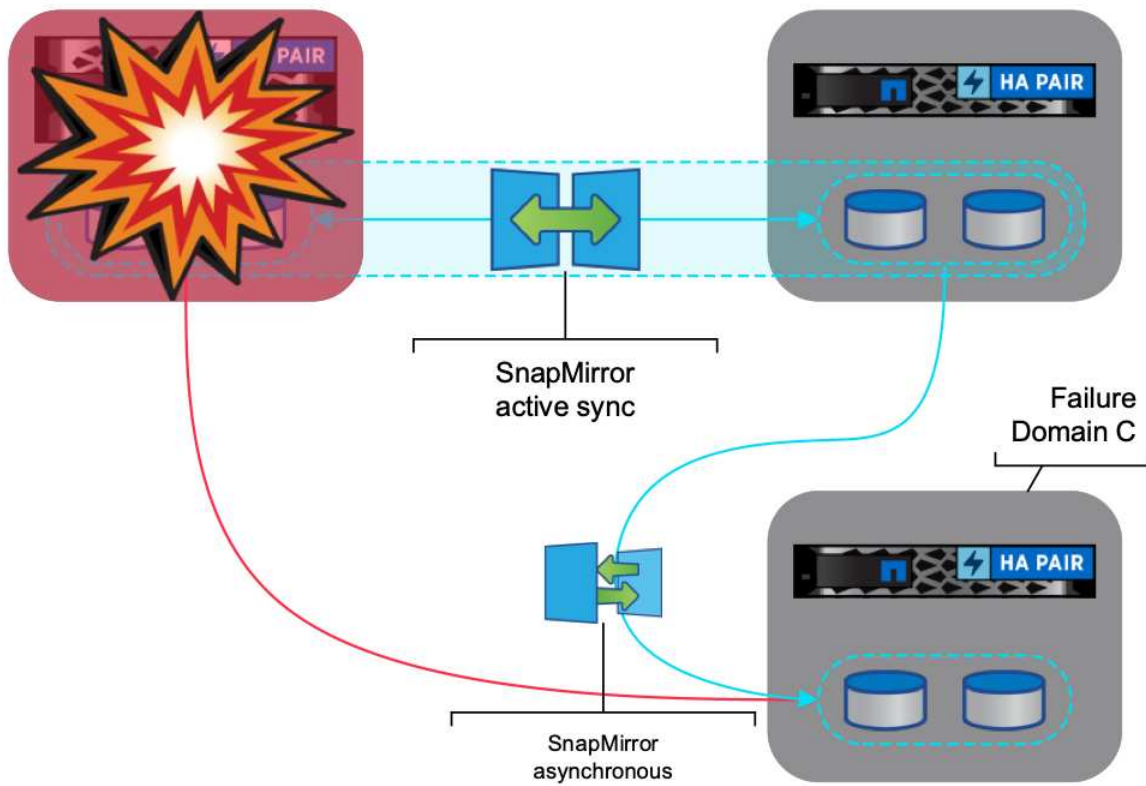
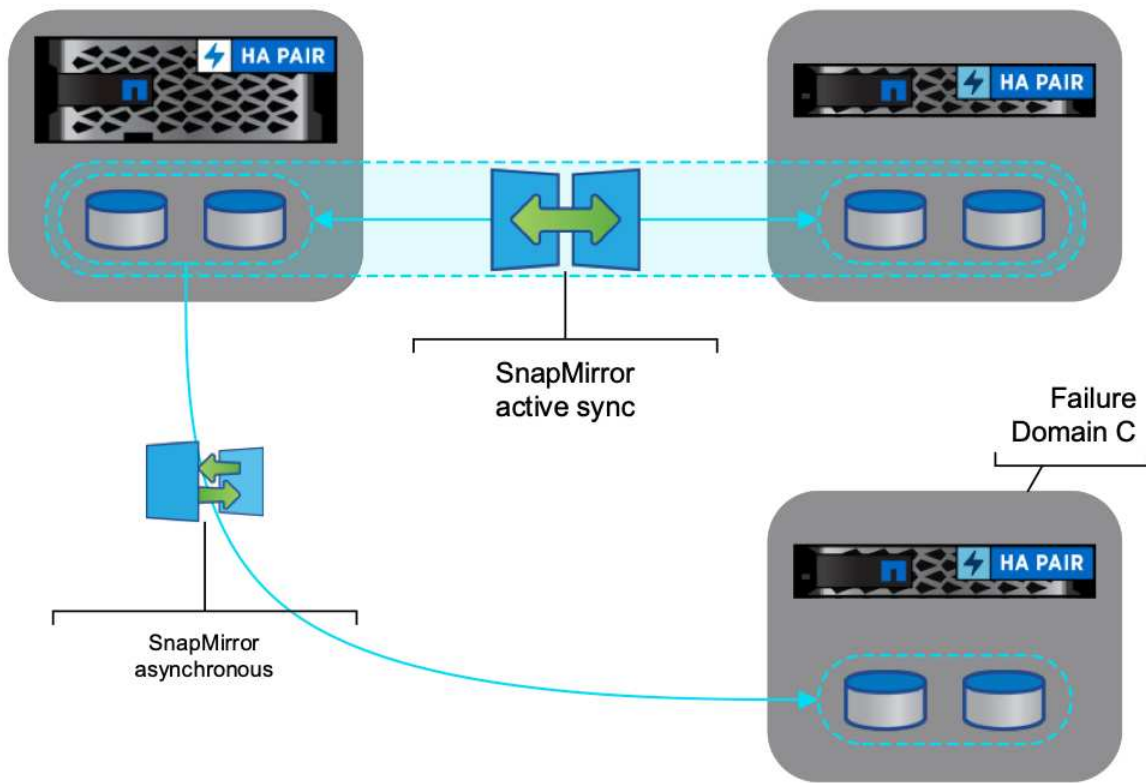
10. Für weitere Details und zum Aktualisieren der Host-Proximity-Informationen kann die Option Host-Cluster-Beziehungen unter den ONTAP-Tools verwendet werden.



VM-Schutz mit SnapCenter Plug-in für VMware vSphere

SnapCenter Plug-in für VMware vSphere (SCV) 6.0 oder höher unterstützt SnapMirror Active Sync und auch in Kombination mit SnapMirror Async zur Replizierung auf die dritte Fehlerdomäne.



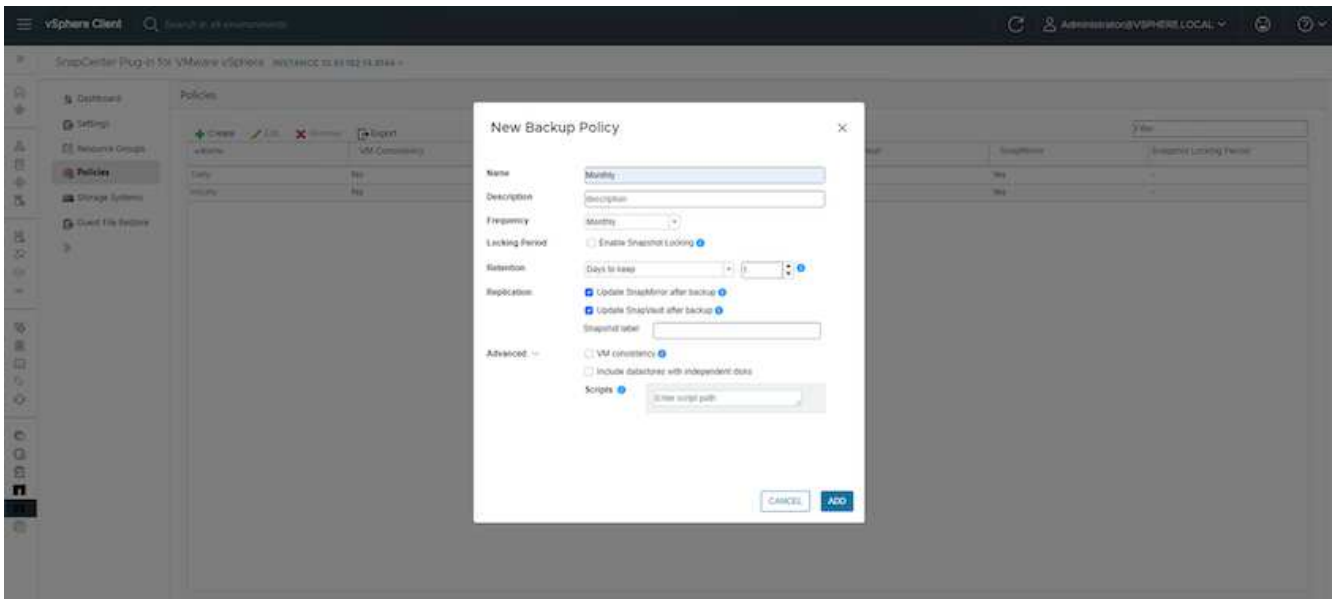


Zu den unterstützten Anwendungsbeispielen gehören: * Sicherung und Wiederherstellung der VM oder des Datenspeichers aus einer der Fehlerdomänen mit SnapMirror Active Sync. * Wiederherstellen von Ressourcen aus der dritten Fehlerdomäne.

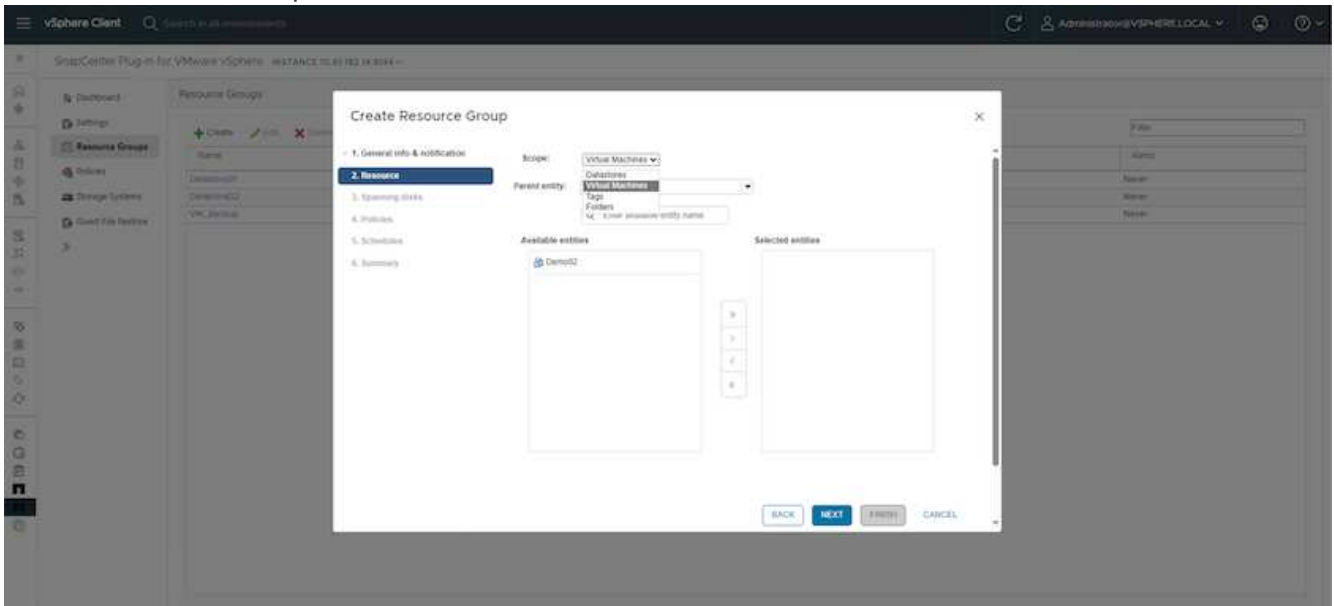
1. Fügen Sie alle ONTAP-Speichersysteme hinzu, die in SCV verwendet werden sollen.



2. Erstellen Sie Eine Richtlinie. Stellen Sie sicher, dass die SnapMirror nach dem Backup auf SM-AS überprüft wird, und aktualisieren Sie auch die SnapVault nach dem Backup für die asynchrone Replikation auf die dritte Fehlerdomäne.



3. Ressourcengruppe mit gewünschten Elementen erstellen, die geschützt werden müssen, der Richtlinie zuordnen und dem Zeitplan zuordnen.



HINWEIS: Snapshot-Name mit der Endung _recent wird bei SM-AS nicht unterstützt.

- Backups werden zu einem geplanten Zeitpunkt basierend auf der der Ressourcengruppe zugeordneten Richtlinie durchgeführt. Jobs können über die Jobüberwachung des Dashboards oder über die Backup-Informationen auf diesen Ressourcen überwacht werden.

The screenshot shows the SnapCenter dashboard in vSphere Client. It features several key sections:

- RECENT JOB ACTIVITIES:** A list of backup jobs with columns for Name, Job Number, Status, and Getting Started. Recent jobs include 'Backup Warning VM_Backup' (failed) and several 'Backup Successful' jobs for 'Datastore1' and 'VM_Backup'.
- JOB STATUS:** A donut chart showing overall job performance: 52% Successful, 7% Warning, and 1 Running.
- LATEST PROTECTION SUMMARY:** Three donut charts for Primary, Secondary, and VMs. Primary is 60% Protected, Secondary is 20% Replicated, and VMs are 40% Not replicated.
- STORAGE:** A bar chart showing storage usage for Snapshots (Primary and Secondary) and a summary of storage savings: 66.46 x Storage Savings, resulting in 303.43 GB Saved and 4.64 GB Storage Consumed.

The screenshot shows the configuration page for 'Datastore01' in SnapCenter. The 'Backups' section is active, displaying a table of backup jobs:

Name	Status	Locations	Snapshot Lock Expi.	Created Time	Mounted	Policy	VMware Snapshot
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 4:00:16 PM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 3:28:09 PM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 3:00:21 PM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 2:28:09 PM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 2:00:16 PM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 1:28:09 PM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 1:00:17 PM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 12:28:10 PM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 12:00:18 PM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 11:28:10 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 10:00:18 AM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 9:28:12 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 9:00:21 AM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 8:28:09 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 8:00:16 AM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 7:28:09 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 7:00:15 AM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 6:28:10 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 6:00:17 AM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 5:28:09 AM	No	Hourly	No
VM_Backup_08-11	Completed	Primary & Second	-	8/11/2024 5:00:17 AM	No	Hourly	No
Datastore01_08-11	Completed	Primary & Second	-	8/11/2024 4:28:09 AM	No	Hourly	No

6. Eine ähnliche Option ist auch für den Datastore-Mount-Vorgang verfügbar.

Mount Backup ×

ESXi host name

Selected backup VM_Backup_08-11-2024_16.00.02.0270

Select datastore

<input type="checkbox"/>	Name	Location
<input type="checkbox"/>	Datastore01	Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270
<input type="checkbox"/>	Datastore02	Primary:172.21.228.10:Datastore01:VM_Backup_08-11-2024_16.00.02.0270 Secondary:svms2:vol_Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270 Secondary:zoneb:Datastore01_dest:VM_Backup_08-11-2024_16.00.02.0270
<input type="checkbox"/>		
<input type="checkbox"/>		

⚠ Warning for ONTAP 9.12.1 and below version ×

Unterstützung bei weiteren Vorgängen mit SCV finden Sie unter "[Dokumentation zum SnapCenter Plug-in für VMware vSphere](#)"

VMware Cloud Foundation

VMware Cloud Foundation

VMware Cloud Foundation (VCF) ist eine Reihe von Technologien, die einen einfachen Zugang zu einer Hybrid-Cloud-Umgebung ermöglichen. Innerhalb der VCF-Lösung werden sowohl native Kubernetes- als auch Virtual Machine-basierte Workloads unterstützt. Wesentliche Services wie VMware vSphere, VMware vSAN, VMware NSX-T Data Center und VMware vRealize Cloud Management sind Bestandteile des VCF-Pakets. Zusammen bilden diese Services eine softwaredefinierte Infrastruktur, die Computing-, Storage-, Netzwerk-, Sicherheits- und Cloud-Management unterstützt. Diese kollektive Infrastruktur bietet eine hybride Nutzung, bei der das VCF-Framework die Umgebung vom Datacenter vor Ort auf Amazon Web Services (AWS), Azure und Google Cloud erweitert.

Dokumentationsressourcen

Detaillierte Informationen zu NetApp Angeboten für VMware Cloud Foundation finden Sie in der folgenden Blog-Reihe mit vier (4) Teilen:

- "[NetApp und VMware Cloud Foundation leicht gemacht Teil 1: Die ersten Schritte](#)"

- ["NetApp und VMware Cloud Foundation leicht gemacht Teil 2: VCF und ONTAP Principal Storage"](#)
- ["NetApp und VMware Cloud Foundation leicht gemacht Teil 3: VCF und Element Principal Storage"](#)
- ["NetApp und VMware Cloud Foundation leicht gemacht – Teil 4: ONTAP-Tools für VMware und ergänzenden Storage"](#)

VMware Cloud Foundation mit NetApp All-Flash-SAN-Arrays

- ["VCF mit NetApp ASA Arrays, Einführung und Technologieübersicht"](#)
- ["Verwenden Sie ONTAP-Tools, um iSCSI-Datstores in einer VCF-Managementdomäne bereitzustellen"](#)
- ["Implementieren Sie VVols \(iSCSI\)-Datstores mit ONTAP Tools in einer VI-Workload-Domäne"](#)
- ["Konfigurieren Sie NVMe over TCP-Datstores für die Verwendung in einer VI-Workload-Domäne"](#)
- ["Implementieren Sie das SnapCenter Plug-in für VMware vSphere und verwenden Sie es, um VMs in einer VI-Workload-Domäne zu sichern und wiederherzustellen"](#)

VMware Cloud Foundation mit NetApp All-Flash-AFF-Arrays

- ["VCF mit NetApp AFF Arrays, Einführung und Technologieübersicht"](#)
- ["Verwenden Sie ONTAP mit NFS als Haupt-Storage für VI-Workload-Domänen"](#)
- ["Verwenden Sie ONTAP Tools, um NFS-Datstores in einer VI-Workload-Domäne zu implementieren"](#)

NetApp FlexPod Lösungen für VMware Cloud Foundation

- ["Erweiterung der FlexPod Hybrid Cloud mit VMware Cloud Foundation"](#)
- ["FlexPod als Workload-Domäne für VMware Cloud Foundation verwendet"](#)
- ["FlexPod as a Workload Domain for VMware Cloud Foundation – Designleitfaden"](#)

VCF mit NetApp ASA-Arrays

VMware Cloud Foundation mit NetApp All-Flash-SAN-Arrays

VMware Cloud Foundation (VCF) ist eine integrierte softwaredefinierte Datacenter-Plattform (SDDC), die einen vollständigen Stack von softwaredefinierter Infrastruktur für die Ausführung von Enterprise-Applikationen in einer Hybrid-Cloud-Umgebung bereitstellt. Sie kombiniert Computing-, Storage-, Netzwerk- und Managementfunktionen in einer einheitlichen Plattform und ermöglicht so ein konsistentes Betriebserlebnis in Private und Public Clouds.

Autor: Josh Powell

Dieses Dokument enthält Informationen zu Storage-Optionen, die für VMware Cloud Foundation mit dem NetApp All-Flash-SAN-Array zur Verfügung stehen. Unterstützte Storage-Optionen werden mit spezifischen Anweisungen zur Implementierung von iSCSI-Datstores als ergänzenden Storage für Management-Domänen sowie für vVol (iSCSI)- und NVMe/TCP-Datstores als ergänzende Datstores für Workload-Domänen abgedeckt. Ebenfalls behandelt wird die Datensicherung von VMs und Datstores mit SnapCenter für VMware vSphere.

Anwendungsfälle

Anwendungsfälle in dieser Dokumentation:

- Storage-Optionen für Kunden, die einheitliche Umgebungen sowohl in privaten als auch in öffentlichen Clouds benötigen.
- Automatisierte Lösung zur Bereitstellung einer virtuellen Infrastruktur für Workload-Domänen.
- Skalierbare Storage-Lösung, die auf neue Anforderungen zugeschnitten ist, auch wenn sie nicht direkt auf die Anforderungen von Computing-Ressourcen ausgerichtet ist
- Mit ONTAP Tools für VMware vSphere stellen Sie zusätzlichen Storage für Management- und VI-Workload-Domänen bereit.
- Sichern Sie VMs und Datastores mit dem SnapCenter Plug-in für VMware vSphere.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Lösungsarchitekten, die flexiblere Storage-Optionen für VMware Umgebungen benötigen und ihre TCO maximieren möchten.
- Lösungsarchitekten, die auf der Suche nach VCF Storage-Optionen sind, die Datensicherungs- und Disaster Recovery-Optionen bei den großen Cloud-Providern bieten.
- Storage-Administratoren, die eine spezifische Anleitung zur Konfiguration von VCF mit Haupt- und zusätzlichem Speicher wünschen.
- Storage-Administratoren, die spezifische Anweisungen zum Schutz von VMs und Datenspeichern auf ONTAP Storage benötigen.

Technologischer Überblick

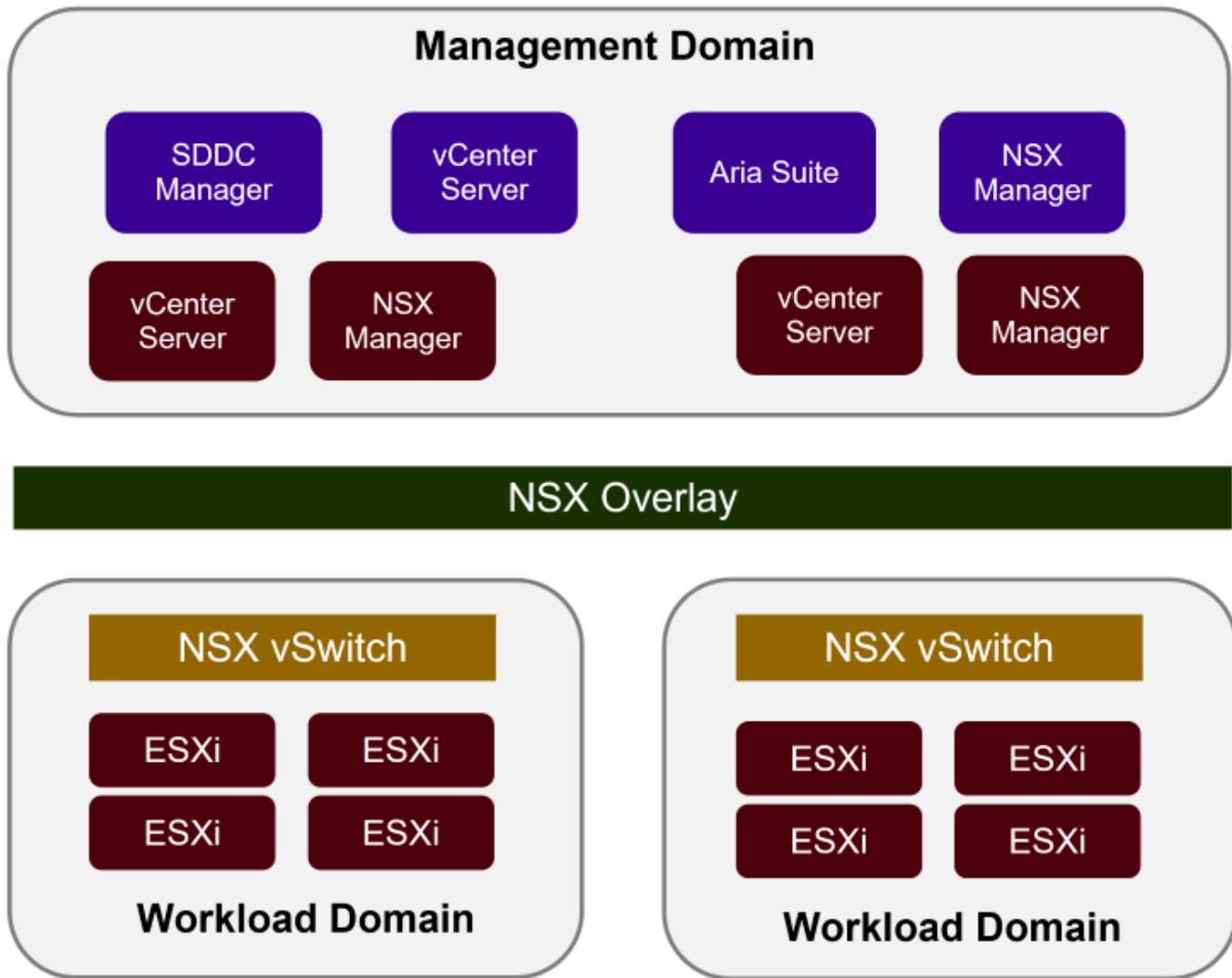
Die VCF mit NetApp ASA-Lösung besteht aus den folgenden Hauptkomponenten:

VMware Cloud Foundation

VMware Cloud Foundation erweitert die vSphere Hypervisor-Angebote von VMware durch die Kombination wichtiger Komponenten wie SDDC Manager, vSphere, vSAN, NSX und VMware Aria Suite zur Erstellung eines softwaredefinierten Datacenters.

Die VCF Lösung unterstützt sowohl native Kubernetes-Workloads als auch Workloads, die auf Virtual Machines basieren. Zentrale Services wie VMware vSphere, VMware vSAN, VMware NSX-T Data Center und VMware Aria Cloud Management sind Bestandteile des VCF-Pakets. Zusammen bilden diese Services eine softwaredefinierte Infrastruktur, die ein effizientes Management von Computing, Storage, Netzwerken, Sicherheit und Cloud-Management ermöglicht.

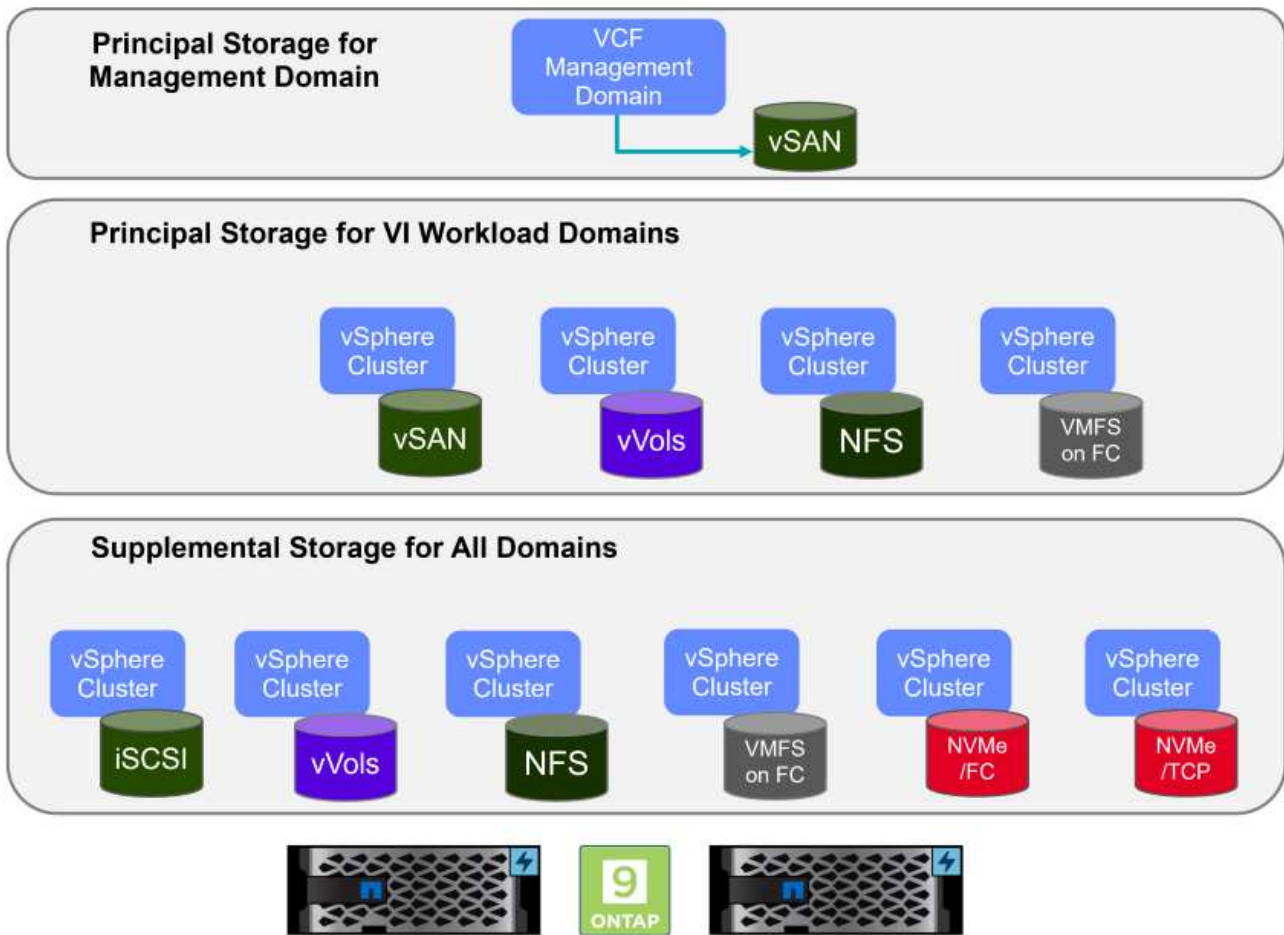
VCF besteht aus einer einzelnen Management-Domäne und bis zu 24 VI-Workload-Domänen, die jeweils eine Einheit für applikationsfähige Infrastrukturen darstellen. Eine Workload-Domäne besteht aus einem oder mehreren vSphere Clustern, die von einer einzelnen vCenter Instanz gemanagt werden.



Weitere Informationen zur Architektur und Planung von VCF finden Sie unter "[Architekturmodelle und Workload-Domänen-Typen in VMware Cloud Foundation](#)".

VCF Storage-Optionen

VMware unterteilt Speicheroptionen für VCF in **Principal** und **Supplemental** Speicher. Die VCF-Management-Domäne muss vSAN als Haupt-Storage verwenden. Es gibt jedoch zahlreiche zusätzliche Storage-Optionen für die Managementdomäne sowie Haupt- und ergänzende Storage-Optionen für VI-Workload-Domänen.



Hauptspeicher für Workload-Domänen

Hauptspeicher bezieht sich auf jeden Storage-Typ, der während des Setups im SDDC Manager direkt mit einer VI-Workload-Domäne verbunden werden kann. Der Hauptspeicher wird mit dem SDDC Manager als Teil der Cluster-Erstellungs-Orchestrierung bereitgestellt und ist der erste für eine Workload-Domäne konfigurierte Datastore. Sie umfasst vSAN, vVols (VMFS), NFS und VMFS auf Fibre Channel.

Ergänzender Speicher für Management- und Workload-Domänen

Zusätzlicher Storage ist der Storage-Typ, der dem Management oder den Workload-Domänen jederzeit nach der Erstellung des Clusters hinzugefügt werden kann. Zusätzlicher Storage umfasst die größte Auswahl an unterstützten Storage-Optionen, die alle von NetApp ASA Arrays unterstützt werden. Für die meisten Storage-Protokolltypen kann zusätzlicher Storage mit den ONTAP Tools für VMware vSphere implementiert werden.

Zusätzliche Dokumentationsressourcen für VMware Cloud Foundation:

- * ["Dokumentation zu VMware Cloud Foundation"](#)
- * ["Unterstützte Storage-Typen für VMware Cloud Foundation"](#)
- * ["Management von Storage in VMware Cloud Foundation"](#)

NetApp All-Flash-SAN-Arrays

Das rein Flash-basierte SAN-Array NetApp (ASA) ist eine hochperformante Storage-Lösung, die auf die hohen Anforderungen moderner Datacenter ausgerichtet ist. Sie kombiniert die Geschwindigkeit und Zuverlässigkeit von Flash Storage mit den erweiterten Datenmanagement-Funktionen von NetApp und bietet dadurch herausragende Performance, Skalierbarkeit und Datensicherung.

Die Produktpalette von ASA umfasst sowohl Die Modelle Der A-Serie als auch der C-Serie.

All-NVMe-Flash-Arrays der NetApp A-Serie wurden für hochperformante Workloads entwickelt und bieten eine äußerst niedrige Latenz und hohe Ausfallsicherheit. Dadurch sind sie für geschäftskritische Applikationen geeignet.



QLC Flash-Arrays der C-Serie richten sich an Anwendungsfälle mit höherer Kapazität, die die Geschwindigkeit von Flash mit der Wirtschaftlichkeit von Hybrid Flash bieten.



Ausführliche Informationen finden Sie im ["NetApp ASA Landing Page"](#).

Unterstützte Storage-Protokolle

Das ASA unterstützt alle standardmäßigen SAN-Protokolle, einschließlich iSCSI, Fibre Channel (FC), Fibre Channel over Ethernet (FCoE) und NVME over Fabrics.

iSCSI - NetApp ASA bietet robuste Unterstützung für iSCSI und ermöglicht den Zugriff auf Speichergeräte auf Blockebene über IP-Netzwerke. Die nahtlose Integration mit iSCSI-Initiatoren ermöglicht eine effiziente Bereitstellung und Verwaltung von iSCSI-LUNs. Die erweiterten Funktionen von ONTAP wie Multi-Pathing, CHAP-Authentifizierung und ALUA-Unterstützung

Designanleitungen zu iSCSI-Konfigurationen finden Sie im ["Referenzdokumentation zur SAN-Konfiguration"](#).

Fibre Channel - NetApp ASA bietet umfassende Unterstützung für Fibre Channel (FC), eine Hochgeschwindigkeits-Netzwerktechnologie, die häufig in Storage Area Networks (SANs) verwendet wird. ONTAP lässt sich nahtlos in FC-Infrastrukturen integrieren und bietet zuverlässigen und effizienten Zugriff auf Storage-Geräte auf Blockebene. Mit Funktionen wie Zoning, Multi-Pathing und Fabric Login (FLOGI) wird die Performance optimiert, die Sicherheit erhöht und die nahtlose Konnektivität in FC-Umgebungen sichergestellt.

Anleitungen zum Design von Fibre Channel-Konfigurationen finden Sie im ["Referenzdokumentation zur SAN-Konfiguration"](#).

NVMe over Fabrics: NetApp ONTAP und ASA unterstützen NVMe over Fabrics. NVMe/FC ermöglicht die Verwendung von NVMe-Storage-Geräten über Fibre-Channel-Infrastruktur und NVMe/TCP über Storage-IP-Netzwerke.

Eine Anleitung zum Design für NVMe finden Sie unter ["Konfiguration, Support und Einschränkungen von NVMe"](#)

Aktiv/aktiv-Technologie

NetApp All-Flash SAN Arrays ermöglichen aktiv/aktiv-Pfade durch beide Controller. Dadurch muss das Host-Betriebssystem nicht auf einen Ausfall eines aktiven Pfads warten, bevor der alternative Pfad aktiviert wird. Das bedeutet, dass der Host alle verfügbaren Pfade auf allen Controllern nutzen kann und sicherstellen kann, dass immer aktive Pfade vorhanden sind, unabhängig davon, ob sich das System in einem stabilen Zustand befindet oder ob ein Controller Failover durchgeführt wird.

Darüber hinaus bietet die NetApp ASA eine herausragende Funktion, die die Geschwindigkeit des SAN-Failover enorm erhöht. Jeder Controller repliziert kontinuierlich wichtige LUN-Metadaten an seinen Partner. So ist jeder Controller bereit, bei einem plötzlichen Ausfall des Partners die Verantwortung für die Datenüberlassung zu übernehmen. Diese Bereitschaft ist möglich, da der Controller bereits über die notwendigen Informationen verfügt, um die Laufwerke zu nutzen, die zuvor vom ausgefallenen Controller verwaltet wurden.

Beim aktiv/aktiv-Pathing haben sowohl geplante als auch ungeplante Takeovers I/O-Wiederaufnahme-Zeiten von 2-3 Sekunden.

Weitere Informationen finden Sie unter ["TR-4968: NetApp All-SAS-Array – Datenverfügbarkeit und Datenintegrität mit der NetApp ASA"](#).

Storage-Garantien

NetApp bietet mit All-Flash-SAN-Arrays von NetApp einzigartige Storage-Garantien. Einzigartige Vorteile:

Storage-Effizienz-Garantie: mit der Storage-Effizienz-Garantie erzielen Sie eine hohe Performance bei gleichzeitiger Minimierung der Storage-Kosten. 4:1 für SAN-Workloads.

6 Nines (99.9999%) Data Availability guarantee: garantiert die Behebung von ungeplanten Ausfallzeiten in mehr als 31.56 Sekunden pro Jahr.

Ransomware Recovery-Garantie: Garantierte Datenwiederherstellung im Falle eines Ransomware-Angriffs.

Siehe ["NetApp ASA Produktportal"](#) Finden Sie weitere Informationen.

NetApp ONTAP Tools für VMware vSphere

Mit den ONTAP Tools für VMware vSphere können Administratoren NetApp Storage direkt innerhalb des vSphere Clients managen. Mit den ONTAP Tools können Sie Datastores implementieren und managen und vVol Datastores bereitstellen.

Mit ONTAP Tools können Datenspeicher Storage-Funktionsprofilen zugeordnet werden, die eine Reihe von

Attributen des Storage-Systems bestimmen. Dadurch können Datastores mit bestimmten Attributen wie Storage-Performance oder QoS erstellt werden.

ONTAP Tools umfassen zudem einen **VMware vSphere APIs for Storage Awareness (VASA) Provider** für ONTAP Storage-Systeme, der die Bereitstellung von VMware Virtual Volumes (VVols) Datastores, die Erstellung und Verwendung von Storage-Funktionsprofilen, Compliance-Überprüfung und Performance-Monitoring ermöglicht.

Weitere Informationen zu NetApp ONTAP-Tools finden Sie im ["ONTAP-Tools für VMware vSphere - Dokumentation"](#) Seite.

SnapCenter Plug-in für VMware vSphere

Das SnapCenter Plug-in für VMware vSphere (SCV) ist eine Softwarelösung von NetApp, die umfassende Datensicherung für VMware vSphere Umgebungen bietet. Er vereinfacht und optimiert den Prozess des Schutzes und des Managements von Virtual Machines (VMs) und Datastores. SCV verwendet Storage-basierten Snapshot und Replikation zu sekundären Arrays, um kürzere Recovery Time Objectives zu erreichen.

Das SnapCenter Plug-in für VMware vSphere bietet folgende Funktionen in einer einheitlichen Oberfläche, die in den vSphere Client integriert ist:

Policy-basierte Snapshots - mit SnapCenter können Sie Richtlinien für die Erstellung und Verwaltung von anwendungskonsistenten Snapshots von virtuellen Maschinen (VMs) in VMware vSphere definieren.

Automatisierung - automatisierte Snapshot-Erstellung und -Verwaltung auf Basis definierter Richtlinien unterstützen einen konsistenten und effizienten Datenschutz.

Schutz auf VM-Ebene - granularer Schutz auf VM-Ebene ermöglicht effizientes Management und Recovery einzelner virtueller Maschinen.

Funktionen zur Storage-Effizienz - durch die Integration in NetApp Storage-Technologien können Storage-Effizienz-Funktionen wie Deduplizierung und Komprimierung für Snapshots erzielt werden, was die Speicheranforderungen minimiert.

Das SnapCenter-Plug-in orchestriert die Stilllegung von Virtual Machines in Verbindung mit hardwarebasierten Snapshots auf NetApp Storage-Arrays. Die SnapMirror Technologie wird eingesetzt, um Backup-Kopien auf sekundäre Storage-Systeme einschließlich in der Cloud zu replizieren.

Weitere Informationen finden Sie im ["Dokumentation zum SnapCenter Plug-in für VMware vSphere"](#).

Die Integration von BlueXP ermöglicht 3-2-1-1-Backup-Strategien zur Erweiterung von Datenkopien auf Objekt-Storage in der Cloud.

Weitere Informationen zu 3-2-1-1-Backup-Strategien mit BlueXP finden Sie unter ["3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs"](#).

Lösungsüberblick

Die in dieser Dokumentation vorgestellten Szenarien zeigen, wie ONTAP-Storage-Systeme als zusätzlicher Storage für Management- und Workload-Domänen eingesetzt werden. Darüber hinaus wird das SnapCenter Plug-in für VMware vSphere zur Sicherung von VMs und Datastores verwendet.

Szenarien in dieser Dokumentation:

- **Verwenden Sie ONTAP-Tools, um iSCSI-Datstores in einer VCF-Management-Domain bereitzustellen.** Klicken Sie Auf ["Hier"](#) Für Bereitstellungsschritte.
- **Verwenden von ONTAP-Tools zur Bereitstellung von VVols (iSCSI) Datstores in einer VI Workload-Domäne.** Klicken Sie Auf ["Hier"](#) Für Bereitstellungsschritte.
- **Konfiguration von NVMe over TCP Datstores für die Verwendung in einer VI Workload Domain.** Klicken Sie Auf ["Hier"](#) Für Bereitstellungsschritte.
- **Bereitstellen und Verwenden des SnapCenter Plug-ins für VMware vSphere zum Schutz und zur Wiederherstellung von VMs in einer VI-Workload-Domäne.** Klicken Sie Auf ["Hier"](#) Für Bereitstellungsschritte.

Verwenden Sie ONTAP-Tools, um zusätzlichen Speicher für VCF-Verwaltungsdomänen zu konfigurieren

In diesem Szenario zeigen wir, wie Sie ONTAP Tools für VMware vSphere (OTV) bereitstellen und verwenden, um einen iSCSI-Datstore für eine VCF-Verwaltungsdomäne zu konfigurieren.

Autor: Josh Powell

Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

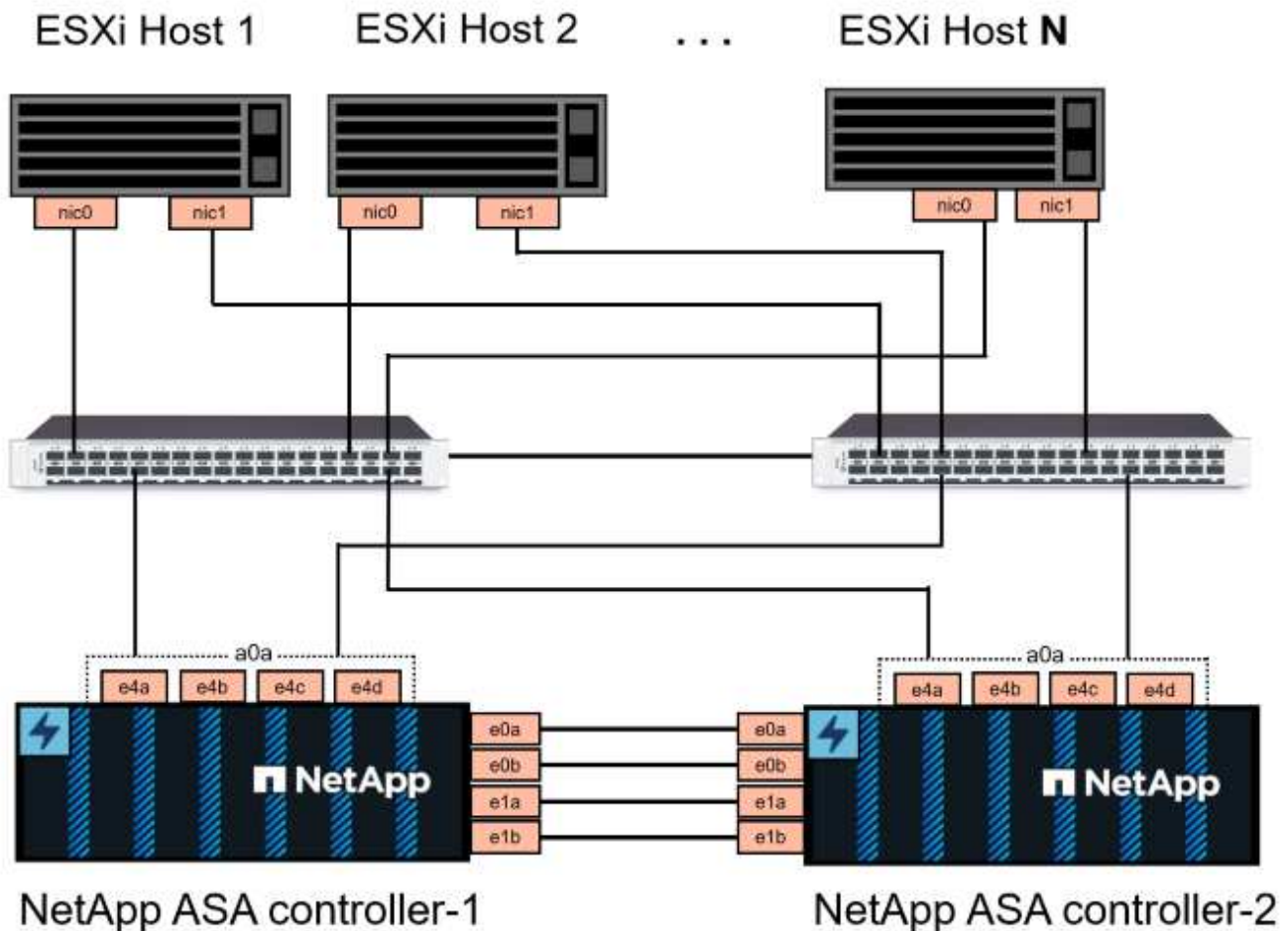
- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VCF-Verwaltungsdomäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VCF-Managementdomäne.
- Stellen Sie ONTAP Tools auf der VCF-Managementdomäne bereit.
- Erstellen Sie einen neuen VMFS Datstore in der VCF-Managementdomäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.

NetApp empfiehlt für iSCSI vollständig redundante Netzwerkdesigns. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration für Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Weitere Informationen finden Sie im NetApp ["Referenz zur SAN-Konfiguration"](#) Finden Sie weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten ethernet-Netzwerken.

In dieser Dokumentation wird der Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adressinformationen für die Erstellung mehrerer LIFs für iSCSI-Datenverkehr demonstriert. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter "[LIF erstellen \(Netzwerkschnittstelle\)](#)".

Weitere Informationen zur Verwendung von VMFS iSCSI-Datstores mit VMware finden Sie unter "[VSphere VMFS Datenspeicher – iSCSI-Storage-Back-End mit ONTAP](#)".



In Situationen, in denen mehrere VMkernel-Adapter auf demselben IP-Netzwerk konfiguriert sind, wird empfohlen, die iSCSI-Port-Bindung für die ESXi-Hosts zu verwenden, um sicherzustellen, dass der Lastausgleich über die Adapter hinweg erfolgt. Siehe KB-Artikel "[Überlegungen zur Verwendung der Software-iSCSI-Portbindung in ESX/ESXi \(2038869\)](#)".

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und zum Erstellen eines VMFS-Datstore in der VCF-Managementdomäne zu verwenden:

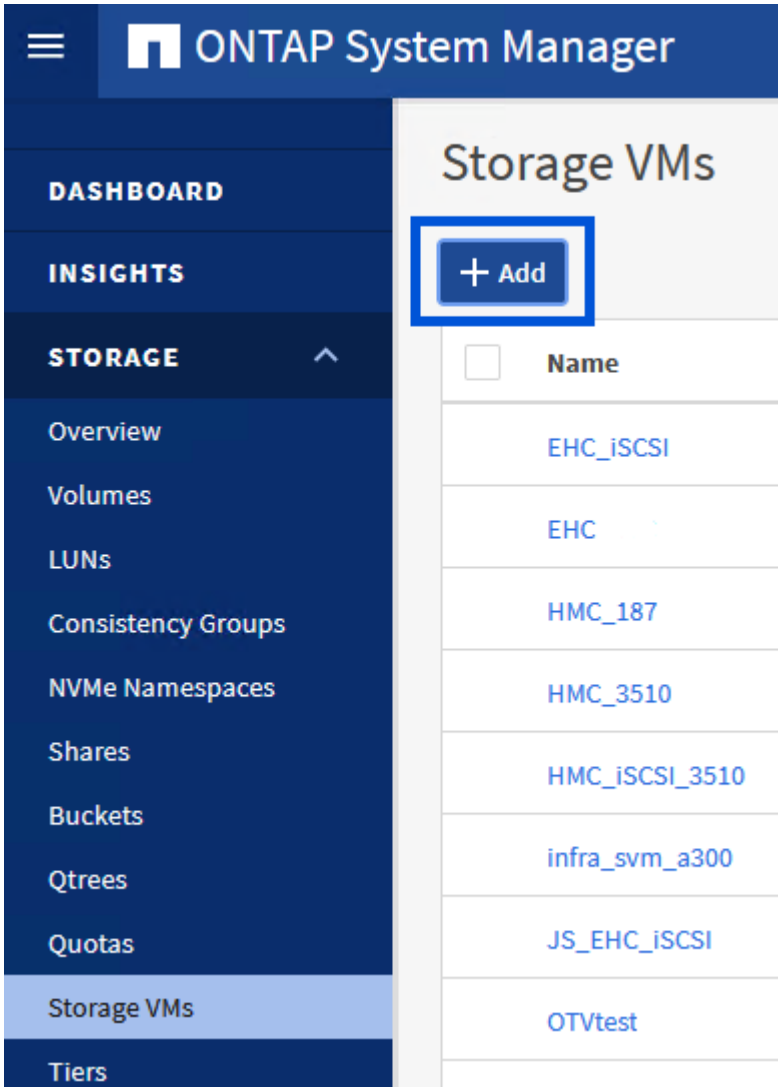
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager durchgeführt.

Storage-VM und LIFs erstellen

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für iSCSI-Datenverkehr zu erstellen.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf **+ Hinzufügen**, um zu starten.



2. Im **Add Storage VM** Wizard geben Sie einen **Namen** für die SVM an, wählen Sie den **IP Space** aus und klicken Sie dann unter **Access Protocol auf die Registerkarte *iSCSI** und aktivieren Sie das Kontrollkästchen **enable iSCSI**.

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. Geben Sie im Abschnitt **Network Interface** die **IP-Adresse**, **Subnetzmaske** und **Broadcast Domain und Port** für die erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert sein, um allgemeine Einstellungen für alle verbleibenden LIFs zu verwenden oder separate Einstellungen zu verwenden.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten Ethernet-Netzwerken.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Wählen Sie aus, ob das Storage VM Administration-Konto aktiviert werden soll (für mandantenfähige Umgebungen), und klicken Sie auf **Speichern**, um die SVM zu erstellen.

Storage VM Administration

Manage administrator account

Save

Cancel

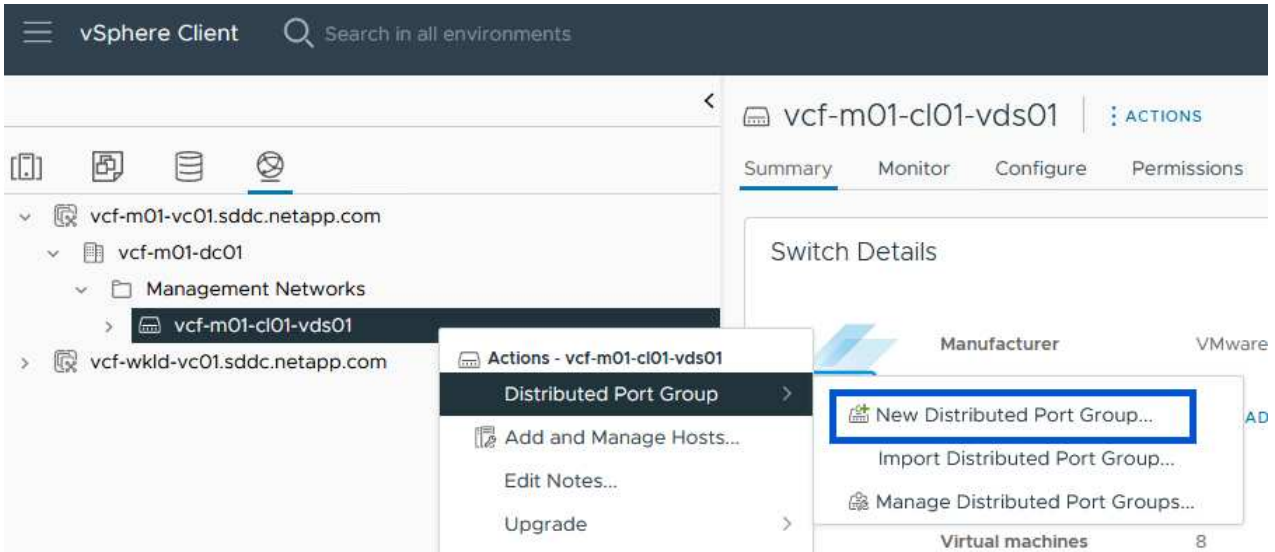
Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein

Die folgenden Schritte werden auf dem VCF-Management-Domain-Cluster unter Verwendung des vSphere-Clients durchgeführt.

Erstellen Sie verteilte Portgruppen für iSCSI-Datenverkehr

Gehen Sie wie folgt vor, um eine neue verteilte Portgruppe für jedes iSCSI-Netzwerk zu erstellen:

1. Navigieren Sie im vSphere-Client für den Management Domain Cluster zu **Inventar > Netzwerk**. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen von **New Distributed Port Group...** aus.



2. Geben Sie im Assistenten **New Distributed Port Group** einen Namen für die neue Portgruppe ein und klicken Sie auf **Next**, um fortzufahren.
3. Füllen Sie auf der Seite **Configure settings** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige VLAN-ID angeben. Klicken Sie auf **Weiter**, um fortzufahren.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding Static binding

Port allocation Elastic ⓘ

Number of ports 8

Network resource pool (default)

VLAN

VLAN type VLAN

VLAN ID 3374

Advanced

Customize default policies configuration

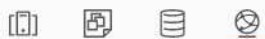
CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen und sicherzustellen, dass Sie die richtige **VLAN-ID** eingegeben haben.
- Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.

vSphere Client Search in all environments



- vcf-m01-vc01.sddc.netapp.com
 - vcf-m01-dc01
 - Management Networks
 - vcf-m01-cl01-vds01
 - SDDC-DPortGroup-VM-Mgmt
 - vcf-m01-cl01-vds-DVUplinks-19
 - vcf-m01-cl01-vds01-ns-iscsi-a**
 - vcf-m01-cl01-vds0
 - vcf-m01-cl01-vds0
 - vcf-m01-cl01-vds0
 - vcf-m01-cl01-vds0
- vcf-wkld-vc01.sddc.netapp.com

Actions - vcf-m01-cl01-vds01-pg-iscsi-a

Edit Settings...

Export Configuration...

Restore Configuration...

vcf-m01-cl01-vds01-pg-iscsi-a ACTIONS

Summary Monitor Configure Permissions Ports

Distributed Port Group Details



Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-m01-cl01-vds0
Network protocol profile	--
Network resource pool	--
Hosts	4

7. Navigieren Sie auf der Seite **Distributed Port Group - Edit Settings** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **unused Uplinks** zu verschieben.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

General	Load balancing	Route based on originating virtual por ▾
Advanced	Network failure detection	Link status only ▾
VLAN	Notify switches	Yes ▾
Security	Failback	Yes ▾
Traffic shaping		
Teaming and failover		
Monitoring	Failover order ⓘ	
Miscellaneous	Active uplinks	
	uplink1	
	Standby uplinks	
	Unused uplinks	
	uplink2	

CANCEL OK

8. Wiederholen Sie diesen Schritt für die zweite iSCSI-Portgruppe. Allerdings bewegt sich dieses Mal **Uplink1** zu **unbenutzten Uplinks**.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual por 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 

MOVE UP MOVE DOWN

Active uplinks

 uplink2

Standby uplinks

Unused uplinks

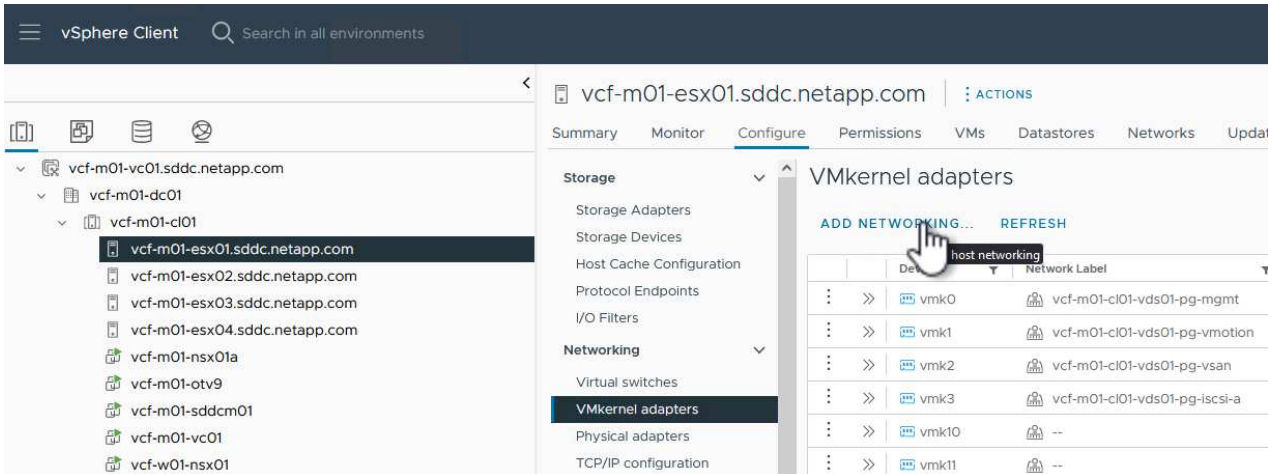
 uplink1



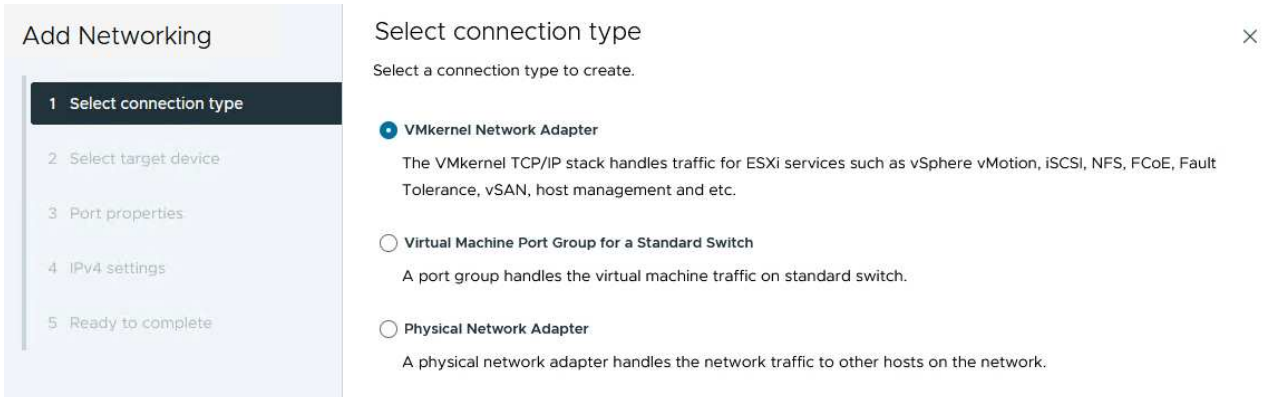
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

Wiederholen Sie diesen Vorgang auf jedem ESXi-Host in der Managementdomäne.

1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts im Inventar der Verwaltungsdomäne. Wählen Sie auf der Registerkarte **Configure VMkernel Adapter** und klicken Sie auf **Add Networking...**, um zu starten.



2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für iSCSI aus.

Add Networking

- 1 Select connection type
- 2 Select target device**
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-ci01-vds01
<input checked="" type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-a	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-b	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-mgmt	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vmotion	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vsan	--	vcf-m01-ci01-vds01

Manage Columns 6 items

CANCEL

BACK

NEXT

4. Behalten Sie auf der Seite **Port Properties** die Standardeinstellungen bei und klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties**
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label vcf-m01-ci01-vds01-pg-iscsi-a (vcf-m01-ci01-vds01)

MTU Get MTU from switch 9000

TCP/IP stack Default

Available services

- Enabled services
- vMotion
 - Provisioning
 - Fault Tolerance logging
 - Management
 - vSphere Replication
 - vSphere Replication NFC
 - vSAN
 - vSAN Witness
 - vSphere Backup NFC
 - NVMe over TCP
 - NVMe over RDMA

5. Geben Sie auf der Seite **IPv4 settings** die **IP-Adresse**, **Subnetzmaske** ein, und geben Sie eine neue Gateway-IP-Adresse ein (nur bei Bedarf). Klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

6. Überprüfen Sie Ihre Auswahl auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um den VMkernel-Adapter zu erstellen.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-m01-cl01-vds01-pg-iscsi-a

Distributed switch vcf-m01-cl01-vds01
- ▼ Port properties

New port group vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.114 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

7. Wiederholen Sie diesen Vorgang, um einen VMkernel Adapter für das zweite iSCSI-Netzwerk zu erstellen.

Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools

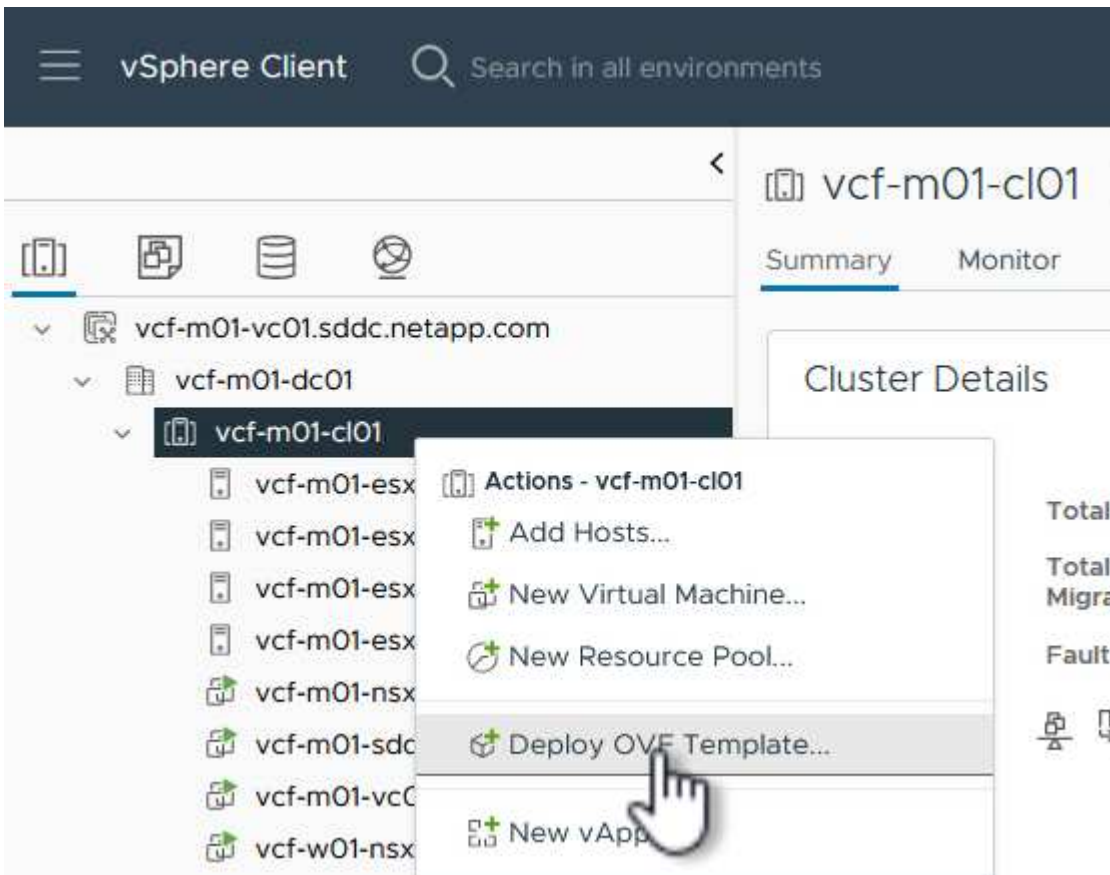
Die folgenden Schritte werden auf dem VCF-Management-Domänencluster unter Verwendung des vSphere-Clients durchgeführt und umfassen die Bereitstellung von OTV, die Erstellung eines VMFS-iSCSI-Datastore und die Migration von Management-VMs auf den neuen Datastore.

Implementieren Sie ONTAP-Tools für VMware vSphere

ONTAP Tools für VMware vSphere (OTV) werden als VM-Appliance implementiert und verfügen über eine integrierte vCenter-Benutzeroberfläche zum Management von ONTAP Storage.

Füllen Sie die folgenden Schritte aus, um ONTAP Tools für VMware vSphere zu implementieren:

1. Rufen Sie das OVA-Image der ONTAP-Tools auf "[NetApp Support Website](#)" Und in einen lokalen Ordner herunterladen.
2. Melden Sie sich bei der vCenter Appliance für die VCF-Managementdomäne an.
3. Klicken Sie in der vCenter-Appliance-Oberfläche mit der rechten Maustaste auf den Management-Cluster und wählen Sie **Deploy OVF Template...** aus



4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei für ONTAP-Tools aus.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie für den Speicherort der Konfigurations- und Festplattendateien den vSAN Datastore des VCF Management Domain Clusters aus.

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

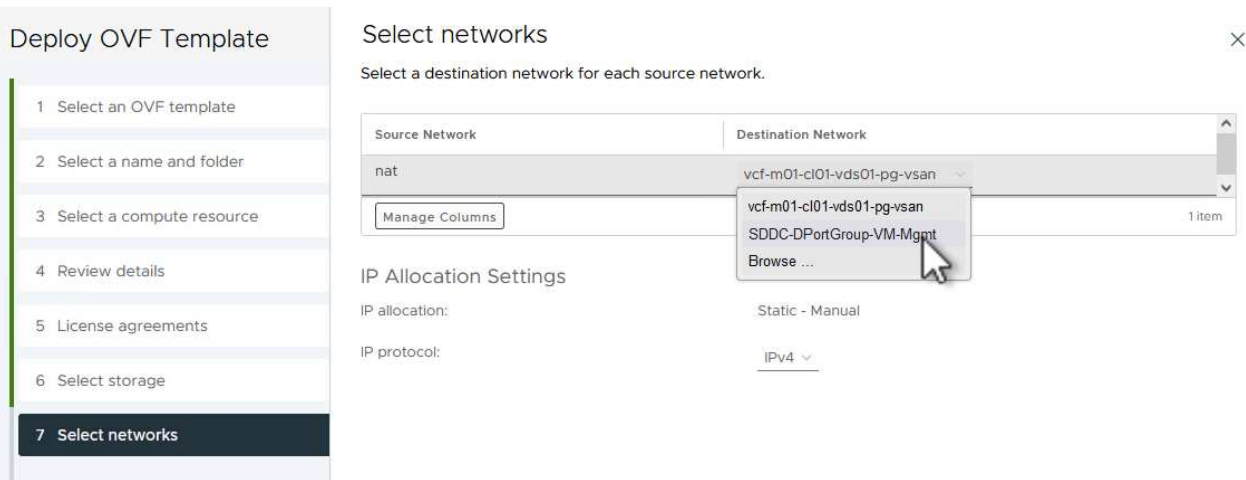
VM Storage Policy

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 5 items

7. Wählen Sie auf der Seite Netzwerk auswählen das Netzwerk aus, das für den Verwaltungsdatenverkehr verwendet wird.



8. Geben Sie auf der Seite Vorlage anpassen alle erforderlichen Informationen ein:

- Passwort für administrativen Zugriff auf OTV.
- NTP-Server-IP-Adresse.
- Passwort für das OTV-Wartungskonto.
- OTV Derby DB-Kennwort.
- Aktivieren Sie nicht das Kontrollkästchen, um VMware Cloud Foundation (VCF)* zu aktivieren. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
- FQDN oder IP-Adresse der vCenter-Appliance und Anmeldeinformationen für vCenter angeben.
- Geben Sie die erforderlichen Felder für Netzwerkeigenschaften an.

Klicken Sie auf **Weiter**, um fortzufahren.

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

Customize template

Customize the deployment properties of this software solution.

! 2 properties have invalid values ✕

System Configuration	4 settings
Application User Password (*)	Password to assign to the administrator account. 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.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. <input type="text" value="172.21.166.1"/>
Maintenance User Password (*)	Password to assign to maint user account.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>

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

Customize template

Configure vCenter or Enable VCF	5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="172.21.166.140"/>
Port (*)	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
Username (*)	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
Password (*)	Specify the password of an existing vCenter to register to.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>
Network Properties	8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-m01-otv9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is

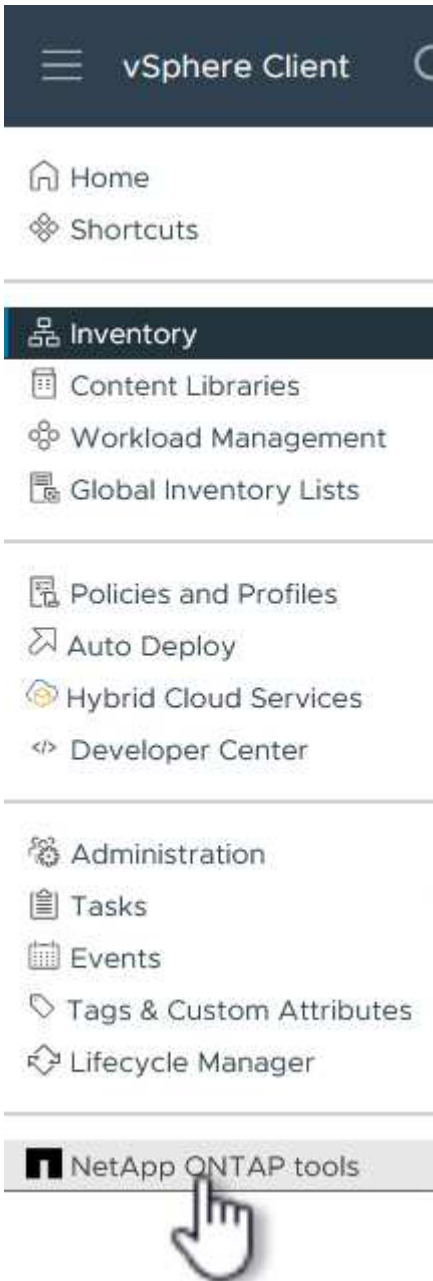
CANCEL BACK NEXT

9. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der OTV-Appliance zu beginnen.

Konfigurieren Sie einen VMFS-iSCSI-Datstore in der Management-Domain mit OTV

Führen Sie die folgenden Schritte aus, um einen VMFS-iSCSI-Datstore als zusätzlichen Speicher in der Management-Domäne zu konfigurieren:

1. Navigieren Sie im vSphere-Client zum Hauptmenü und wählen Sie **NetApp ONTAP-Tools**.



2. Klicken Sie in **ONTAP-Tools** auf der Seite erste Schritte (oder von **Speichersystemen**) auf **Hinzufügen**, um ein neues Speichersystem hinzuzufügen.

vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings


Reports

- Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report
- Log Integrity Report

ONTAP tools for VMware vSphere


Getting Started Traditional Dashboard vVols Dashboard


ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.



Add Storage System


Add storage systems to ONTAP tools for VMware vSphere.





Provision Datastore

Create traditional or vVols datastores.




[What's new?](#)
September 4, 2023


- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

Resources

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)

Next Steps



 [View Dashboard](#)
View and monitor the datastores in ONTAP tools for VMware vSphere.

 [Settings](#)
Configure administrative settings such as credentials, alarm thresholds.

3. Geben Sie die IP-Adresse und Anmeldeinformationen des ONTAP-Speichersystems ein und klicken Sie auf **Hinzufügen**.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server	vcf-m01-vc01.sddc.netapp.com 
Name or IP address:	172.16.9.25
Username:	admin
Password:	●●●●●●●●
Port:	443
Advanced options	


CANCEL

SAVE & ADD MORE

ADD 

4. Klicken Sie auf **Yes**, um das Clusterzertifikat zu autorisieren und das Speichersystem hinzuzufügen.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server

vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

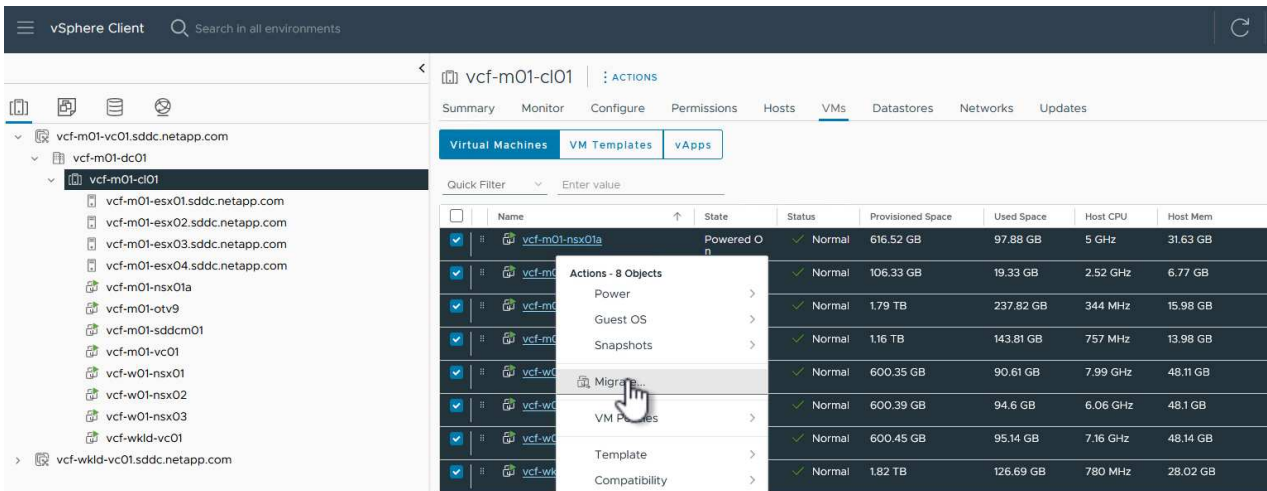
ADD

Migration von Management-VM's auf iSCSI-Datenspeicher

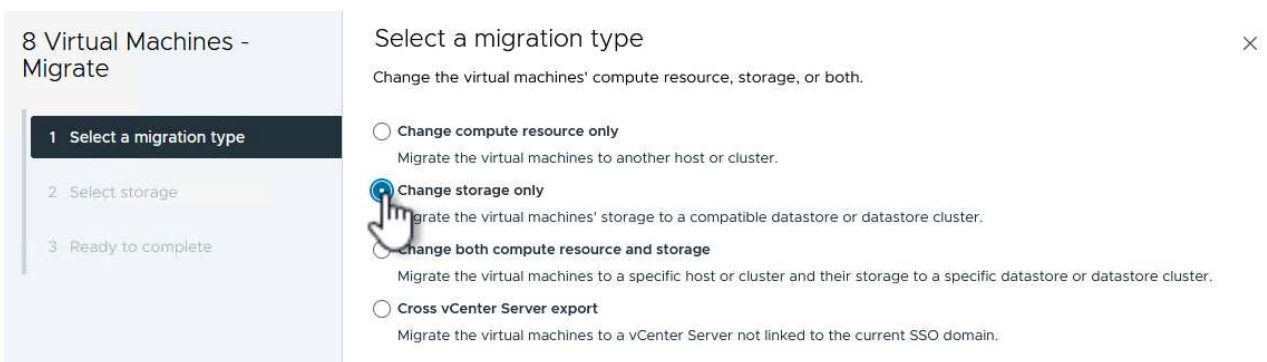
In Fällen, in denen es bevorzugt wird, ONTAP Storage zum Schutz der VCF Management-VM zu verwenden, kann vMotion zur Migration der VMs zum neu erstellten iSCSI-Datenspeicher verwendet werden.

Führen Sie die folgenden Schritte aus, um die VCF-Management-VMs auf den iSCSI-Datenspeicher zu migrieren.

1. Navigieren Sie vom vSphere Client zum Management Domain Cluster und klicken Sie auf die Registerkarte **VMs**.
2. Wählen Sie die VMs aus, die zum iSCSI-Datenspeicher migriert werden sollen, klicken Sie mit der rechten Maustaste und wählen Sie **Migrate..** aus.



3. Wählen Sie im Assistenten **Virtual Machines - Migrate** als Migrationstyp **nur Speicher ändern** aus und klicken Sie auf **Weiter**, um fortzufahren.



4. Wählen Sie auf der Seite **Select Storage** den iSCSI-Datastore aus und wählen Sie **Next**, um fortzufahren.

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free
mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB
vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB

Manage Columns Items per page 10 2 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

- Überprüfen Sie die Auswahl und klicken Sie auf **Fertig stellen**, um die Migration zu starten.
- Der Status der Verlagerung kann im Bereich **Letzte Aufgaben** angezeigt werden.

Task Name	Target	Status	Details
Relocate virtual machine	vcf-w01-nsx03	38%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-wkld-vc01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-otv9	36%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-nsx01a	49%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx02	47%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-sddcm01	39%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-w01-nsx01	42%	Migrating Virtual Machine active state
Relocate virtual machine	vcf-m01-vc01	44%	Migrating Virtual Machine active state

Weitere Informationen

Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

Video-Demo für diese Lösung

[iSCSI-Datenspeicher als ergänzender Speicher für VCF-Management-Domänen](#)

Konfigurieren Sie zusätzlichen Storage (VVols) für VCF-Workload-Domänen mit den ONTAP-Tools

In diesem Szenario zeigen wir, wie Sie ONTAP Tools für VMware vSphere implementieren und verwenden, um einen **VVols-Datastore** für eine VCF-Workload-Domain zu konfigurieren.

iSCSI wird als Storage-Protokoll für den VVols Datastore verwendet.

Autor: Josh Powell

Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

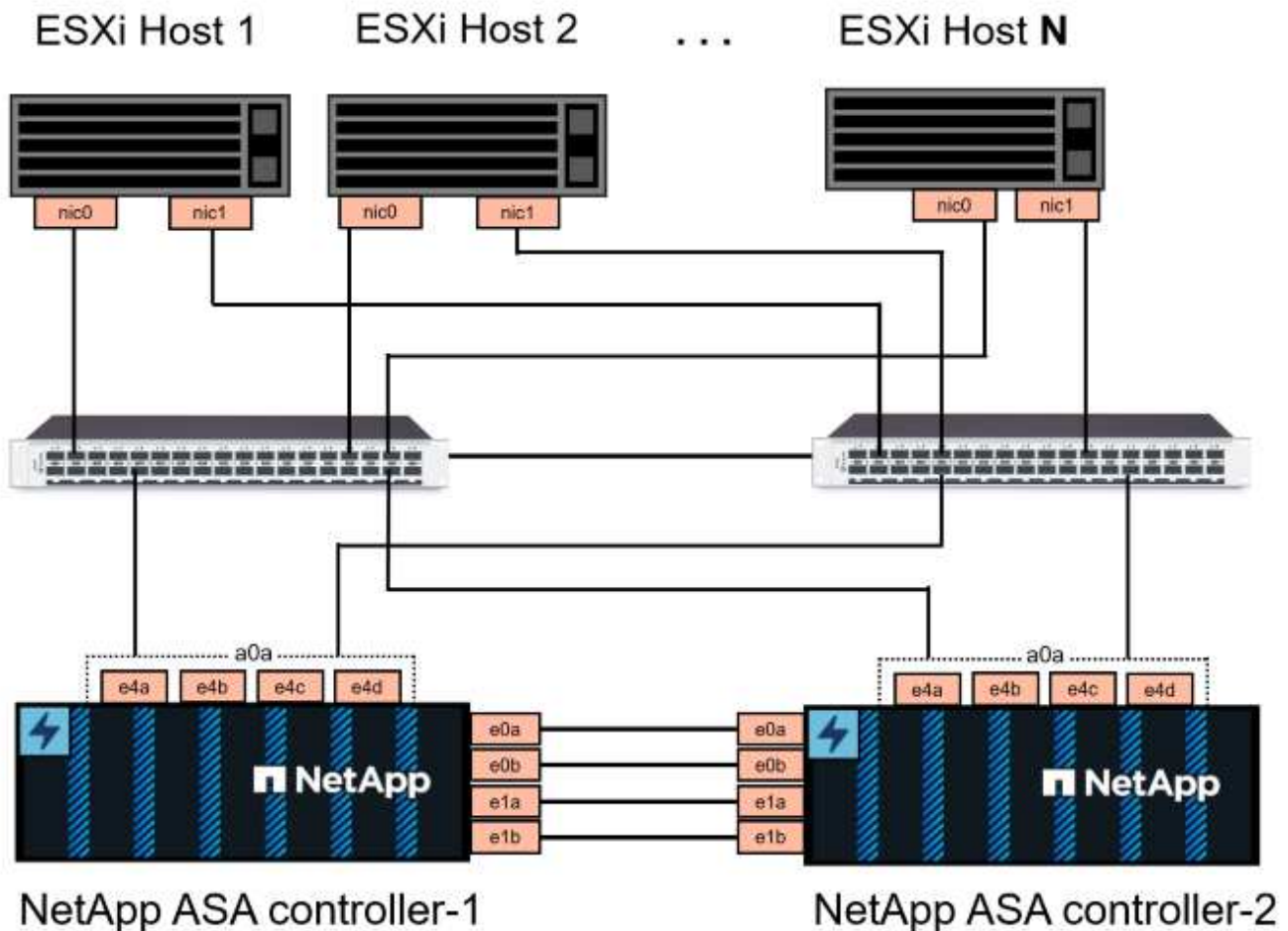
- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workload-Domäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workload-Domäne.
- Implementieren Sie ONTAP Tools in der VI-Workload-Domäne.
- Erstellen Sie einen neuen VVols-Datastore auf der VI-Workload-Domäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.

NetApp empfiehlt für iSCSI vollständig redundante Netzwerkdesigns. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration für Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Weitere Informationen finden Sie im NetApp ["Referenz zur SAN-Konfiguration"](#) Finden Sie weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten ethernet-Netzwerken.

In dieser Dokumentation wird der Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adressinformationen für die Erstellung mehrerer LIFs für iSCSI-Datenverkehr demonstriert. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter ["LIF erstellen \(Netzwerkschnittstelle\)"](#).



In Situationen, in denen mehrere VMkernel-Adapter auf demselben IP-Netzwerk konfiguriert sind, wird empfohlen, die iSCSI-Port-Bindung für die ESXi-Hosts zu verwenden, um sicherzustellen, dass der Lastausgleich über die Adapter hinweg erfolgt. Siehe KB-Artikel ["Überlegungen zur Verwendung der Software-iSCSI-Portbindung in ESX/ESXi \(2038869\)"](#).

Weitere Informationen zur Verwendung von VMFS iSCSI-Datstores mit VMware finden Sie unter ["VSphere VMFS Datenspeicher – iSCSI-Storage-Back-End mit ONTAP"](#).

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools zu implementieren und damit einen VVols Datastore auf der VCF-Managementdomäne zu erstellen:

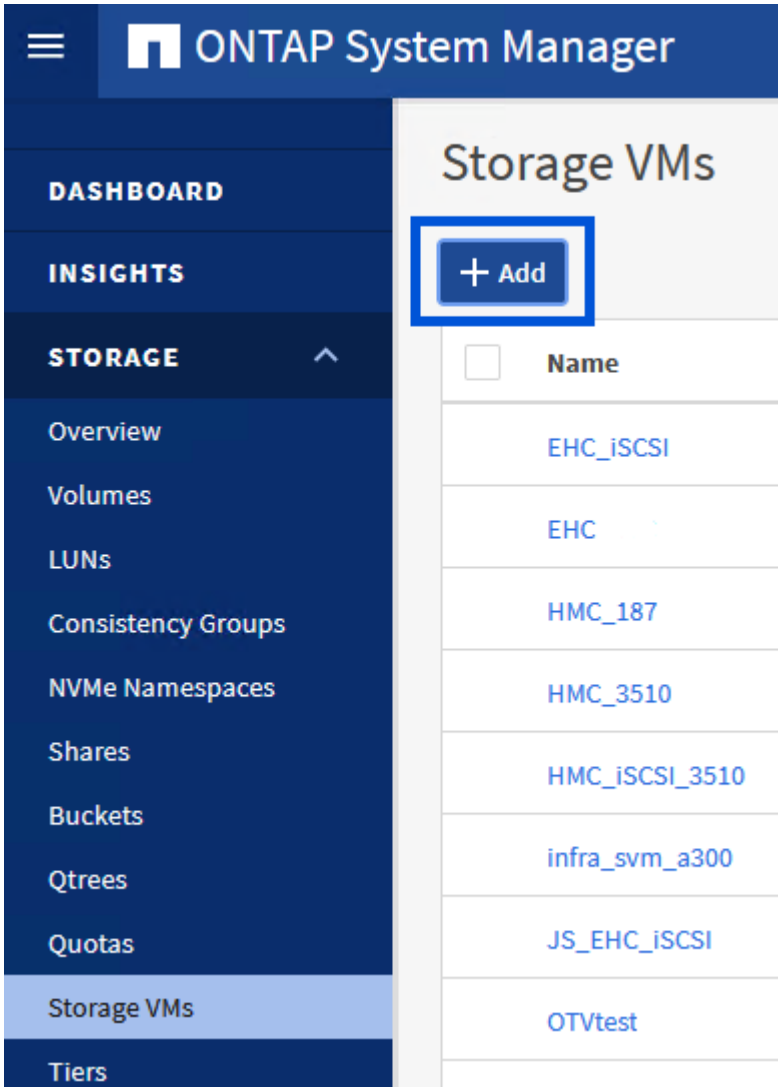
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

Storage-VM und LIFs erstellen

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für iSCSI-Datenverkehr zu erstellen.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf **+ Hinzufügen**, um zu starten.



2. Im **Add Storage VM** Wizard geben Sie einen **Namen** für die SVM an, wählen Sie den **IP Space** aus und klicken Sie dann unter **Access Protocol** auf die Registerkarte **iSCSI** und aktivieren Sie das Kontrollkästchen **enable iSCSI**.

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable iSCSI

3. Geben Sie im Abschnitt **Network Interface** die **IP-Adresse**, **Subnetzmaske** und **Broadcast Domain und Port** für die erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert sein, um allgemeine Einstellungen für alle verbleibenden LIFs zu verwenden oder separate Einstellungen zu verwenden.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten Ethernet-Netzwerken.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.179

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374

IP ADDRESS

172.21.119.180

PORT

a0a-3375

4. Wählen Sie aus, ob das Storage VM Administration-Konto aktiviert werden soll (für mandantenfähige Umgebungen), und klicken Sie auf **Speichern**, um die SVM zu erstellen.

Storage VM Administration

Manage administrator account

Save

Cancel

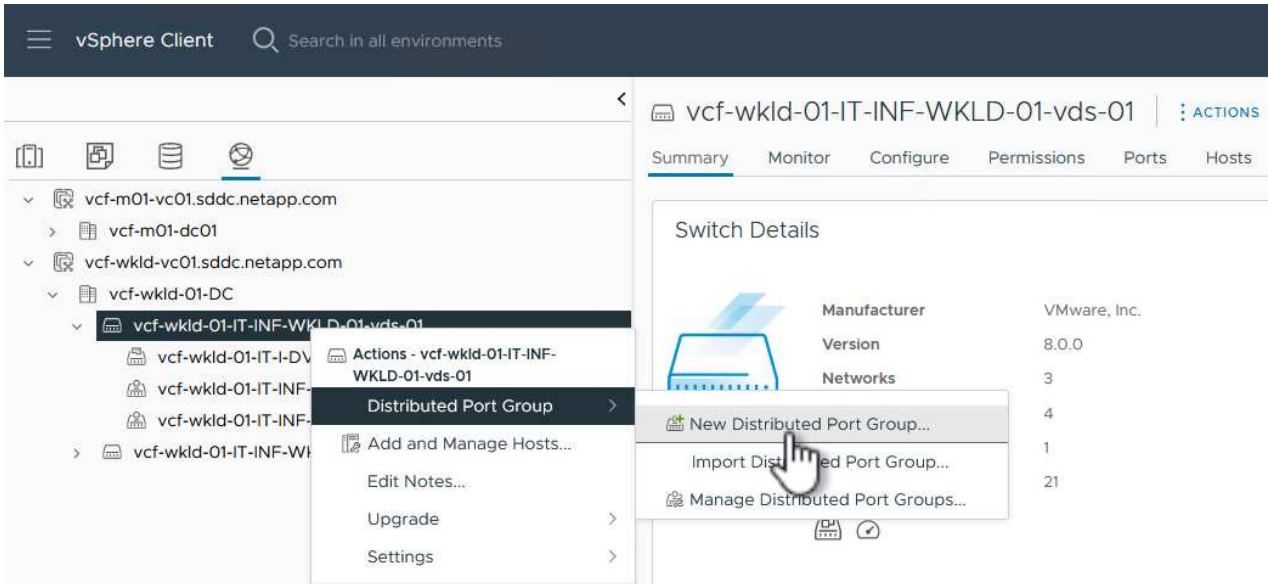
Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein

Die folgenden Schritte werden für den VI Workload Domain Cluster mithilfe des vSphere Clients durchgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client in der Management- und Workload-Domäne einheitlich ist.

Erstellen Sie verteilte Portgruppen für iSCSI-Datenverkehr

Gehen Sie wie folgt vor, um eine neue verteilte Portgruppe für jedes iSCSI-Netzwerk zu erstellen:

1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workload-Domäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen von **New Distributed Port Group...** aus.



2. Geben Sie im Assistenten **New Distributed Port Group** einen Namen für die neue Portgruppe ein und klicken Sie auf **Next**, um fortzufahren.
3. Füllen Sie auf der Seite **Configure settings** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige VLAN-ID angeben. Klicken Sie auf **Weiter**, um fortzufahren.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding	Static binding
Port allocation	Elastic ⓘ
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen und sicherzustellen, dass Sie die richtige **VLAN-ID** eingegeben haben.
- Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.

The screenshot shows the vSphere Client interface. On the left, a tree view displays the environment structure, with the path **vcf-wkld-01-iscsi-a** selected. A context menu is open over this selection, showing options like **Actions - vcf-wkld-01-iscsi-a** and **Edit Settings...**. On the right, the **Distributed Port Group Details** panel is visible, showing the following configuration:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Network protocol profile	--

7. Navigieren Sie auf der Seite **Distributed Port Group - Edit Settings** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **unused Uplinks** zu verschieben.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-a ×

General	Load balancing	Route based on originating virtual por. ▾
Advanced	Network failure detection	Link status only ▾
VLAN	Notify switches	Yes ▾
Security	Failback	Yes ▾
Traffic shaping		
Teaming and failover		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL **OK**

8. Wiederholen Sie diesen Schritt für die zweite iSCSI-Portgruppe. Allerdings bewegt sich dieses Mal **Uplink1** zu **unbenutzten Uplinks**.

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General	Load balancing	Route based on originating virtual por. ▾
Advanced	Network failure detection	Link status only ▾
VLAN	Notify switches	Yes ▾
Security	Failback	Yes ▾
Traffic shaping		
Teaming and failover		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

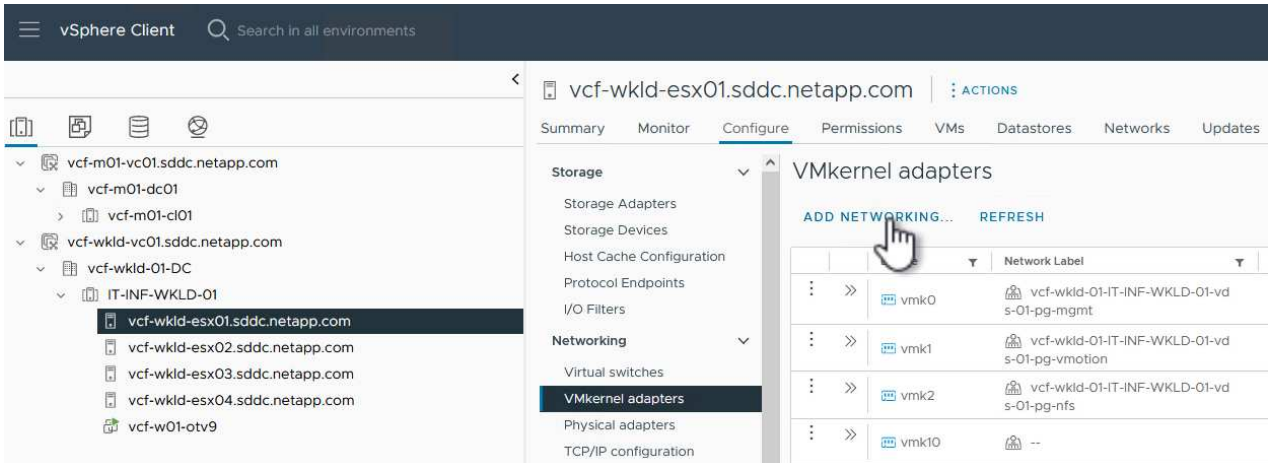
Unused uplinks

uplink1

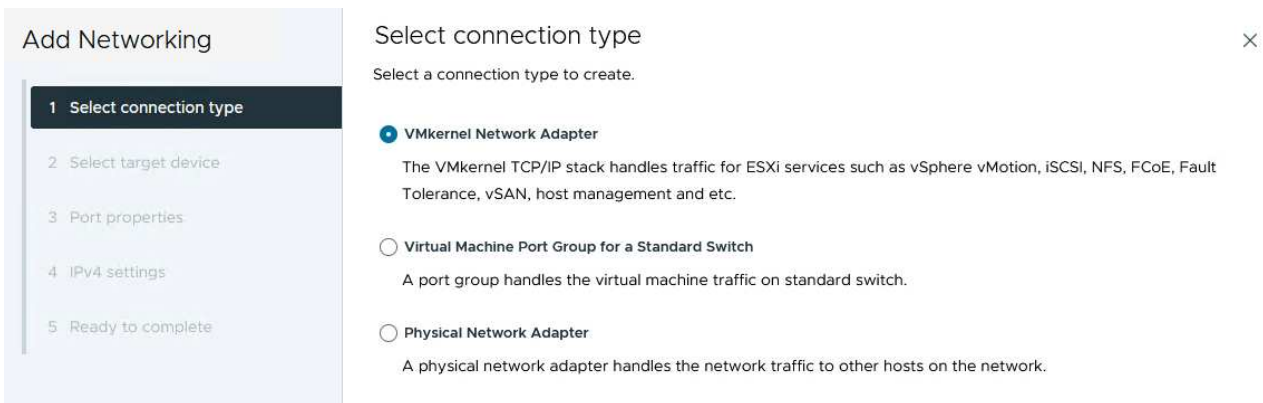
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

Wiederholen Sie diesen Vorgang auf jedem ESXi-Host in der Workload-Domäne.

1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts in der Workload-Domäneninventarisierung. Wählen Sie auf der Registerkarte **Configure VMkernel Adapter** und klicken Sie auf **Add Networking...**, um zu starten.



2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für iSCSI aus.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Select target device

Select a target device for the new connection.

Select an existing network
 Select an existing standard switch
 New standard switch

Quick Filter

	Name	NSX Port Group ID	Distributed Switch
<input checked="" type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

5 items

CANCEL BACK NEXT

4. Behalten Sie auf der Seite **Port Properties** die Standardeinstellungen bei und klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

vMotion

vSphere Replication NFC

NVMe over RDMA

Provisioning

vSAN

Fault Tolerance logging

vSAN Witness

Management

vSphere Backup NFC

vSphere Replication

NVMe over TCP

5. Geben Sie auf der Seite **IPv4 settings** die **IP-Adresse**, **Subnetzmaske** ein, und geben Sie eine neue Gateway-IP-Adresse ein (nur bei Bedarf). Klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically
 Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

6. Überprüfen Sie Ihre Auswahl auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um den VMkernel-Adapter zu erstellen.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

- ▼ **Select target device**

Distributed port group vcf-wkld-01-iscsi-a

Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
- ▼ **Port properties**

New port group vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ **IPv4 settings**

IPv4 address 172.21.118.127 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

7. Wiederholen Sie diesen Vorgang, um einen VMkernel Adapter für das zweite iSCSI-Netzwerk zu erstellen.

Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools

Die folgenden Schritte werden auf dem VCF-Management-Domänencluster mithilfe des vSphere-Clients durchgeführt. Dazu gehören die Implementierung von ONTAP-Tools, die Erstellung eines VVols-iSCSI-Datastore und die Migration von Management-VMs auf den neuen Datastore.

Für VI-Workload-Domänen wird ONTAP Tools im VCF-Managementcluster installiert, aber bei dem vCenter registriert, das der VI-Workload-Domäne zugeordnet ist.

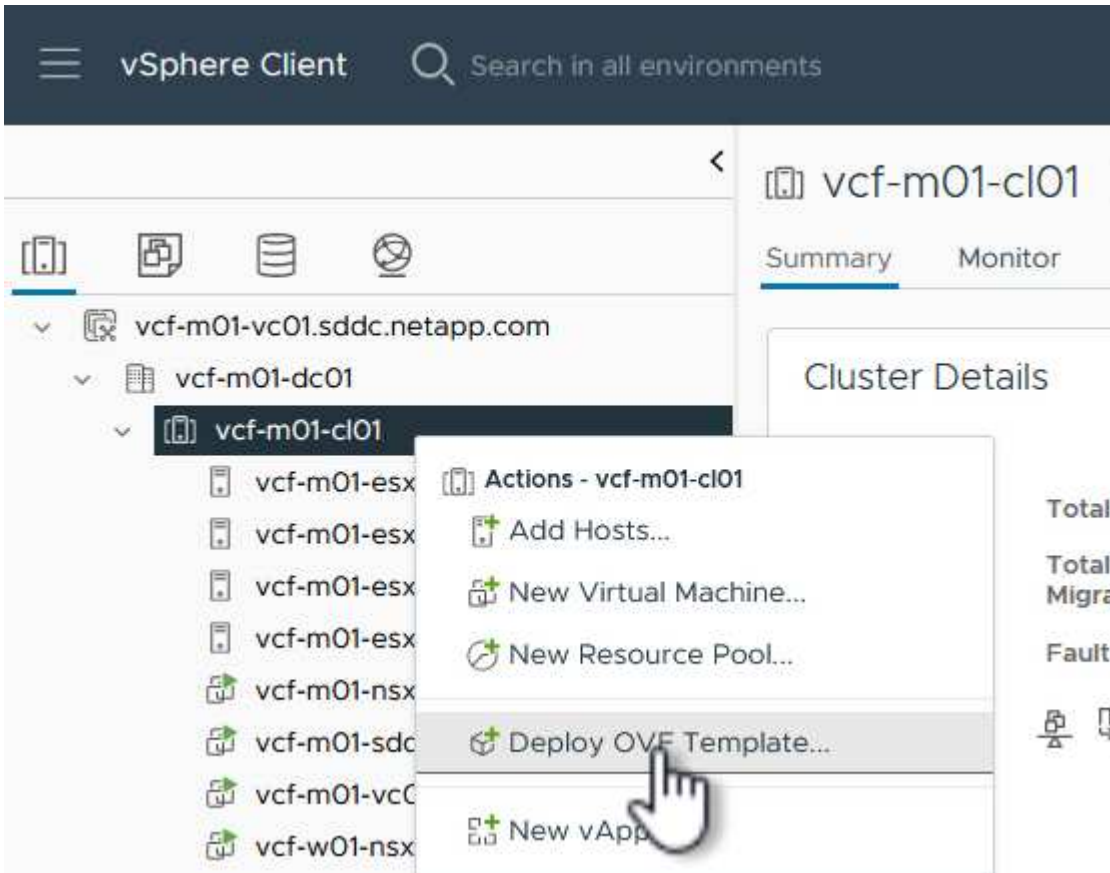
Weitere Informationen zum Implementieren und Verwenden von ONTAP Tools in einer Umgebung mit mehreren vCenter finden Sie unter ["Voraussetzungen für die Registrierung von ONTAP-Tools in einer Umgebung mit mehreren vCenter-Servern"](#).

Implementieren Sie ONTAP-Tools für VMware vSphere

ONTAP Tools für VMware vSphere werden als VM-Appliance implementiert und verfügen über eine integrierte vCenter UI zum Managen von ONTAP Storage.

Füllen Sie die folgenden Schritte aus, um ONTAP Tools für VMware vSphere zu implementieren:

1. Rufen Sie das OVA-Image der ONTAP-Tools auf "[NetApp Support Website](#)" Und in einen lokalen Ordner herunterladen.
2. Melden Sie sich bei der vCenter Appliance für die VCF-Managementdomäne an.
3. Klicken Sie in der vCenter-Appliance-Oberfläche mit der rechten Maustaste auf den Management-Cluster und wählen Sie **Deploy OVF Template...** aus



4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei für ONTAP-Tools aus.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vmware-9.13-9554.ova

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie für den Speicherort der Konfigurations- und Festplattendateien den vSAN Datastore des VCF Management Domain Clusters aus.

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

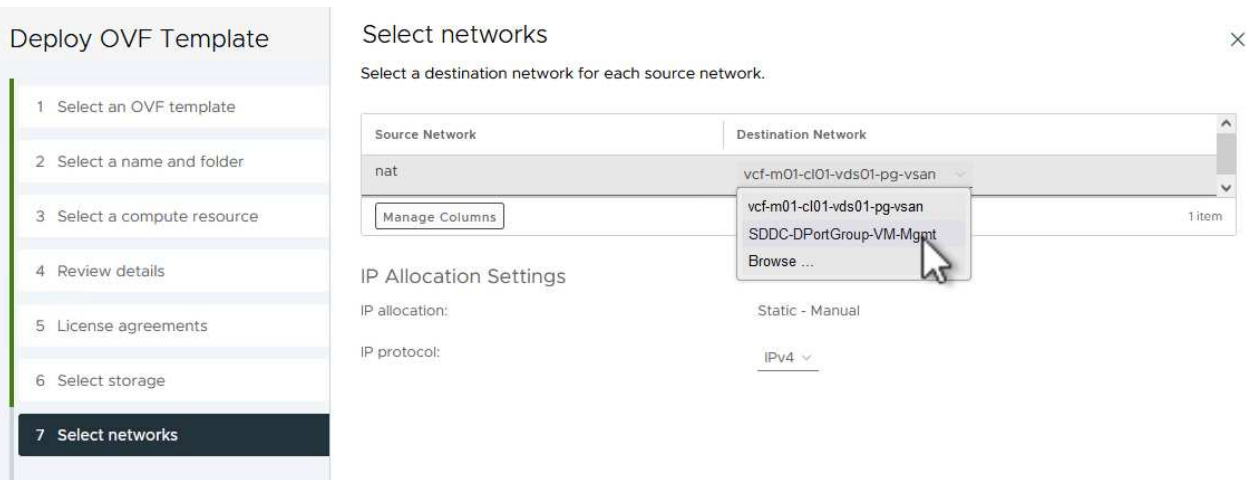
VM Storage Policy

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 5 items

7. Wählen Sie auf der Seite Netzwerk auswählen das Netzwerk aus, das für den Verwaltungsdatenverkehr verwendet wird.



8. Geben Sie auf der Seite Vorlage anpassen alle erforderlichen Informationen ein:

- Kennwort für administrativen Zugriff auf ONTAP-Tools.
- NTP-Server-IP-Adresse.
- Kennwort für das Wartungskonto von ONTAP Tools.
- ONTAP Tools Derby DB Passwort.
- Aktivieren Sie nicht das Kontrollkästchen, um VMware Cloud Foundation (VCF)* zu aktivieren. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
- FQDN oder IP-Adresse der vCenter-Appliance für die **VI Workload Domain**
- Zugangsdaten für die vCenter-Appliance der **VI Workload Domain**
- Geben Sie die erforderlichen Felder für Netzwerkeigenschaften an.

Klicken Sie auf **Weiter**, um fortzufahren.

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

Customize template

Customize the deployment properties of this software solution.

❗ 2 properties have invalid values ✕

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. 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.	
	Password 👁
	Confirm Password 👁
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1	
Maintenance User Password (*)	Password to assign to maint user account.	
	Password 👁
	Confirm Password 👁

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

Customize template

❗ 2 properties have invalid values ✕

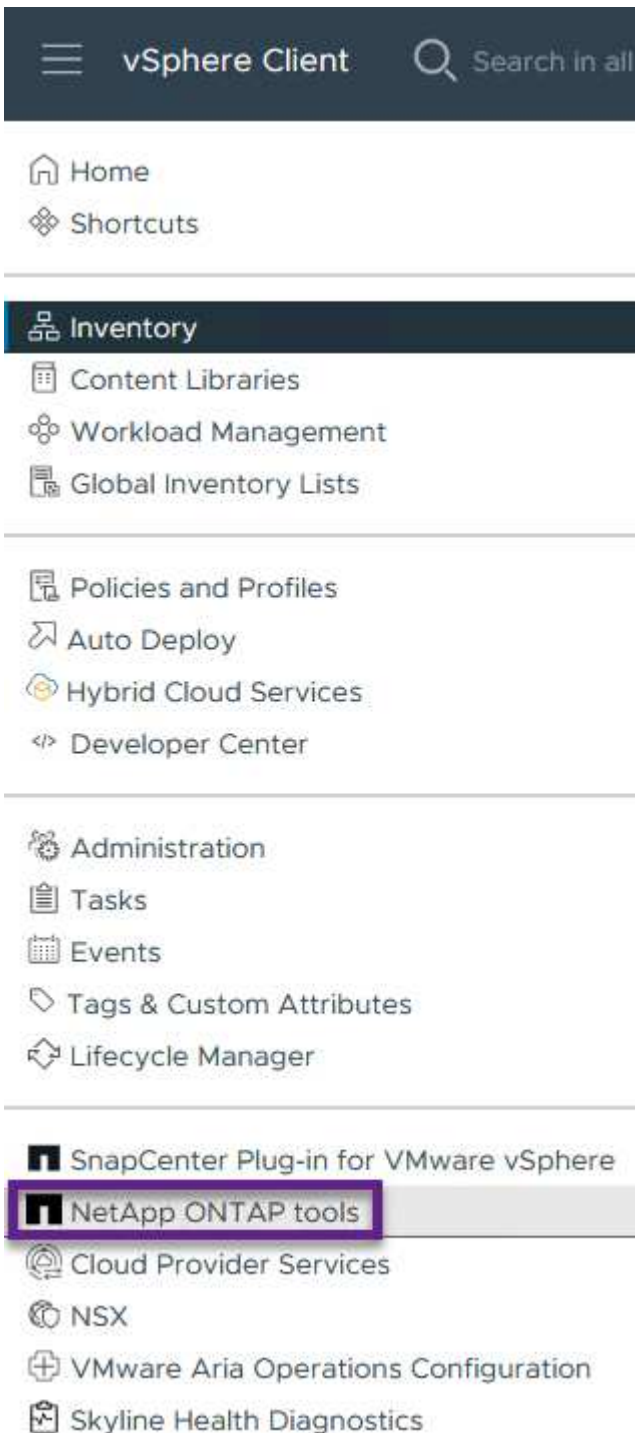
Configure vCenter or Enable VCF		3 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
Port (*)	Specify the HTTPS port of an existing vCenter to register to. 443	
Username (*)	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password 👁
	Confirm Password 👁
Network Properties		8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL BACK NEXT

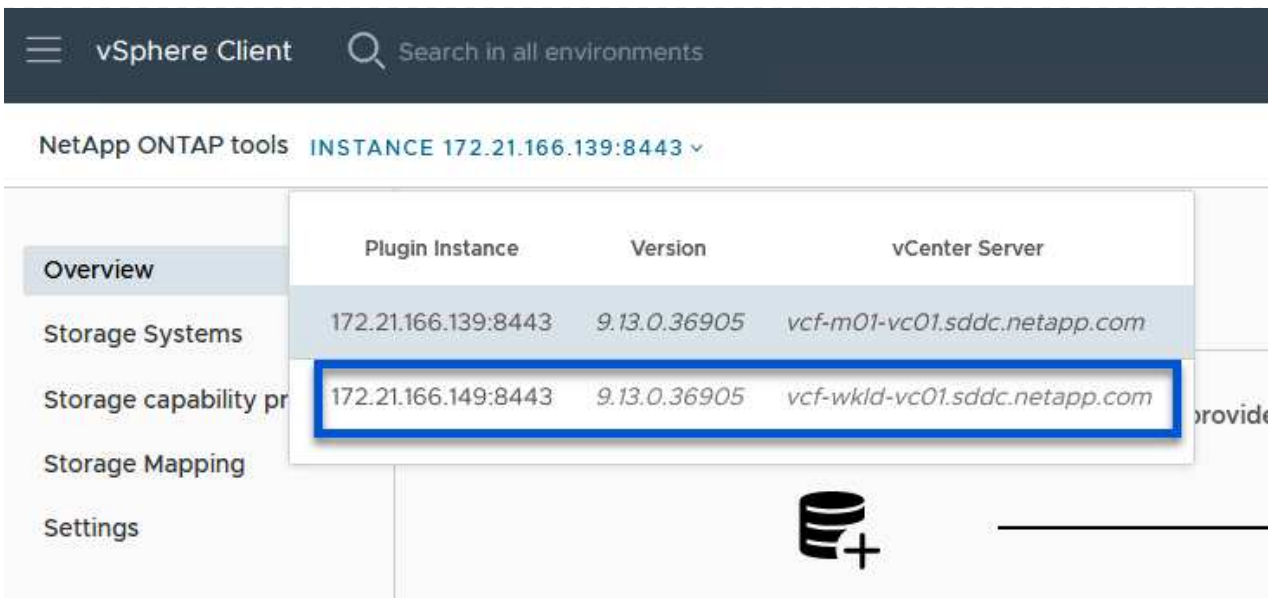
9. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der ONTAP-Tools-Appliance zu beginnen.

Fügen Sie ONTAP Tools ein Storage-System hinzu.

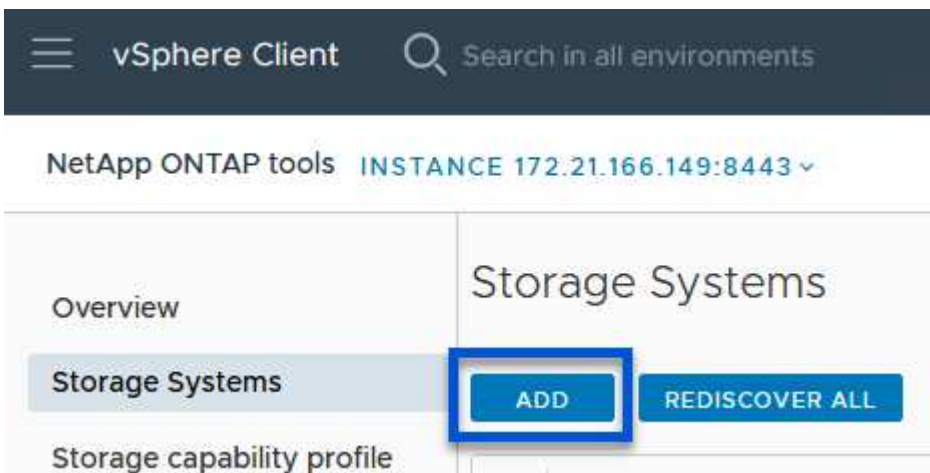
1. Greifen Sie auf die NetApp ONTAP-Tools zu, indem Sie sie im Hauptmenü des vSphere-Clients auswählen.



2. Wählen Sie aus dem Dropdown-Menü **INSTANCE** in der Benutzeroberfläche des ONTAP-Tools die Instanz des ONTAP-Tools aus, die der zu verwaltenden Workload-Domain zugeordnet ist.



3. Wählen Sie in den ONTAP-Tools im linken Menü **Speichersysteme** aus, und drücken Sie dann **Hinzufügen**.





4. Geben Sie die IP-Adresse, die Anmeldeinformationen des Speichersystems und die Portnummer ein. Klicken Sie auf **Add**, um den Ermittlungsvorgang zu starten.



VVol erfordert ONTAP-Cluster-Anmeldeinformationen statt der SVM-Anmeldeinformationen. Weitere Informationen finden Sie unter "[Storage-Systeme hinzufügen](#)" In der Dokumentation zu ONTAP Tools.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.

vCenter server vcf-m01-vc01.sddc.netapp.com 

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options 

ONTAP Cluster Certificate: Automatically fetch Manually upload

CANCEL

SAVE & ADD MORE

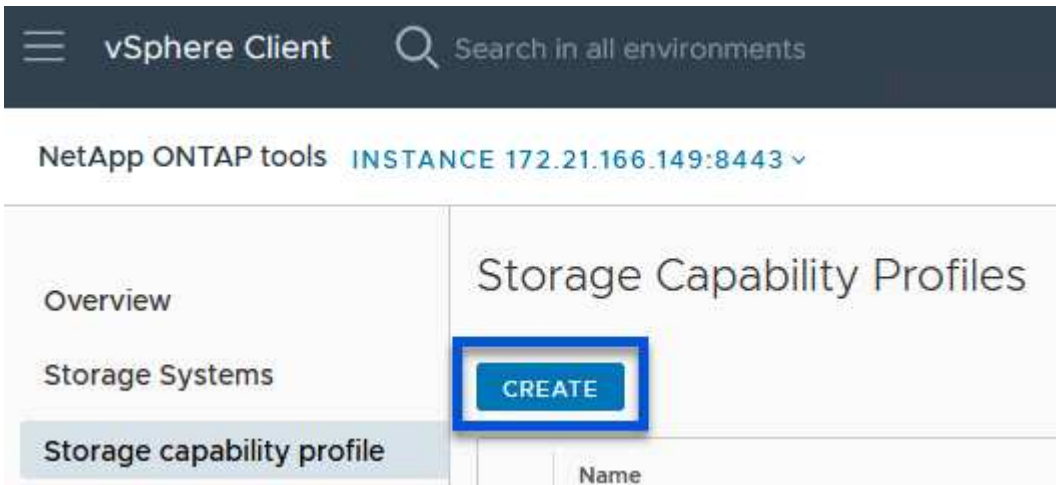
ADD

Erstellen Sie in ONTAP-Tools ein Storage-Funktionsprofil

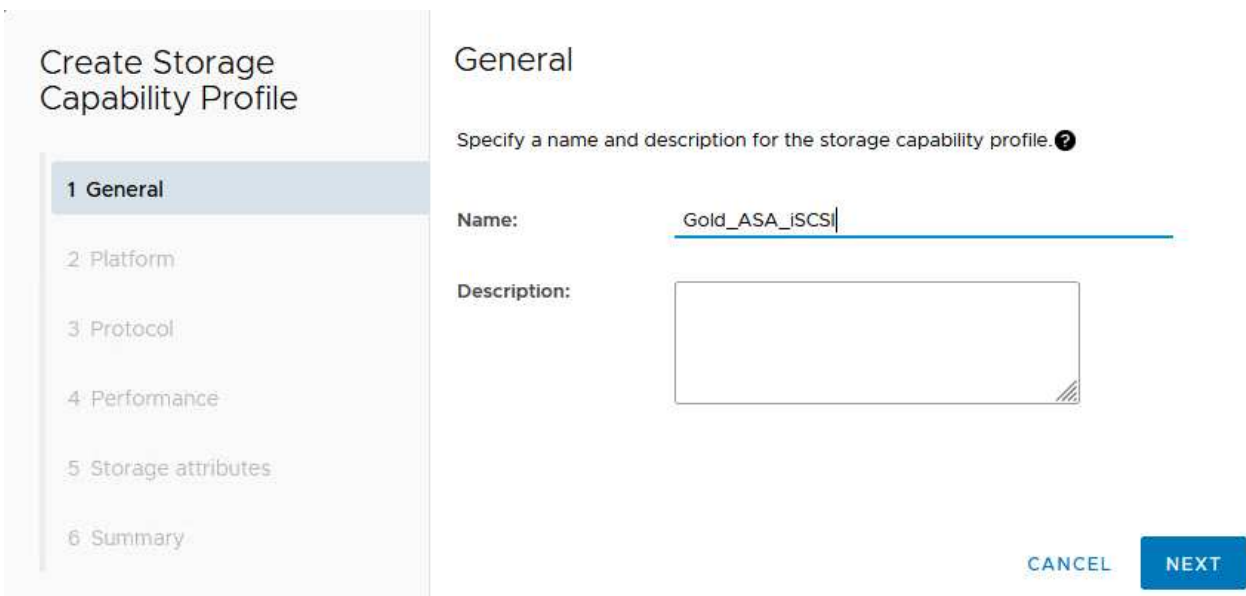
Storage-Funktionsprofile beschreiben die Funktionen eines Storage-Arrays oder Storage-Systems. Sie umfassen Definitionen zur Servicequalität und werden zur Auswahl von Storage-Systemen verwendet, die die im Profil definierten Parameter erfüllen. Eines der zur Verfügung gestellten Profile kann verwendet oder neue erstellt werden.

Führen Sie die folgenden Schritte aus, um ein Storage-Funktionsprofil in ONTAP Tools zu erstellen:

1. Wählen Sie in den ONTAP-Tools im linken Menü **Speicherfähigkeitsprofil** aus und drücken Sie dann **Erstellen**.



2. Geben Sie im Assistenten **Create Storage Capability Profile** einen Namen und eine Beschreibung des Profils ein und klicken Sie auf **Weiter**.



3. Wählen Sie den Plattfortmtyp aus und geben Sie an, dass das Speichersystem ein All-Flash-SAN-Array sein soll. Setzen Sie **Asymmetric** auf FALSE.

Create Storage Capability Profile

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

Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

4. Wählen Sie als nächstes das gewünschte Protokoll oder **any** aus, um alle möglichen Protokolle zuzulassen. Klicken Sie auf **Weiter**, um fortzufahren.

Create Storage Capability Profile

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

Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

5. Die Seite **Performance** ermöglicht die Einstellung der Servicequalität in Form von erlaubten Mindest- und Höchstwerten.

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

6. Füllen Sie die Seite **Storage-Attribute** aus und wählen Sie nach Bedarf Storage-Effizienz, Speicherplatzreservierung, Verschlüsselung und beliebige Tiering-Richtlinien aus.

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:

No



Tiering policy (FabricPool):

None



CANCEL

BACK

NEXT

7. Überprüfen Sie abschließend die Zusammenfassung, und klicken Sie auf Fertig stellen, um das Profil zu erstellen.

Create Storage Capability Profile

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

Summary

Name:	ASA_Gold_iSCSI
Description:	N/A
Platform:	Performance
Asymmetric:	No
Protocol:	Any
Max IOPS:	6000 IOPS
Space reserve:	Thin
Deduplication:	Yes
Compression:	Yes
Encryption:	Yes
Tiering policy (FabricPool):	None

CANCEL

BACK

FINISH



Erstellen Sie einen VVols-Datstore in ONTAP Tools

Führen Sie die folgenden Schritte aus, um einen VVols-Datstore in ONTAP Tools zu erstellen:

1. Wählen Sie in den ONTAP-Tools **Übersicht** und klicken Sie im Register **erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.

The screenshot shows the vSphere Client interface. At the top, there's a search bar and the instance name 'NetApp ONTAP tools INSTANCE 172.21.166.149:8443'. The left sidebar has a menu with 'Overview' selected. The main area shows 'ONTAP tools for VMware vSphere' with tabs for 'Getting Started', 'Traditional Dashboard', and 'vVols Dashboard'. Below the tabs, there's a diagram with two main steps: 'Add Storage System' and 'Provision Datstore'. The 'Provision' button is highlighted with a blue box.

2. Wählen Sie auf der Seite **Allgemein** des Assistenten für neue Datenspeicher das vSphere Datacenter- oder Cluster-Ziel aus. Wählen Sie als Datstore-Typ **VVols** aus, geben Sie einen Namen für den Datstore ein und wählen Sie als Protokoll **iSCSI** aus. Klicken Sie auf **Weiter**, um fortzufahren.

The screenshot shows the 'New Datastore' wizard. The 'General' tab is selected. The 'Provisioning destination' is 'IT-INF-WKLD-01'. The 'Type' is 'vVols'. The 'Name' is 'VCF_WKLD_02_VVOLS'. The 'Protocol' is 'iSCSI'. The 'Description' field is empty. 'CANCEL' and 'NEXT' buttons are at the bottom right.

3. Wählen Sie auf der Seite **Storage System** das Speicherfähigkeitsprofil, das Speichersystem und die SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profiles:

- AFF_Encrypted_Min50_ASA_A
- FAS_Default
- FAS_Max20
- Custom profiles
- ASA_Gold_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_iSCSI

CANCEL BACK NEXT

4. Wählen Sie auf der Seite **Speicherattribute** aus, um ein neues Volume für den Datenspeicher zu erstellen und die Speicherattribute des zu erstellenden Volumes auszufüllen. Klicken Sie auf **Add**, um das Volume zu erstellen, und dann auf **Next**, um fortzufahren.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
 FlexVol volumes are not added.			

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCaggr02 - (27053.3 GE	Thin

CANCEL ADD BACK NEXT

5. Überprüfen Sie abschließend die Zusammenfassung und klicken Sie auf **Finish**, um den vVol Datastore-Erstellungsprozess zu starten.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

Datastore type: vVols
Protocol: iSCSI
Storage capability profile: ASA_Gold_iSCSI

Storage system details
Storage system: ntaphci-a300e9u25
SVM: VCF_iSCSI

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCAggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

CANCEL BACK FINISH

Weitere Informationen

Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

Konfigurieren Sie zusätzlichen NVMe/TCP-Storage für VCF-Workload-Domänen

In diesem Szenario zeigen wir, wie zusätzlicher NVMe/TCP Storage für eine VCF-Workload-Domäne konfiguriert wird.

Autor: Josh Powell

Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

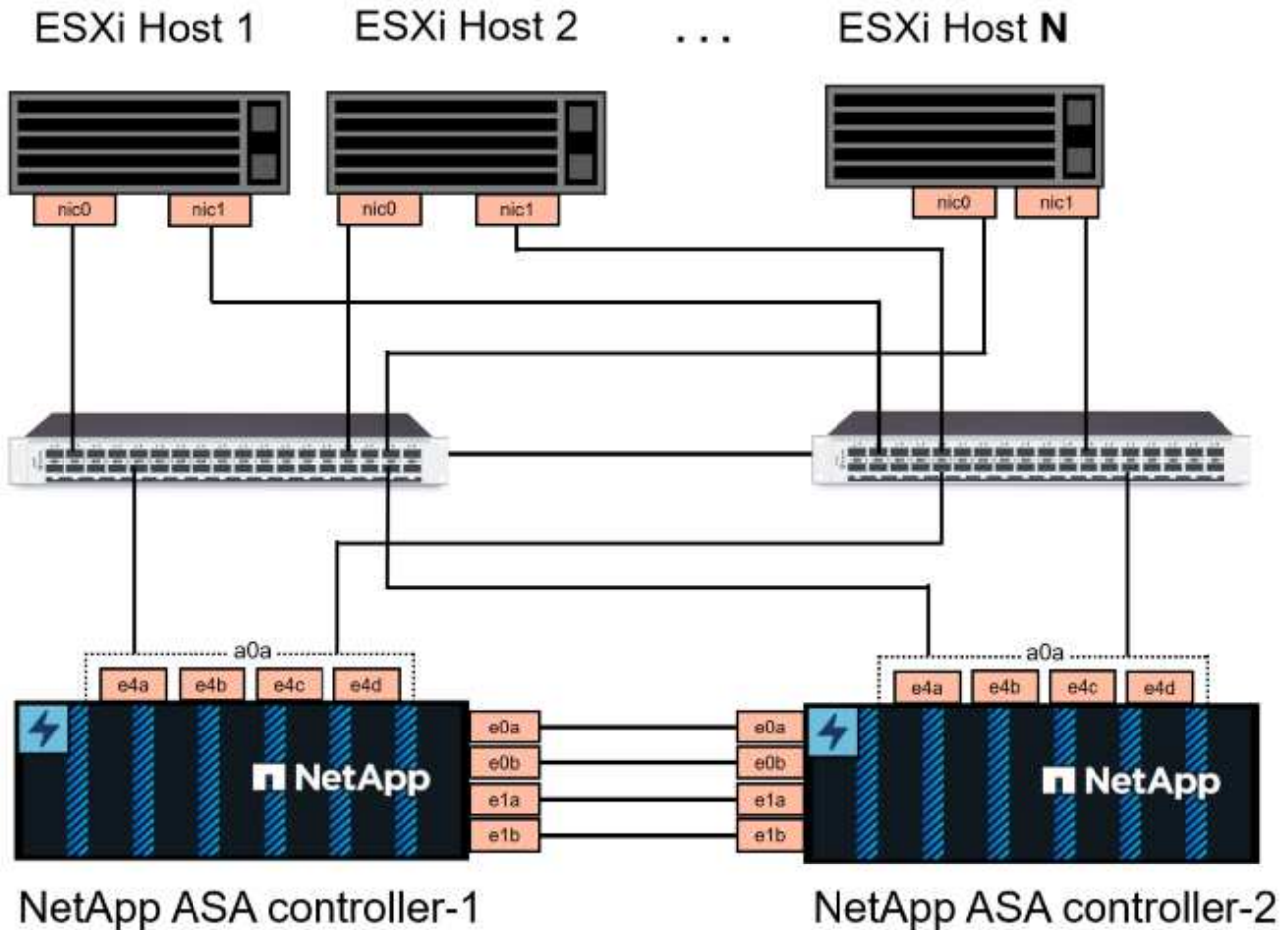
- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für NVMe/TCP-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workload-Domäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workload-Domäne.
- Fügen Sie NVMe/TCP-Adapter auf ESXi-Hosts hinzu.
- Implementieren von NVMe/TCP-Datastore

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.

NetApp empfiehlt vollständig redundante Netzwerkdesigns für NVMe/TCP. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration für Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Weitere Informationen finden Sie im NetApp ["Referenz zur SAN-Konfiguration"](#) Finden Sie weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in NVMe/TCP-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten ethernet-Netzwerken.

Diese Dokumentation zeigt den Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adressinformationen für die Erstellung mehrerer LIFs für NVMe/TCP-Datenverkehr. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter ["LIF erstellen \(Netzwerkschnittstelle\)"](#).

Weitere Informationen zu Überlegungen zum NVMe-Design für ONTAP Storage-Systeme finden Sie unter ["Konfiguration, Support und Einschränkungen von NVMe"](#).

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um einen VMFS Datastore auf einer VCF-Workload-Domäne mithilfe von NVMe/TCP zu erstellen.

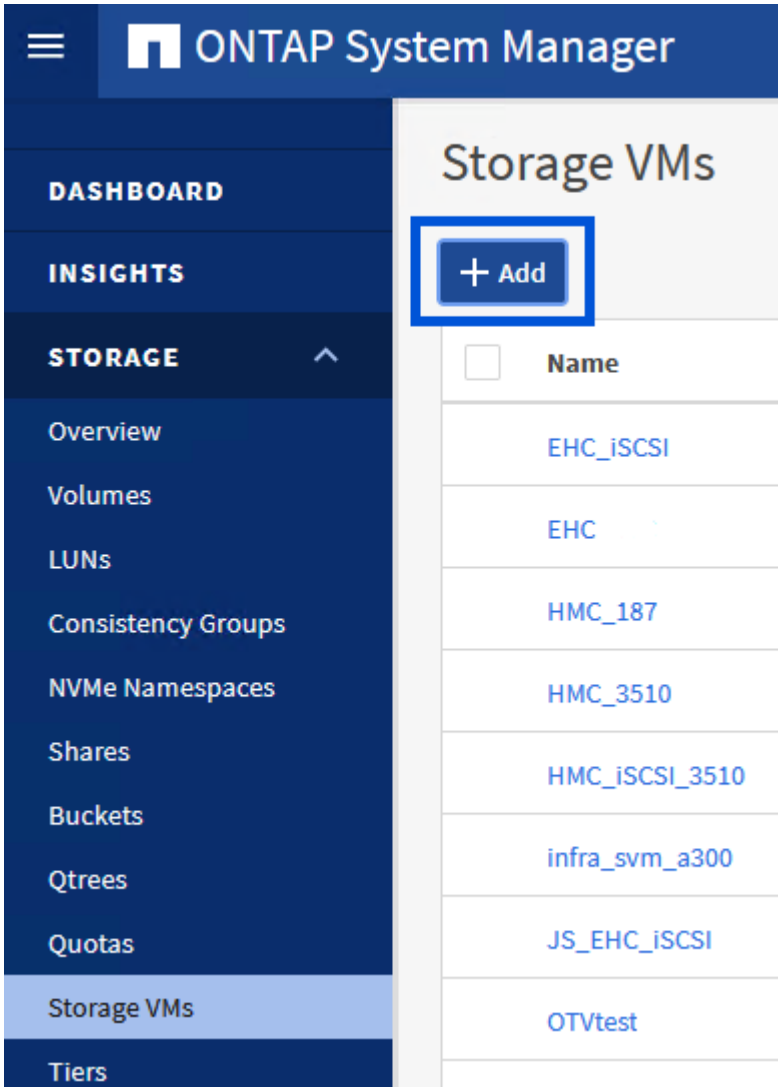
Erstellung von SVMs, LIFs und NVMe Namespace auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

Storage-VM und LIFs erstellen

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für NVMe/TCP-Datenverkehr zu erstellen.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf **+ Hinzufügen**, um zu starten.



2. Im **Add Storage VM** Wizard geben Sie einen **Namen** für die SVM an, wählen Sie den **IP Space** aus und klicken dann unter **Access Protocol** auf die Registerkarte **NVMe** und aktivieren Sie das Kontrollkästchen **enable NVMe/TCP**.

Add Storage VM



STORAGE VM NAME

VCF_NVMe

IPSPACE

Default

Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

Enable NVMe/FC

Enable NVMe/TCP

3. Geben Sie im Abschnitt **Network Interface** die **IP-Adresse**, **Subnetzmaske** und **Broadcast Domain und Port** für die erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert sein, um allgemeine Einstellungen für alle verbleibenden LIFs zu verwenden oder separate Einstellungen zu verwenden.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in NVMe/TCP-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten Ethernet-Netzwerken.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT 


NFS_iSCSI 

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

IP ADDRESS

172.21.119.189

PORT


a0a-3375 

ntaphci-a300-02

IP ADDRESS

172.21.118.190


PORT

a0a-3374 

IP ADDRESS

172.21.119.190

PORT

a0a-3375 

Storage VM Administration

Manage administrator account

Save

Cancel

4. Wählen Sie aus, ob das Storage VM Administration-Konto aktiviert werden soll (für mandantenfähige Umgebungen), und klicken Sie auf **Speichern**, um die SVM zu erstellen.

Storage VM Administration

Manage administrator account

Save

Cancel

Erstellen des NVMe-Namespaces

NVMe-Namespace entsprechen LUNs für iSCSI oder FC. Der NVMe-Namespace muss erstellt werden, bevor ein VMFS-Datstore aus dem vSphere Client heraus implementiert werden kann. Zum Erstellen des NVMe Namespace muss zunächst der NVMe Qualified Name (NQN) von jedem ESXi Host im Cluster abgerufen werden. ONTAP verwendet die NQN, um die Zugriffssteuerung für den Namespace bereitzustellen.

Führen Sie die folgenden Schritte aus, um einen NVMe-Namespace zu erstellen:

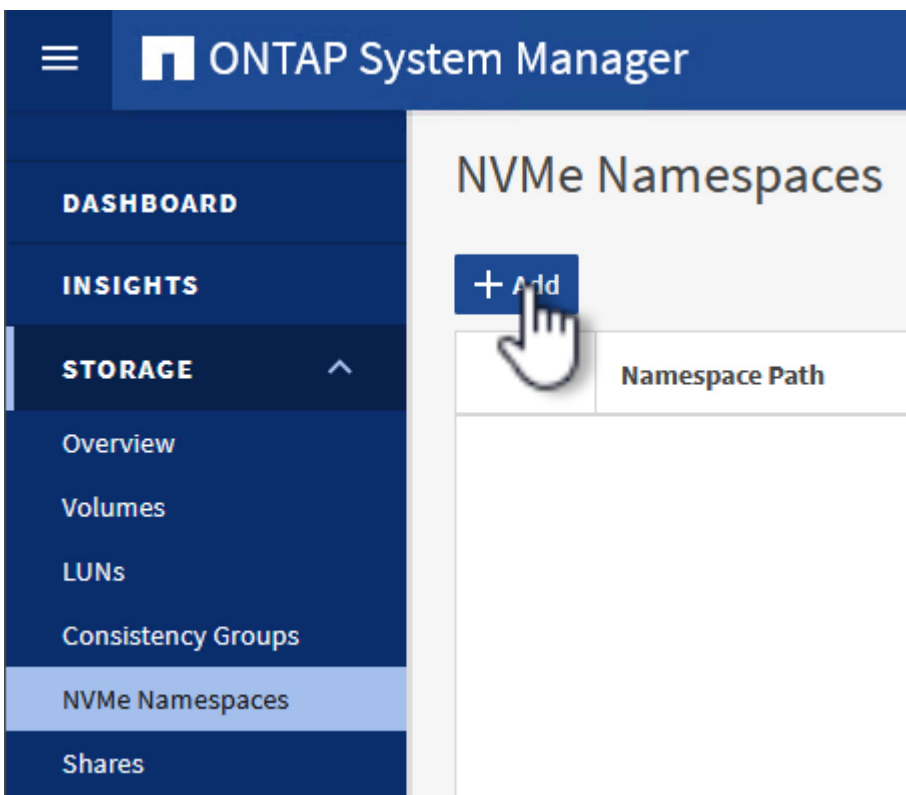
1. Öffnen Sie eine SSH-Sitzung mit einem ESXi-Host im Cluster, um dessen NQN zu erhalten. Verwenden Sie den folgenden Befehl aus der CLI:

```
esxcli nvme info get
```

Es sollte eine Ausgabe ähnlich der folgenden angezeigt werden:

```
Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
```

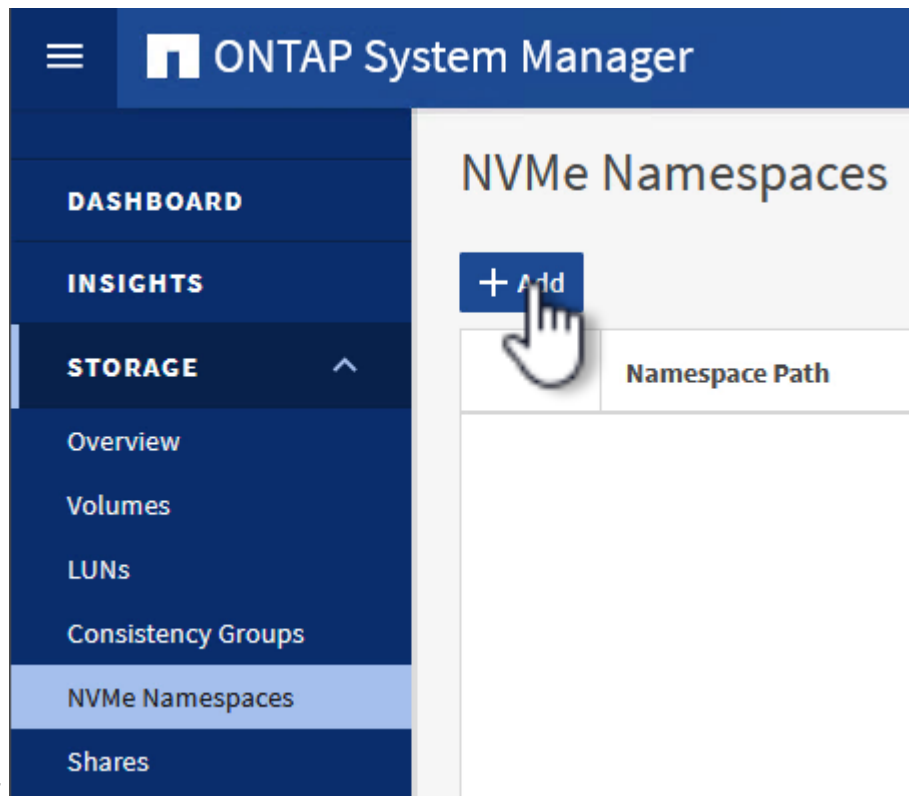
2. Notieren Sie die NQN für jeden ESXi-Host im Cluster
3. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **NVMe Namespaces** und klicken Sie auf **+ Hinzufügen**, um zu starten.



4. Geben Sie auf der Seite **Add NVMe Namespace** ein Namenspräfix, die Anzahl der zu erstellenden

Namespaces, die Größe des Namespace und das Host-Betriebssystem ein, das auf den Namespace zugreift. Erstellen Sie im Abschnitt **Host NQN** eine kommasetrennte Liste der NQN's, die zuvor von den ESXi-Hosts erfasst wurden, die auf die Namespaces zugreifen werden.

Klicken Sie auf **Weitere Optionen**, um zusätzliche Elemente wie die Snapshot-Schutzrichtlinie zu konfigurieren. Klicken Sie abschließend auf **Speichern**, um den NVMe-Namespaces zu erstellen.



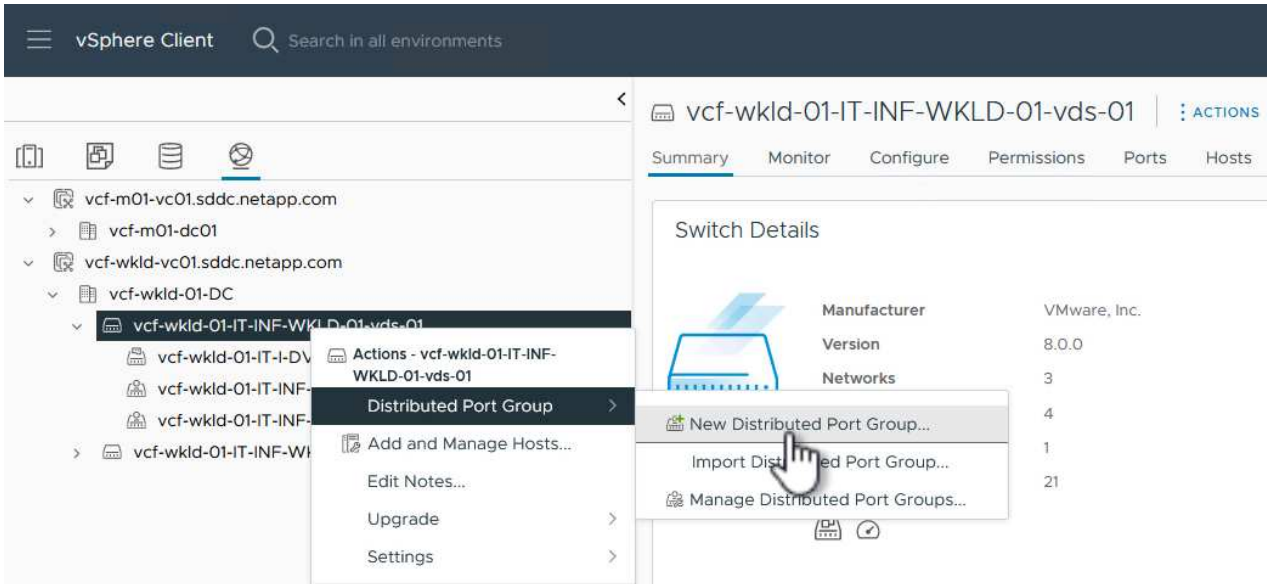
Richten Sie Netzwerk- und NVMe-Softwareadapter auf ESXi-Hosts ein

Folgende Schritte werden für den VI-Workload-Domänen-Cluster mithilfe des vSphere Clients durchgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client sowohl für die Management- als auch für die Workload-Domäne gemeinsam ist.

Verteilte Portgruppen für NVME/TCP-Datenverkehr erstellen

Führen Sie die folgenden Schritte aus, um eine neue verteilte Portgruppe für jedes NVMe/TCP-Netzwerk zu erstellen:

1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workload-Domäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen von **New Distributed Port Group...** aus.



2. Geben Sie im Assistenten **New Distributed Port Group** einen Namen für die neue Portgruppe ein und klicken Sie auf **Next**, um fortzufahren.
3. Füllen Sie auf der Seite **Configure settings** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige VLAN-ID angeben. Klicken Sie auf **Weiter**, um fortzufahren.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

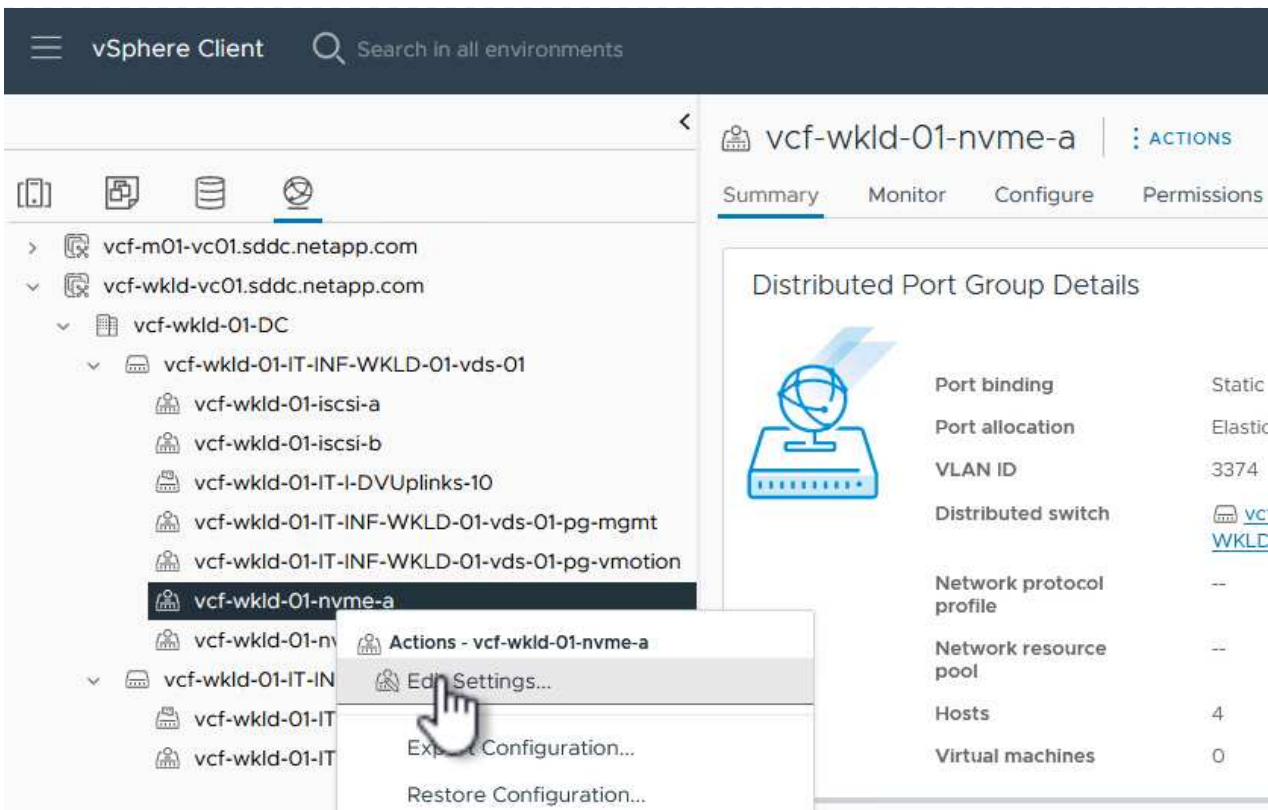
Port binding	Static binding
Port allocation	Elastic ?
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

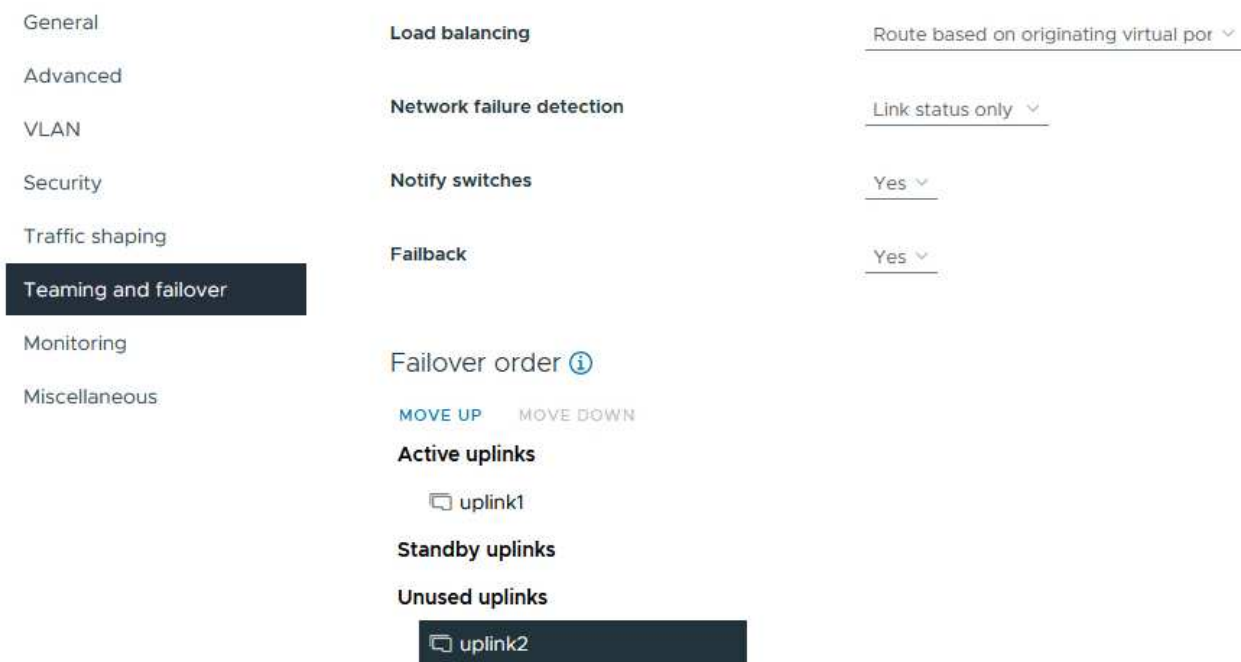
NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete NVMe/TCP-Netzwerk zu erstellen und sicherzustellen, dass Sie die korrekte **VLAN-ID** eingegeben haben.
- Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.



7. Navigieren Sie auf der Seite **Distributed Port Group - Edit Settings** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **unused Uplinks** zu verschieben.

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a



8. Wiederholen Sie diesen Schritt für die zweite NVMe/TCP-Portgruppe. Allerdings bewegt sich dieses

Mal Uplink1 zu unbenutzten Uplinks.

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and fallover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual por

Network failure detection

Link status only

Notify switches

Yes

Failback

Yes

Failover order ⓘ

[MOVE UP](#) [MOVE DOWN](#)

Active uplinks

uplink2

Standby uplinks

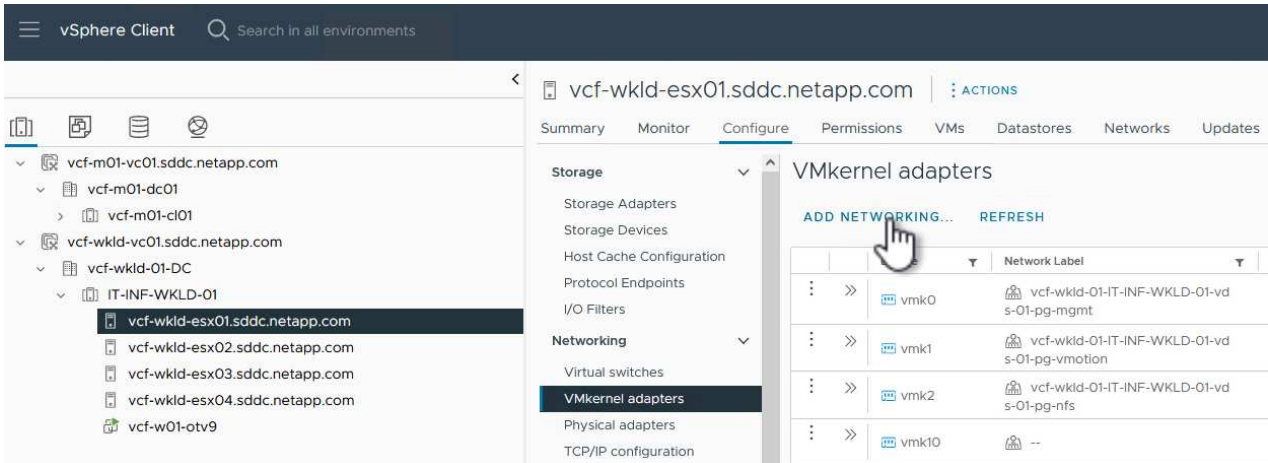
Unused uplinks

uplink1

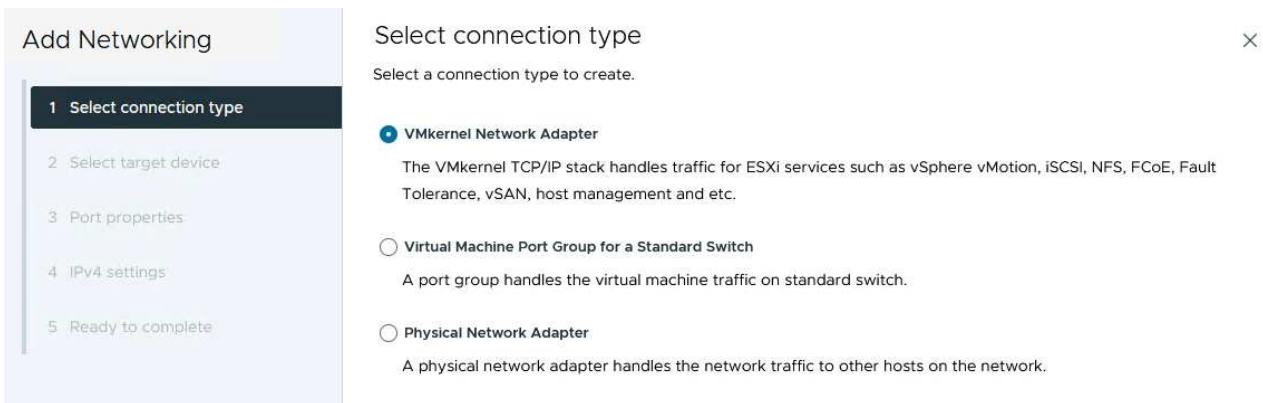
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

Wiederholen Sie diesen Vorgang auf jedem ESXi-Host in der Workload-Domäne.

1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts in der Workload-Domäneninventarisierung. Wählen Sie auf der Registerkarte **Configure VMkernel Adapter** und klicken Sie auf **Add Networking...**, um zu starten.



2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für iSCSI aus.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device








×

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	 vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	 vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	 vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	 vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 7 Items

CANCEL

BACK

NEXT

Packages

4. Klicken Sie auf der Seite **Port Properties** auf das Feld für **NVMe over TCP** und klicken Sie auf **Next**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

Enabled services

<input checked="" type="checkbox"/> vMotion	<input type="checkbox"/> vSphere Replication NFC	<input type="checkbox"/> NVMe over RDMA
<input type="checkbox"/> Provisioning	<input type="checkbox"/> vSAN	
<input type="checkbox"/> Fault Tolerance logging	<input type="checkbox"/> vSAN Witness	
<input type="checkbox"/> Management	<input type="checkbox"/> vSphere Backup NFC	
<input type="checkbox"/> vSphere Replication	<input checked="" type="checkbox"/> NVMe over TCP	

CANCEL BACK NEXT

5. Geben Sie auf der Seite **IPv4 settings** die **IP-Adresse**, **Subnetzmaske** ein, und geben Sie eine neue Gateway-IP-Adresse ein (nur bei Bedarf). Klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically

Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway Override default gateway for this adapter

DNS server addresses

6. Überprüfen Sie Ihre Auswahl auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um den VMkernel-Adapter zu erstellen.

Add Networking

- 1 Select connection type
- 2 Select target device
- 3 Port properties
- 4 IPv4 settings
- 5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ Port properties

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

▼ IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

CANCEL

BACK

FINISH

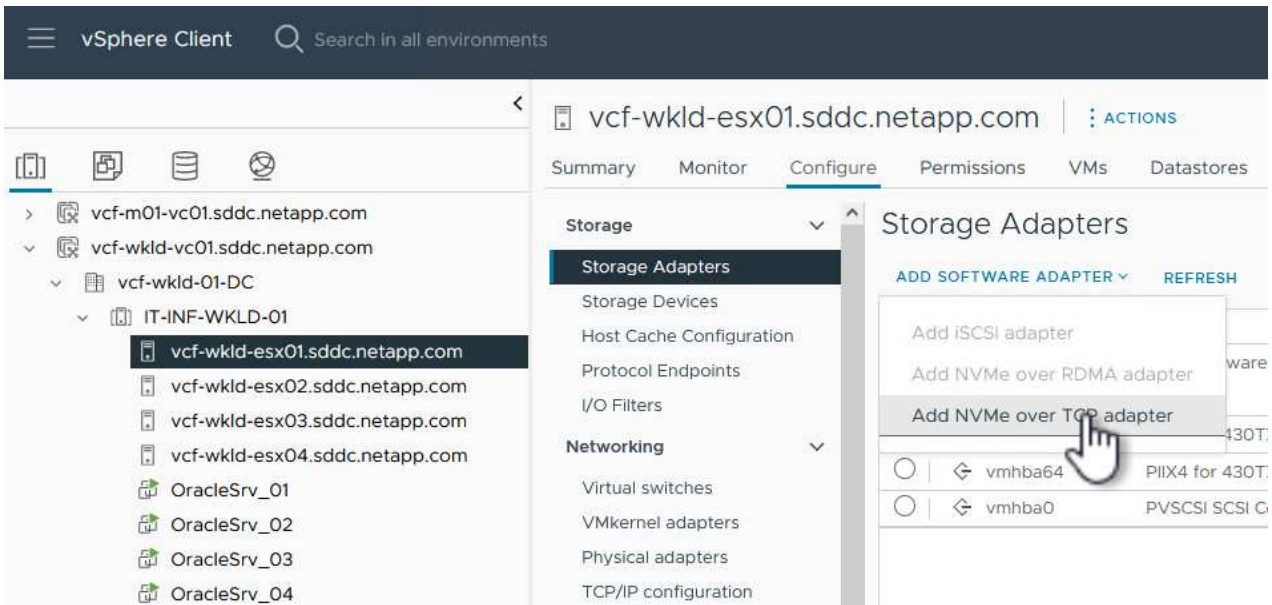
7. Wiederholen Sie diesen Vorgang, um einen VMkernel Adapter für das zweite iSCSI-Netzwerk zu erstellen.

Fügen Sie einen NVMe-over-TCP-Adapter hinzu

Für jedes etablierte NVMe/TCP-Netzwerk, das für Storage-Datenverkehr reserviert ist, muss auf jedem ESXi Host im Workload-Domänencluster ein NVMe-over-TCP-Softwareadapter installiert sein.

Führen Sie folgende Schritte aus, um NVMe over TCP-Adapter zu installieren und die NVMe-Controller zu ermitteln:

1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Klicken Sie auf der Registerkarte **Configure** im Menü auf **Speicheradapter** und wählen Sie dann aus dem Dropdown-Menü **Add Software Adapter Add NVMe over TCP Adapter**.



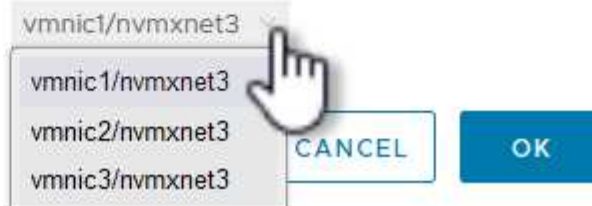
2. Öffnen Sie im Fenster **Add Software NVMe over TCP Adapter** das Dropdown-Menü **Physical Network Adapter** und wählen Sie den richtigen physischen Netzwerkadapter aus, auf dem der NVMe Adapter aktiviert werden soll.

Add Software NVMe over TCP adapter

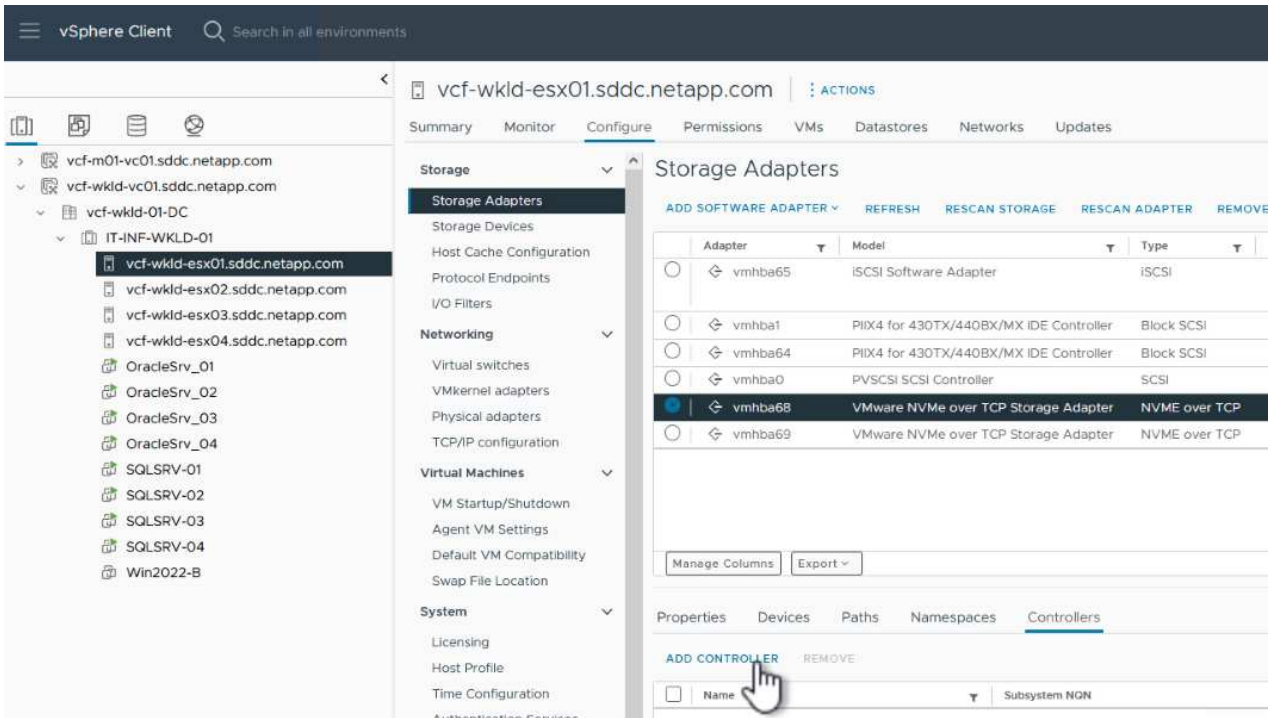
vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter



3. Wiederholen Sie diesen Vorgang für das zweite Netzwerk, das NVMe-over-TCP-Datenverkehr zugewiesen wurde, und weisen Sie den richtigen physischen Adapter zu.
4. Wählen Sie einen der neu installierten NVMe over TCP Adapter aus und wählen Sie auf der Registerkarte **Controller Controller** aus.



5. Wählen Sie im Fenster **Controller hinzufügen** die Registerkarte **automatisch** aus und führen Sie die folgenden Schritte aus.
 - Geben Sie für eine der logischen SVM-Schnittstellen im gleichen Netzwerk eine IP-Adresse ein, die dem physischen Adapter zugewiesen ist, der diesem NVMe over TCP-Adapter zugewiesen ist.
 - Klicken Sie auf die Schaltfläche **Controller entdecken**.
 - Aktivieren Sie in der Liste der erkannten Controller das Kontrollkästchen für die beiden Controller, deren Netzwerkadressen mit diesem NVMe-over-TCP-Adapter übereinstimmen.
 - Klicken Sie auf die Schaltfläche **OK**, um die ausgewählten Controller hinzuzufügen.

Add controller | vmhba68



Automatically

Manually

Host NQN

nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

COPY

IP

1

172.21.118.189

Enter IPv4 / IPv6 address

Central discovery controller

Port Number

Range more from 0

Digest parameter

Header digest

Data digest

DISCOVER CONTROLLERS

2

Select which controller to connect

<input type="checkbox"/>	Id	Subsystem NQN	Transport Type	IP	Port Number
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvm	172.21.118.190	4420

Manage Columns 4 items

3

4

OK

6. Nach einigen Sekunden sollte der NVMe Namespace auf der Registerkarte „Geräte“ angezeigt werden.

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.net app.com:794177624:65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

Manage Columns Export ▾ 6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

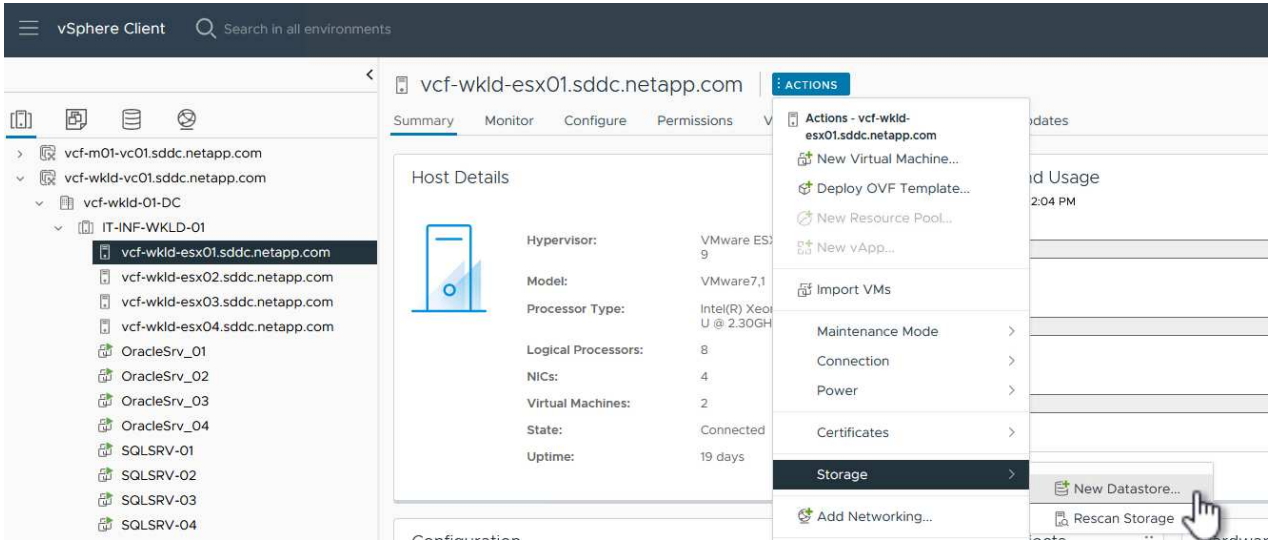
Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NVMe TCP Disk (uuid.929a6a9045764784 9146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRAN: RT

7. Wiederholen Sie dieses Verfahren, um einen NVMe over TCP-Adapter für das zweite Netzwerk zu erstellen, das für NVMe/TCP-Datenverkehr eingerichtet wurde.

NVMe over TCP Datastore implementieren

Führen Sie die folgenden Schritte aus, um einen VMFS-Datastore im NVMe Namespace zu erstellen:

1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Wählen Sie im Menü **actions Storage > New Datastore....**



2. Wählen Sie im Assistenten **New Datastore VMFS** als Typ aus. Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Name und Geräteauswahl** einen Namen für den Datastore ein und wählen Sie den NVMe Namespace aus der Liste der verfügbaren Geräte aus.

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection

Specify datastore name and a disk/LUN for provisioning the datastore.

Name

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V S
<input checked="" type="radio"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

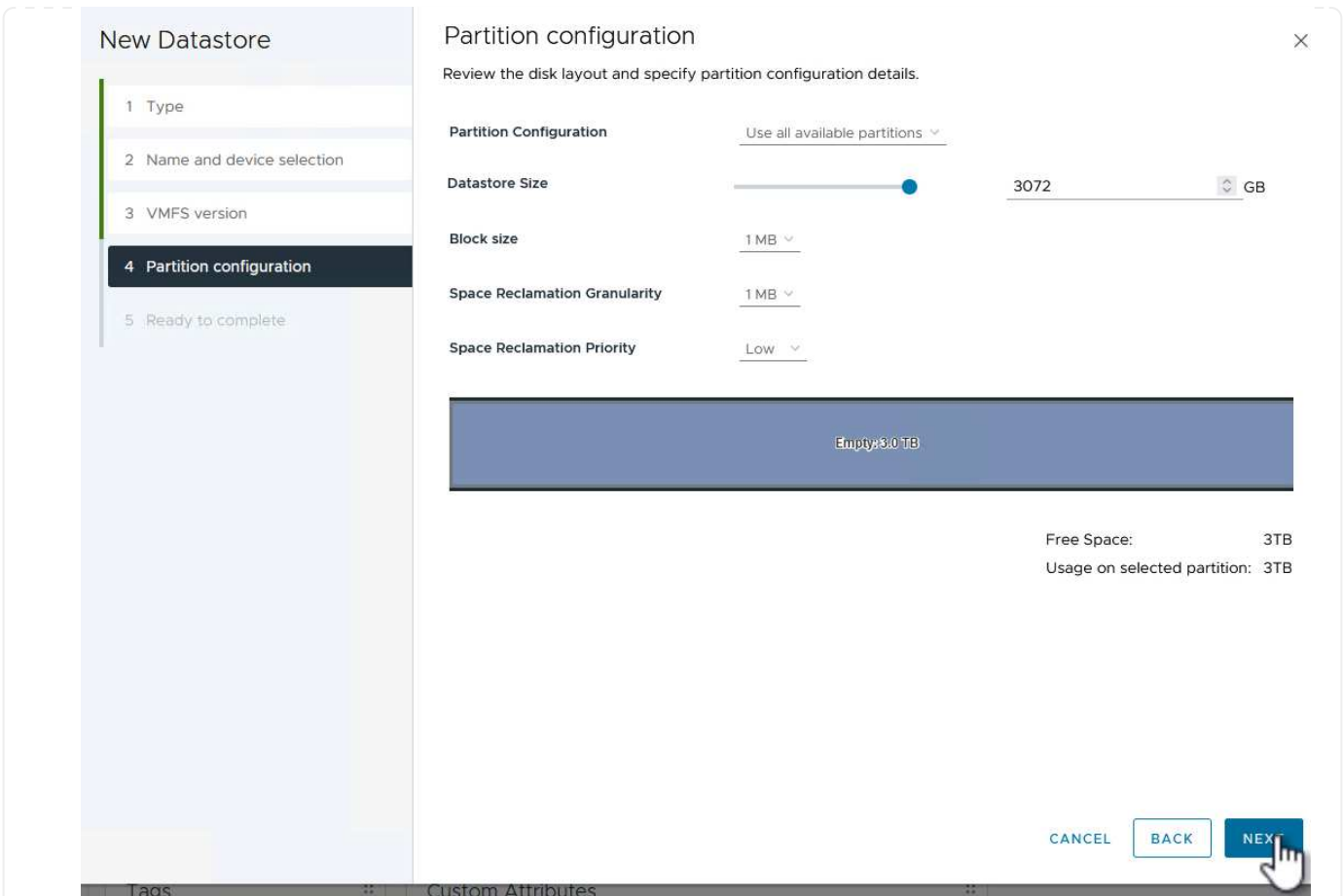
Manage Columns Export 3 items

CANCEL

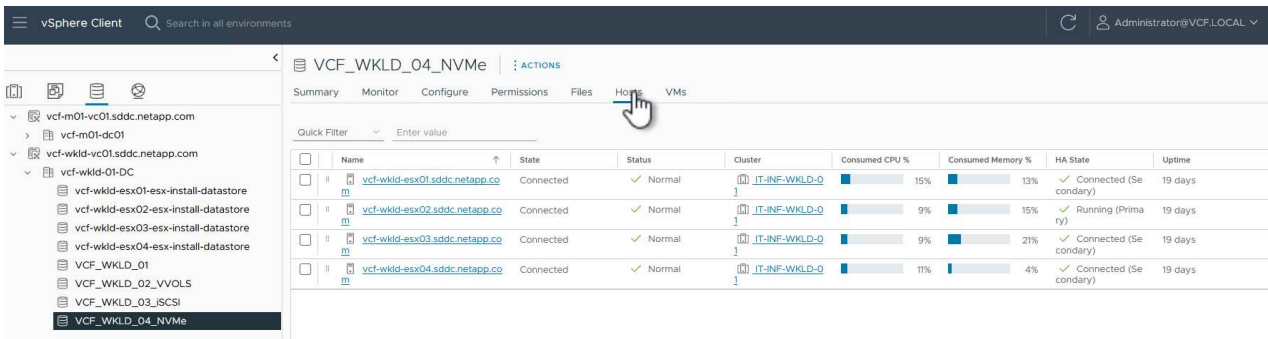
BACK

NEXT

4. Wählen Sie auf der Seite **VMFS Version** die Version von VMFS für den Datastore aus.
5. Nehmen Sie auf der Seite **Partition Configuration** die gewünschten Änderungen am Standard-Partitionsschema vor. Klicken Sie auf **Weiter**, um fortzufahren.



6. Überprüfen Sie auf der Seite **Ready to Complete** die Zusammenfassung und klicken Sie auf **Finish**, um den Datastore zu erstellen.
7. Navigieren Sie zum neuen Datastore im Bestand und klicken Sie auf die Registerkarte **Hosts**. Bei korrekter Konfiguration sollten alle ESXi-Hosts im Cluster aufgeführt sein und Zugriff auf den neuen Datastore haben.



Weitere Informationen

Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

Schützen Sie VMs in VCF-Workload-Domänen mit dem SnapCenter Plug-in für VMware vSphere

In diesem Szenario wird gezeigt, wie das SnapCenter Plug-in für VMware vSphere (SCV) implementiert und verwendet wird, um VMs und Datastores in einer VCF Workload-Domäne zu sichern und wiederherzustellen. SCV verwendet die ONTAP Snapshot-Technologie, um schnelle und effiziente Backup-Kopien der ONTAP-Speicher-Volumes zu erstellen, die vSphere-Datastores hosten. SnapMirror und SnapVault Technologie werden verwendet, um sekundäre Backups auf einem separaten Storage-System und mit Aufbewahrungsrichtlinien zu erstellen, die das Original-Volume imitieren oder zur langfristigen Aufbewahrung vom Original-Volume unabhängig sein können.

iSCSI wird als Speicherprotokoll für den VMFS-Datastore in dieser Lösung verwendet.

Autor: Josh Powell

Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Stellen Sie das SnapCenter Plug-in für VMware vSphere (SCV) in der VI-Workload-Domäne bereit.
- Fügen Sie dem SCV Speichersysteme hinzu.
- Erstellen Sie Backup-Richtlinien in SCV.
- Ressourcengruppen in SCV erstellen.
- Verwenden Sie SCV, um Datastores oder bestimmte VMs zu sichern.
- Verwenden Sie SCV, um VMs an einem anderen Speicherort im Cluster wiederherzustellen.
- Verwenden Sie SCV, um Dateien in einem Windows-Dateisystem wiederherzustellen.

Voraussetzungen

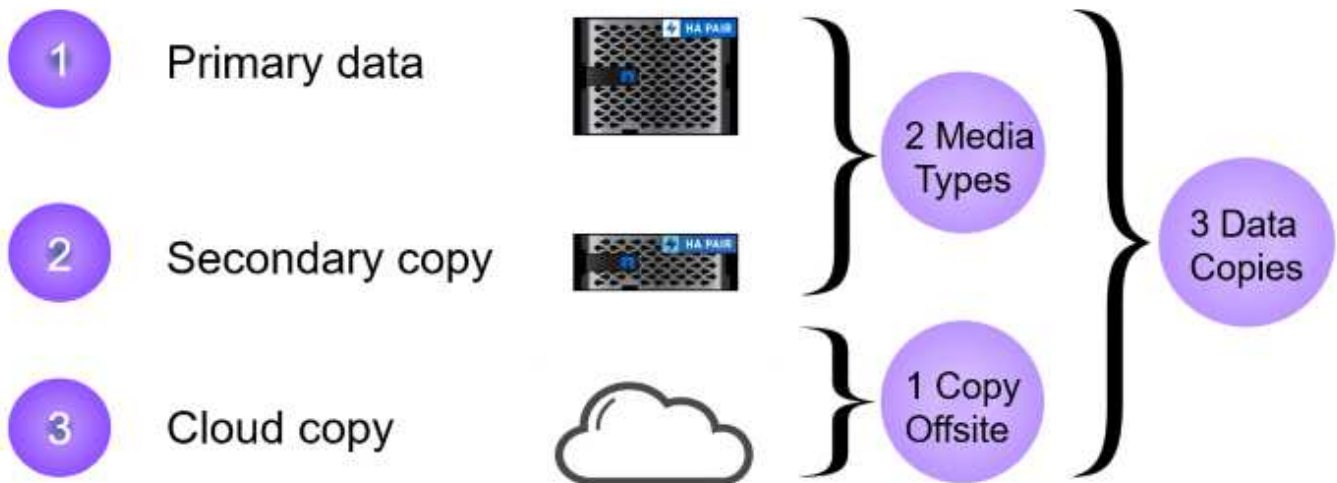
Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA-Speichersystem mit iSCSI-VMFS-Datenspeichern, die dem Workload-Domänencluster zugewiesen sind.
- Ein sekundäres ONTAP Storage-System, das für empfangene sekundäre Backups mit SnapMirror konfiguriert ist.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.
- Virtuelle Maschinen sind auf dem Cluster vorhanden SCV ist zum Schutz vorgesehen.

Informationen zum Konfigurieren von iSCSI-VMFS-Datastores als zusätzlichen Speicher finden Sie unter ["iSCSI als zusätzlicher Speicher für Management Domains"](#) Genutzt werden. Die Verwendung von OTV zur Implementierung von Datastores ist in Management- und Workload-Domänen identisch.



Zusätzlich zur Replizierung von Backups, die mit SCV auf sekundärem Storage erstellt werden, können externe Datenkopien auf Objekt-Storage auf einem der drei (3) führenden Cloud-Provider erstellt werden, der NetApp BlueXP Backup und Recovery für VMs nutzt. Weitere Informationen finden Sie in der Lösung ["3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs"](#).



Implementierungsschritte

Gehen Sie wie folgt vor, um das SnapCenter-Plug-in zu implementieren und zum Erstellen von Backups sowie zum Wiederherstellen von VMs und Datastores zu verwenden:

Stellen Sie SCV bereit und verwenden Sie diese, um Daten in einer VI-Workload-Domäne zu sichern

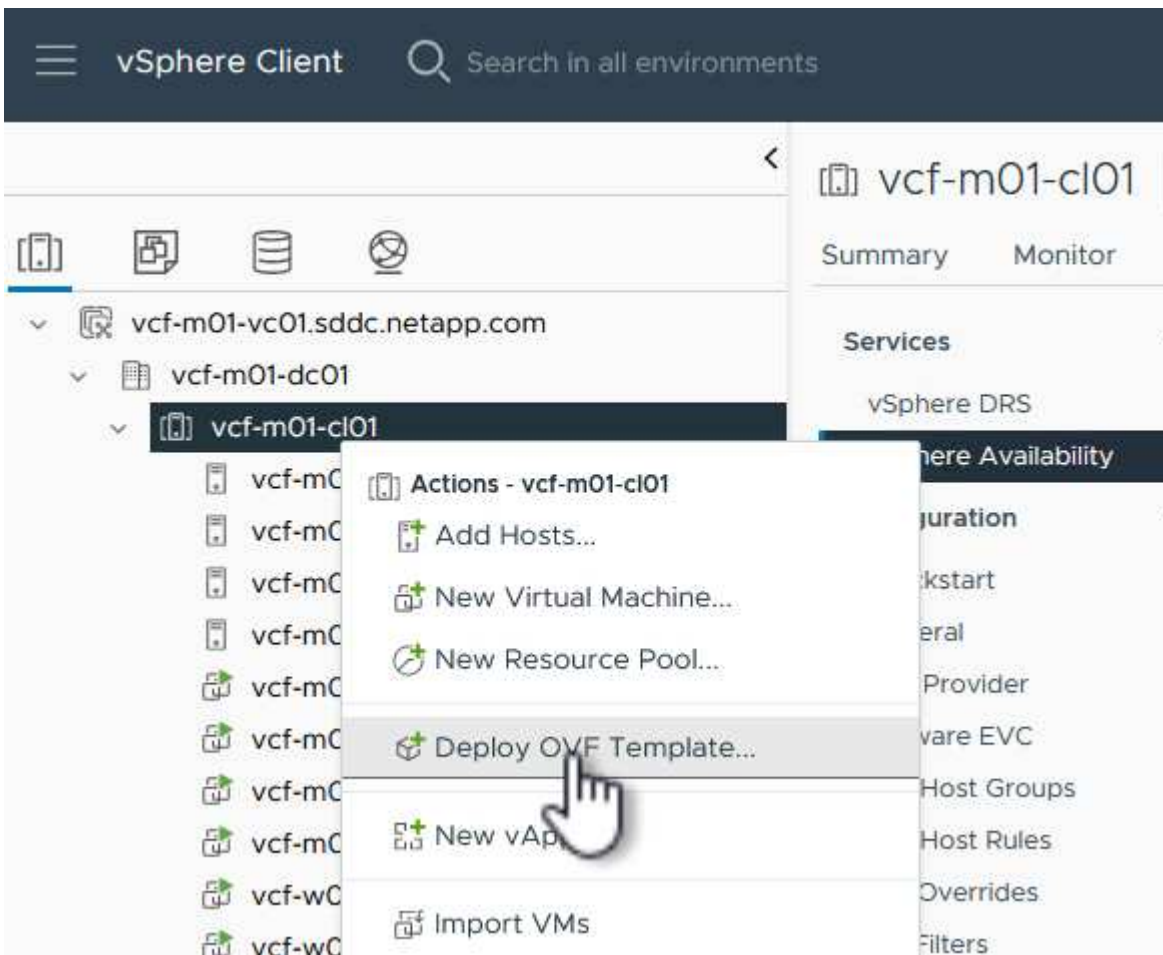
Führen Sie die folgenden Schritte durch, um SCV bereitzustellen, zu konfigurieren und zum Schutz von Daten in einer VI-Workload-Domäne zu verwenden:

Implementieren Sie das SnapCenter Plug-in für VMware vSphere

Das SnapCenter-Plug-in wird in der VCF-Managementdomäne gehostet, aber für die VI-Workload-Domäne in vCenter registriert. Eine SCV-Instanz ist für jede vCenter-Instanz erforderlich. Beachten Sie, dass eine Workload-Domäne mehrere Cluster umfassen kann, die von einer einzelnen vCenter-Instanz gemanagt werden.

Führen Sie die folgenden Schritte vom vCenter-Client aus, um SCV für die VI-Workload-Domäne bereitzustellen:

1. Laden Sie die OVA-Datei für die SCV-Bereitstellung im Downloadbereich der NetApp Support-Website herunter "[HIER](#)".
2. Wählen Sie in der Management Domain vCenter Client **Deploy OVF Template...** aus.



3. Klicken Sie im Assistenten **Deploy OVF Template** auf das Optionsfeld **Lokale Datei** und wählen Sie dann aus, um die zuvor heruntergeladene OVF-Vorlage hochzuladen. Klicken Sie auf **Weiter**, um fortzufahren.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

UPLOAD FILES

scv-5.OP2-240310_1514.ova

4. Geben Sie auf der Seite **Select Name and folder** einen Namen für die SCV Data Broker VM und einen Ordner auf der Management Domain an. Klicken Sie auf **Weiter**, um fortzufahren.
5. Wählen Sie auf der Seite **Select a Compute Resource** den Management Domain Cluster oder einen bestimmten ESXi Host innerhalb des Clusters aus, auf dem die VM installiert werden soll.
6. Lesen Sie die Informationen zur OVF-Vorlage auf der Seite **Details überprüfen** und stimmen Sie den Lizenzbedingungen auf der Seite **Lizenzvereinbarungen** zu.
7. Wählen Sie auf der Seite **Select Storage** den Datenspeicher aus, auf den die VM installiert werden soll, und wählen Sie das **virtuelle Laufwerksformat** und **VM-Speicherrichtlinie** aus. In dieser Lösung wird die VM auf einem iSCSI-VMFS-Datenspeicher auf einem ONTAP-Speichersystem installiert, wie zuvor in einem separaten Abschnitt dieser Dokumentation bereitgestellt. Klicken Sie auf **Weiter**, um fortzufahren.

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

Select virtual disk format

VM Storage Policy

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/> mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	
<input type="radio"/> vcf-m01-cl01-ds-vsant01	--	999.97 GB	49.16 GB	957.54 GB	
<input type="radio"/> vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	
<input type="radio"/> vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	

Compatibility

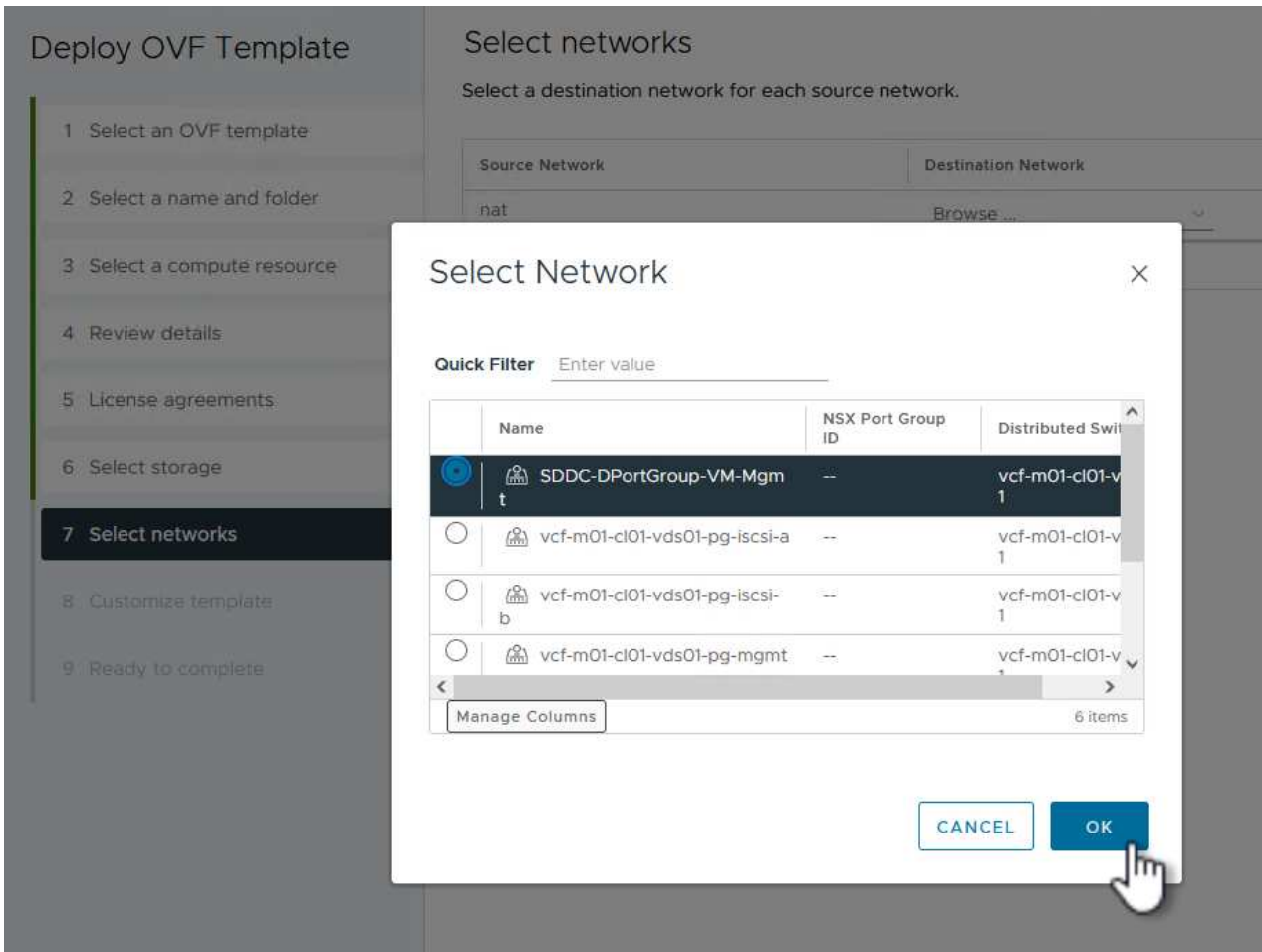
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Wählen Sie auf der Seite **Select Network** das Managementnetzwerk aus, das mit der Workload Domain vCenter Appliance und den primären und sekundären ONTAP Speichersystemen kommunizieren kann.



9. Geben Sie auf der Seite **Vorlage anpassen** alle für die Bereitstellung erforderlichen Informationen ein:

- FQDN oder IP und Anmeldeinformationen für die vCenter Appliance der Workload-Domäne.
- Anmeldeinformationen für das SCV-Administratorkonto.
- Anmeldeinformationen für das SCV-Wartungskonto.
- Details zu den IPv4-Netzwerkeigenschaften (IPv6 kann auch verwendet werden).
- Datums- und Uhrzeiteinstellungen.

Klicken Sie auf **Weiter**, um fortzufahren.

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

Customize template

Customize the deployment properties of this software solution.

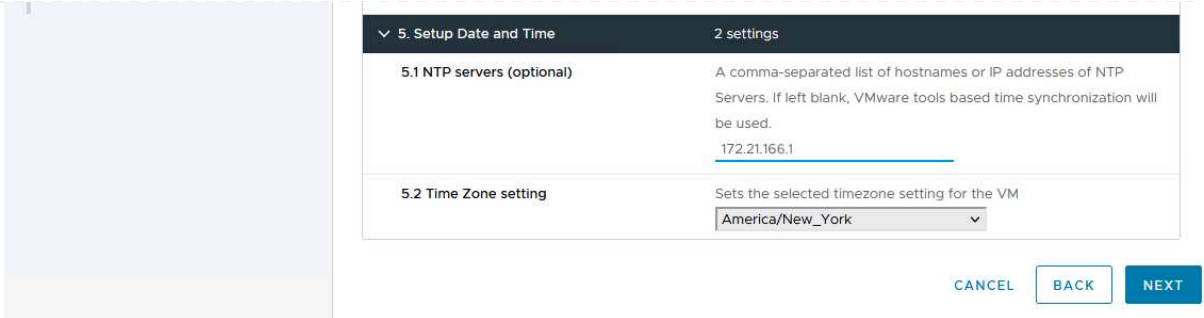
1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	<input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>	
1.2 vCenter username	<input type="text" value="administrator@vcf.local"/>	
1.3 vCenter password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
1.4 vCenter port	<input type="text" value="443"/>	
2. Create SCV Credentials		2 settings
2.1 Username	<input type="text" value="admin"/>	
2.2 Password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
3. System Configuration		1 settings

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

Customize template

4.2 Setup IPv4 Network Properties		6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.148"/>	
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="255.255.255.0"/>	
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.1"/>	
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) <input type="text" value="10.61.185.231"/>	
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) <input type="text" value="10.61.186.231"/>	
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) <input type="text" value="netapp.com,sddc.netapp.com"/>	
3.3 Setup IPv6 Network Properties		6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text"/>	
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired) <input type="text"/>	

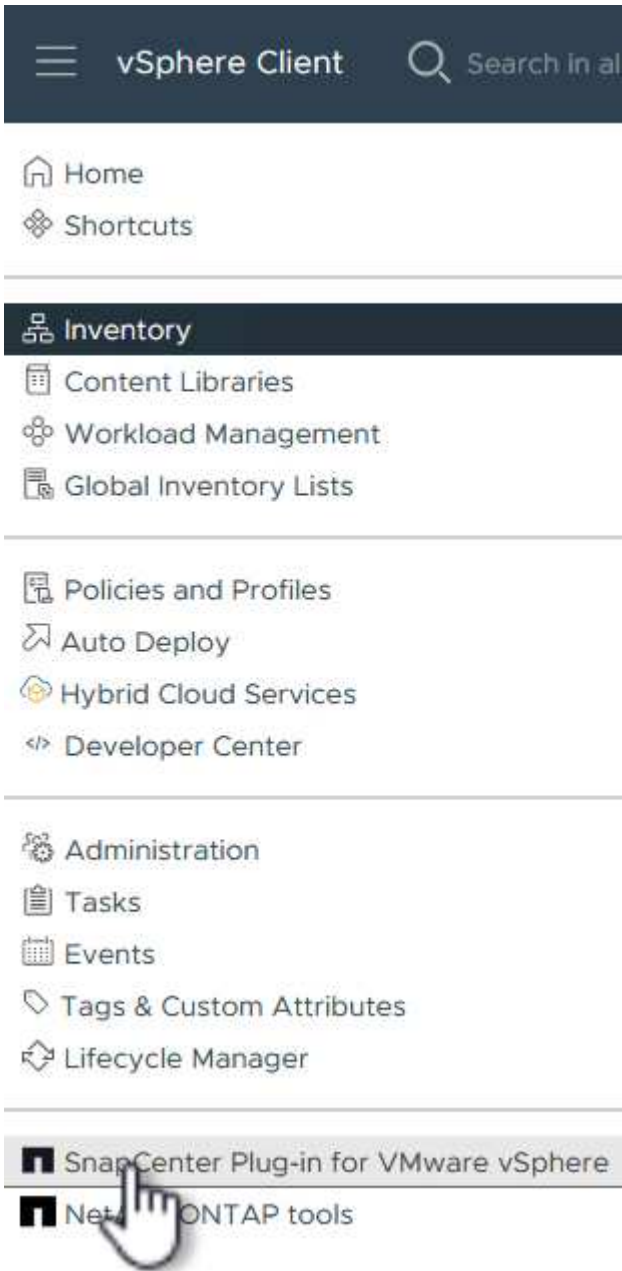


10. Überprüfen Sie abschließend auf der Seite **bereit zur Fertigstellung** alle Einstellungen und klicken Sie auf Fertig stellen, um die Bereitstellung zu starten.

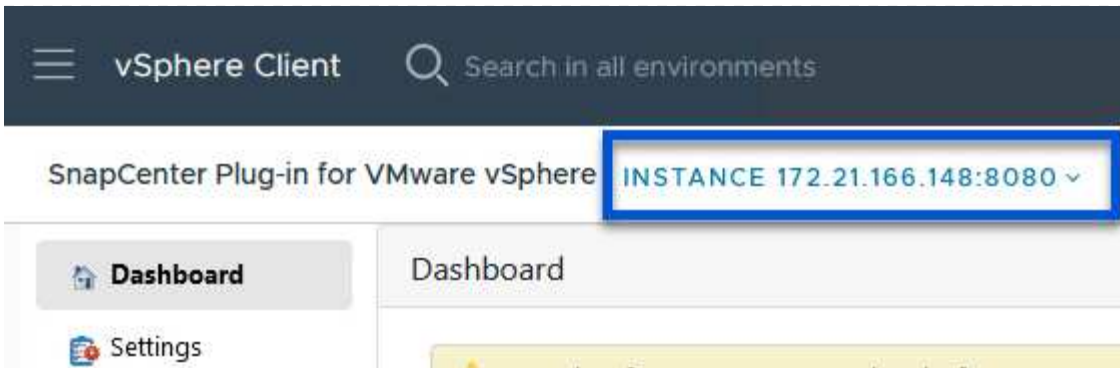
Fügen Sie dem SCV Speichersysteme hinzu

Führen Sie nach der Installation des SnapCenter-Plug-ins die folgenden Schritte aus, um dem SCV Speichersysteme hinzuzufügen:

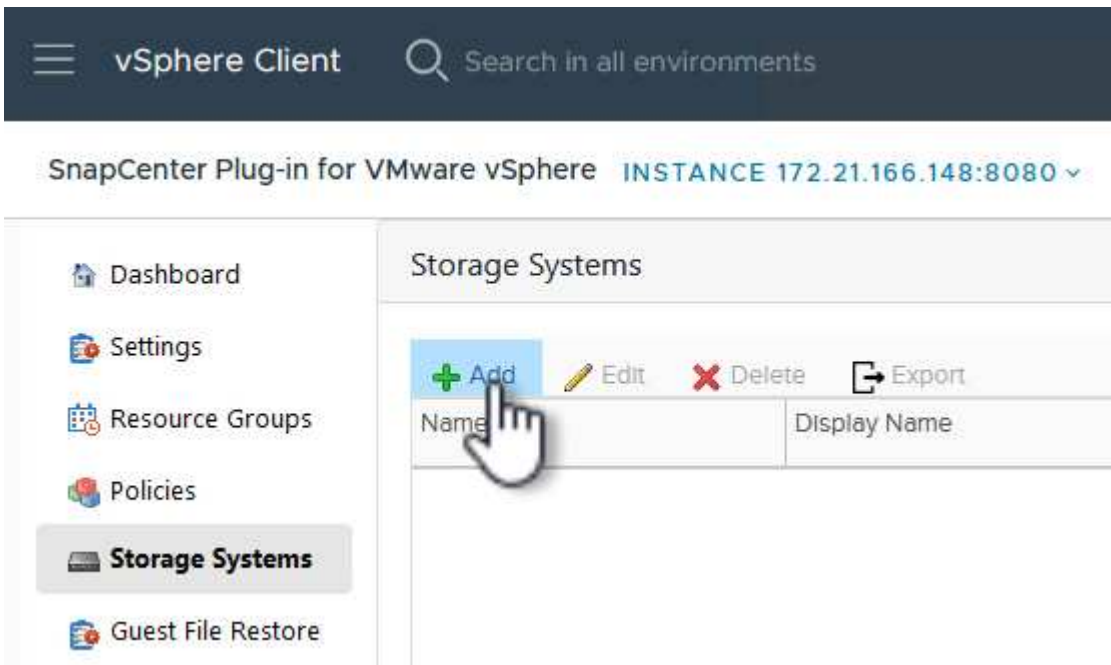
1. Auf SCV kann über das Hauptmenü im vSphere Client zugegriffen werden.



2. Wählen Sie oben in der SCV-Benutzeroberfläche die richtige SCV-Instanz aus, die dem zu schützenden vSphere-Cluster entspricht.



3. Navigieren Sie im linken Menü zu **Storage Systems** und klicken Sie auf **Add**, um zu beginnen.



4. Geben Sie im Formular **Speichersystem hinzufügen** die IP-Adresse und Zugangsdaten des hinzuzufügenden ONTAP-Speichersystems ein, und klicken Sie auf **Hinzufügen**, um die Aktion abzuschließen.

Add Storage System



Storage System	<input type="text" value="172.16.9.25"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> Seconds
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>

Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system



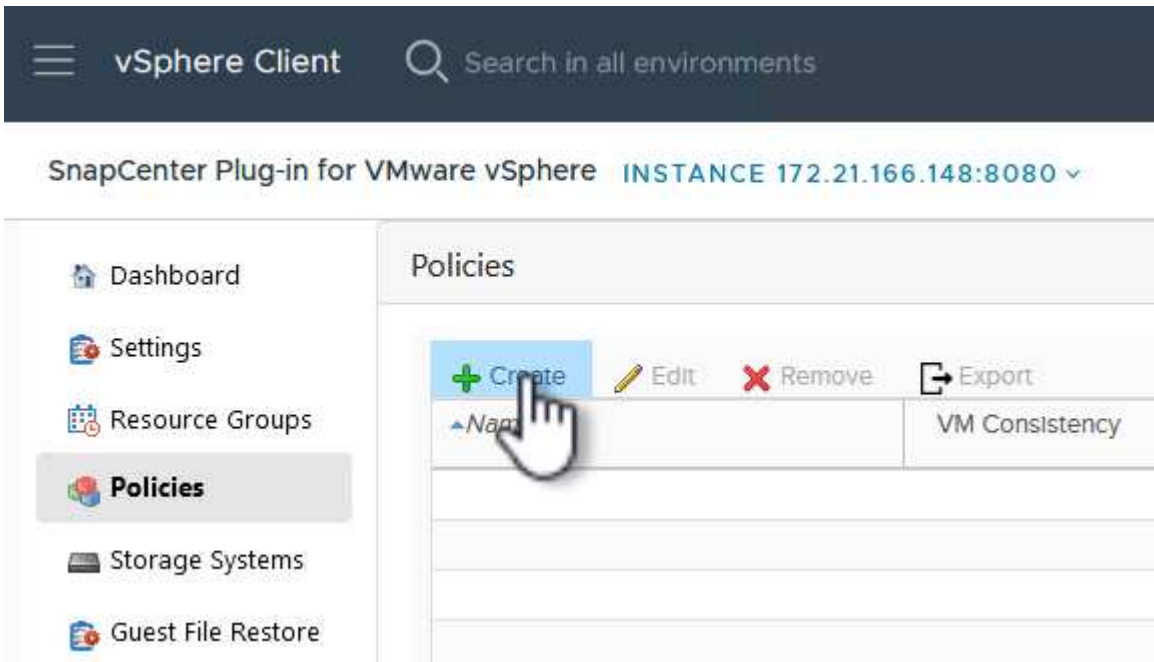
5. Wiederholen Sie diesen Vorgang für alle zusätzlichen zu verwaltenden Speichersysteme, einschließlich aller Systeme, die als sekundäre Backup-Ziele verwendet werden sollen.

Konfigurieren Sie Backup-Richtlinien in SCV

Weitere Informationen zum Erstellen von SCV-Backup-Richtlinien finden Sie unter "[Erstellen von Backup-Richtlinien für VMs und Datastores](#)".

Führen Sie die folgenden Schritte durch, um eine neue Backup-Richtlinie zu erstellen:

1. Wählen Sie im linken Menü **Richtlinien** und klicken Sie auf **Erstellen**, um zu beginnen.



2. Geben Sie im Formular **New Backup Policy** einen **Namen** und eine **Beschreibung** für die Policy, die **Häufigkeit**, bei der die Backups durchgeführt werden, und die **Aufbewahrungsfrist** an, die angibt, wie lange das Backup aufbewahrt wird.

Sperrfrist aktiviert die ONTAP SnapLock-Funktion, um manipulationssichere Schnappschüsse zu erstellen und ermöglicht die Konfiguration der Sperrfrist.

Für **Replication** Wählen Sie diese Option, um die zugrunde liegenden SnapMirror- oder SnapVault-Beziehungen für das ONTAP-Speichervolume zu aktualisieren.



SnapMirror und SnapVault Replizierung ähneln darin, dass sie beide zur asynchronen Replizierung von Storage Volumes auf ein sekundäres Storage-System ONTAP SnapMirror Technologie einsetzen. Dies steigert den Schutz und die Sicherheit. Bei SnapMirror Beziehungen regelt der in der SCV-Backup-Richtlinie angegebene Aufbewahrungszeitplan die Aufbewahrung sowohl für das primäre als auch für das sekundäre Volume. Bei SnapVault Beziehungen kann auf dem sekundären Storage-System für längere Zeiträume oder unterschiedliche Zeitpläne für die Aufbewahrung ein separater Aufbewahrungsplan erstellt werden. In diesem Fall wird das Snapshot-Label in der SCV-Backup-Policy und in der Policy im Zusammenhang mit dem sekundären Volume angegeben, um zu ermitteln, auf welche Volumes der unabhängige Aufbewahrungsplan angewendet werden soll.

Wählen Sie zusätzliche erweiterte Optionen und klicken Sie auf **Hinzufügen**, um die Richtlinie zu

erstellen.

New Backup Policy



Name

Description

Frequency

Locking Period Enable Snapshot Locking ⓘ

Retention ⓘ

Replication Update SnapMirror after backup ⓘ
 Update SnapVault after backup ⓘ

Snapshot label

Advanced ▾ VM consistency ⓘ
 Include datastores with independent disks

Scripts ⓘ

CANCEL

ADD

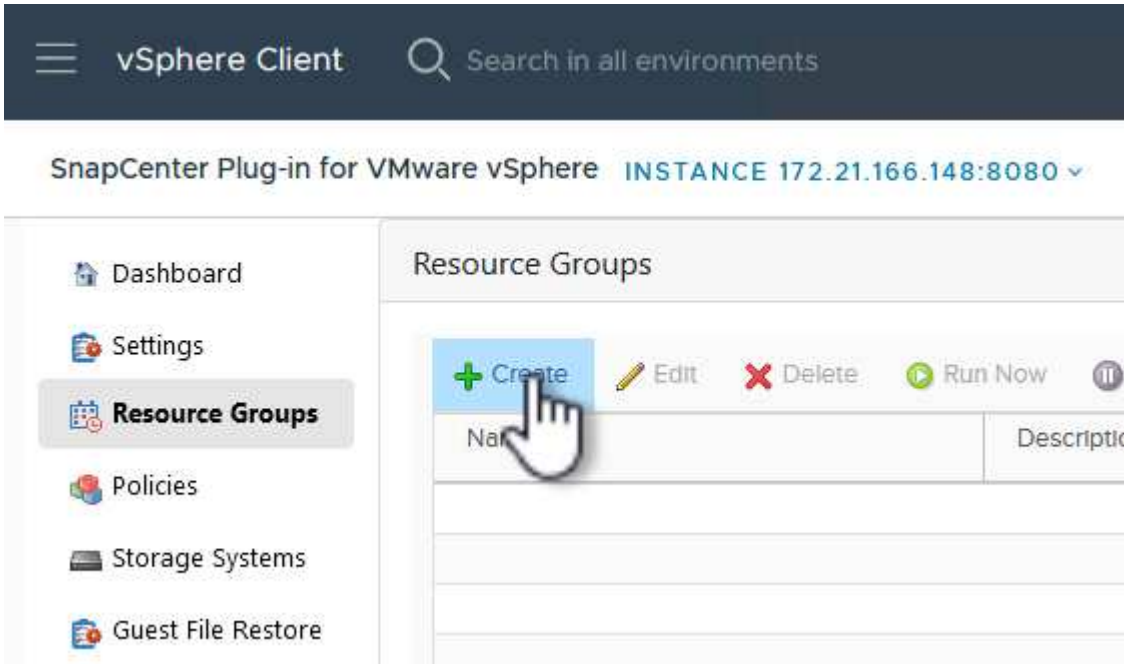


Erstellen Sie Ressourcengruppen in SCV

Weitere Informationen zum Erstellen von SCV-Ressourcengruppen finden Sie unter "[Erstellen von Ressourcengruppen](#)".

Führen Sie die folgenden Schritte aus, um eine neue Ressourcengruppe zu erstellen:

1. Wählen Sie im linken Menü **Ressourcengruppen** und klicken Sie auf **Erstellen**, um zu beginnen.



2. Geben Sie auf der Seite **General info & notification** einen Namen für die Ressourcengruppe, Benachrichtigungseinstellungen und alle zusätzlichen Optionen für die Benennung der Snapshots ein.
3. Wählen Sie auf der Seite **Resource** die Datastores und VMs aus, die in der Ressourcengruppe geschützt werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.



Auch wenn nur bestimmte VMs ausgewählt sind, wird der gesamte Datastore immer gesichert. Das liegt daran, dass ONTAP Snapshots des Volumes erstellt, das den Datastore hostet. Beachten Sie jedoch, dass die Auswahl von nur bestimmten VMs für Backups die Möglichkeit zur Wiederherstellung auf nur diese VMs beschränkt.

Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities

OracleSrv_01
OracleSrv_02
OracleSrv_03
OracleSrv_04

Selected entities

SQLSRV-01
SQLSRV-02
SQLSRV-03
SQLSRV-04

BACK NEXT FINISH CANCEL

4. Wählen Sie auf der Seite **Spanning Disks** die Option für den Umgang mit VMs mit VMDK's, die mehrere Datastores umfassen. Klicken Sie auf **Weiter**, um fortzufahren.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

Manually select the spanning datastores to be included ⓘ

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BACK NEXT FINISH CANCEL

5. Wählen Sie auf der Seite **Policies** eine zuvor erstellte Policy oder mehrere Policies aus, die mit dieser Ressourcengruppe verwendet werden. Klicken Sie auf **Weiter**, um fortzufahren.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily_Snapmi... ▼

Type Daily

Every 1 Day(s)

Starting 04/04/2024

At 04 45 PM

BACK

NEXT

FINISH

CANCEL

- Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um die Ressourcengruppe zu erstellen.

Create Resource Group

- 1. General info & notification
- 2. Resource
- 3. Spanning disks
- 4. Policies
- 5. Schedules
- 6. Summary**

Name	SQL_Servers		
Description			
Send email	Never		
Latest Snapshot name	None ⓘ		
Custom snapshot format	None ⓘ		
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04		
Spanning	False		
Policies	Name	Frequency	Snapshot Locking Period
	Daily_Snapmir...	Daily	-

BACK

NEXT

FINISH

CANCEL

8. Klicken Sie bei der erstellten Ressourcengruppe auf die Schaltfläche **Jetzt ausführen**, um das erste Backup auszuführen.

vSphere Client

SnapCenter Plug-in for VMware vSphere **INSTANCE 172.21.166.148:8080** ▾

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

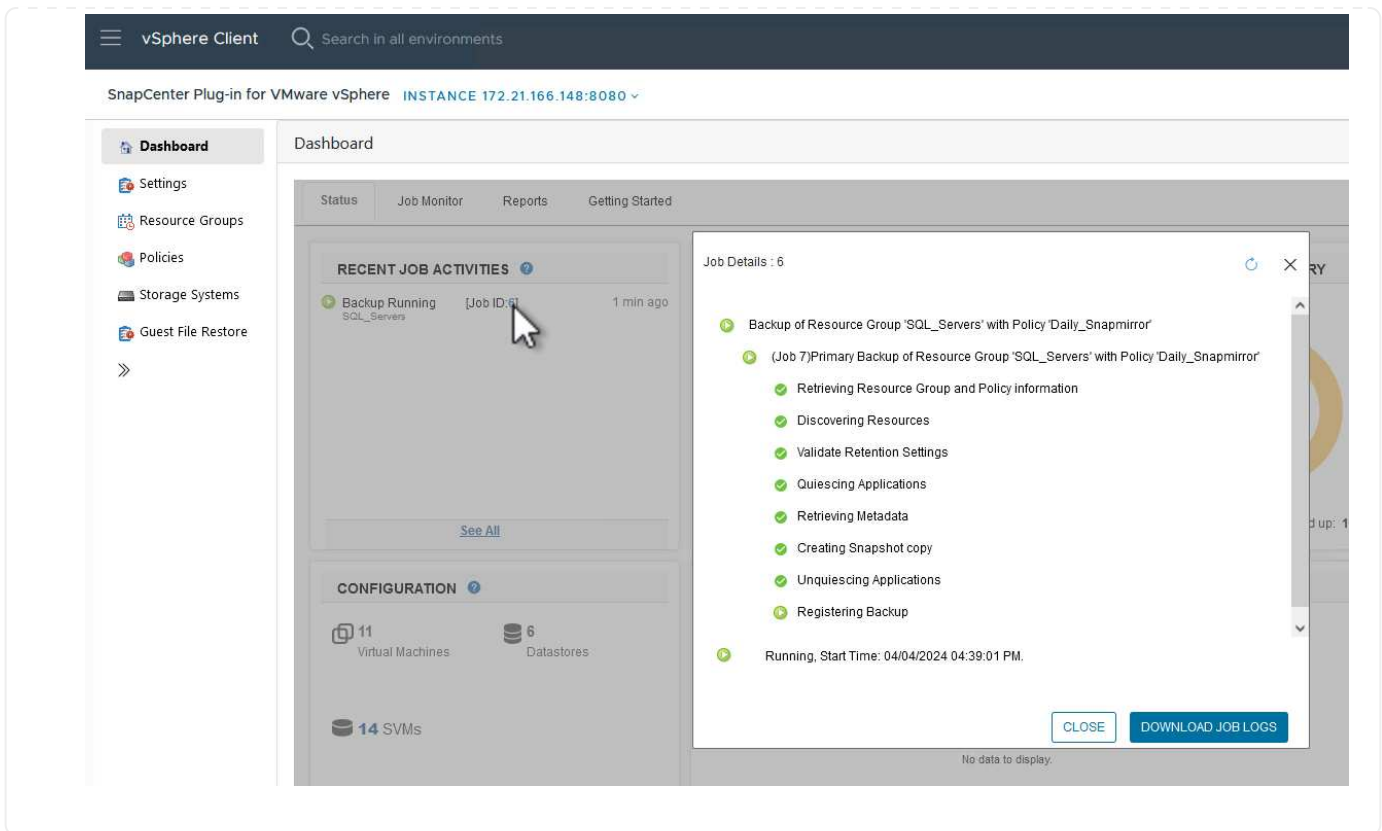
»

Resource Groups

+ Create **✎ Edit** **✖ Delete** **▶ Run Now** **⏸ Suspend** **▶ Resume** **📄 Export**

Name	Description	Polik
SQL_Servers		Daily_

9. Navigieren Sie zum **Dashboard** und klicken Sie unter **Letzte Jobaktivitäten** auf die Nummer neben **Job ID**, um den Job-Monitor zu öffnen und den Fortschritt des laufenden Jobs anzuzeigen.



Stellen Sie VMs, VMDKs und Dateien mit SCV wieder her

Das SnapCenter Plug-in ermöglicht die Wiederherstellung von VMs, VMDKs, Dateien und Ordnern von primären und sekundären Backups.

VMs können auf dem ursprünglichen Host, auf einem alternativen Host im selben vCenter Server oder auf einem alternativen ESXi-Host, der vom gleichen vCenter oder einem beliebigen vCenter im verknüpften Modus verwaltet wird, wiederhergestellt werden.

VVol VMs können auf dem ursprünglichen Host wiederhergestellt werden.

VMDKs in herkömmlichen VMs können entweder auf dem Original oder auf einem alternativen Datenspeicher wiederhergestellt werden.

VMDKs in vVol VMs können im ursprünglichen Datenspeicher wiederhergestellt werden.

Einzelne Dateien und Ordner in einer Gastdatei-Wiederherstellungssitzung können wiederhergestellt werden, wodurch eine Sicherungskopie einer virtuellen Festplatte angehängt und die ausgewählten Dateien oder Ordner wiederhergestellt werden.

Führen Sie folgende Schritte aus, um VMs, VMDKs oder einzelne Ordner wiederherzustellen.

Stellen Sie VMs mit dem SnapCenter Plug-in wieder her

Führen Sie die folgenden Schritte aus, um eine VM mit SCV wiederherzustellen:

1. Navigieren Sie zu der VM, die im vSphere-Client wiederhergestellt werden soll, klicken Sie mit der rechten Maustaste, und navigieren Sie zu **SnapCenter-Plug-in für VMware vSphere**. Wählen Sie im Untermenü * Restore* aus.

The screenshot shows the vSphere Client interface. On the left is a navigation tree with folders like 'vcf-m01-vc01.sddc.netapp.com' and 'vcf-wkld-01-IT-INF-WKLD-01-vc'. The main area displays the 'OracleSrv_04' VM summary page, including tabs for 'Summary', 'Monitor', 'Configure', and 'Permissions'. A context menu is open over the VM, listing various actions. The 'Restore' option is highlighted, and a mouse cursor is pointing at it. Below the main menu, a sub-menu is visible with options: 'Create Resource Group', 'Add to Resource Group', 'Attach Virtual Disk(s)', 'Detach Virtual Disk(s)', 'Restore', and 'File Restore'. The 'Restore' option is currently selected.

OracleSrv_04 | Summary | Monitor | Configure | Permissions

Guest OS | Virtual Mac

Actions - OracleSrv_04

- Power
- Guest OS
- Snapshots
- Open Remote Console
- Migrate...
- Clone
- Fault Tolerance
- VM Policies
- Template
- Compatibility
- Export System Logs...
- Edit Settings...
- Move to folder...
- Rename...
- Edit Notes...
- Tags & Custom Attributes
- Add Permission...
- Alarms
- Remove from Inventory
- Delete from Disk
- vSAN
- NetApp ONTAP tools
- SnapCenter Plug-in for VMware vSphere

4 CPU(s), 22 MHz used

32 GB, 0 GB memory active

100 GB | Thin Provision | VCF_WKLD_03_ISCSI

(of 2) vcf-wkld-01-IT-INF-WKLD-01-vc (connected) | 00:50:56:83:02:f

Disconnected

ESXI 7.0 U2 and later (VM vers

Recent Tasks

Task Name

Manage Columns

Run

Create Resource Group

Add to Resource Group

Attach Virtual Disk(s)

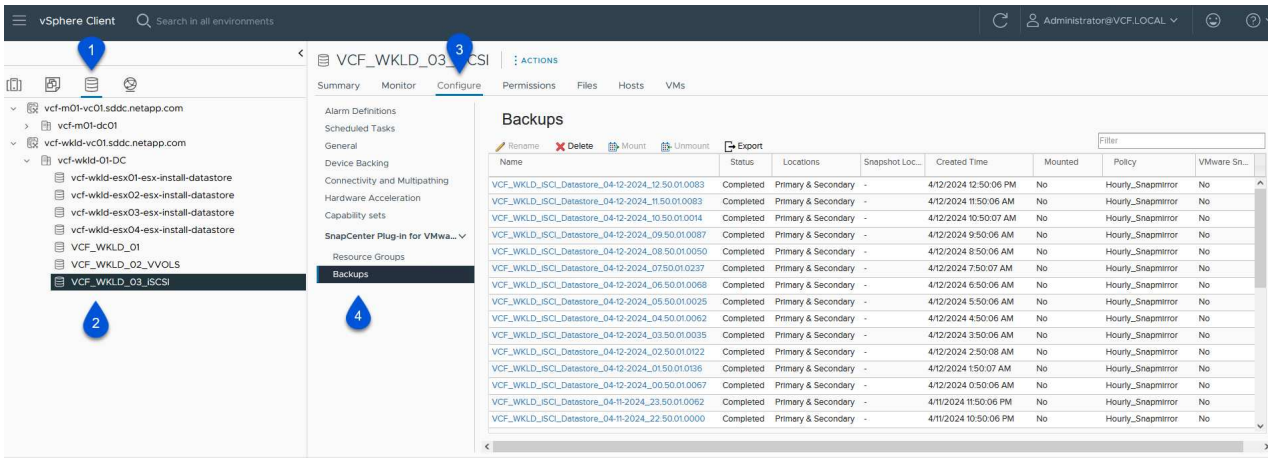
Detach Virtual Disk(s)

Restore

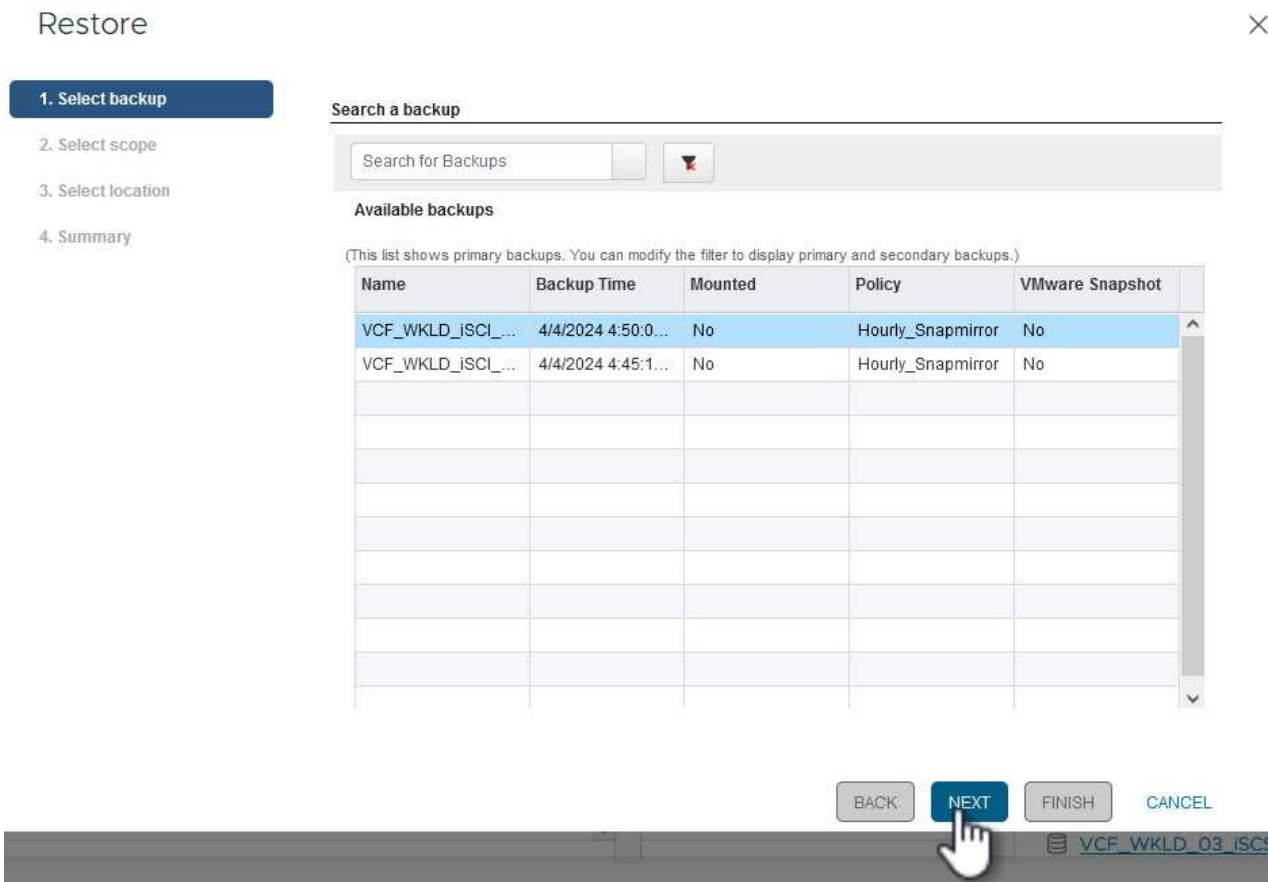
File Restore



Alternativ können Sie zum Datastore im Bestand navigieren und dann unter der Registerkarte **Configure** zu **SnapCenter Plug-in für VMware vSphere > Backups** wechseln. Wählen Sie aus dem ausgewählten Backup die VMs aus, die wiederhergestellt werden sollen.



2. Wählen Sie im **Restore-Assistenten** das zu verwendende Backup aus. Klicken Sie auf **Weiter**, um fortzufahren.



3. Füllen Sie auf der Seite **Bereich auswählen** alle erforderlichen Felder aus:

- **Umfang wiederherstellen** - Wählen Sie, um die gesamte virtuelle Maschine wiederherzustellen.
- **Neustart VM** - Wählen Sie, ob die VM nach der Wiederherstellung gestartet werden soll.
- **Speicherort wiederherstellen** - Wählen Sie die Wiederherstellung an der ursprünglichen Position oder an einem anderen Ort. Wählen Sie bei der Auswahl eines alternativen Speicherorts die Optionen aus den einzelnen Feldern aus:

- **Ziel vCenter Server** - Lokales vCenter oder alternatives vCenter im verknüpften Modus
- **Ziel-ESXi-Host**
- **Netzwerk**
- **VM-Name nach Wiederherstellung**
- **Datastore auswählen:**

Restore

1. Select backup

2. Select scope

3. Select location

4. Summary

Restore scope: Entire virtual machine

Restart VM:

Restore Location:

- Original Location
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)
- Alternate Location
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server: 172.21.166.143

Destination ESXi host: vcf-wkld-esx04.sddc.netapp.com

Network: vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-

VM name after restore: OracleSrv_04_restored

Select Datastore: VCF_WKLD_03_ISCSI

BACK NEXT FINISH CANCEL

VCF_WKLD_03_ISCSI

Klicken Sie auf **Weiter**, um fortzufahren.

4. Wählen Sie auf der Seite **Speicherort auswählen** aus, ob die VM vom primären oder sekundären ONTAP-Speichersystem wiederhergestellt werden soll. Klicken Sie auf **Weiter**, um fortzufahren.

Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location**
- 4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest
	< >

5. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um den Wiederherstellungsauftrag zu starten.

Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary**

Virtual machine to be restored	OracleSrv_04
Backup name	VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.143
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com
VM Network	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
Destination datastore	VCF_WKLD_03_iSCSI
VM name after restore	OracleSrv_04_restored



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

FINISH

CANCEL

6. Der Fortschritt des Wiederherstellungsjobs kann im Bereich **Letzte Aufgaben** im vSphere Client und über den Job Monitor in SCV überwacht werden.

- Dashboard
- Settings
- Resource Groups
- Policies
- Storage Systems
- Guest File Restore
- >>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago
VCF_WKLD_ISCI_Datastore_04-04-2024...
- Backup Successful [Job ID:15] 8 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:12] 13 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:9] 13 min ago
SQL_Servers
- Backup Successful [Job ID:6] 19 min ago
SQL_Servers

[See All](#)

CONFIGURATION

11 Virtual Machines 6 Datastores

14 SVMs

2 Resource Groups 2 Backup Policies

Job Details : 18

- Restoring backup with name: VCF_WKLD_ISCI_Datastore_04-04-2024_16:50:00.0940
- Preparing for Restore: Retrieving Backup metadata from Repository.
- Pre Restore
- Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

CLOSE DOWNLOAD JOB LOGS

No data to display.

Recent Tasks Alarms

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	vcf-wkld-esx04.sdd c.netapp.com	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 P M
NetApp Restore	vcf-wkld-esx04.sdd c.netapp.com	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 P M

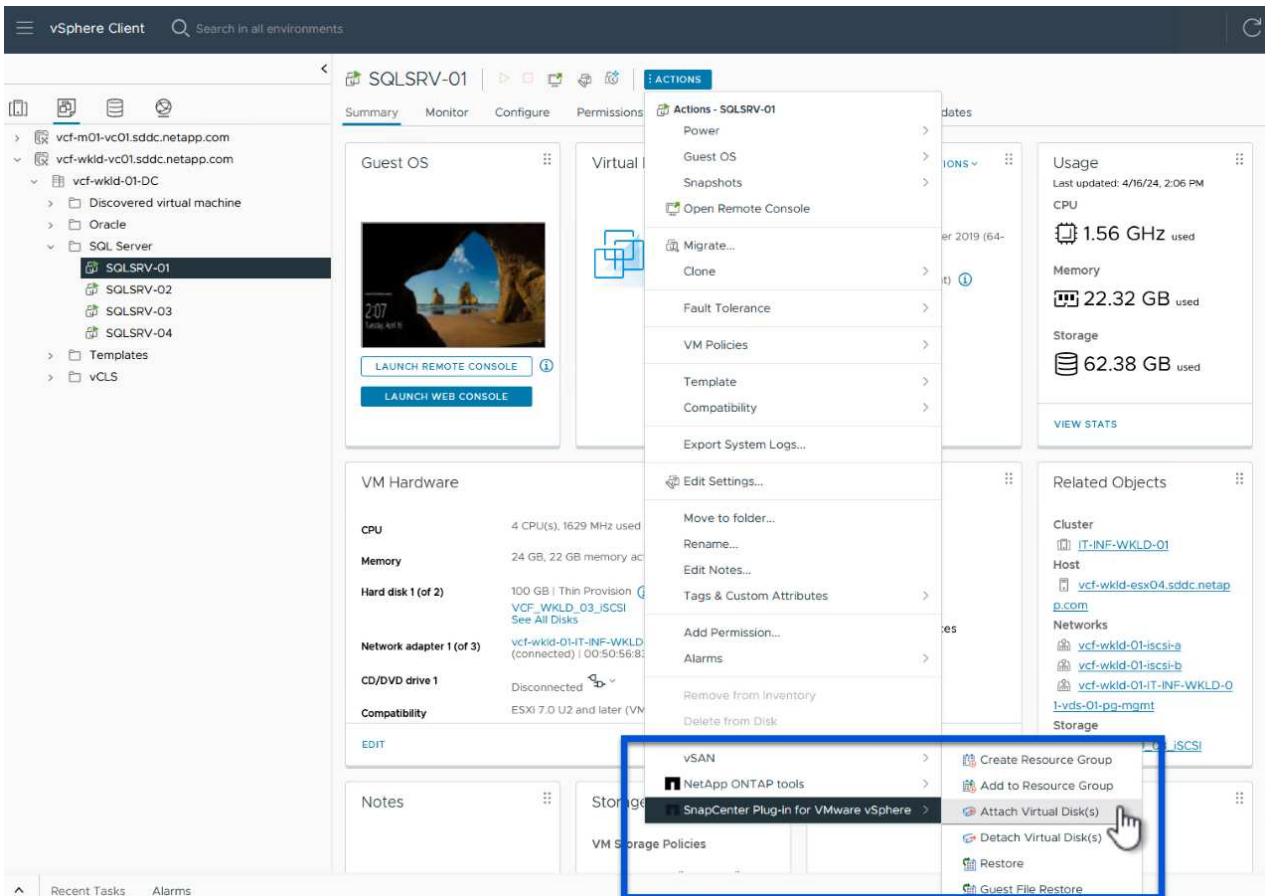
Manage Columns Running More Tasks

Stellen Sie VMDKs mit dem SnapCenter Plug-in wieder her

Mit den ONTAP-Tools können VMDK-Dateien am ursprünglichen Speicherort vollständig wiederhergestellt werden, oder es kann eine VMDK als neue Festplatte an ein Host-System angeschlossen werden. In diesem Szenario wird eine VMDK an einen Windows Host angeschlossen, um auf das Dateisystem zuzugreifen.

Gehen Sie wie folgt vor, um eine VMDK aus einem Backup anzubinden:

1. Navigieren Sie im vSphere-Client zu einer VM und wählen Sie im Menü **actions SnapCenter Plug-in für VMware vSphere > Virtuelle Festplatte(n) anhängen** aus.



2. Wählen Sie im **Attach Virtual Disk(s)** Wizard die zu verwendende Backup-Instanz und die anzuhängende VMDK aus.

Attach Virtual Disk(s)



Click here to attach to alternate VM

Backup

(This list shows primary backups. **1** modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Filteroptionen können verwendet werden, um Backups zu suchen und Backups von primären und sekundären Speichersystemen anzuzeigen.

Attach Virtual Disk(s)



Click here to attach to alternate VM

Backup

(This list shows primary backups)

Name
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231

Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Time range

From

Hour Minute Second

To

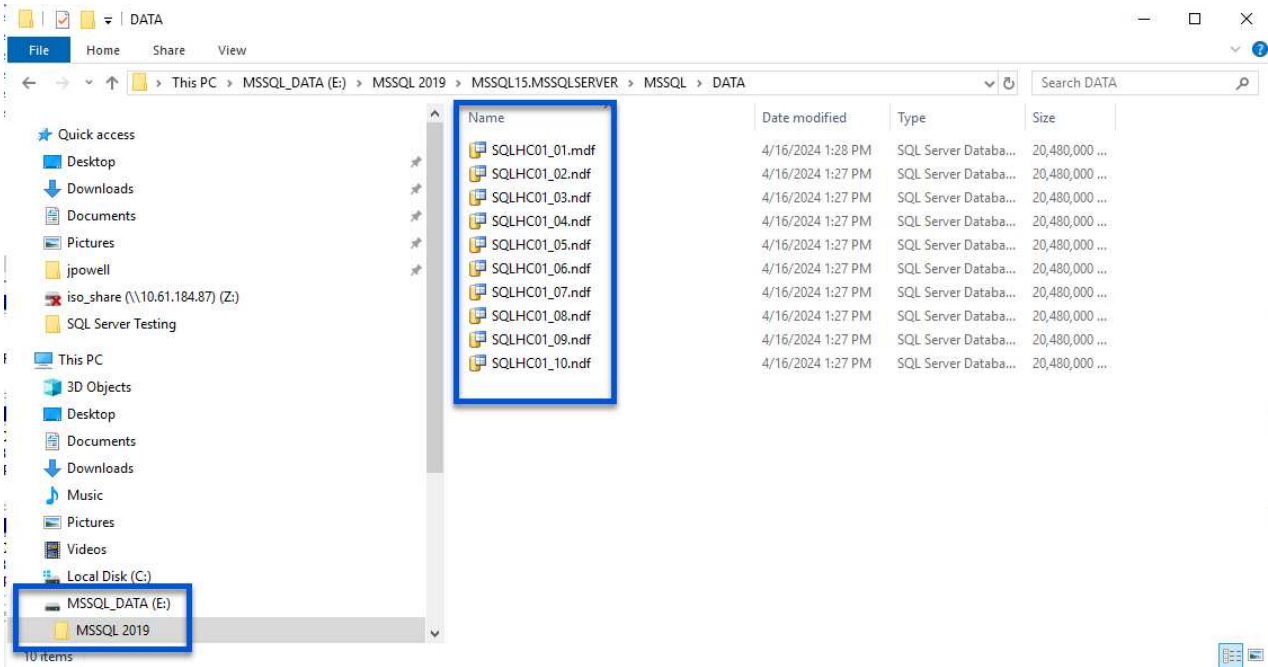
Hour Minute Second

VMware snapshot

Mounted

Location

3. Nachdem Sie alle Optionen ausgewählt haben, klicken Sie auf die Schaltfläche **Anhängen**, um den Wiederherstellungsvorgang zu starten und die VMDK an den Host anzuhängen.
4. Nach Abschluss des Anschlussvorgangs kann über das Betriebssystem des Hostsystems auf die Festplatte zugegriffen werden. In diesem Fall hat SCV die Festplatte mit ihrem NTFS-Dateisystem an das Laufwerk E: Unseres Windows SQL Servers angeschlossen und die SQL-Datenbankdateien auf dem Dateisystem sind über den Datei-Explorer zugänglich.



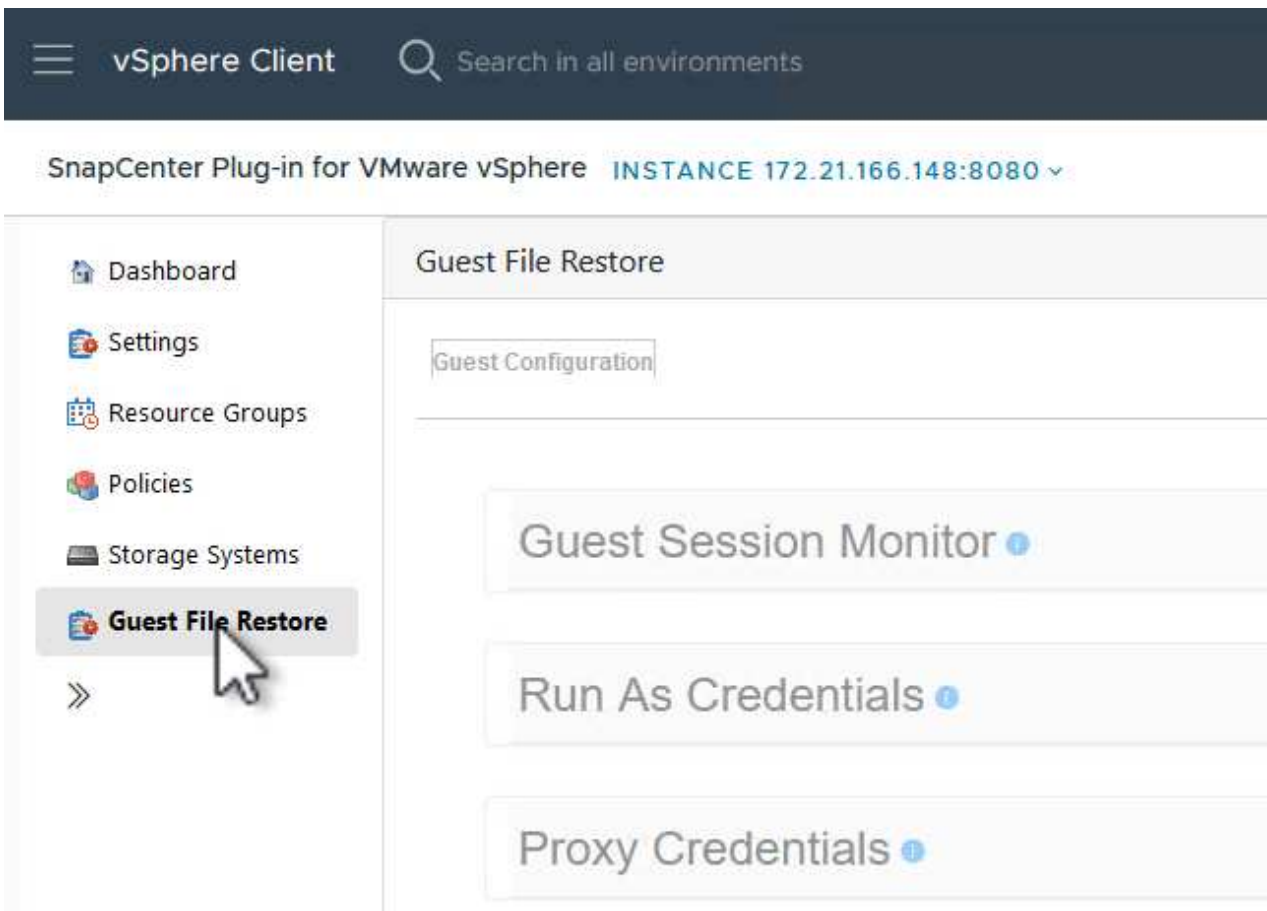
Wiederherstellung des Gastdateisystems mit dem SnapCenter Plug-in

ONTAP Tools bietet Gast-Dateisystem-Wiederherstellung von einer VMDK auf Windows Server Betriebssystemen. Diese wird zentral über die SnapCenter-Plug-in-Schnittstelle vorgeformt.

Ausführliche Informationen finden Sie unter "[Wiederherstellung von Gastdateien und Ordnern](#)" An der SCV-Dokumentationsstelle.

Führen Sie die folgenden Schritte durch, um eine Wiederherstellung des Gastdateisystems für ein Windows-System durchzuführen:

1. Der erste Schritt besteht darin, Run As Credentials zu erstellen, um Zugriff auf das Windows-Hostsystem zu ermöglichen. Navigieren Sie im vSphere Client zur CSV-Plug-in-Oberfläche und klicken Sie im Hauptmenü auf **Guest File Restore**.



2. Klicken Sie unter **Run As Credentials** auf das **+**-Symbol, um das Fenster **Run As Credentials** zu öffnen.
3. Geben Sie einen Namen für den Datensatz mit den Anmeldeinformationen, einen Administratorbenutzernamen und ein Kennwort für das Windows-System ein, und klicken Sie dann auf die Schaltfläche **Select VM**, um eine optionale Proxy-VM auszuwählen, die für die Wiederherstellung verwendet werden soll.

Run As Credentials



Run As Name ⓘ

Username ⓘ

Password ⓘ

Authentication Mode

VM Name



CANCEL

SAVE

4. Geben Sie auf der Seite Proxy-VM einen Namen für die VM ein, und suchen Sie sie nach ESXi-Host oder Namen. Klicken Sie nach der Auswahl auf **Speichern**.

Proxy VM



VM Name

SQLSRV-01

Search by ESXi Host

ESXi Host

vcf-wkld-esx04.sddc.netapp.com

Virtual Machine

SQLSRV-01

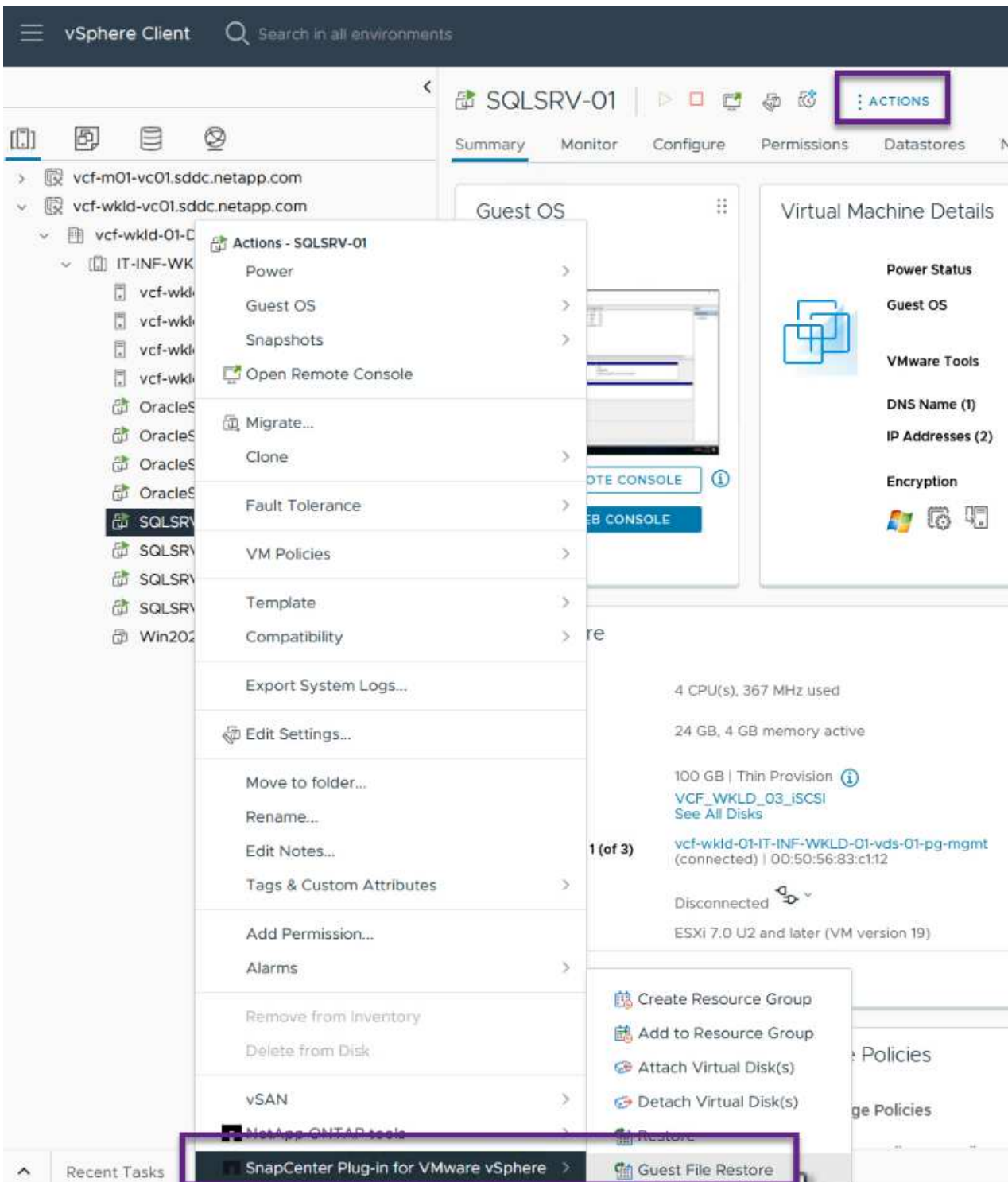
Search by Virtual Machine name

CANCEL

SAVE



5. Klicken Sie im Fenster **Run As Credentials** erneut auf **Save**, um das Speichern des Datensatzes abzuschließen.
6. Navigieren Sie anschließend zu einer VM im Bestand. Wählen Sie im Menü **actions** oder durch Rechtsklick auf die VM **SnapCenter Plug-in für VMware vSphere > Gastdateiwiederherstellung** aus.



- Wählen Sie auf der Seite **Restore Scope** des **Guest File Restore**-Assistenten das wiederherzustellende Backup, die jeweilige VMDK und den Speicherort (primär oder sekundär) aus, um die VMDK wiederherzustellen. Klicken Sie auf **Weiter**, um fortzufahren.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iscsi_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iscsi:VCF_WKLD_03_iscsi:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iscsi_dest:SQL_Servers_04-16-2024_13.52.34.0329

BACK NEXT FINISH CANCEL



8. Wählen Sie auf der Seite **Guest Details** die Option **Guest VM** oder **Use Gues File Restore Proxy VM** für die Wiederherstellung aus. Füllen Sie auf Wunsch auch hier die Einstellungen für die E-Mail-Benachrichtigung aus. Klicken Sie auf **Weiter**, um fortzufahren.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

Use Guest File Restore proxy VM

Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

- Überprüfen Sie abschließend die Seite **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um die Sitzung zur Systemwiederherstellung der Gastdatei zu starten.
- Navigieren Sie wieder in der SnapCenter-Plug-in-Oberfläche zu **Gastdateiwiederherstellung** und zeigen Sie die laufende Sitzung unter **Gastsitzungsmonitor** an. Klicken Sie auf das Symbol unter **Dateien durchsuchen**, um fortzufahren.

The screenshot shows the vSphere Client interface for the SnapCenter Plug-in for VMware vSphere. The main window displays the 'Guest File Restore' configuration page. Below the configuration, the 'Guest Session Monitor' table is visible, showing a single session. A mouse cursor is hovering over the 'Browse Files' column for the session.

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13.52.34.0329	SQLSRV-01	[VCF_WKLD_03_JSCSI(cc-202404161419...	E:\	23h:58m	

- Wählen Sie im **Guest File Browse**-Assistenten den Ordner oder die Dateien, die wiederhergestellt werden sollen, und den Dateisystemspeicherort, in dem sie wiederhergestellt werden sollen. Klicken Sie abschließend auf **Wiederherstellen**, um den Vorgang **Wiederherstellen** zu starten.

Guest File Browse



Select File(s)/Folder(s) to Restore



E:\MSSQL 2019

	Name	Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		^
			v

Selected 0 Files / 1 Directory

Name	Path	Size	Delete	
MSSQL 2019	E:\MSSQL 2019			^
				v

Select Restore Location



Select address family for UNC path:

IPv4

IPv6

Either Files to Restore or Restore Location is not selected!

CANCEL

RESTORE

12. Der Wiederherstellungsauftrag kann über den Aufgabenbereich von vSphere Client überwacht werden.

Weitere Informationen

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zur Verwendung des SnapCenter-Plug-ins für VMware vSphere finden Sie im ["Dokumentation zum SnapCenter Plug-in für VMware vSphere"](#).

VCF mit NetApp AFF-Arrays

VMware Cloud Foundation mit NetApp AFF-Arrays

VMware Cloud Foundation (VCF) ist eine integrierte softwaredefinierte Datacenter-Plattform (SDDC), die einen vollständigen Stack von softwaredefinierter Infrastruktur für die Ausführung von Enterprise-Applikationen in einer Hybrid-Cloud-Umgebung bereitstellt. Sie kombiniert Computing-, Storage-, Netzwerk- und Managementfunktionen in einer einheitlichen Plattform und ermöglicht so ein konsistentes Betriebserlebnis in Private und Public Clouds.

Autor: Josh Powell, Ravi BCB

Dieses Dokument enthält Informationen zu Storage-Optionen, die für VMware Cloud Foundation mithilfe des NetApp All-Flash AFF Storage-Systems zur Verfügung stehen. Unterstützte Storage-Optionen werden durch spezifische Anweisungen zum Erstellen von Workload-Domänen mit NFS- und vVol-Datstores als Haupt-Storage sowie eine Reihe zusätzlicher Storage-Optionen abgedeckt.

Anwendungsfälle

Anwendungsfälle in dieser Dokumentation:

- Storage-Optionen für Kunden, die einheitliche Umgebungen sowohl in privaten als auch in öffentlichen Clouds benötigen.
- Automatisierte Lösung zur Bereitstellung einer virtuellen Infrastruktur für Workload-Domänen.
- Skalierbare Storage-Lösung, die auf neue Anforderungen zugeschnitten ist, auch wenn sie nicht direkt auf die Anforderungen von Computing-Ressourcen ausgerichtet ist
- Stellen Sie VCF VI Workload Domains unter Verwendung von ONTAP als Hauptspeicher bereit.
- Stellen Sie mit ONTAP Tools für VMware vSphere zusätzlichen Speicher für VI-Workload-Domänen bereit.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Lösungsarchitekten, die flexiblere Storage-Optionen für VMware Umgebungen benötigen und ihre TCO maximieren möchten.
- Lösungsarchitekten, die auf der Suche nach VCF Storage-Optionen sind, die Datensicherungs- und Disaster Recovery-Optionen bei den großen Cloud-Providern bieten.
- Storage-Administratoren, die mehr über die Konfiguration von VCF mit Haupt- und zusätzlichem Storage erfahren möchten.

Technologischer Überblick

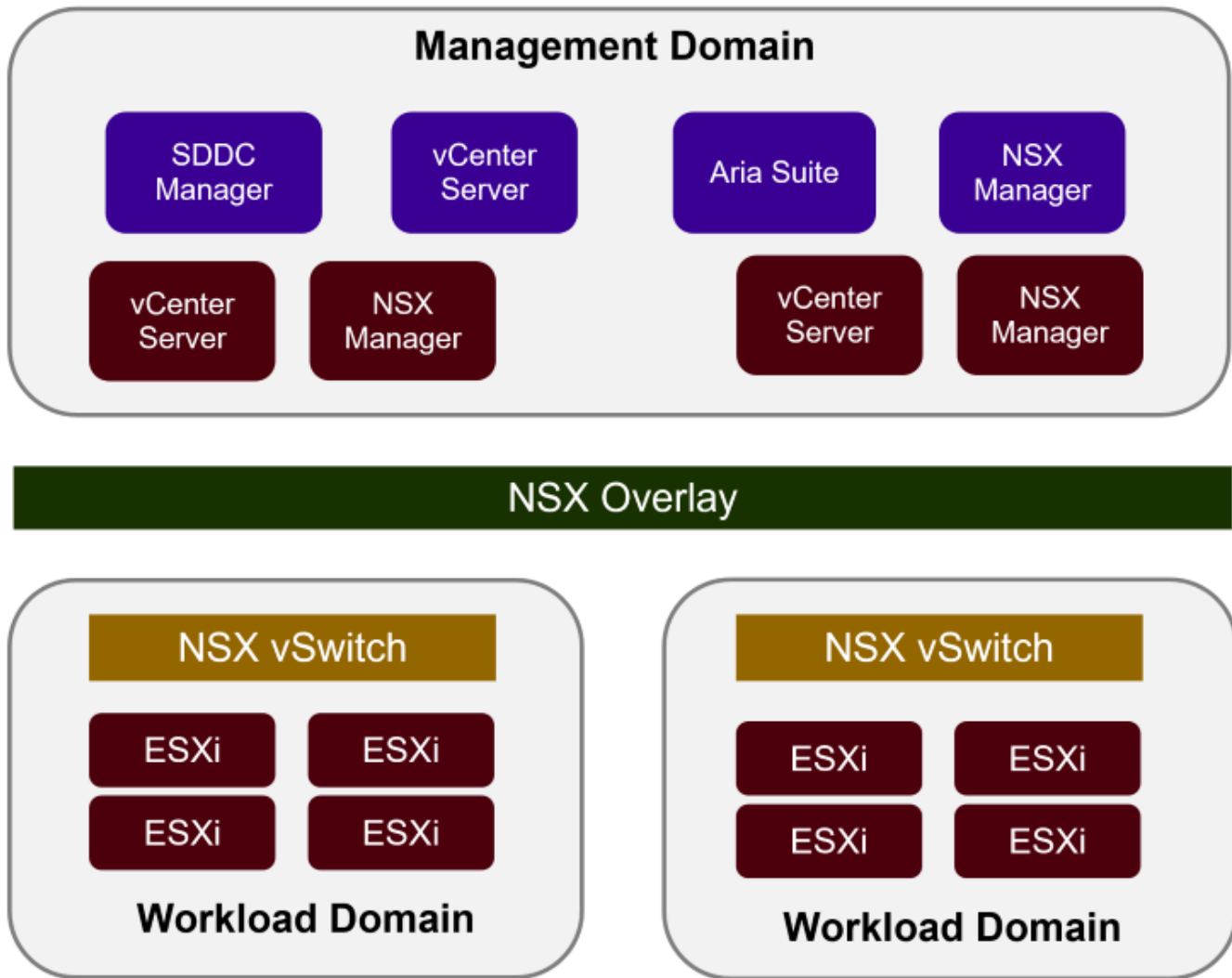
Die VCF mit NetApp AFF-Lösung besteht aus den folgenden Hauptkomponenten:

VMware Cloud Foundation

VMware Cloud Foundation erweitert die vSphere Hypervisor-Angebote von VMware durch die Kombination wichtiger Komponenten wie SDDC Manager, vSphere, vSAN, NSX und VMware Aria Suite, um ein virtualisiertes Datacenter zu erstellen.

Die VCF Lösung unterstützt sowohl native Kubernetes-Workloads als auch Workloads, die auf Virtual Machines basieren. Wichtige Services wie VMware vSphere, VMware vSAN, VMware NSX-T Data Center und VMware vRealize Cloud Management sind integrale Bestandteile des VCF Pakets. Zusammen bilden diese Services eine softwaredefinierte Infrastruktur, die ein effizientes Management von Computing, Storage, Netzwerken, Sicherheit und Cloud-Management ermöglicht.

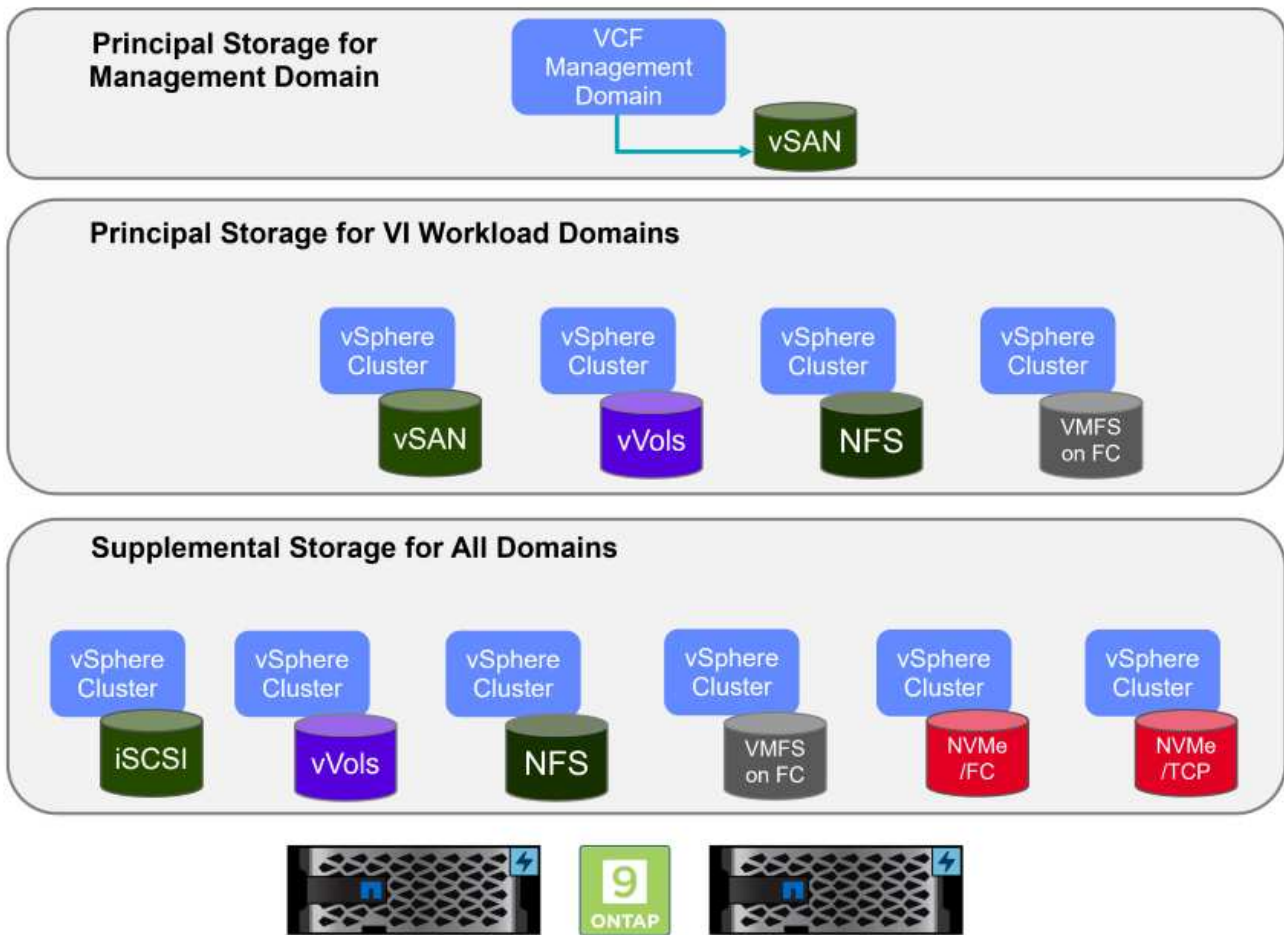
VCF besteht aus einer einzelnen Management-Domäne und bis zu 24 VI-Workload-Domänen, die jeweils eine Einheit für applikationsfähige Infrastrukturen darstellen. Eine Workload-Domäne besteht aus einem oder mehreren vSphere Clustern, die von einer einzelnen vCenter Instanz gemanagt werden.



Weitere Informationen zur Architektur und Planung von VCF finden Sie unter "[Architekturmodelle und Workload-Domänen-Typen in VMware Cloud Foundation](#)".

VCF Storage-Optionen

VMware unterteilt Speicheroptionen für VCF in **Principal** und **Supplemental** Speicher. Die VCF Management Domain muss vSAN als Hauptspeicher verwenden. Es gibt jedoch zahlreiche zusätzliche Speicheroptionen für die Verwaltungsdomäne und sowohl Haupt- als auch ergänzende Speicheroptionen für VI-Workload-Domänen.



Hauptspeicher für Workload-Domänen

Principal Storage bezieht sich auf jeden Speichertyp, der während des Setups innerhalb des SDDC Manager direkt mit einer VI Workload Domain verbunden werden kann. Principal Storage ist der erste für eine Workload Domain konfigurierte Datastore und umfasst vSAN, vVols (VMFS), NFS und VMFS auf Fibre Channel.

Ergänzender Speicher für Management- und Workload-Domänen

Zusätzlicher Storage ist der Storage-Typ, der dem Management oder den Workload-Domänen jederzeit nach der Erstellung des Clusters hinzugefügt werden kann. Zusätzlicher Storage umfasst die größte Auswahl an unterstützten Storage-Optionen, die alle von NetApp AFF Arrays unterstützt werden.

Zusätzliche Dokumentationsressourcen für VMware Cloud Foundation:

- * ["Dokumentation zu VMware Cloud Foundation"](#)
- * ["Unterstützte Storage-Typen für VMware Cloud Foundation"](#)
- * ["Management von Storage in VMware Cloud Foundation"](#)

Rein Flash-basierte Storage-Arrays von NetApp

NetApp AFF (All Flash FAS) Arrays sind hochperformante Storage-Lösungen, die die Geschwindigkeit und Effizienz der Flash-Technologie nutzen. AFF Arrays integrieren integrierte Datenmanagement-Funktionen wie Snapshot-basierte Backups, Replizierung, Thin Provisioning und Datensicherungsfunktionen.

NetApp AFF Arrays verwenden das ONTAP Storage-Betriebssystem und bieten umfassende Unterstützung der Storage-Protokolle für alle mit VCF kompatiblen Storage-Optionen innerhalb einer Unified Architecture.

NetApp AFF Storage-Arrays sind in den leistungsstärksten A-Serie und QLC Flash-basierten C-Serie verfügbar. Beide Serien verwenden NVMe-Flash-Laufwerke.

Weitere Informationen zu NetApp AFF Storage-Arrays der A-Serie finden Sie im ["NetApp AFF A-Serie" Landing Page](#) an.

Weitere Informationen zu NetApp Speicherarrays der C-Serie finden Sie im ["NetApp AFF C-Serie" Landing Page](#) an.

NetApp ONTAP Tools für VMware vSphere

Mit den ONTAP Tools für VMware vSphere (OTV) können Administratoren NetApp Storage direkt aus dem vSphere Client heraus managen. Mit den ONTAP Tools können Sie Datastores implementieren und managen und vVol Datastores bereitstellen.

Mit ONTAP Tools können Datenspeicher Storage-Funktionsprofilen zugeordnet werden, die eine Reihe von Attributen des Storage-Systems bestimmen. Dadurch können Datastores mit bestimmten Attributen wie Storage-Performance oder QoS erstellt werden.

ONTAP Tools umfassen zudem einen **VMware vSphere APIs for Storage Awareness (VASA) Provider** für ONTAP Storage-Systeme, der die Bereitstellung von VMware Virtual Volumes (VVols) Datastores, die Erstellung und Verwendung von Storage-Funktionsprofilen, Compliance-Überprüfung und Performance-Monitoring ermöglicht.

Weitere Informationen zu NetApp ONTAP-Tools finden Sie im ["ONTAP-Tools für VMware vSphere - Dokumentation"](#) Seite.

Lösungsüberblick

In den Szenarien, die in dieser Dokumentation vorgestellt werden, zeigen wir, wie ONTAP-Speichersysteme als Hauptspeicher für VCF VI-Workload-Domänen-Bereitstellungen verwendet werden. Darüber hinaus installieren und verwenden wir ONTAP Tools für VMware vSphere, um zusätzliche Datastores für VI-Workload-Domänen zu konfigurieren.

Szenarien in dieser Dokumentation:

- **Konfigurieren und verwenden Sie einen NFS-Datystore als Hauptspeicher während der VI-Workload-Domain-Bereitstellung.** Klicken Sie auf ["Hier"](#) Für Bereitstellungsschritte.
- **Installieren und demonstrieren Sie die Verwendung von ONTAP-Tools, um NFS-Datastores als zusätzlichen Speicher in VI-Workload-Domänen zu konfigurieren und zu mounten.** Klicken Sie auf ["Hier"](#) Für Bereitstellungsschritte.

NFS als Hauptspeicher für VI-Workload-Domänen

In diesem Szenario zeigen wir, wie ein NFS-Datystore als Hauptspeicher für die Bereitstellung einer VI-Workload-Domain in VCF konfiguriert wird. Sofern zutreffend, beziehen wir uns auf die externe Dokumentation für die Schritte, die im SDDC Manager von VCF durchgeführt werden müssen, und behandeln die Schritte, die spezifisch für den Bereich der Speicherkonfiguration sind.

Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Überprüfen Sie das Netzwerk für die ONTAP Storage Virtual Machine (SVM) und ob eine logische Schnittstelle (LIF) für den NFS-Traffic vorhanden ist.
- Eine Exportrichtlinie erstellen, um den ESXi Hosts den Zugriff auf das NFS-Volume zu ermöglichen.
- Erstellen Sie ein NFS-Volume auf dem ONTAP Storage-System.
- Erstellen Sie einen Netzwerkpool für NFS- und vMotion-Datenverkehr im SDDC Manager.
- Provision für Hosts in VCF für die Verwendung in einer VI-Workload-Domäne.
- Stellen Sie eine VI-Workload-Domäne in VCF unter Verwendung eines NFS-Datastore als Hauptspeicher bereit.
- Installation des NetApp NFS Plug-ins für VMware VAAI

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- NetApp AFF Storage-System mit einer Storage Virtual Machine (SVM), die für NFS-Datenverkehr konfiguriert ist
- Die logische Schnittstelle (LIF) wurde im IP-Netzwerk erstellt, das NFS-Datenverkehr überträgt und mit der SVM verknüpft ist.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und auf die SDDC Manager-Schnittstelle kann zugegriffen werden.
- 4 x ESXi-Hosts, die für die Kommunikation im VCF-Managementnetzwerk konfiguriert sind.
- IP-Adressen, die für vMotion und NFS-Storage-Verkehr im zu diesem Zweck eingerichteten VLAN oder Netzwerksegment reserviert sind.



Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk zum NFS-Server routenfähig ist oder 2) eine LIF für das Managementnetzwerk zur SVM, die das NFS-Datastore-Volumen hostet, hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

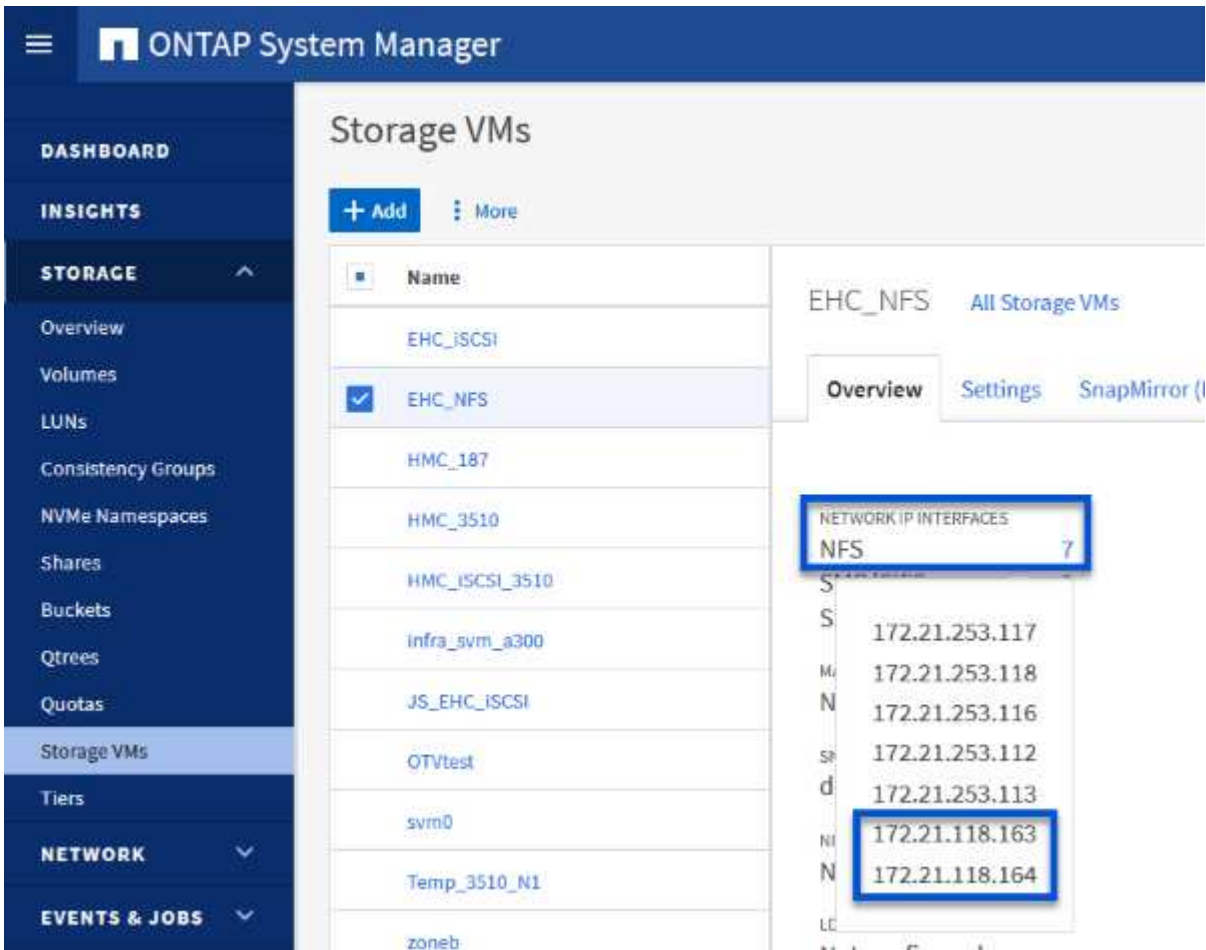
Implementierungsschritte

Gehen Sie wie folgt vor, um eine VI-Workload-Domäne mit einem NFS-Datastore als Hauptspeicher bereitzustellen:

Netzwerk für ONTAP SVM überprüfen

Vergewissern Sie sich, dass die erforderlichen logischen Schnittstellen für das Netzwerk vorhanden sind, die NFS-Datenverkehr zwischen dem ONTAP Storage-Cluster und der VI Workload Domain transportieren.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf die SVM, die für den NFS-Datenverkehr verwendet werden soll. Klicken Sie auf der Registerkarte **Übersicht** unter **NETZWERK-IP-SCHNITTSTELLEN** auf den numerischen Wert rechts von **NFS**. Überprüfen Sie in der Liste, ob die erforderlichen LIF-IP-Adressen aufgeführt sind.



The screenshot shows the ONTAP System Manager interface. The left sidebar contains a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE (expanded), and NETWORK. Under STORAGE, 'Storage VMs' is selected. The main area displays a list of Storage VMs with 'EHC_NFS' selected. To the right, the 'Overview' tab for 'EHC_NFS' is active, showing 'All Storage VMs'. Below this, the 'NETWORK IP INTERFACES' section is visible, with 'NFS' selected and a count of '7'. A list of IP addresses is shown, with '172.21.118.163' and '172.21.118.164' highlighted by blue boxes.

Alternativ können Sie mit dem folgenden Befehl die LIFs, die einer SVM zugeordnet sind, über die ONTAP-CLI überprüfen:

```
network interface show -vserver <SVM_NAME>
```

1. Überprüfen Sie, ob die ESXi-Hosts mit dem ONTAP-NFS-Server kommunizieren können. Melden Sie sich über SSH beim ESXi Host an und pingen Sie die SVM LIF:

```
vmkping <IP Address>
```

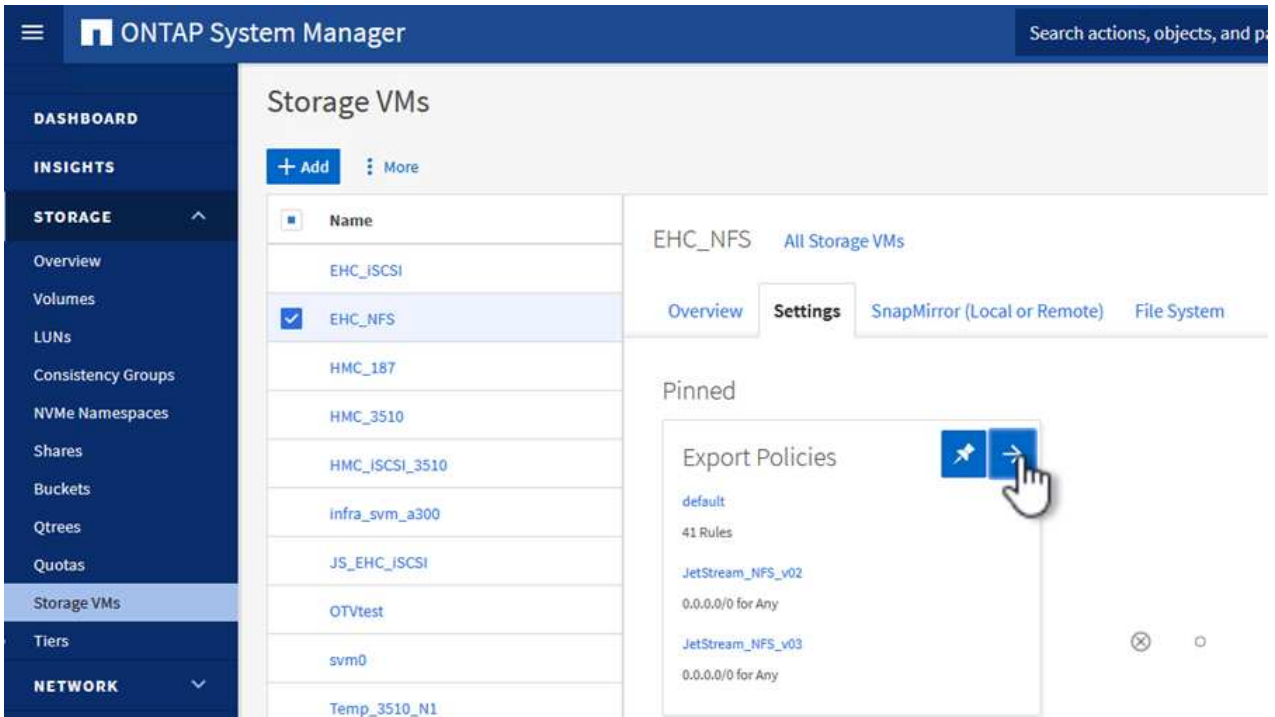



Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk zum NFS-Server routingfähig ist oder 2) eine LIF für das Managementnetzwerk zur SVM, die das NFS-Datastore-Volumen hostet, hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

Erstellen Sie eine Exportrichtlinie für die gemeinsame Nutzung von NFS-Volumen

Eine Richtlinie für den Export in ONTAP System Manager erstellen, um die Zugriffssteuerung für NFS Volumes zu definieren.

1. Klicken Sie im ONTAP System Manager im linken Menü auf **Speicher-VMs** und wählen Sie eine SVM aus der Liste aus.
2. Suchen Sie auf der Registerkarte **Settings Export Policies** und klicken Sie auf den Pfeil, um darauf zuzugreifen.



3. Fügen Sie im Fenster **Neue Exportrichtlinie** einen Namen für die Richtlinie hinzu, klicken Sie auf die Schaltfläche **Neue Regeln hinzufügen** und dann auf die Schaltfläche **+Hinzufügen**, um mit dem Hinzufügen einer neuen Regel zu beginnen.

New export policy

NAME

WKLD_DM01

Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. Geben Sie die IP-Adressen, den IP-Adressbereich oder das Netzwerk ein, die Sie in die Regel aufnehmen möchten. Deaktivieren Sie die Kontrollkästchen **SMB/CIFS** und **FlexCache** und treffen Sie eine Auswahl für die unten stehenden Zugriffsdetails. Die Auswahl der UNIX-Felder ist für den ESXi-Hostzugriff ausreichend.

New Rule



CLIENT SPECIFICATION

ACCESS PROTOCOLS

 SMB/CIFS FlexCache NFS NFSv3 NFSv4

ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



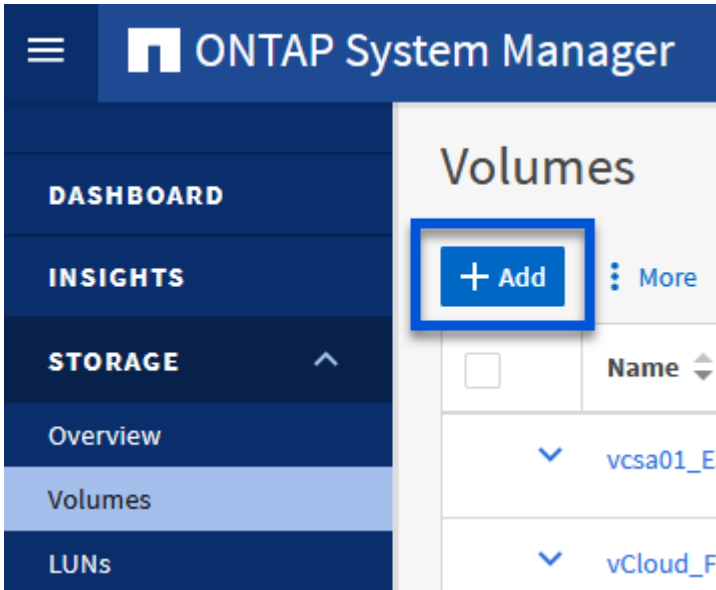
Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass die Exportrichtlinie das VCF-Managementnetzwerk umfasst, damit die Validierung fortgesetzt werden kann.

- Nachdem alle Regeln eingegeben wurden, klicken Sie auf die Schaltfläche **Speichern**, um die neue Exportrichtlinie zu speichern.
- Alternativ können Sie Richtlinien und Regeln für den Export in der ONTAP CLI erstellen. Weitere Informationen finden Sie in den Schritten zum Erstellen einer Exportrichtlinie und zum Hinzufügen von Regeln in der ONTAP-Dokumentation.
 - Verwenden Sie die ONTAP-CLI für "[Erstellen Sie eine Exportrichtlinie](#)".
 - Verwenden Sie die ONTAP-CLI für "[Fügen Sie eine Regel zu einer Exportrichtlinie hinzu](#)".

Erstellen Sie ein NFS-Volume

Erstellen Sie ein NFS-Volume auf dem ONTAP-Speichersystem, das als Datastore in der Workload-Domain-Bereitstellung verwendet werden soll.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher > Volumes** und klicken Sie auf **+Hinzufügen**, um ein neues Volume zu erstellen.



2. Fügen Sie einen Namen für das Volume hinzu, füllen Sie die gewünschte Kapazität aus und wählen Sie die Storage-VM aus, die das Volume hosten soll. Klicken Sie auf **Weitere Optionen**, um fortzufahren.

Add Volume



NAME

VCF_WKLD_01

CAPACITY

5



TiB



STORAGE VM

EHC_NFS



Export via NFS

More Options

Cancel


Save

3. Wählen Sie unter Zugriffsberechtigungen die Exportrichtlinie aus, die das VCF-Verwaltungsnetzwerk oder die IP-Adresse und die NFS-Netzwerk-IP-Adressen umfasst, die sowohl für die Validierung des NFS-Servers als auch für den NFS-Datenverkehr verwendet werden.

Access Permissions

Export via NFS

GRANT ACCESS TO HOST

default 

JetStream_NFS_v04
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01
3 rules

NFSmountTestReno01
Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols
Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv_VPN
Clients : 172.21.254.0/24 | Access protocols : Any

VCF_WKLD
2 rules

WKLD_DM01
2 rules

Wkld01_NFS
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.252.208

+



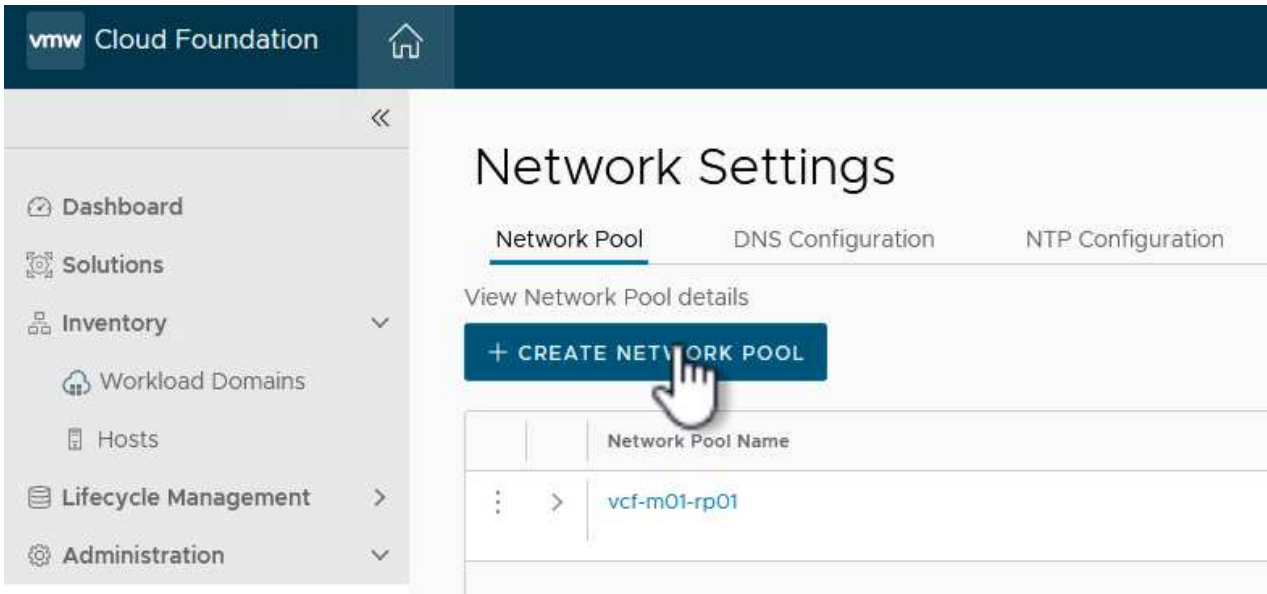
Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk zum NFS-Server routingfähig ist oder 2) eine LIF für das Managementnetzwerk zur SVM, die das NFS-Datastore-Volumen hostet, hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

1. Alternativ können ONTAP Volumes auch über die ONTAP CLI erstellt werden. Weitere Informationen finden Sie im ["lun erstellen"](#) In der Dokumentation zu ONTAP-Befehlen.

Netzwerkpool im SDDC Manager erstellen

Vor der Inbetriebnahme der ESXi-Hosts muss ein Arbeitspool im SDDC Manager erstellt werden, um sie in einer VI-Workload-Domäne bereitzustellen. Der Netzwerkpool muss die Netzwerkinformationen und IP-Adressbereiche für VMkernel-Adapter enthalten, die für die Kommunikation mit dem NFS-Server verwendet werden sollen.

1. Navigieren Sie von der SDDC Manager-Weboberfläche aus im linken Menü zu **Netzwerkeinstellungen** und klicken Sie auf die Schaltfläche **+ Netzwerkpool erstellen**.



2. Geben Sie einen Namen für den Netzwerkpool ein, aktivieren Sie das Kontrollkästchen für NFS, und geben Sie alle Netzwerkdetails ein. Wiederholen Sie dies für die vMotion Netzwerkinformationen.

vmw Cloud Foundation

Network Settings

Network Pool DNS Configuration NTP Configuration

Create Network Pool

Ensure that all required networks are selected based on their usage for workload domains.

Network Pool Name: NFS_NPOOL

Network Type: vSAN NFS iSCSI vMotion

NFS Network Information

VLAN ID	3374
MTU	9000
Network	172.21.118.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.118.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.118.145	To	172.21.118.148	REMOVE
xxx.xxx.xxx.xxx	To	xxx.xxx.xxx.xxx	ADD

vMotion Network Information

VLAN ID	3423
MTU	9000
Network	172.21.167.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.167.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.167.121	To	172.21.167.124	REMOVE
xxx.xxx.xxx.xxx	To	xxx.xxx.xxx.xxx	ADD

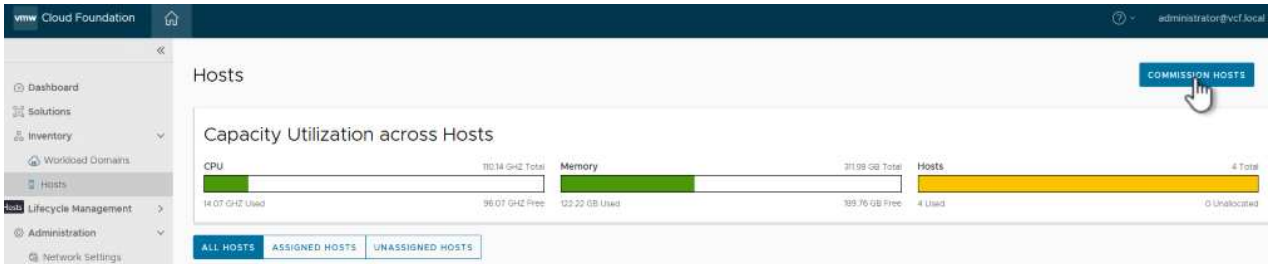
3. Klicken Sie auf die Schaltfläche **Speichern**, um die Erstellung des Netzwerkpools abzuschließen.

Provisionswirte

Bevor ESXi-Hosts als Workload-Domäne bereitgestellt werden können, müssen sie dem Bestand des SDDC-Managers hinzugefügt werden. Dazu gehören die Bereitstellung der erforderlichen Informationen, die bestehende Validierung und der Beginn des Inbetriebnahmeprozesses.

Weitere Informationen finden Sie unter "[Provisionswirte](#)" Im VCF-Administrationshandbuch.

1. Navigieren Sie von der SDDC-Manager-Oberfläche aus im linken Menü zu **Hosts** und klicken Sie auf die Schaltfläche **Provision Hosts**.



2. Die erste Seite ist eine Checkliste für Voraussetzungen. Markieren Sie alle Voraussetzungen, und aktivieren Sie alle Kontrollkästchen, um fortzufahren.

Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- Select All**
- Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- Host is configured with DNS server for forward and reverse lookup and FQDN.
- Hostname should be same as the FQDN.
- Management IP is configured to first NIC port.
- Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- Host hardware health status is healthy without any errors.
- All disk partitions on HDD / SSD are deleted.
- Ensure required network pool is created and available before host commissioning.
- Ensure hosts to be used for vSAN workload domain are associated with vSAN enabled network pool.
- Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED

3. Füllen Sie im Fenster **Host Addition and Validation** die Felder **Host FQDN**, **Storage Type**, **Network Pool** aus, die die für die Workload-Domain zu verwendenden vMotion- und NFS-Speicher-IP-Adressen sowie die Anmeldeinformationen für den Zugriff auf den ESXi-Host enthalten. Klicken Sie auf **Add**, um den Host zur Gruppe der zu validierenden Hosts hinzuzufügen.

1 Host Addition and Validation

2 Review

Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

Add new Import

Host FQDN

Storage Type vSAN NFS VMFS on FC vVol

Network Pool Name

User Name

Password

ADD

Hosts Added

Hosts added successfully. Add more or confirm fingerprint and validate host

REMOVE

Confirm all Finger Prints

VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01	172.21.166.135	<input checked="" type="checkbox"/> SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVdp6v EGM	<input type="checkbox"/> Not Validated

1 hosts

CANCEL

NEXT

4. Wenn alle zu validierenden Hosts hinzugefügt wurden, klicken Sie auf die Schaltfläche **Alle validieren**, um fortzufahren.

5. Wenn alle Hosts validiert sind, klicken Sie auf **Weiter**, um fortzufahren.

Hosts Added

✔ Host Validated Successfully. ✕

REMOVE Confirm all Finger Prints (i) VALIDATE ALL

<input checked="" type="checkbox"/>	⋮	FGDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01 (i)	172.21.166.138	✔ SHA256:9Kg+9 nQaE4SQkOMs QPON/ k5gZB9zyKN+6 CBPmXsvLBc	✔ Valid
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01 (i)	172.21.166.137	✔ SHA256:nPX4/ mei/ 2zmLJHfmPwbk 6zhapoUxV2IO wZDPFH+z0	✔ Valid
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01 (i)	172.21.166.136	✔ SHA256:AMhyR 60OpTQ1YYq0 DJhqVbj/M/ GvrQaqUy7Ce+ M4IWY	✔ Valid
<input checked="" type="checkbox"/>	⋮	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 (i)	172.21.166.135	✔ SHA256:CKbsinf EOG+ +z/ lpFUoFDI2tLuY FZ47WicVDp6v EQM	✔ Valid

CANCEL NEXT

- Überprüfen Sie die Liste der Hosts, die beauftragt werden sollen, und klicken Sie auf die Schaltfläche **Provision**, um den Prozess zu starten. Überwachen Sie den Inbetriebnahmeprozess im SDDC-Manager im Aufgabenbereich.

Commission Hosts

1 Host Addition and Validation

2 **Review**

Review

Skip failed hosts during commissioning  On

Validated Host(s)	
vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

CANCEL

BACK

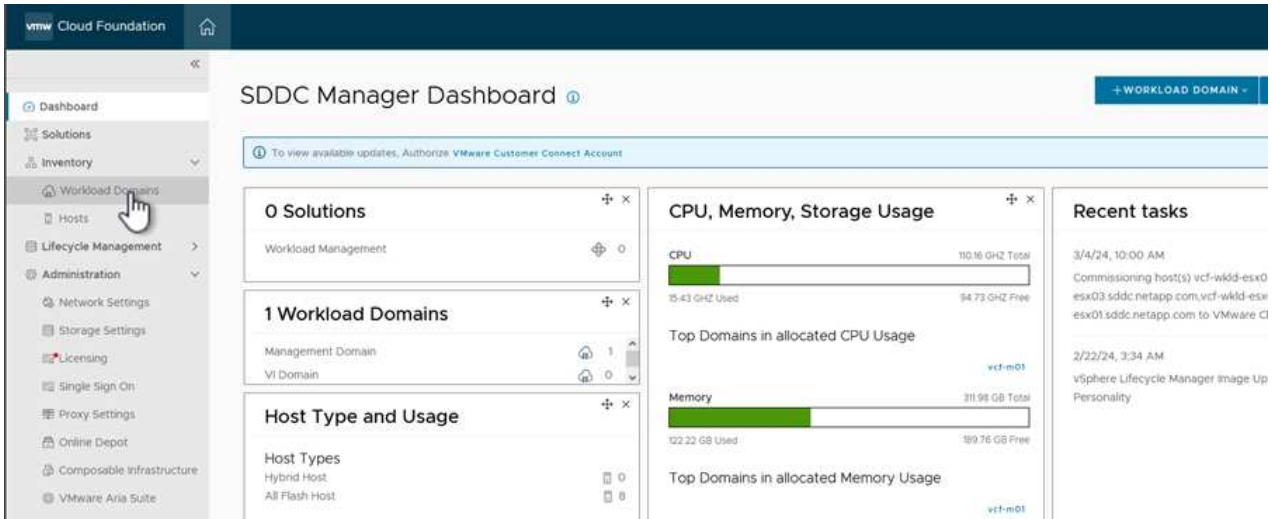
COMMISSION

Implementieren Sie VI Workload Domain

Die Implementierung von VI-Workload-Domänen erfolgt über die Schnittstelle des VCF Cloud Manager. Hier werden nur die Schritte in Bezug auf die Speicherkonfiguration dargestellt.

Schritt-für-Schritt-Anweisungen zur Bereitstellung einer VI-Workload-Domäne finden Sie unter "[Stellen Sie eine VI-Workload-Domäne über die SDDC Manager-Benutzeroberfläche bereit](#)".

1. Klicken Sie im SDDC Manager Dashboard auf **+ Workload Domain** in der oberen rechten Ecke, um eine neue Workload Domain zu erstellen.



2. Füllen Sie im VI Configuration Wizard die Abschnitte für **Allgemeine Informationen**, **Cluster**, **Datenverarbeitung**, **Netzwerk** und **Host Selection** nach Bedarf aus.

Informationen zum Ausfüllen der im VI-Konfigurationsassistenten erforderlichen Informationen finden Sie unter "[Stellen Sie eine VI-Workload-Domäne über die SDDC Manager-Benutzeroberfläche bereit](#)".

VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

7 Switch Configuration

8 License

9 Review

+

1. Füllen Sie im Abschnitt NFS-Storage den Datenspeichernamen, den Ordner-Bereitstellungspunkt des NFS-Volume und die IP-Adresse der logischen Schnittstelle des ONTAP NFS-Storage VM aus.

The screenshot shows the VI Configuration Wizard with the 'NFS Storage' step selected. The configuration details are as follows:

NFS Storage	
NFS Share Details	
Datastore Name ⓘ	VCF_WKLD_01
Folder ⓘ	/VCF_WKLD_01
NFS Server IP Address ⓘ	172.21.118.163

2. Führen Sie im VI Configuration Wizard die Schritte Switch Configuration und License aus, und klicken Sie dann auf **Finish**, um die Erstellung der Workload Domain zu starten.

VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage
- 7 Switch Configuration
- 8 License
- 9 Review

Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxc101.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL
BACK
FINISH

3. Überwachen Sie den Prozess und beheben Sie alle während des Prozesses auftretenden Validierungsprobleme.

Installation des NetApp NFS Plug-ins für VMware VAAI

Das NetApp-NFS-Plug-in für VMware VAAI integriert die auf dem ESXi-Host installierten VMware Virtual Disk Libraries und bietet höhere Performance-Klonvorgänge, die schneller abgeschlossen werden können. Dies wird empfohlen, wenn Sie ONTAP Storage-Systeme mit VMware vSphere verwenden.

Schritt-für-Schritt-Anweisungen zum Bereitstellen des NetApp-NFS-Plug-ins für VMware VAAI finden Sie unter "[Installation des NetApp NFS Plug-ins für VMware VAAI](#)".

Video-Demo für diese Lösung

[NFS-Datenspeicher als Principal Storage für VCF Workload Domains](#)

Konfigurieren Sie zusätzlichen Storage (NFS und VVols) für VCF-Workload-Domänen mit den ONTAP-Tools

In diesem Szenario zeigen wir, wie ONTAP Tools für VMware vSphere implementiert und verwendet werden, um sowohl einen **NFS Datastore** als auch einen **VVols Datastore** für eine VCF Workload-Domäne zu konfigurieren.

NFS wird als Storage-Protokoll für den VVols Datastore verwendet.

Autor: Josh Powell, Ravi BCB

Szenarioübersicht

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für NFS-Traffic erstellen.
- Erstellen Sie eine verteilte Portgruppe für das NFS-Netzwerk in der VI-Workload-Domäne.
- Erstellen Sie auf den ESXi Hosts für die VI-Workload-Domäne einen VMkernel-Adapter für NFS.
- Implementieren Sie ONTAP Tools in der VI-Workload-Domäne.
- Erstellen Sie einen neuen NFS-Datenspeicher in der VI-Workload-Domäne.
- Erstellen Sie einen neuen VVols-Datstore auf der VI-Workload-Domäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.

NetApp empfiehlt ein redundantes Netzwerkdesign für NFS und liefert Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Je nach den Architektur Anforderungen ist es üblich, NFS mit einem einzigen oder mehreren Subnetzen bereitzustellen.

Siehe "[Best Practices für die Ausführung von NFS mit VMware vSphere](#)" Für detaillierte Informationen speziell zu VMware vSphere.

Eine Anleitung zum Netzwerk mit ONTAP mit VMware vSphere finden Sie im "[Netzwerkconfiguration – NFS](#)" Der Dokumentation zu NetApp Enterprise-Applikationen.

In dieser Dokumentation wird der Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adresseninformationen für die Erstellung mehrerer LIFs für NFS-Traffic demonstriert. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter "[LIF erstellen \(Netzwerkschnittstelle\)](#)".

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools zu implementieren und damit einen VVols und NFS Datastore in der VCF-Managementdomäne zu erstellen:

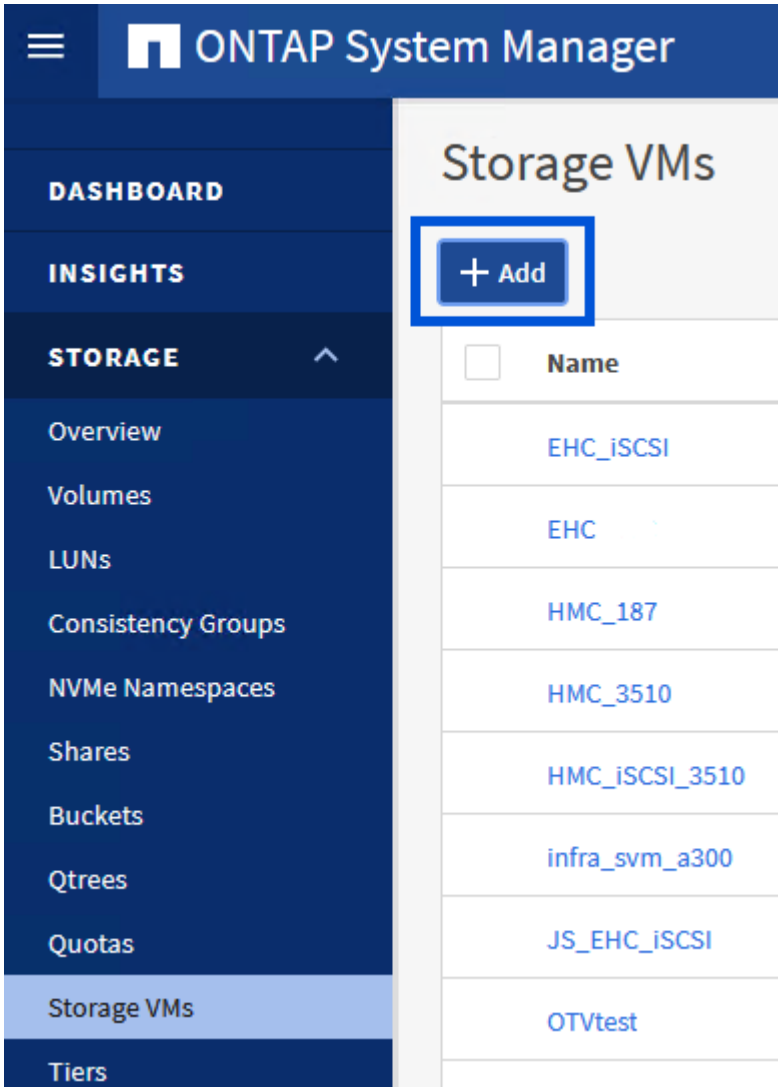
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

Storage-VM und LIFs erstellen

Führen Sie die folgenden Schritte aus, um eine SVM sowie mehrere LIFs für NFS-Datenverkehr zu erstellen.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf **+ Hinzufügen**, um zu starten.



2. Im **Add Storage VM** Wizard geben Sie einen **Namen** für die SVM an, wählen Sie den **IP Space** aus und klicken dann unter **Access Protocol** auf die Registerkarte **SMB/CIFS, NFS, S3** und aktivieren Sie das Kontrollkästchen **enable NFS**.

Add Storage VM



STORAGE VM NAME

VCF_NFS

IPSPACE

Default


Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC NVMe

Enable SMB/CIFS

Enable NFS

Allow NFS client access

 Add at least one rule to allow NFS clients to access volumes in this storage VM. [?](#)

EXPORT POLICY

Default

Enable S3

DEFAULT LANGUAGE [?](#)

c.utf_8



Es ist nicht notwendig, hier die Schaltfläche **NFS-Client-Zugriff zulassen** zu aktivieren, da ONTAP-Tools für VMware vSphere zur Automatisierung des Datastore-Bereitstellungsprozesses verwendet werden. Dazu gehört auch die Bereitstellung des Client-Zugriffs für die ESXi-Hosts.

3. Geben Sie im Abschnitt **Network Interface** die **IP-Adresse**, **Subnetzmaske** und **Broadcast Domain und Port** für die erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert sein, um allgemeine Einstellungen für alle verbleibenden LIFs zu verwenden oder separate Einstellungen zu verwenden.

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

Use the same subnet mask, gateway, and broadcast domain for all of the following interfaces

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

4. Wählen Sie aus, ob das Storage VM Administration-Konto aktiviert werden soll (für mandantenfähige Umgebungen), und klicken Sie auf **Speichern**, um die SVM zu erstellen.

Storage VM Administration

Manage administrator account

Save

Cancel

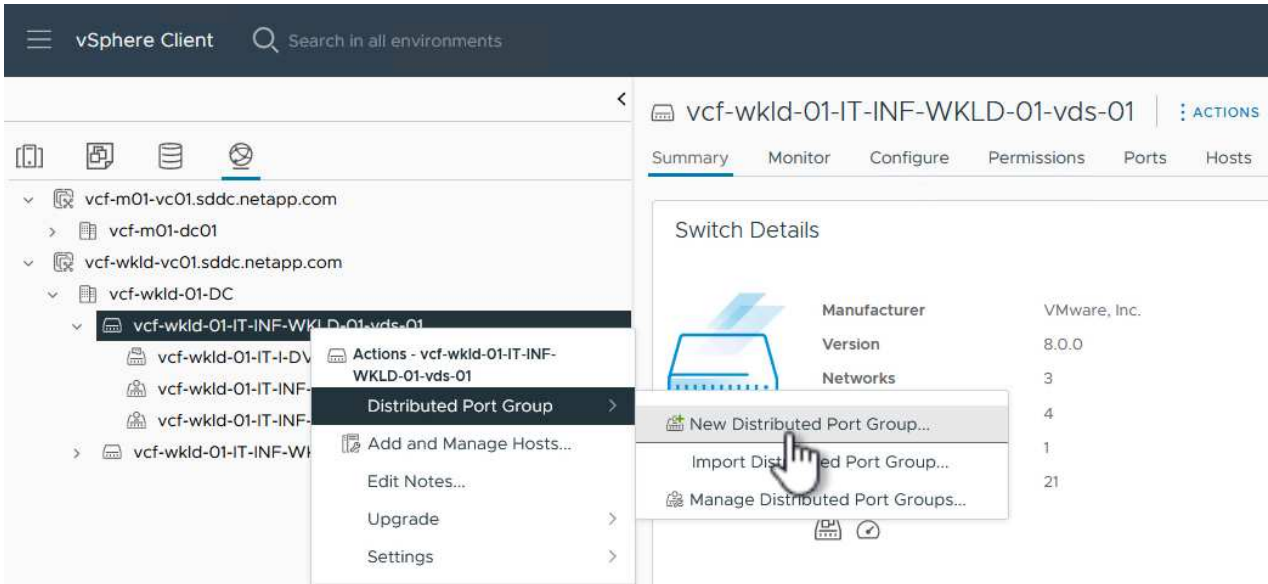
Richten Sie das Netzwerk für NFS auf ESXi-Hosts ein

Die folgenden Schritte werden für den VI Workload Domain Cluster mithilfe des vSphere Clients durchgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client in der Management- und Workload-Domäne einheitlich ist.

Erstellen Sie eine verteilte Portgruppe für NFS-Datenverkehr

Gehen Sie wie folgt vor, um eine neue verteilte Portgruppe für das Netzwerk zu erstellen, die NFS-Datenverkehr übertragen soll:

1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workload-Domäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen von **New Distributed Port Group...** aus.



2. Geben Sie im Assistenten **New Distributed Port Group** einen Namen für die neue Portgruppe ein und klicken Sie auf **Next**, um fortzufahren.
3. Füllen Sie auf der Seite **Configure settings** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige VLAN-ID angeben. Klicken Sie auf **Weiter**, um fortzufahren.

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

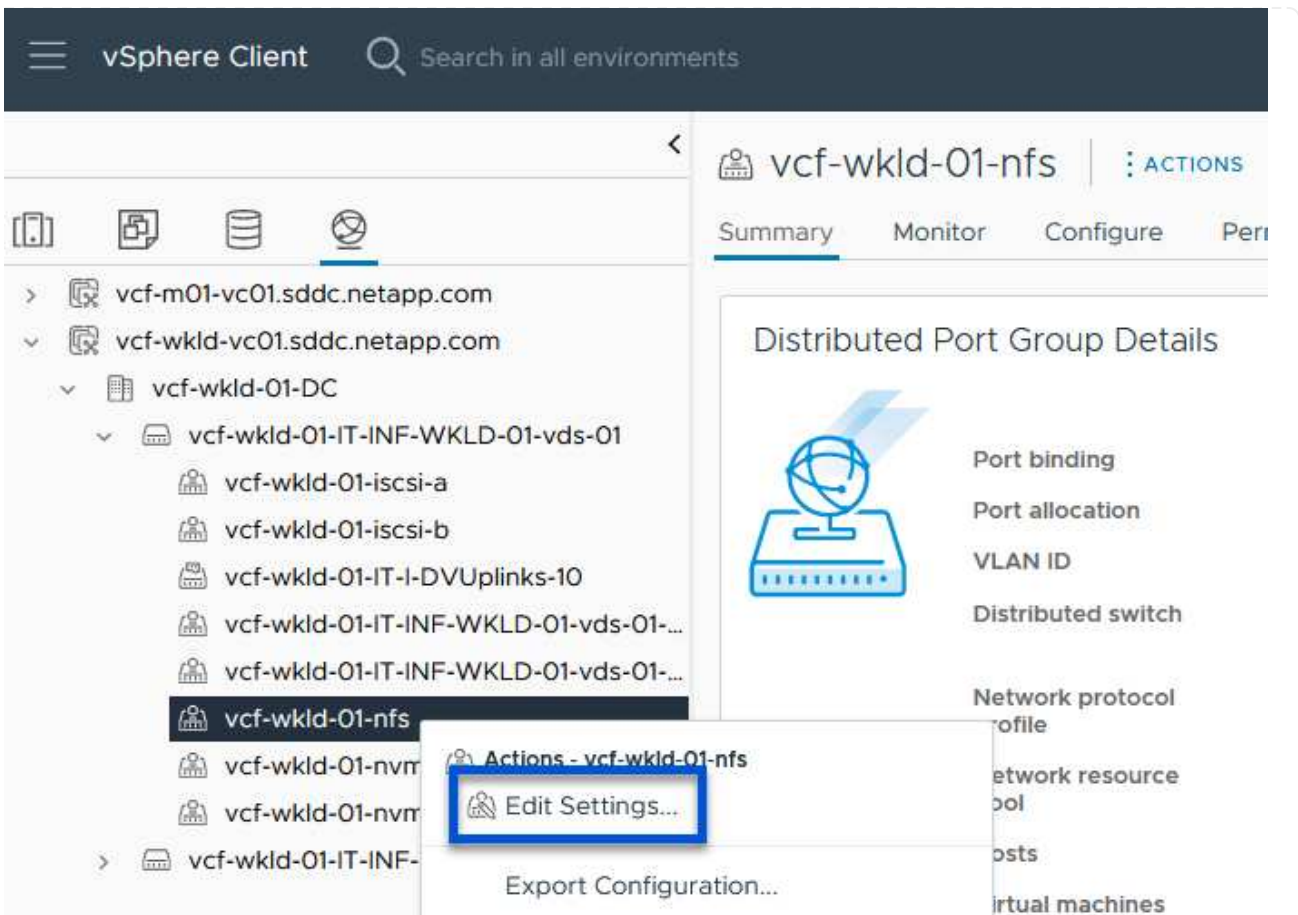
Port binding	Static binding
Port allocation	Elastic ?
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Nachdem die Portgruppe erstellt wurde, navigieren Sie zur Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.



6. Navigieren Sie auf der Seite **Distributed Port Group - Einstellungen bearbeiten** im linken Menü zu **Teaming und Failover**. Aktivieren Sie Teaming für die Uplinks, die für NFS-Verkehr verwendet werden sollen, indem Sie sicherstellen, dass sie sich im Bereich **Active Uplinks** befinden. Verschieben Sie alle nicht verwendeten Uplinks nach unten zu **unused Uplinks**.

Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 

MOVE UP MOVE DOWN

Active uplinks

 uplink2

 uplink1

Standby uplinks

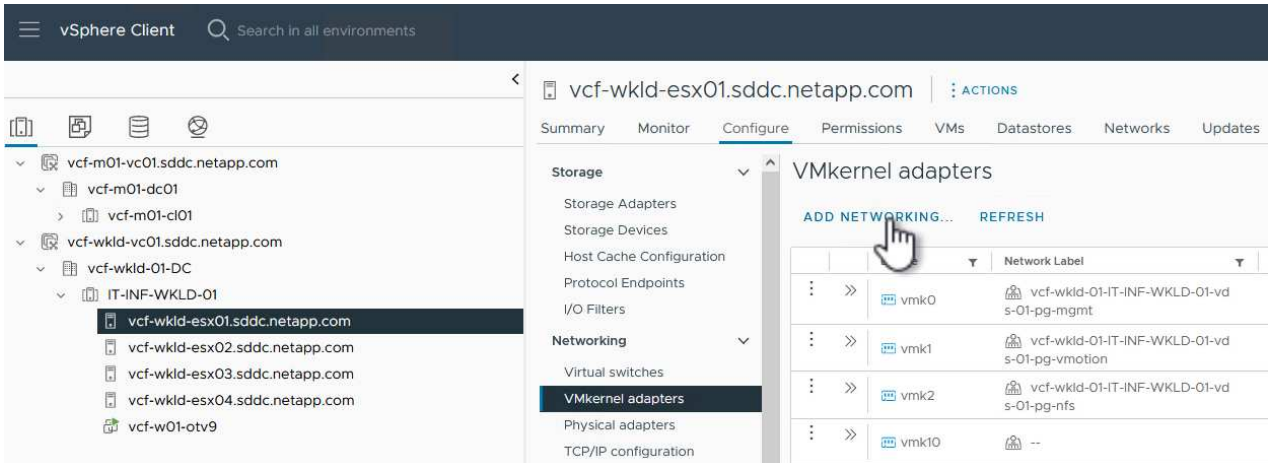
Unused uplinks

7. Wiederholen Sie diesen Vorgang für jeden ESXi-Host im Cluster.

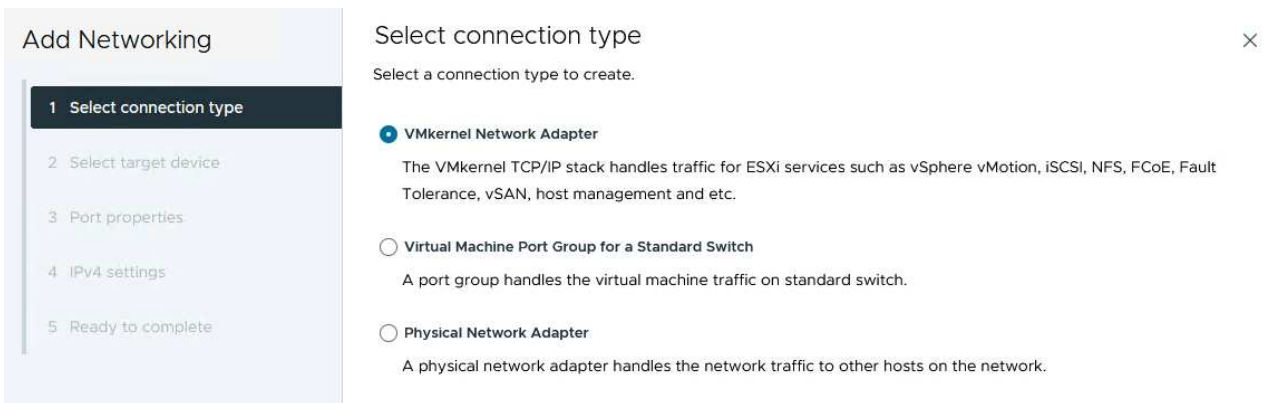
Erstellen Sie auf jedem ESXi-Host einen VMkernel-Adapter

Wiederholen Sie diesen Vorgang auf jedem ESXi-Host in der Workload-Domäne.

1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts in der Workload-Domäneninventarisierung. Wählen Sie auf der Registerkarte **Configure VMkernel Adapter** und klicken Sie auf **Add Networking...**, um zu starten.



2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für NFS aus.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

- Select an existing network
- Select an existing standard switch
- New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 8 items

CANCEL

BACK

NEXT

4. Behalten Sie auf der Seite **Port Properties** die Standardeinstellungen (keine aktivierten Dienste) bei und klicken Sie auf **Weiter**, um fortzufahren.
5. Geben Sie auf der Seite **IPv4 settings** die **IP-Adresse**, **Subnetzmaske** ein, und geben Sie eine neue Gateway-IP-Adresse ein (nur bei Bedarf). Klicken Sie auf **Weiter**, um fortzufahren.

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

- Obtain IPv4 settings automatically
- Use static IPv4 settings

IPv4 address 172.21.118.145

Subnet mask 255.255.255.0

Default gateway Override default gateway for this adapter

172.21.166.1

DNS server addresses 10.61.185.231

CANCEL

BACK

NEXT

6. Überprüfen Sie Ihre Auswahl auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um den VMkernel-Adapter zu erstellen.

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- Ready to complete**

Ready to complete ✕

Review your selections before finishing the wizard

▼ **Select target device**

Distributed port group	vcf-wkld-01-nfs
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ **Port properties**

New port group	vcf-wkld-01-nfs (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled

[CANCEL](#) [BACK](#) [FINISH](#)

Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools

Die folgenden Schritte werden auf dem VCF-Management-Domänencluster mithilfe des vSphere-Clients durchgeführt. Dazu gehören die Implementierung von OTV, die Erstellung eines VVols NFS-Datastore und die Migration von Management-VMs auf den neuen Datastore.

Für VI-Workload-Domänen wird OTV im VCF Management Cluster installiert, aber bei dem vCenter registriert, das der VI-Workload-Domäne zugeordnet ist.

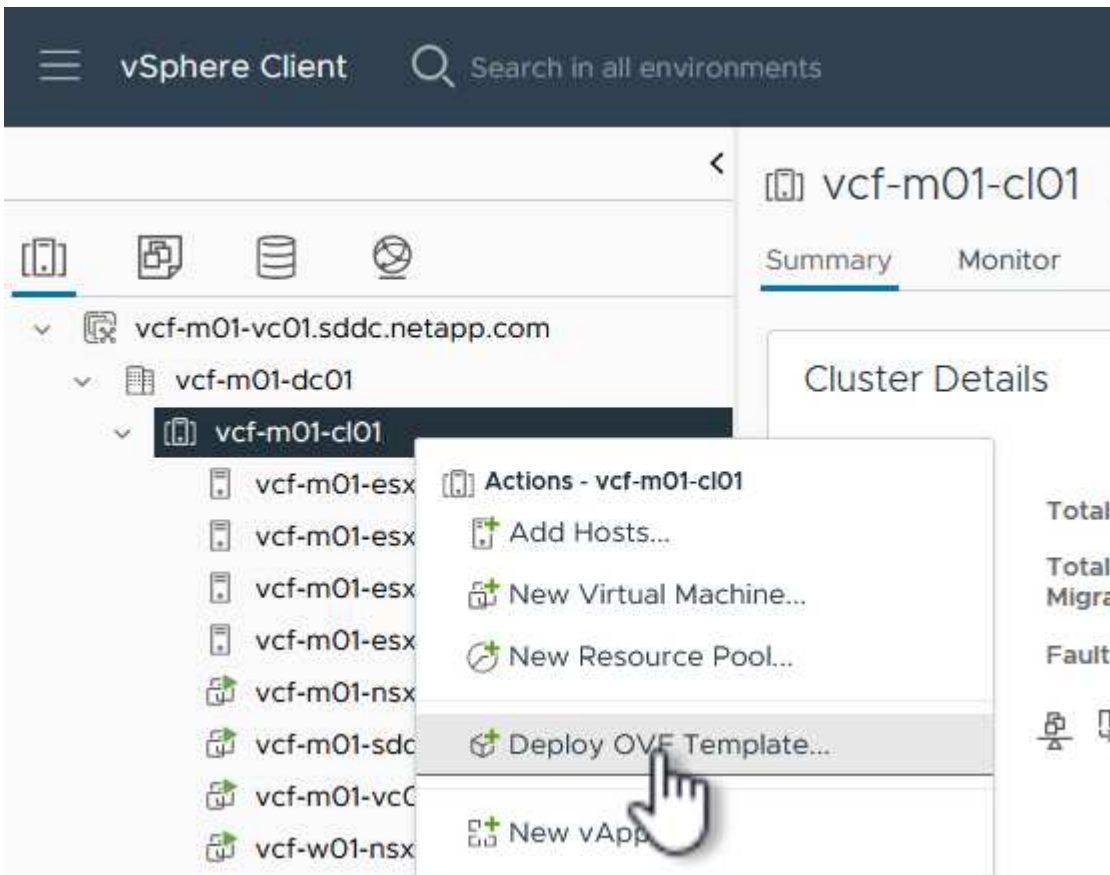
Weitere Informationen zum Implementieren und Verwenden von ONTAP Tools in einer Umgebung mit mehreren vCenter finden Sie unter ["Voraussetzungen für die Registrierung von ONTAP-Tools in einer Umgebung mit mehreren vCenter-Servern"](#).

Implementieren Sie ONTAP-Tools für VMware vSphere

ONTAP Tools für VMware vSphere (OTV) werden als VM-Appliance implementiert und verfügen über eine integrierte vCenter-Benutzeroberfläche zum Management von ONTAP Storage.

Füllen Sie die folgenden Schritte aus, um ONTAP Tools für VMware vSphere zu implementieren:

1. Rufen Sie das OVA-Image der ONTAP-Tools auf "[NetApp Support Website](#)" Und in einen lokalen Ordner herunterladen.
2. Melden Sie sich bei der vCenter Appliance für die VCF-Managementdomäne an.
3. Klicken Sie in der vCenter-Appliance-Oberfläche mit der rechten Maustaste auf den Management-Cluster und wählen Sie **Deploy OVF Template...** aus



4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei für ONTAP-Tools aus.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

URL

Local file

netapp-ontap-tools-for-vmware-vsphere-9.13-9554.ova

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie für den Speicherort der Konfigurations- und Festplattendateien den vSAN Datastore des VCF Management Domain Clusters aus.

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

Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

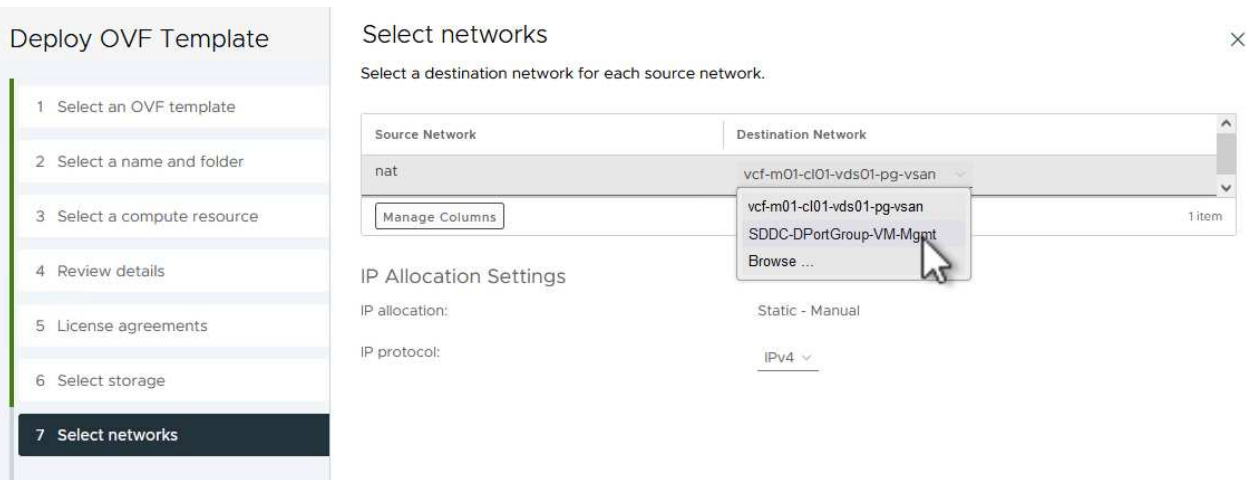
VM Storage Policy

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 5 items

7. Wählen Sie auf der Seite Netzwerk auswählen das Netzwerk aus, das für den Verwaltungsdatenverkehr verwendet wird.



8. Geben Sie auf der Seite Vorlage anpassen alle erforderlichen Informationen ein:

- Passwort für administrativen Zugriff auf OTV.
- NTP-Server-IP-Adresse.
- Passwort für das OTV-Wartungskonto.
- OTV Derby DB-Kennwort.
- Aktivieren Sie nicht das Kontrollkästchen, um VMware Cloud Foundation (VCF)* zu aktivieren. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
- FQDN oder IP-Adresse der vCenter-Appliance für die **VI Workload Domain**
- Zugangsdaten für die vCenter-Appliance der **VI Workload Domain**
- Geben Sie die erforderlichen Felder für Netzwerkeigenschaften an.

Klicken Sie auf **Weiter**, um fortzufahren.

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

Customize template

Customize the deployment properties of this software solution.

! 2 properties have invalid values X

System Configuration		4 settings
Application User Password (*)	Password to assign to the administrator account. 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.	
	Password 👁
	Confirm Password 👁
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1	
Maintenance User Password (*)	Password to assign to maint user account.	
	Password 👁
	Confirm Password 👁

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

Customize template

! 2 properties have invalid values X

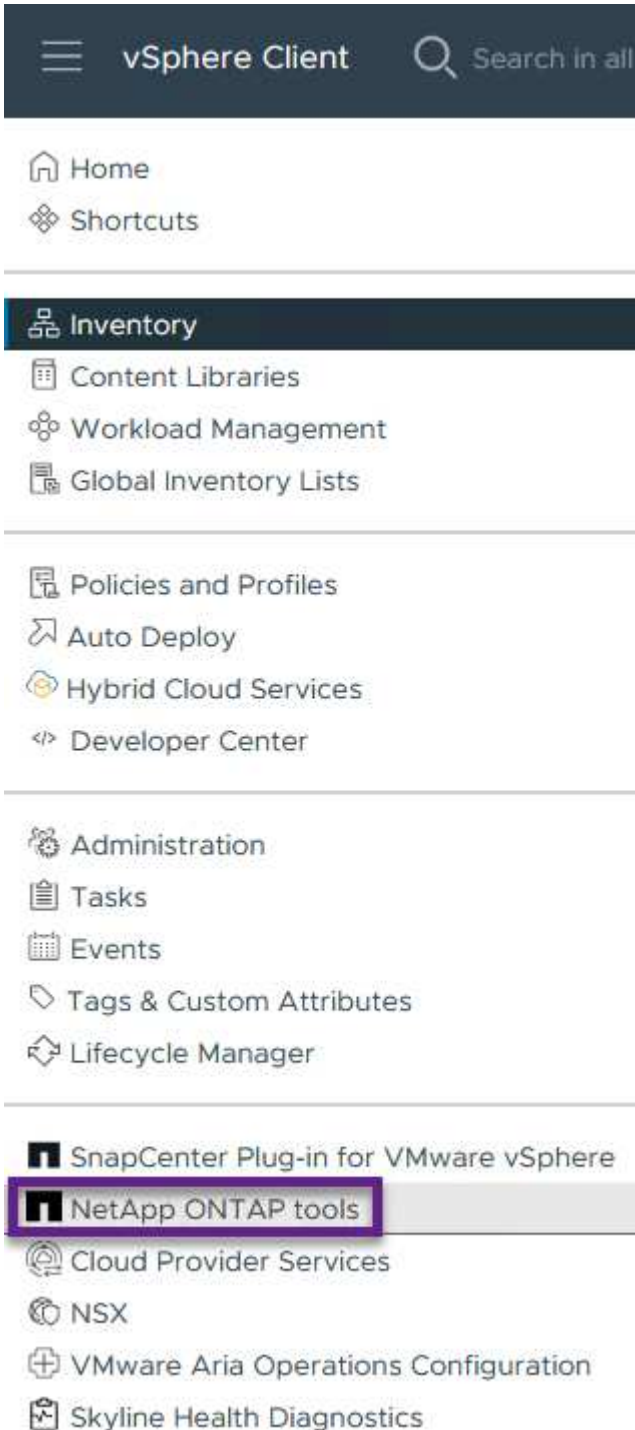
Configure vCenter or Enable vCenter		3 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
Port (*)	Specify the HTTPS port of an existing vCenter to register to. 443	
Username (*)	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
Password (*)	Specify the password of an existing vCenter to register to.	
	Password 👁
	Confirm Password 👁
Network Properties		8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL BACK NEXT

9. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der OTV-Appliance zu beginnen.

Fügen Sie ONTAP Tools ein Storage-System hinzu.

1. Greifen Sie auf die NetApp ONTAP-Tools zu, indem Sie sie im Hauptmenü des vSphere-Clients auswählen.



2. Wählen Sie aus dem Dropdown-Menü **INSTANCE** in der Benutzeroberfläche des ONTAP-Tools die OTV-Instanz aus, die der zu verwaltenden Workload-Domain zugeordnet ist.

NetApp ONTAP tools **INSTANCE 172.21.166.139:8443** ▾

Plugin Instance	Version	vCenter Server
172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com

Overview
Storage Systems
Storage capability profile
Storage Mapping
Settings

provide

3. Wählen Sie in den ONTAP-Tools im linken Menü **Speichersysteme** aus, und drücken Sie dann **Hinzufügen**.


NetApp ONTAP tools **INSTANCE 172.21.166.149:8443** ▾


Overview
Storage Systems
Storage capability profile

ADD **REDISCOVER ALL**

4. Geben Sie die IP-Adresse, die Anmeldeinformationen des Speichersystems und die Portnummer ein. Klicken Sie auf **Add**, um den Ermittlungsvorgang zu starten.

Add Storage System

 Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.


vCenter server vcf-m01-vc01.sddc.netapp.com 

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options 

ONTAP Cluster Certificate: Automatically fetch Manually upload

CANCEL

SAVE & ADD MORE

ADD

Erstellen Sie einen NFS-Datstore in ONTAP-Tools

Gehen Sie wie folgt vor, um einen auf NFS ausgeführten ONTAP Datstore mit ONTAP-Tools zu implementieren.

1. Wählen Sie in den ONTAP-Tools **Übersicht** und klicken Sie im Register **erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.

NetApp ONTAP tools INSTANCE 172.21.166.149:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

Reports

- ▼ Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report
- Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi

Add Storage System Provision Datstore

Add storage systems to ONTAP tools for VMware vSphere. Create traditional or vVols datastores.

ADD PROVISION

2. Wählen Sie auf der Seite **Allgemein** des Assistenten für neue Datenspeicher das vSphere Datacenter- oder Cluster-Ziel aus. Wählen Sie **NFS** als Datenspeichertyp aus, geben Sie einen Namen für den Datstore ein und wählen Sie das Protokoll aus. Legen Sie fest, ob Sie FlexGroup Volumes verwenden und ob Sie eine Storage-Funktionsdatei für die Bereitstellung verwenden möchten. Klicken Sie auf **Weiter**, um fortzufahren.

Hinweis: Durch Auswahl von **Verteilung der Datastore-Daten über den Cluster** wird das zugrunde liegende Volume als FlexGroup Volume erstellt, was die Verwendung von Storage Capability Profiles ausschließt. Siehe "[Unterstützte und nicht unterstützte Konfigurationen für FlexGroup Volumes](#)"
Weitere Informationen zur Verwendung von FlexGroup Volumes

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision. ②

Provisioning destination: vcf-wkld-01-DC [BROWSE](#)

Type: NFS VMFS vVols

Name: VCF_WKLD_05_NFS

Size: 2 TB

Protocol: NFS 3 NFS 4.1

Distribute datastore data across the ONTAP cluster.

Use storage capability profile for provisioning

[Advanced options >](#)

[CANCEL](#)

[NEXT](#)

3. Wählen Sie auf der Seite **Storage System** das Speicherfähigkeitsprofil, das Speichersystem und die SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profile: Platinum_AFF_A

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF_NFS

4. Wählen Sie auf der Seite **Speicherattribute** das zu verwendende Aggregat aus und klicken Sie dann auf **Weiter**, um fortzufahren.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Aggregate: EHCAGgr02 - (25350.17 GB Free)

Volumes: Automatically creates a new volume.

[Advanced options >](#)

5. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um mit der

Erstellung des NFS-Datostores zu beginnen.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary**

Summary

General

vCenter server:	vcf-wkld-vc01.sddc.netapp.com
Provisioning destination:	vcf-wkld-01-DC
Datastore name:	VCF_WKLD_05_NFS
Datastore size:	2 TB
Datastore type:	NFS
Protocol:	NFS 3
Datastore cluster:	None
Storage capability profile:	Platinum_AFF_A

Storage system details

Storage system:	ntaphci-a300e9u25
SVM:	VCF_NFS

Storage attributes

Aggregate:	FHCAsqr02
------------	-----------

CANCEL

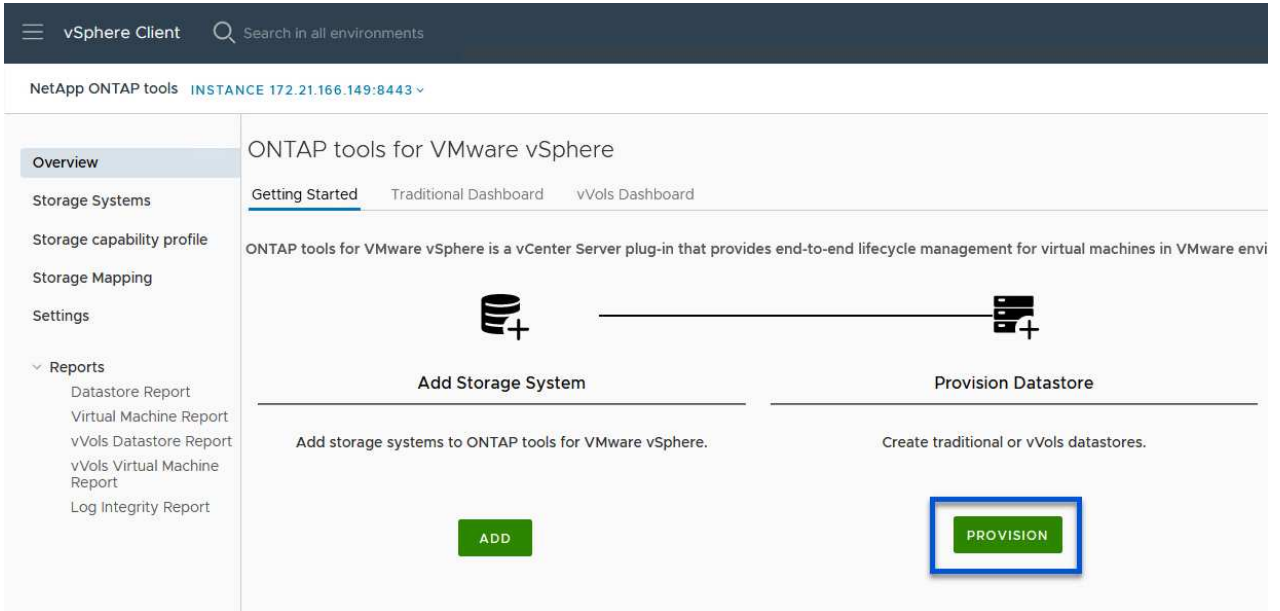
BACK

FINISH

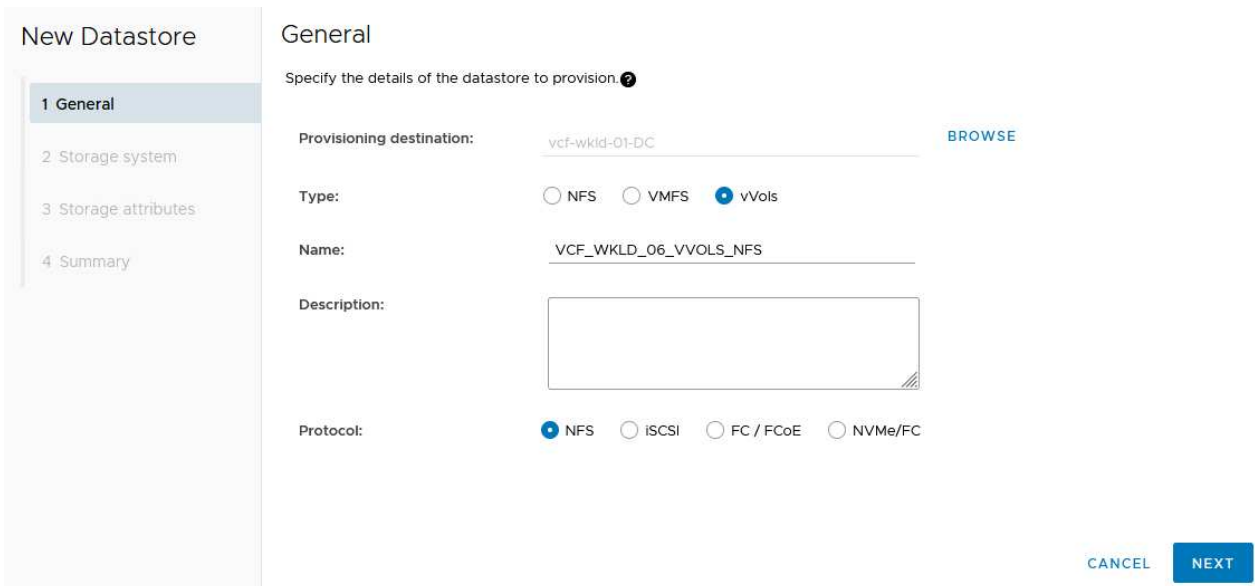
Erstellen Sie einen VVols-Datstore in ONTAP Tools

Führen Sie die folgenden Schritte aus, um einen VVols-Datstore in ONTAP Tools zu erstellen:

1. Wählen Sie in den ONTAP-Tools **Übersicht** und klicken Sie im Register **erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.



2. Wählen Sie auf der Seite **Allgemein** des Assistenten für neue Datenspeicher das vSphere Datacenter- oder Cluster-Ziel aus. Wählen Sie als Datstore-Typ **VVols** aus, geben Sie einen Namen für den Datstore ein und wählen Sie als Protokoll **NFS** aus. Klicken Sie auf **Weiter**, um fortzufahren.



3. Wählen Sie auf der Seite **Storage System** das Speicherfähigkeitsprofil, das Speichersystem und die SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

Specify the storage capability profiles and the storage system you want to use.

Storage capability profile:	Platinum_AFF_A	▼
Storage system:	ntaphci-a300e9u25 (172.16.9.25)	▼
Storage VM:	VCF_NFS	▼

4. Wählen Sie auf der Seite **Speicherattribute** aus, um ein neues Volume für den Datenspeicher zu erstellen und die Speicherattribute des zu erstellenden Volumes auszufüllen. Klicken Sie auf **Add**, um das Volume zu erstellen, und dann auf **Next**, um fortzufahren.

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vvc	2000	Platinum_AFF_A	EHCaggr02 - (25404 GB I	Thin

ADD

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: Create new volumes Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCaggr02

1 - 1 of 1 Item

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
		Platinum_AFF_A	EHCaggr02 - (25407.15 G	Thin

ADD

Default storage capability profile: Platinum_AFF_A

CANCEL

BACK

NEXT

5. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um den vVol Datastore-Erstellungsprozess zu starten.

New Datastore

- 1 General
- 2 Storage system
- 3 Storage attributes
- 4 Summary

Summary

General

vCenter server: vcf-wkld-vc01.sddc.netapp.com

Provisioning destination: vcf-wkld-01-DC

Datastore name: VCF_WKLD_06_VVOLS_NFS

Datastore type: vVols

Protocol: NFS

Storage capability profile: Platinum_AFF_A

Storage system details

Storage system: ntaphci-a300e9u25

SVM: EHC_NFS

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

Weitere Informationen

Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

Informationen zum Konfigurieren von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation"](#).

Migration von VMs

Migrieren Sie VMs zu ONTAP Datastores

Autor: Suresh Thoppay

VMware vSphere von Broadcom unterstützt VMFS-, NFS- und vVol-Datstores zum Hosten von Virtual Machines. Kunden haben die Möglichkeit, diese Datastores mit hyperkonvergenten Infrastrukturen oder zentralisierten Shared-Storage-Systemen zu erstellen. Kunden sehen häufig den Nutzen, wenn sie auf ONTAP-basierten Storage-Systemen hosten, um platzsparende Snapshots und Klone von virtuellen Maschinen bereitzustellen, Flexibilität bei der Auswahl verschiedener Implementierungsmodelle in den Rechenzentren und Clouds, betriebliche Effizienz durch Überwachungs- und Warnungswerkzeuge, Sicherheit, Governance und optionale Compliance-Tools zur Prüfung von VM-Daten, usw.

VMs, die auf ONTAP Datastores gehostet werden, können mit dem SnapCenter Plug-in für VMware vSphere (SCV) gesichert werden. SCV erstellt speicherbasierte Snapshots und repliziert auch auf ONTAP Remote-Speichersystem. Wiederherstellungen können entweder auf primären oder sekundären Storage-Systemen durchgeführt werden.

Kunden können zwischen Cloud Insights und Aria Operations oder einer Kombination aus Tools von beiden oder anderen Anbietern wählen, die die ONTAP API für Fehlerbehebung, Performance-Überwachung, Berichterstellung und Alarmbenachrichtigungen verwenden.

Kunden können Datenspeicher mit dem vCenter Plug-in der ONTAP Tools einfach bereitstellen. Ihre APIs und VMs können zu ONTAP Datastores migriert werden, während dieses aktiviert ist.



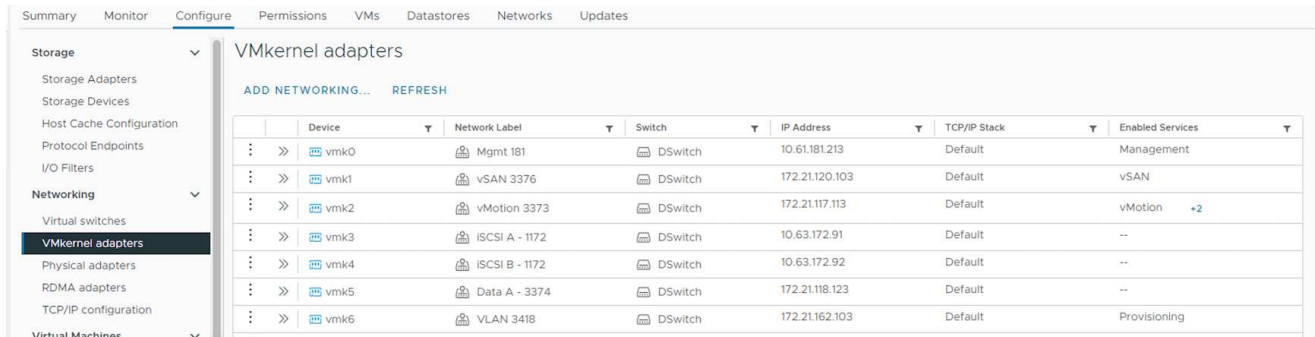
Einige VMs, die mit externen Managementtools wie Aria Automation, Tanzu (oder anderen Kubernetes-Varianten) implementiert werden, sind in der Regel von der VM-Storage-Richtlinie abhängig. Wenn eine Migration zwischen Datenspeichern innerhalb derselben VM-Storage-Richtlinie durchgeführt werden sollte, sollte dies die Auswirkungen für Applikationen verringern. Wenden Sie sich an Applikationseigentümer, um diese VMs ordnungsgemäß zu einem neuen Datenspeicher zu migrieren. VSphere 8 eingeführt "[VMotion Benachrichtigung](#)" Um die Anwendung für vMotion vorzubereiten.

Netzwerkanforderungen

VM-Migration mit vMotion

Es wird angenommen, dass ein duales Storage-Netzwerk für den ONTAP Datastore bereits vorhanden ist, um Konnektivität, Fehlertoleranz und Performance-Steigerung zu ermöglichen.

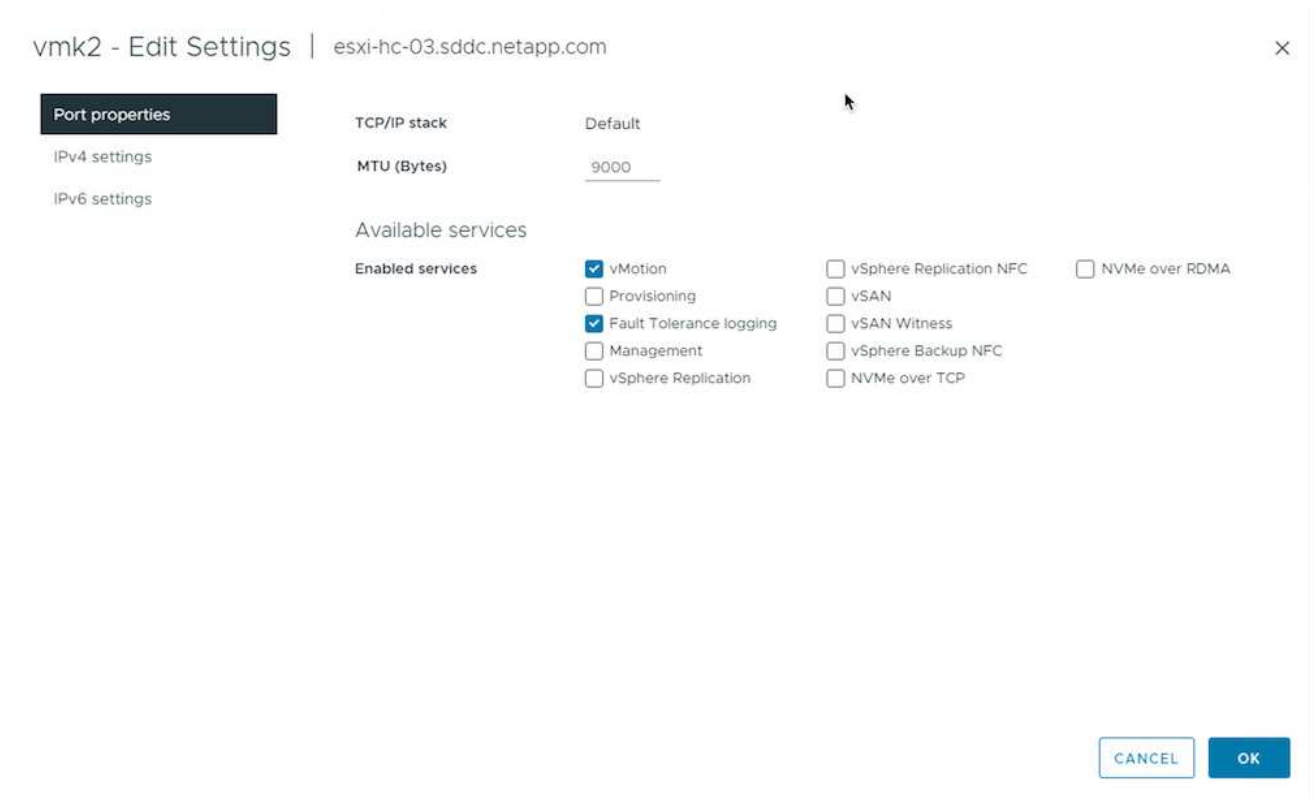
Die Migration von VMs auf vSphere Hosts erfolgt ebenfalls über die VMkernel Schnittstelle des vSphere Hosts. Für die Migration bei laufendem Betrieb (auf VMs) wird eine VMkernel-Schnittstelle mit aktiviertem vMotion Service verwendet, und für kalte Migration (über die VMs abgeschaltet) wird die VMkernel-Schnittstelle mit aktiviertem Provisioning-Service verwendet, um die Daten zu verschieben. Wenn keine gültige Schnittstelle gefunden wurde, verschiebt das Unternehmen die Daten über die Managementoberfläche, die für bestimmte Anwendungsfälle nicht wünschenswert sind.



The screenshot shows the 'Configure' tab for VMkernel adapters. The left sidebar lists various networking options, with 'VMkernel adapters' selected. The main area displays a table of configured adapters.

Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
vmk2	vMotion 3373	DSwitch	172.21.117.113	Default	vMotion +2
vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
vmk5	Data A - 3374	DSwitch	172.21.118.123	Default	--
vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

Wenn Sie die VMkernel-Schnittstelle bearbeiten, können Sie hier die erforderlichen Dienste aktivieren.



The screenshot shows the 'vmk2 - Edit Settings' dialog box for the vSphere host 'esxi-hc-03.sddc.netapp.com'. The 'Port properties' tab is active, showing 'TCP/IP stack' set to 'Default' and 'MTU (Bytes)' set to '9000'. Under 'Available services', the 'Enabled services' section has 'vMotion' and 'Fault Tolerance logging' checked. Other services like 'Provisioning', 'Management', 'vSphere Replication', 'vSphere Replication NFC', 'vSAN', 'vSAN Witness', 'vSphere Backup NFC', and 'NVMe over RDMA' are unchecked. 'NVMe over TCP' is also present but unchecked. 'CANCEL' and 'OK' buttons are at the bottom right.



Stellen Sie sicher, dass für die von vMotion und Provisioning VMkernel Schnittstellen verwendete Portgruppe mindestens zwei schnelle aktive Uplink-nics verfügbar sind.

VM-Migrationsszenarien

VMotion wird häufig verwendet, um die VMs unabhängig von ihrem Einschaltzustand zu migrieren. Weitere Überlegungen und Migrationsverfahren für spezifische Szenarien finden Sie unten.

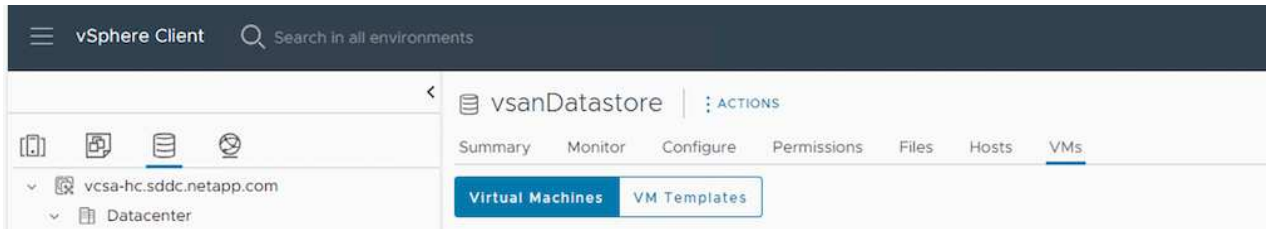


Verstehen "[VM-Bedingungen und Einschränkungen von vSphere vMotion](#)" Bevor Sie mit den Optionen für die VM-Migration fortfahren.

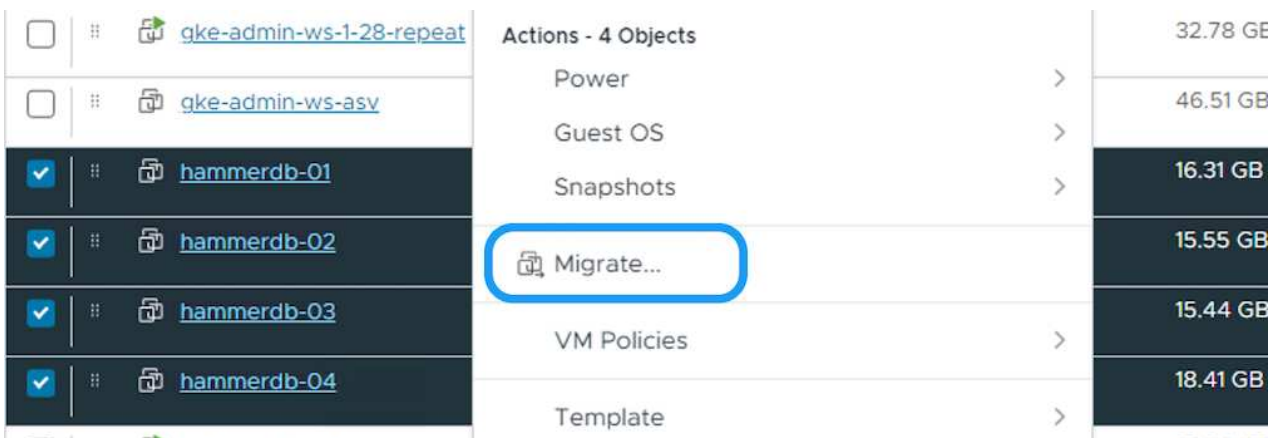
Migration von VMs aus spezifischen vSphere Datastores

Gehen Sie wie folgt vor, um VMs mithilfe der Benutzeroberfläche auf einen neuen Datastore zu migrieren.

1. Wählen Sie unter vSphere Web Client den Datenspeicher aus dem Speicherbestand aus und klicken Sie auf die Registerkarte VMs.



2. Wählen Sie die VMs aus, die migriert werden sollen, und klicken Sie mit der rechten Maustaste, um die Option Migrieren auszuwählen.



3. Wählen Sie die Option, um nur den Speicher zu ändern, und klicken Sie auf Weiter

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only
Migrate the virtual machines to another host or cluster.
- Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Wählen Sie die gewünschte VM-Storage-Richtlinie aus und wählen Sie den kompatiblen Datenspeicher aus. Klicken Sie Auf Weiter.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE CONFIGURE PER DISK

Select virtual disk format Thin Provision

VM Storage Policy NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/> ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/> DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
<input type="radio"/> destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
<input type="radio"/> DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
<input type="radio"/> E13A400_JCSI	Incompatible	2 TB	858.66 GB	1.85 TB	N

Manage Columns Items per page 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Überprüfen Sie, und klicken Sie auf Fertig stellen.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

×

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

Um VMs mithilfe von PowerCLI zu migrieren, sehen Sie hier das Beispielskript.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

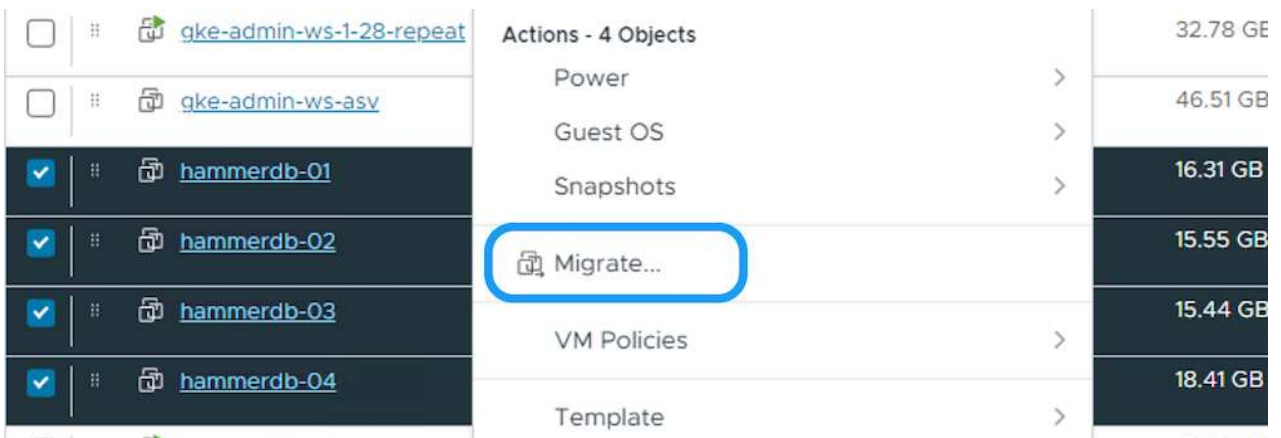

Migration von VMs im gleichen vSphere-Cluster

Gehen Sie wie folgt vor, um VMs mithilfe der Benutzeroberfläche auf einen neuen Datastore zu migrieren.

1. Wählen Sie bei vSphere Web Client den Cluster aus dem Host- und Cluster-Inventar aus und klicken Sie auf die Registerkarte VMs.



2. Wählen Sie die VMs aus, die migriert werden sollen, und klicken Sie mit der rechten Maustaste, um die Option Migrieren auszuwählen.



3. Wählen Sie die Option, um nur den Speicher zu ändern, und klicken Sie auf Weiter

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Wählen Sie die gewünschte VM-Storage-Richtlinie aus und wählen Sie den kompatiblen Datenspeicher aus. Klicken Sie Auf Weiter.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

[BATCH CONFIGURE](#) [CONFIGURE PER DISK](#)

Select virtual disk format Thin Provision

VM Storage Policy NetApp Storage

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/> ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/> DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	N
<input type="radio"/> destination	Incompatible	250 GB	31.8 MB	249.97 GB	N
<input type="radio"/> DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	N
<input type="radio"/> E13A400_JCSI	Incompatible	2 TB	858.66 GB	1.85 TB	N

Manage Columns Items per page 5 1 - 5 of 14 items < < 1 / 3 > >

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Überprüfen Sie, und klicken Sie auf Fertig stellen.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete

×

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

Um VMs mithilfe von PowerCLI zu migrieren, sehen Sie hier das Beispielskript.

```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```



Wenn Datastore Cluster mit vollautomatisiertem Storage DRS (Dynamic Resource Scheduling) verwendet wird und beide (Quell- und Ziel-) Datastores vom gleichen Typ sind (VMFS/NFS/vVol), behalten Sie beide Datastores im gleichen Storage-Cluster und migrieren Sie VMs vom Quell-Datastore, indem Sie den Wartungsmodus auf der Quelle aktivieren. Die Erfahrung ähnelt der Handhabung von Rechner-Hosts für Wartungsarbeiten.

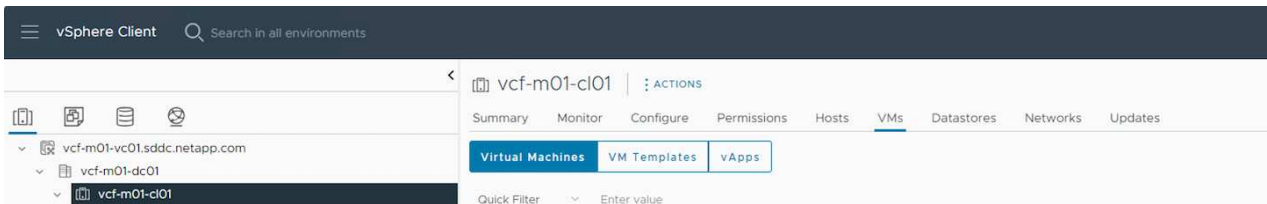
Migration von VMs über mehrere vSphere-Cluster hinweg



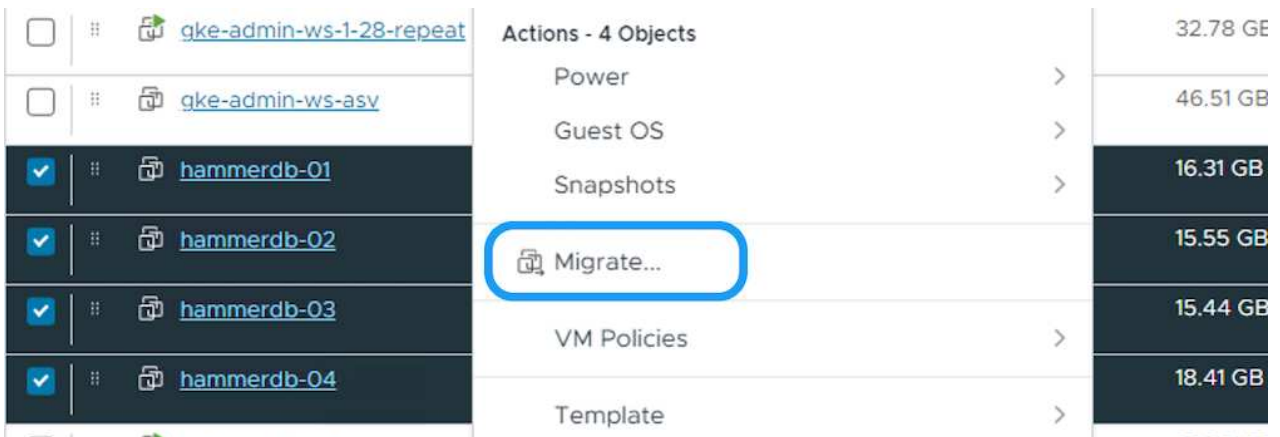
Siehe "[CPU-Kompatibilität und vSphere Enhanced vMotion-Kompatibilität](#)" Wenn Quell- und Ziel-Hosts unterschiedlicher CPU-Familie oder -Modell sind.

Gehen Sie wie folgt vor, um VMs mithilfe der Benutzeroberfläche auf einen neuen Datastore zu migrieren.

1. Wählen Sie bei vSphere Web Client den Cluster aus dem Host- und Cluster-Inventar aus und klicken Sie auf die Registerkarte VMs.



2. Wählen Sie die VMs aus, die migriert werden sollen, und klicken Sie mit der rechten Maustaste, um die Option Migrieren auszuwählen.



3. Wählen Sie die Option, um Compute-Ressource und Speicher zu ändern, und klicken Sie auf Weiter

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Navigieren Sie zu dem zu migrierenden Cluster, und wählen Sie es aus.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼  vcf-m01-vc01.sddc.netapp.com
 - >  vcf-m01-dc01
- ▼  vcf-wkld-vc01.sddc.netapp.com
 - ▼  vcf-wkld-01-DC
 - >  IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Wählen Sie die gewünschte VM-Storage-Richtlinie aus und wählen Sie den kompatiblen Datenspeicher aus. Klicken Sie Auf Weiter.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage**
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision
VM Storage Policy NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

6. Wählen Sie den VM-Ordner aus, um die Ziel-VMs zu platzieren.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder**
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - Discovered virtual machine**
 - vCLS

✓ Compatibility checks succeeded.

CANCEL **BACK** **NEXT**

7. Wählen Sie die Zielpartgruppe aus.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks**
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Überprüfen Sie, und klicken Sie auf Fertig stellen.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

Um VMs mithilfe von PowerCLI zu migrieren, sehen Sie hier das Beispielskript.


```

#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration

```

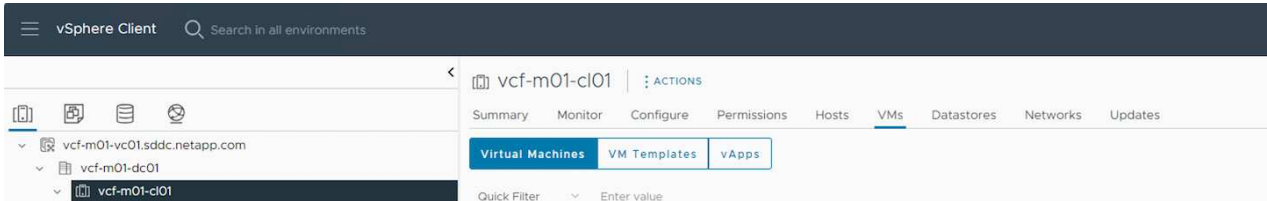
Migration von VMs über vCenter Server in derselben SSO-Domäne hinweg

Gehen Sie wie folgt vor, um VMs auf einen neuen vCenter-Server zu migrieren, der auf derselben vSphere Client-Benutzeroberfläche aufgeführt ist.

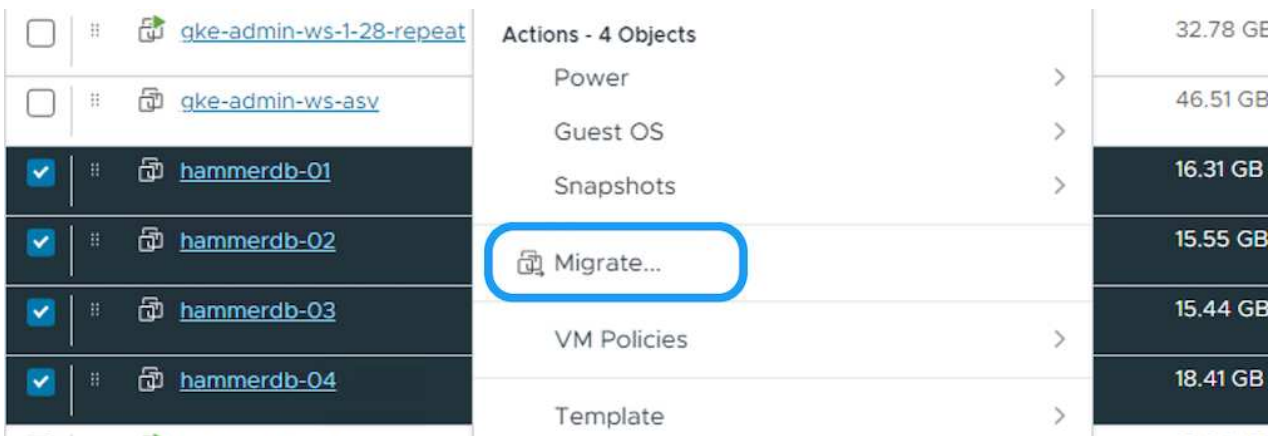


Weitere Anforderungen wie Quell- und Ziel-vCenter-Versionen usw. finden Sie unter ["vSphere-Dokumentation zu Anforderungen für vMotion zwischen vCenter-Serverinstanzen"](#)

1. Wählen Sie bei vSphere Web Client den Cluster aus dem Host- und Cluster-Inventar aus und klicken Sie auf die Registerkarte VMs.



2. Wählen Sie die VMs aus, die migriert werden sollen, und klicken Sie mit der rechten Maustaste, um die Option Migrieren auszuwählen.



3. Wählen Sie die Option, um Compute-Ressource und Speicher zu ändern, und klicken Sie auf Weiter

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

Change compute resource only

Migrate the virtual machines to another host or cluster.

Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Wählen Sie das Ziel-Cluster im Ziel-vCenter-Server aus.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ▼ vcf-wkld-vc01.sddc.netapp.com
 - ▼ vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Wählen Sie die gewünschte VM-Storage-Richtlinie aus und wählen Sie den kompatiblen Datenspeicher aus. Klicken Sie Auf Weiter.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage**
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision

VM Storage Policy NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

6. Wählen Sie den VM-Ordner aus, um die Ziel-VMs zu platzieren.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder**
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

vcf-wkld-01-DC

Discovered virtual machine

vCLS

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

7. Wählen Sie die Zielpartgruppe aus.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select a compute resource
- 3 Select storage
- 4 Select folder
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
» SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

[ADVANCED >>](#)

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Überprüfen Sie die Migrationsoptionen, und klicken Sie auf Fertig stellen.

4 Virtual Machines - Migrate

- 1 Select a migration type
- 2 Select storage
- 3 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Um VMs mithilfe von PowerCLI zu migrieren, sehen Sie hier das Beispielskript.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

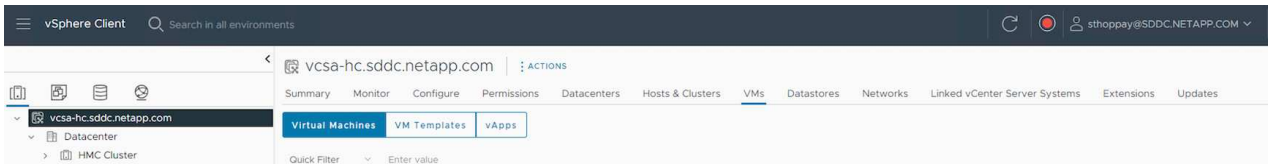
Migration von VMs über vCenter-Server in einer anderen SSO-Domain hinweg



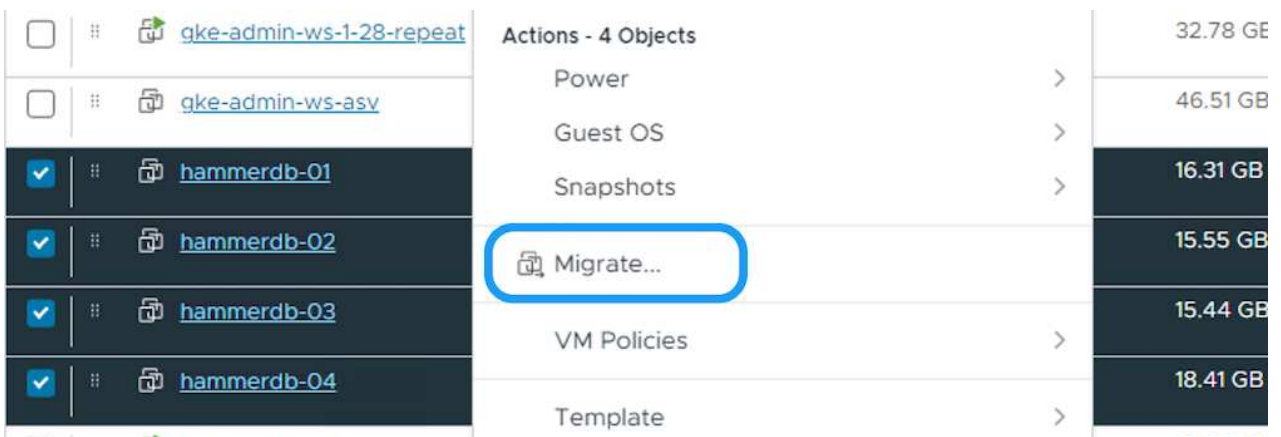
Dieses Szenario setzt voraus, dass die Kommunikation zwischen den vCenter Servern besteht. Andernfalls prüfen Sie das unten aufgeführte Szenario für den Standort von Across-Rechenzentren. Voraussetzungen prüfen "[VSphere-Dokumentation auf Advanced Cross vCenter vMotion](#)"

Gehen Sie wie folgt vor, um VMs auf einen anderen vCenter Server über die Benutzeroberfläche zu migrieren.

1. Wählen Sie unter vSphere Web Client den vCenter-Quellserver aus und klicken Sie auf die Registerkarte VMs.



2. Wählen Sie die VMs aus, die migriert werden sollen, und klicken Sie mit der rechten Maustaste, um die Option Migrieren auszuwählen.



3. Wählen Sie Option vCenter Server-Export, und klicken Sie auf Weiter

4 Virtual Machines - Migrate

1 Select a migration type

- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Select vMotion priority
- 7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- Change compute resource only**
Migrate the virtual machines to another host or cluster.
- Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.
 - Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL NEXT



VM kann auch vom Ziel-vCenter-Server importiert werden. Überprüfen Sie für dieses Verfahren ["Importieren oder Klonen Sie eine Virtual Machine mit Advanced Cross vCenter vMotion"](#)

4. Geben Sie vCenter-Anmeldeinformationen an, und klicken Sie auf Anmelden.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

SAVED VCENTER SERVERS NEW VCENTER SERVER

vCenter Server address
vCenter Server FQDN or IP address

Username
example@domain.local

Password
Password

Save vCenter Server address ⓘ

LOGIN


CANCEL BACK NEXT

5. Bestätigen und akzeptieren Sie den Fingerabdruck des SSL-Zertifikats des vCenter-Servers

Security Alert ✕

Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:
17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

 Connect anyway?

Click Yes if you trust the vCenter Server.
Click No to cancel connecting to the vCenter Server.

6. Erweitern Sie Ziel-vCenter, und wählen Sie das Ziel-Compute-Cluster aus.

Migrate | SQLSRV-05 ✕

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource**
- 4 Select storage
- 5 Select networks
- 6 Ready to complete

Select a compute resource ✕

Select a cluster, host, vApp or resource pool to run the virtual machines. VM ORIGIN ⓘ

- vcf-wkld-vc01.sddc.netapp.com
 - vcf-wkld-01-DC
 - IT-INF-WKLD-01**

Compatibility

✓ Compatibility checks succeeded.

7. Wählen Sie den Ziel-Datastore auf der Grundlage der VM-Speicherrichtlinie aus.

The screenshot shows the 'Select storage' step of a migration wizard. On the left, a sidebar lists seven steps: 1. Select a migration type, 2. Select a target vCenter Server, 3. Select a compute resource, 4. Select storage (highlighted), 5. Select folder, 6. Select networks, and 7. Ready to complete. The main area is titled 'Select storage' and includes a 'VM ORIGIN' link. Below the title are two buttons: 'BATCH CONFIGURE' and 'CONFIGURE PER DISK'. The 'Select virtual disk format' is set to 'Thin Provision' and the 'VM Storage Policy' is set to 'NFS'. A table lists available storage options:

	Name	Storage Compatibility	Capacity	Provisioned	Free
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB
<input type="radio"/>	VCF_WKLD_03_JSCSI	Incompatible	3 TB	1.35 TB	2.59 TB
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB

Below the table is a 'Compatibility' section with a green checkmark and the text 'Compatibility checks succeeded.' At the bottom right are 'CANCEL', 'BACK', and 'NEXT' buttons.

8. Wählen Sie den VM-Zielordner aus.

The screenshot shows the 'Select folder' step of a migration wizard. The sidebar on the left highlights step 5: 'Select folder'. The main area is titled 'Select folder' and includes a 'VM ORIGIN' link. Below the title is the instruction 'Select location for the virtual machine migration.' A tree view shows the folder structure:

- vcf-wkld-01-DC
 - Discovered virtual machine
 - Oracle
 - SQL Server (highlighted)
 - vCLS

Below the tree view is a 'Compatibility' section with a green checkmark and the text 'Compatibility checks succeeded.' At the bottom right are 'CANCEL', 'BACK', and 'NEXT' buttons.

9. Wählen Sie die VM-Portgruppe für jede Netzwerkschnittstellenkarte aus.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete

Select networks

Select destination networks for the virtual machine migration. VM ORIGIN ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
» Mgmt 181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
» Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
» Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

3 Items

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

10. Überprüfen Sie, und klicken Sie auf Fertig stellen, um die vMotion über die vCenter-Server zu starten.

Migrate | SQLSRV-05

- 1 Select a migration type
- 2 Select a target vCenter Server
- 3 Select a compute resource
- 4 Select storage
- 5 Select folder
- 6 Select networks
- 7 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration. VM ORIGIN ⓘ

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

CANCEL
BACK
FINISH

Um VMs mithilfe von PowerCLI zu migrieren, sehen Sie hier das Beispielskript.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster' -server $sourcevc | Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration

```

Migration von VMs zwischen Datacenter-Standorten

- Wenn der Layer-2-Datenverkehr über Rechenzentren verteilt wird, entweder über NSX Federation oder andere Optionen, befolgen Sie das Verfahren zur Migration von VMs über vCenter-Server hinweg.
- HCX bietet verschiedene "Migrationstypen" Mit Hilfe der Replikation unterstützte vMotion über die Rechenzentren hinweg, um die VM ohne Ausfallzeiten zu verschieben.
- "Site Recovery Manager (SRM)" Ist in der Regel für Disaster-Recovery-Zwecke gedacht und wird häufig auch für geplante Migration unter Verwendung von Speicher-Array-basierter Replikation verwendet.
- Continuous Data Protection (CDP)-Produkte werden verwendet "VSphere API für IO (VAIO)" Um die Daten abzufangen und eine Kopie an einen Remote-Standort zu senden, um eine RPO-Lösung von nahezu null zu ermöglichen.
- Auch Backup- und Recovery-Produkte können eingesetzt werden. Dies führt aber oft zu einer längeren RTO.
- "BlueXP Disaster Recovery als Service (DRaaS)" Nutzt Storage Array-basierte Replizierung und automatisiert bestimmte Aufgaben für die Wiederherstellung der VMs am Zielstandort.

Migration von VMs in einer Hybrid-Cloud-Umgebung

- "Konfigurieren Sie Den Hybriden Verknüpften Modus" Und befolgen Sie das Verfahren von "Migration von VMs über vCenter Server in derselben SSO-Domäne hinweg"
- HCX bietet verschiedene "Migrationstypen" Einschließlich Replication unterstützte vMotion über die Datacenter, um die VM zu verschieben, während sie eingeschaltet ist.
 - Link:../ehc/aws-migrate-vmware-hcx.html [TR 4942: Migration von Workloads auf FSX ONTAP-Datastore mit VMware HCX]
 - Link:../ehc/azure-migrate-vmware-hcx.html [TR-4940: Migrieren Sie Workloads mithilfe von VMware HCX zu einem Azure NetApp Files Datastore – QuickStart Guide]
 - Link:../ehc/gcp-migrate-vmware-hcx.html [Workloads auf Google Cloud NetApp Volumes Datastore auf Google Cloud VMware Engine mit VMware HCX migrieren – QuickStart Guide]
- "BlueXP Disaster Recovery als Service (DRaaS)" Nutzt Storage Array-basierte Replizierung und automatisiert bestimmte Aufgaben für die Wiederherstellung der VMs am Zielstandort.
- Mit unterstützten CDP-Produkten (Continuous Data Protection), die verwendet werden "VSphere API für IO (VAIO)" Um die Daten abzufangen und eine Kopie an einen Remote-Standort zu senden, um eine RPO-Lösung von nahezu null zu ermöglichen.



Wenn sich die Quell-VM auf Block-vVol-Datastore befindet, kann sie mit SnapMirror auf Amazon FSX ONTAP oder Cloud Volumes ONTAP (CVO) bei anderen unterstützten Cloud-Providern repliziert und als iSCSI-Volume mit Cloud-nativen VMs genutzt werden.

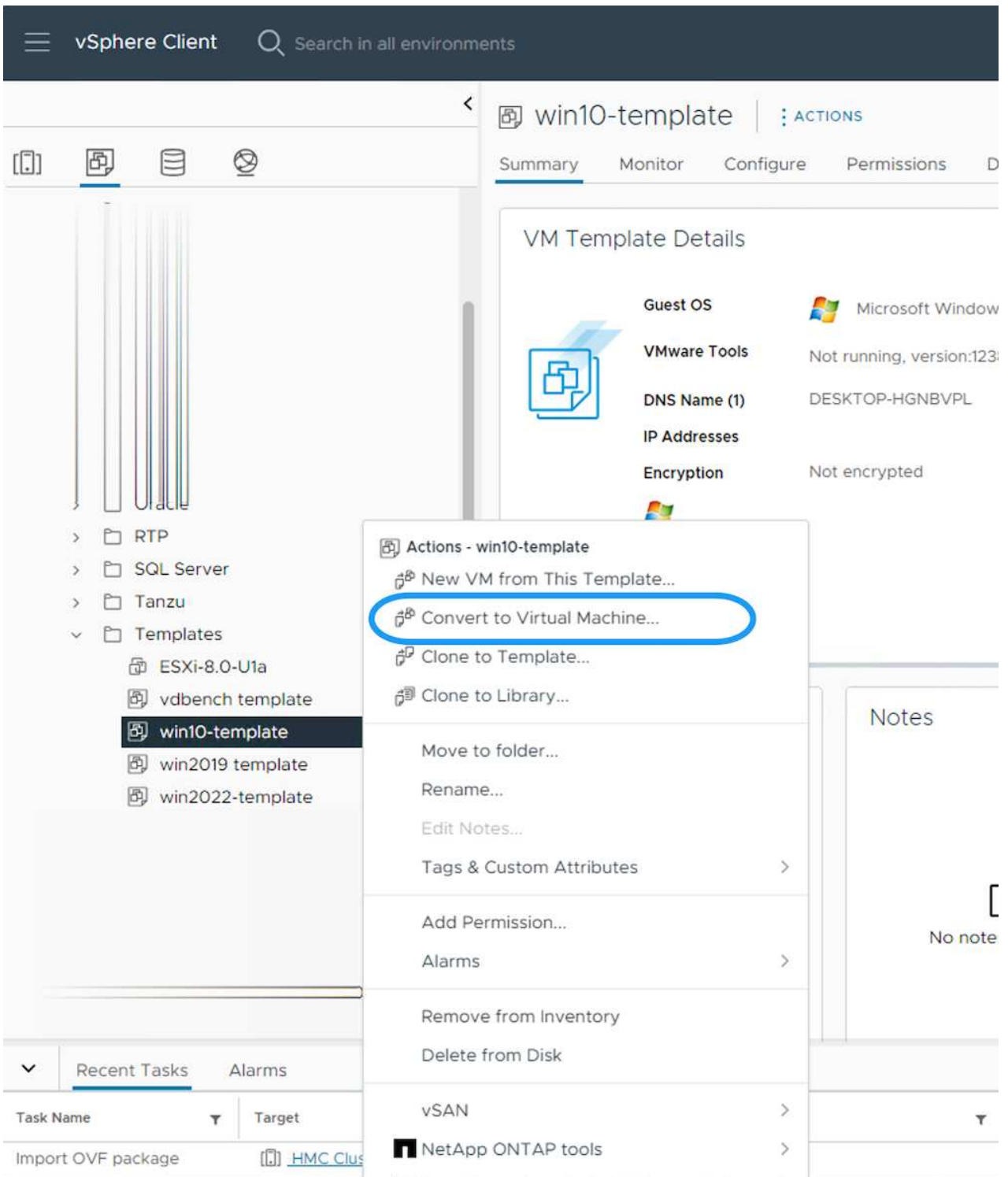
Migrationsszenarien für VM-Vorlagen

VM-Vorlagen können vom vCenter Server oder von einer Content Library gemanagt werden. Verteilung von VM-Vorlagen, OVF- und OVA-Vorlagen, andere Arten von Dateien werden durch die Veröffentlichung in der lokalen Inhaltsbibliothek und Remote-Content-Bibliotheken können sie abonnieren.

- VM-Vorlagen, die im vCenter Inventar gespeichert sind, können in VMs konvertiert werden und verwenden Sie die VM-Migrationsoptionen.
- OVF- und OVA-Vorlagen, andere Dateitypen, die in der Inhaltsbibliothek gespeichert sind, können in anderen Inhaltsbibliotheken geklont werden.
- VM-Vorlagen für die Inhaltsbibliothek können auf jedem Datenspeicher gehostet werden und müssen der neuen Content Library hinzugefügt werden.

Migration von auf einem Datastore gehosteten VM-Vorlagen

1. Klicken Sie in vSphere Web Client mit der rechten Maustaste auf die VM-Vorlage unter der Ordneransicht VM und Vorlagen, und wählen Sie die Option zum Konvertieren in VM aus.




2. Sobald sie als VM konvertiert wurde, folgen Sie den Optionen zur VM-Migration.

Kopieren von Elementen der Inhaltsbibliothek

1. Wählen Sie in vSphere Web Client Content Libraries aus




 Home

 Shortcuts

 Inventory

 Content Libraries

 Workload Management

 Global Inventory Lists

 Policies and Profiles

 Auto Deploy

 Hybrid Cloud Services

 Developer Center

 Administration

 Tasks


 Events

 Tags & Custom Attributes

 Lifecycle Manager

 SnapCenter Plug-in for VMware vSphere

 NetApp ONTAP tools

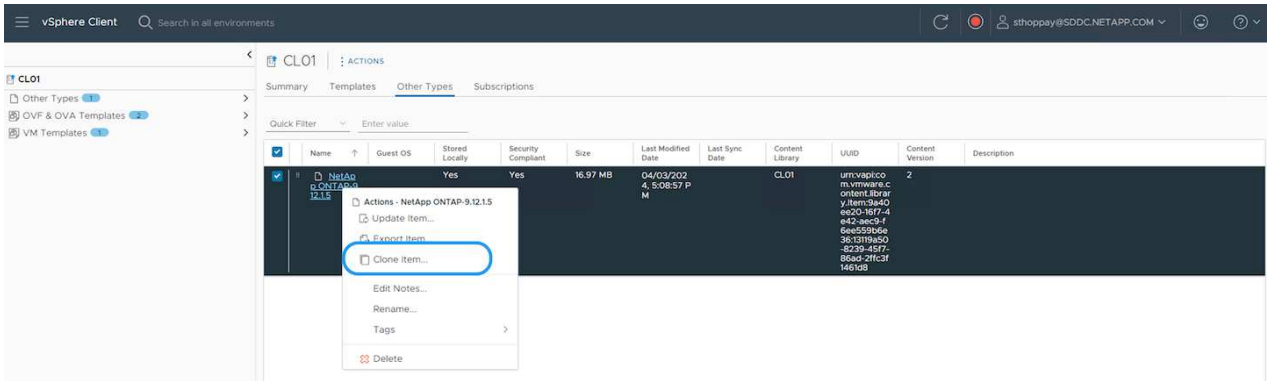
 Cloud Provider Services

 NSX

 VMware Aria Operations Configuration

 Skyline Health Diagnostics

2. Wählen Sie die Inhaltsbibliothek aus, in der das zu klonende Element erstellt werden soll
3. Klicken Sie mit der rechten Maustaste auf das Element und klicken Sie auf Objekt klonen ..



Wenn Sie das Aktionsmenü verwenden, stellen Sie sicher, dass das richtige Zielobjekt aufgeführt ist, um eine Aktion auszuführen.

4. Wählen Sie die Zielbibliothek aus, und klicken Sie auf OK.

Clone Library Item | NetApp ONTAP-9.12.15 ✕

Name

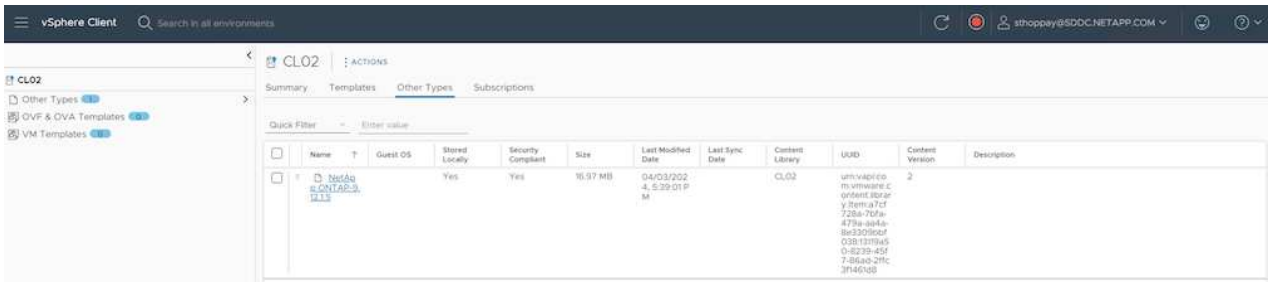
Notes

Select a content library where to clone the library item.

	Name	Notes	Creation Date
<input type="radio"/>	CL01		9/26/2023, 5:02:03 PM
<input checked="" type="radio"/>	CL02		4/1/2024, 12:37:51 PM

CANCEL
OK

5. Überprüfen Sie, ob das Element in der Zielinhaltsbibliothek verfügbar ist.



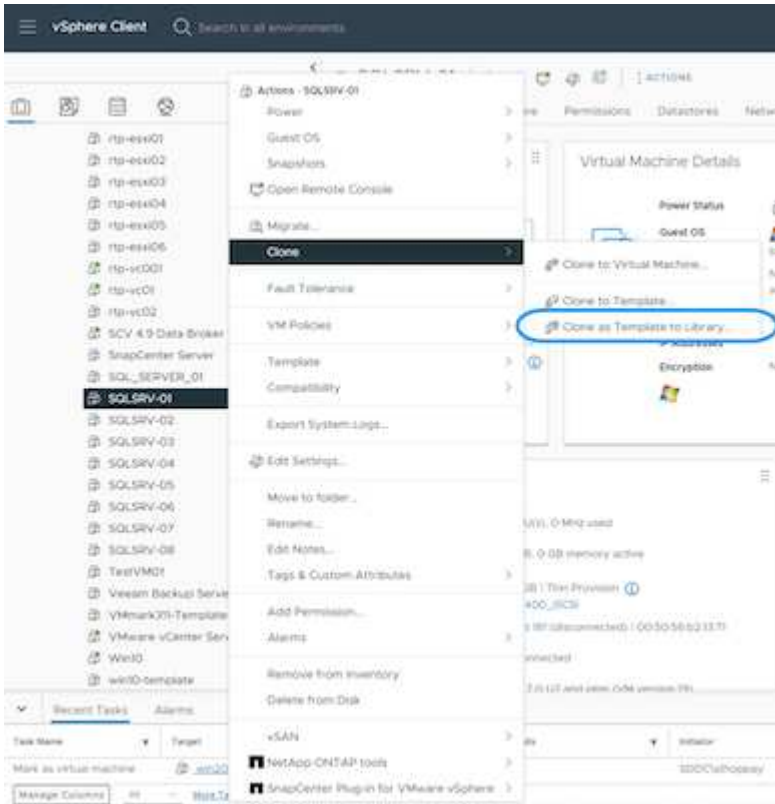
Hier ist das Beispiel für ein PowerCLI-Skript zum Kopieren der Inhalte aus der Inhaltsbibliothek CL01 nach CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL02' -Server
$targetvc)
```

Hinzufügen von VM als Vorlagen in der Content Library

1. Wählen Sie in vSphere Web Client die VM aus, und klicken Sie mit der rechten Maustaste, um in der Bibliothek als Vorlage klonen zu wählen



Wenn die VM-Vorlage zum Klonen in der Bibliothek ausgewählt ist, kann sie nur als OVF- und OVA-Vorlage und nicht als VM-Vorlage gespeichert werden.

2. Bestätigen Sie, dass der Vorlagentyp als VM-Vorlage ausgewählt ist, und befolgen Sie die Antwort auf den Assistenten, um den Vorgang abzuschließen.

SQLSRV-01 - Clone Virtual Machine To Template
Basic information ×

- 1 Basic information
- 2 Location
- 3 Select a compute resource
- 4 Select storage
- 5 Ready to complete

Template type VM Template

Name SQLSRV-01

Notes

Select a folder for the template

v

vcsa-hc.sddc.netapp.com

>

Datacenter

CANCEL
NEXT

i

Weitere Informationen zu VM-Vorlagen auf Content Library finden Sie unter ["Administrationshandbuch für vSphere VM"](#)

Anwendungsfälle

Migration von Storage-Systemen von Drittanbietern (einschließlich vSAN) zu ONTAP Datastores.

- Wählen Sie die VM-Migrationsoptionen von oben aus, basierend auf dem Ort, an dem der ONTAP Datastore bereitgestellt wird.

Migration von einer vorherigen Version auf die neueste Version von vSphere

- Wenn kein in-Place-Upgrade möglich ist, kann eine neue Umgebung einrichten und die oben genannten Migrationsoptionen verwenden.



Importieren Sie in der Option „vCenter-übergreifende Migration“ aus dem Ziel, wenn die Exportoption auf der Quelle nicht verfügbar ist. Überprüfen Sie für dieses Verfahren ["Importieren oder Klonen Sie eine Virtual Machine mit Advanced Cross vCenter vMotion"](#)

Migration auf VCF Workload Domain.

- Migrieren Sie VMs von jedem vSphere Cluster zu einer Ziel-Workload-Domäne.



Um die Netzwerkkommunikation mit vorhandenen VMs auf anderen Clustern im Quell-vCenter zu ermöglichen, erweitern Sie entweder das NSX-Segment, indem Sie die vcenter vSphere-Quell-Hosts zur Transportzone hinzufügen, oder verwenden Sie die L2-Bridge am Edge, um die L2-Kommunikation im VLAN zu ermöglichen. Prüfen Sie die NSX-Dokumentation von ["Konfigurieren Sie eine Edge VM für Bridging"](#)

Weitere Ressourcen

- ["Migration von vSphere Virtual Machines"](#)
- ["Neuerungen in vSphere 8 für vMotion"](#)
- ["Ressourcen für vSphere vMotion"](#)
- ["Tier-0-Gateway-Konfigurationen in NSX Federation"](#)
- ["HCX 4.8 Benutzerhandbuch"](#)
- ["VMware Site Recovery Manager - Dokumentation"](#)
- ["BlueXP Disaster Recovery für VMware"](#)

Migrieren Sie VMs zu Amazon EC2 und verwenden Sie Amazon FSX for ONTAP

Migration von VMs zu Amazon EC2 mit Amazon FSX for ONTAP: Überblick

Unternehmen beschleunigen ihre Migrationen zu Cloud-Computing-Lösungen auf AWS und profitieren von Services wie Amazon Elastic Compute Cloud (Amazon EC2) Instanzen und Amazon FSX for NetApp ONTAP (FSX ONTAP), um ihre IT-Infrastruktur zu modernisieren, Kosteneinsparungen zu erzielen und die betriebliche Effizienz zu verbessern. Diese Angebote von AWS ermöglichen Migrationen, die die Gesamtbetriebskosten (TCO) durch nutzungsbasierte Preismodelle und Storage-Funktionen der Enterprise-Klasse optimieren. Dadurch erhalten Unternehmen die Flexibilität und Skalierbarkeit, die sie an neue globale Geschäftsanforderungen anpassen können.

Überblick

Für Unternehmen, die tief in VMware vSphere investiert haben, ist die Migration zu AWS angesichts der aktuellen Marktbedingungen eine kostengünstige Option, die einzigartige Chance bietet.

Im Zusammenhang mit dem Wechsel zu AWS versuchen diese Unternehmen, die Flexibilität und Kostenvorteile der Cloud zu nutzen und gleichzeitig vertraute Funktionen zu erhalten, insbesondere bei Storage. Der lückenlose Betrieb bekannter Storage-Protokolle, insbesondere iSCSI, Prozesse, Tools und das Know-how ist für die Migration von Workloads und die Einrichtung von Disaster Recovery-Lösungen von entscheidender Bedeutung.

Mit dem AWS Managed Storage Service FSX ONTAP können Unternehmen die Vorteile von AWS ausschöpfen, während sie gleichzeitig die Funktionen für Enterprise-Storage beibehalten, die auch bei On-

Premises-Storage von Drittanbietern gegeben sind. So minimieren sie Unterbrechungen und maximieren ihre zukünftigen Investitionen.

Dieser technische Bericht erläutert, wie lokale VMware vSphere VMs zu einer Amazon EC2 Instanz migriert werden, wobei Festplatten auf FSX ONTAP iSCSI LUNs mithilfe der MigrateOps „Data-Mobility-as-Code“-Funktion der Cirrus Migrate Cloud (CMC) platziert werden.

Anforderungen der Lösung erfüllen

VMware Kunden suchen derzeit nach Lösungen für eine Reihe von Herausforderungen. Diese Unternehmen möchten:

1. Nutzen Sie Enterprise-Storage-Funktionen wie Thin Provisioning, Storage-Effizienztechnologien, Klone ohne zusätzlichen Platzbedarf, integrierte Backups, Replizierung auf Block-Ebene, und Tiering. Dies hilft bei der Optimierung der Migration und der zukunftssicheren Implementierung auf AWS ab Tag 1.
2. Optimieren Sie Storage-Implementierungen derzeit auf AWS, die Amazon EC2 Instanzen verwenden, indem Sie FSX ONTAP und die damit bereitgestellten Kostenoptimierungsfunktionen integrieren.
3. Reduzieren Sie die Gesamtbetriebskosten (TCO) bei der Verwendung von Amazon EC2 Instanzen mit Block-Storage-Lösungen, indem Sie Amazon EC2 Instanzen entsprechend dimensionieren, um die erforderlichen IOPS und Durchsatzparameter zu erfüllen. Bei Block-Storage werden die Bandbreiten- und I/O-Raten von Amazon EC2 Festplattenoperationen Obergrenze erreicht. File-Storage mit FSX ONTAP nutzt Netzwerkbandbreite. Mit anderen Worten: FSX ONTAP besitzt keine I/O-Limits auf VM-Ebene.

Übersicht über die technischen Komponenten

FSX ONTAP-Konzepte

Amazon FSX ONTAP ist ein vollständig gemanagter AWS-Storage-Service, der NetApp® ONTAP®-Dateisysteme mit allen bekannten ONTAP-Datenmanagementfunktionen, Performance und APIs auf AWS bereitstellt. Der hochperformante Storage unterstützt mehrere Protokolle (NFS, SMB, iSCSI) und bietet damit einen einzelnen Service für Workloads mit EC2 Instanzen von Windows, Linux und macOS.

Da FSX ONTAP ein ONTAP-Dateisystem ist, bietet es eine Vielzahl vertrauter NetApp-Funktionen und -Dienste, einschließlich SnapMirror®-Datenreplikationstechnologie, Thin Clones und NetApp Snapshot™ Kopien. FSX ONTAP nutzt eine kostengünstige Kapazitäts-Tier über Daten-Tiering, ist flexibel und kann eine nahezu unbegrenzte Skalierbarkeit erreichen. Dank der charakteristischen Storage-Effizienztechnologie von NetApp lassen sich die Storage-Kosten auf AWS noch weiter senken. Weitere Informationen finden Sie unter ["Erste Schritte mit Amazon FSX ONTAP"](#).

File-System

Die zentrale Ressource von FSX ONTAP ist sein Filesystem, das auf SSD-Storage (Solid-State Drive) basiert. Bei der Bereitstellung eines FSX ONTAP-Dateisystems gibt der Benutzer den gewünschten Durchsatz und die gewünschte Speicherkapazität ein und wählt eine Amazon VPC aus, auf der sich das Filesystem befinden soll.

Die Anwender haben außerdem die Wahl zwischen zwei integrierten Hochverfügbarkeitsimplementierungsmodellen für das Filesystem: Multi-Availability Zone (AZ) oder Single-AZ-Implementierung. Jede dieser Optionen bietet ein eigenes Maß an Langlebigkeit und Verfügbarkeit, das Kunden je nach Business Continuity-Anforderungen ihres Anwendungsfalls auswählen können. Implementierungen mit mehreren Verfügbarkeitszonen bestehen aus Dual-Nodes, die nahtlos über zwei Verfügbarkeitszonen repliziert werden. Mit der kostenoptimierten Single-AZ-Implementierungsoption wird das Filesystem in zwei Nodes strukturiert, die auf zwei separate Fehlerdomänen aufgeteilt sind, die sich beide in einer einzigen Verfügbarkeitszone befinden.

Storage Virtual Machines

Auf die Daten im FSX ONTAP Filesystem wird über eine logische Storage-Partition zugegriffen, die als Storage Virtual Machine (SVM) bezeichnet wird. Eine SVM ist tatsächlich ein eigener Fileserver, der mit eigenen Daten- und Admin-Zugriffspunkten ausgestattet ist. Beim Zugriff auf iSCSI-LUNs auf einem FSX ONTAP-Filesystem wird über eine direkte Schnittstelle zwischen der Amazon EC2 Instanz und der SVM unter Verwendung der iSCSI-Endpunkt-IP-Adresse kommuniziert.

Es ist zwar möglich, eine einzelne SVM in einem Cluster beizubehalten, aber die Option, mehrere SVMs in einem Cluster auszuführen, weist zahlreiche Nutzungen und Vorteile auf. Kunden können die optimale Anzahl an SVMs zu konfigurieren, indem sie ihre geschäftlichen Anforderungen einschließlich der Anforderungen zur Workload-Isolierung berücksichtigen.

Volumes

Die Daten innerhalb einer FSX ONTAP SVM werden in Strukturen, sogenannten Volumes, gespeichert und organisiert, die als virtuelle Container fungieren. Ein einzelnes Volume kann mit einer oder mehreren LUNs konfiguriert werden. Die in den einzelnen Volumes gespeicherten Daten belegen die Storage-Kapazität im File-System. Da FSX ONTAP jedoch das Volume über Thin Provisioning bereitstellt, nimmt das Volume nur Storage-Kapazität für die zu speichernde Datenmenge in Anspruch.

Das Konzept von Cirrus Migrate Cloud MigrateOps

CMC ist ein transactable Software-as-a-Service (SaaS)-Angebot von Cirrus Data Solutions, Inc., das über den AWS Marketplace erhältlich ist. MigrateOps ist eine Data-Mobility-as-Code-Automatisierungsfunktion des CMC, mit der Sie Ihre Datenmobilitätsvorgänge deklarativ im Maßstab mit einfachen Betriebskonfigurationen in YAML verwalten können. Eine MigrateOps-Konfiguration legt fest, wie Ihre Datenmobilitätsaufgaben ausgeführt werden sollen. Weitere Informationen zu MigrateOps finden Sie unter "[Info zu MigrateOps](#)".

MigrateOps verfolgt einen Ansatz, bei dem die Automatisierung an erster Stelle steht. Dieser Ansatz wurde speziell dafür entwickelt, den gesamten Prozess zu optimieren und Cloud-basierte Datenmobilität der Enterprise-Klasse ohne Betriebsunterbrechungen zu gewährleisten. Zusätzlich zu den bereits funktionsreichen Funktionen, die CMC für die Automatisierung bietet, fügt MigrateOps weitere Automatisierungen hinzu, die häufig extern verwaltet werden, z. B.:

- BS-Korrektur
- Applikationsumstellung und Genehmigungsplanung
- Cluster-Migration ohne Ausfallzeiten
- Integration der Public/Private Cloud-Plattform
- Integration der Virtualisierungsplattform
- Integration des Enterprise-Storage-Managements
- SAN-(iSCSI-)Konfiguration

Da die oben genannten Aufgaben vollständig automatisiert sind, sind alle mühsamen Schritte bei der Vorbereitung der lokalen Quell-VM (wie das Hinzufügen von AWS-Agenten und -Tools), der Erstellung von Ziel-FSX-LUNs, der Einrichtung von iSCSI und Multipath/MPIO in der AWS Ziel-Instanz, und alle Aufgaben des Stopps/Startens von Anwendungsdiensten entfallen, indem einfach Parameter in einer YAML-Datei angegeben werden.

FSX ONTAP wird verwendet, um die Daten-LUNs und die Größenanpassung des Amazon EC2 Instanztyps bereitzustellen und gleichzeitig alle Funktionen zu bieten, die Unternehmen zuvor in ihren On-Premises-Umgebungen hatten. Die MigrateOps-Funktion des CMC wird verwendet, um alle erforderlichen Schritte zu

automatisieren, einschließlich der Bereitstellung von zugeordneten iSCSI-LUNs, wodurch dies in einen vorhersagbaren, deklarativen Vorgang umgewandelt wird.

Hinweis: Der CMC benötigt einen sehr dünnen Agenten, der auf den virtuellen Quell- und Zielmaschineninstanzen installiert werden muss, um eine sichere Datenübertragung vom Speicher der Speicherquelle zu FSX ONTAP zu gewährleisten.

Vorteile der Verwendung von Amazon FSX ONTAP mit EC2 Instanzen

FSX ONTAP Storage für Amazon EC2 Instanzen bietet mehrere Vorteile:

- Hoher Durchsatz und Storage mit niedriger Latenz, die eine konsistent hohe Performance für anspruchsvollste Workloads bieten
- Intelligentes NVMe-Caching verbessert die Performance
- Kapazität, Durchsatz und IOPS können im Handumdrehen angepasst und an sich ändernde Storage-Anforderungen angepasst werden
- Blockbasierte Datenreplizierung von lokalem ONTAP Storage zu AWS
- Multi-Protokoll-Zugriff, einschließlich für iSCSI, die in lokalen VMware-Implementierungen weit verbreitet ist
- NetApp Snapshot™ Technologie und DR, orchestriert mit SnapMirror, verhindern Datenverlust und beschleunigen die Recovery
- Storage-Effizienzfunktionen zur Reduzierung von Storage-Platzbedarf und -Kosten, u. a. Thin Provisioning, Datendeduplizierung, Komprimierung und Data-Compaction
- Eine effiziente Replizierung reduziert die Dauer von Backups von Stunden auf wenige Minuten und optimiert so die RTO
- Granulare Optionen für die Sicherung und Wiederherstellung von Dateien mit NetApp SnapCenter®

Die Implementierung von Amazon EC2 Instanzen mit FSX ONTAP als iSCSI-basierte Storage-Ebene bietet hochperformante, geschäftskritische Datenmanagement-Funktionen und kostengünstige Storage-Effizienzfunktionen, die Ihre Implementierung auf AWS transformieren können.

Durch einen Flash Cache, mehrere iSCSI-Sitzungen und die Nutzung einer Arbeitsmenge von 5 % ist es möglich, dass FSX ONTAP IOPS von ~350.000 bietet, sodass Performance-Level verfügbar sind, um selbst die intensivsten Workloads zu erfüllen.

Da gegen FSX ONTAP nur Limits für die Netzwerkbandbreite und nicht für Block-Storage angewendet werden, können Benutzer kleine Amazon EC2 Instanztypen nutzen und gleichzeitig dieselben Performance-Raten wie bei wesentlich größeren Instanztypen erzielen. Die Verwendung solcher kleinen Instanztypen sorgt zudem für niedrige Compute-Kosten und optimiert so die TCO.

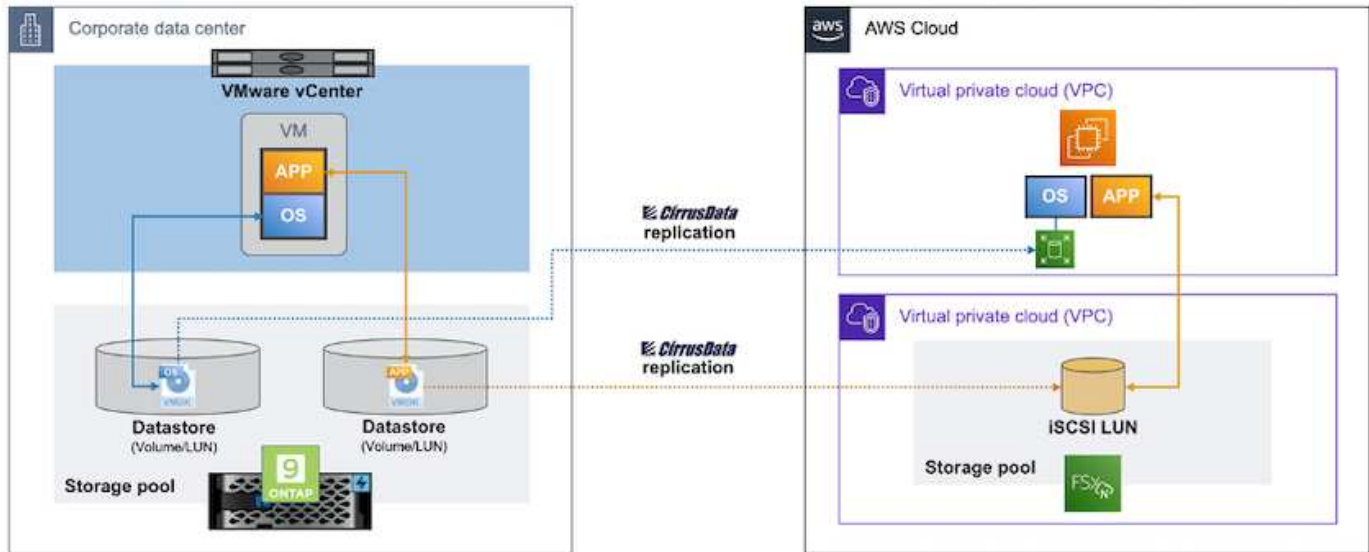
Ein weiterer Vorteil ist, dass FSX ONTAP mehrere Protokolle unterstützen kann. Damit lässt sich ein einziger AWS Storage-Service für eine Vielzahl vorhandener Daten- und Fileservices-Anforderungen standardisieren. Für Unternehmen, die tief in VMware vSphere investiert haben, ist die Migration zu AWS angesichts der aktuellen Marktbedingungen eine kostengünstige Option, die einzigartige Chance bietet.

Migrieren Sie VMs zu Amazon EC2 und verwenden Sie dazu Amazon FSX for NetApp ONTAP: Architektur und Voraussetzungen

Dieser Artikel enthält die grundlegenden Voraussetzungen für die Architektur und Implementierung der Migration.

High-Level-Architektur

Das folgende Diagramm zeigt die übergeordnete Architektur der Migration von VMDK-Daten (Virtual Machine Disk) auf VMware zu AWS mithilfe von CMC MigrateOps:



So migrieren Sie Ihre VMware VMs zu AWS mit Amazon EC2 und FSX ONTAP iSCSI

Voraussetzungen

Stellen Sie vor dem Starten der Walkthrough-Schritte sicher, dass die folgenden Voraussetzungen erfüllt sind:

Auf AWS

- Ein AWS-Konto. Dies umfasst Berechtigungen für Subnetze, VPC-Setup, Routing-Tabellen, Migration von Sicherheitsregeln, Sicherheitsgruppen, und weitere Netzwerkanforderungen wie Lastausgleich. Wie bei jeder Migration sollte der größte Aufwand und die größten Überlegungen in Bezug auf Netzwerke einfließen.
- Geeignete IAM-Rollen, mit denen Sie sowohl FSX ONTAP- als auch Amazon EC2-Instanzen bereitstellen können.
- Routingtabellen und Sicherheitsgruppen dürfen mit FSX ONTAP kommunizieren.
- Fügen Sie der entsprechenden Sicherheitsgruppe eine eingehende Regel hinzu (weitere Details siehe unten), um einen sicheren Datentransfer aus Ihrem lokalen Datacenter zu AWS zu ermöglichen.
- Ein gültiger DNS, der öffentliche Internet-Domännennamen auflösen kann.
- Überprüfen Sie, ob Ihre DNS-Auflösung funktioniert und es Ihnen ermöglicht, Hostnamen aufzulösen.
- Für eine optimale Performance und optimale Dimensionierung verwenden Sie Performance-Daten aus Ihrer Quellumgebung, um Ihren FSX ONTAP-Storage richtig zu dimensionieren.
- Jede MigrateOps-Sitzung verwendet eine EIP. Daher sollte das EIP-Kontingent für mehr Parallelität erhöht werden. Beachten Sie, dass die standardmäßige EIP-Quote 5 ist.
- (Wenn Active Directory-basierte Workloads migriert werden) Einer Windows Active Directory-Domäne auf Amazon EC2.

Für Cirrus Migrate Cloud

- Ein Cirrus Data Cloud Konto bei "cloud.cirrusdata.com" Muss vor der Verwendung des CMC erstellt

werden. Die ausgehende Kommunikation mit CDN, Cirrus Data Endpunkten und Software-Repository über HTTPS muss zulässig sein.

- Ermöglichen Sie die Kommunikation (ausgehend) mit Cirrus Data Cloud-Services über das HTTPS-Protokoll (Port 443).
- Damit ein Host vom CMC-Projekt verwaltet werden kann, muss die bereitgestellte CMC-Software eine einseitige ausgehende TCP-Verbindung zur Cirrus Data Cloud initiieren.
- TCP-Protokoll zulassen, Port 443-Zugriff auf `portal-gateway.cloud.cirrusdata.com`, das sich derzeit bei `208.67.222.222` befindet.
- HTTP-POST-Anforderungen (über HTTPS-Verbindung) mit binären Datennutzlasten (Anwendung/Oktett-Stream) zulassen. Dies ähnelt einem Datei-Upload.
- Stellen Sie sicher, dass `portal-gateway.cloud.cirrusdata.com` von Ihrem DNS (oder über die OS-Hostdatei) aufgelöst werden kann.
- Wenn Sie strenge Regeln für das Verbot von Produktinstanzen zum Herstellen von ausgehenden Verbindungen haben, kann die Funktion „Managementrelais“ des CMC verwendet werden, wenn die ausgehende 443-Verbindung von einem einzelnen sicheren nicht-Produktions-Host aus erfolgt.

Hinweis: Es werden niemals Speicherdaten an den Cirrus Data Cloud Endpunkt gesendet. Es werden nur Management-Metadaten gesendet. Diese können optional maskiert werden, sodass kein echter Host-Name, Volume-Name und Netzwerk-IP enthalten sind.

Für die Migration von Daten aus lokalen Storage-Repositories zu AWS automatisiert MigrateOps das Management einer Host-zu-Host-Verbindung (H2H). Diese sind optimierte, einseitige TCP-basierte Netzwerkverbindungen, die der CMC zur Erleichterung der Remote-Migration verwendet. Dieser Prozess umfasst Always-on-Komprimierung und Verschlüsselung, die je nach Art der Daten den Datenverkehr um das bis zu Achtfache reduzieren kann.

Hinweis: Der CMC ist so ausgelegt, dass während der gesamten Migrationsphase keine Produktionsdaten / E/A das Produktionsnetzwerk verlassen. Daher ist eine direkte Verbindung zwischen dem Quell- und dem Ziel-Host erforderlich.

Migrieren Sie VMs zu Amazon EC2 mithilfe von Amazon FSX for ONTAP – Implementierungsleitfaden

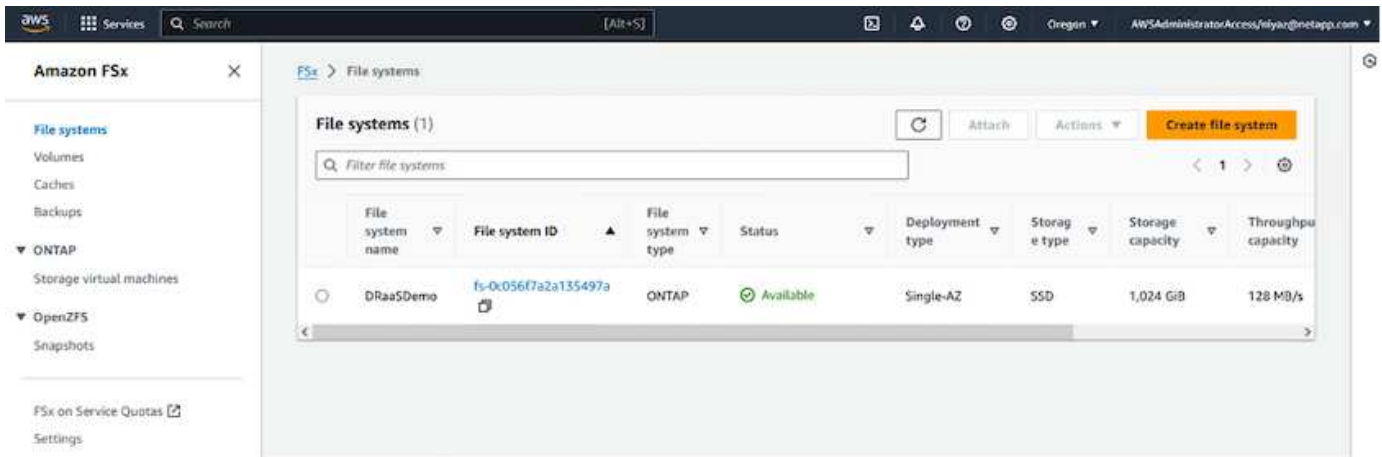
In diesem Artikel wird das Bereitstellungsverfahren für diese Migrationslösungen beschrieben.

FSX ONTAP und Cirrus-Daten für Migrationsvorgänge konfigurieren

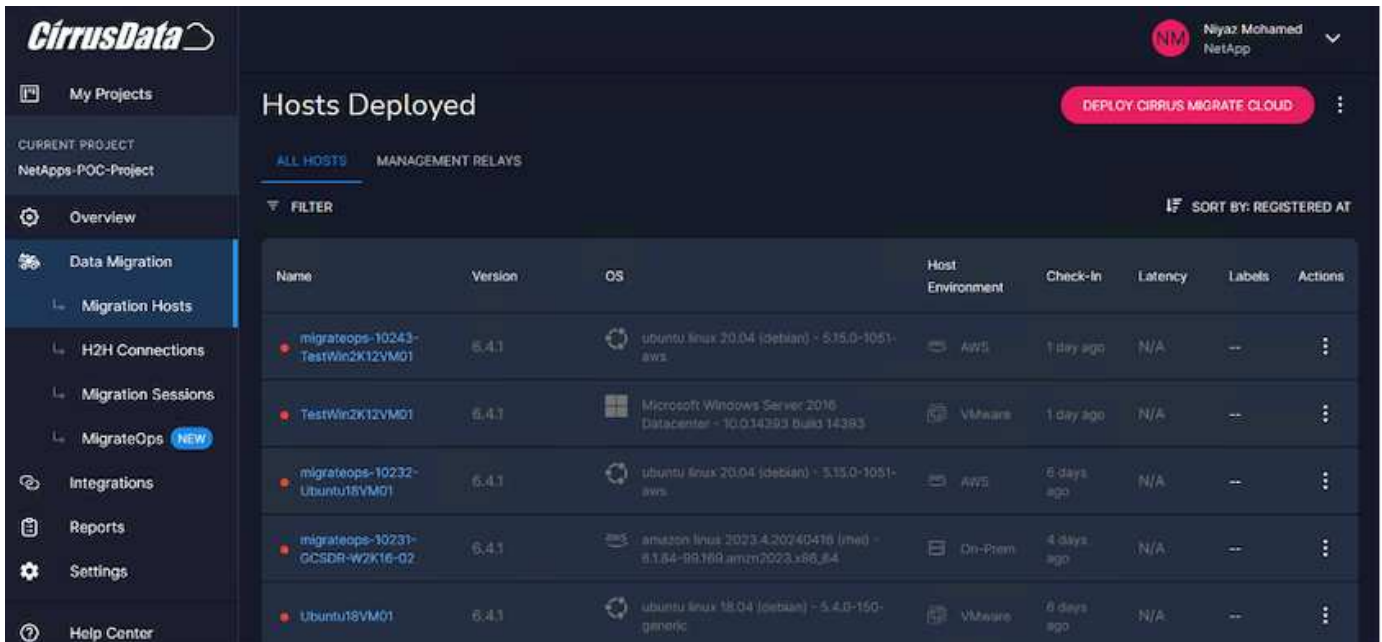
```
https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/getting-started-step1.html["Schrittweiser Implementierungsleitfaden"]
```

So fügen Sie ein FSX ONTAP-Volume zu einer VPC hinzu. Da diese Schritte sequentiell sind, stellen Sie sicher, dass sie in der Reihenfolge abgedeckt sind.

Für die Zwecke dieser Demonstration ist „DRaaS Demo“ der Name des erstellten Dateisystems.



Sobald die AWS VPC konfiguriert ist und FSX ONTAP basierend auf Ihren Performance-Anforderungen bereitgestellt wird, melden Sie sich bei "Erstellen Sie ein neues Projekt" einem vorhandenen Projekt an "cloud.cirrusdata.com" oder greifen Sie auf dieses zu.



Bevor Sie das Rezept für MigrationOps entwickeln, sollte AWS Cloud als Integration hinzugefügt werden. CMC bietet integrierte Integration mit FSX ONTAP und AWS. Die Integration für FSX ONTAP bietet folgende automatisierte Funktionen:

- Bereiten Sie Ihr FSX ONTAP Dateisystem vor:*
- Erstellen Sie neue Volumes und LUNs, die den Quell-Volumes entsprechen

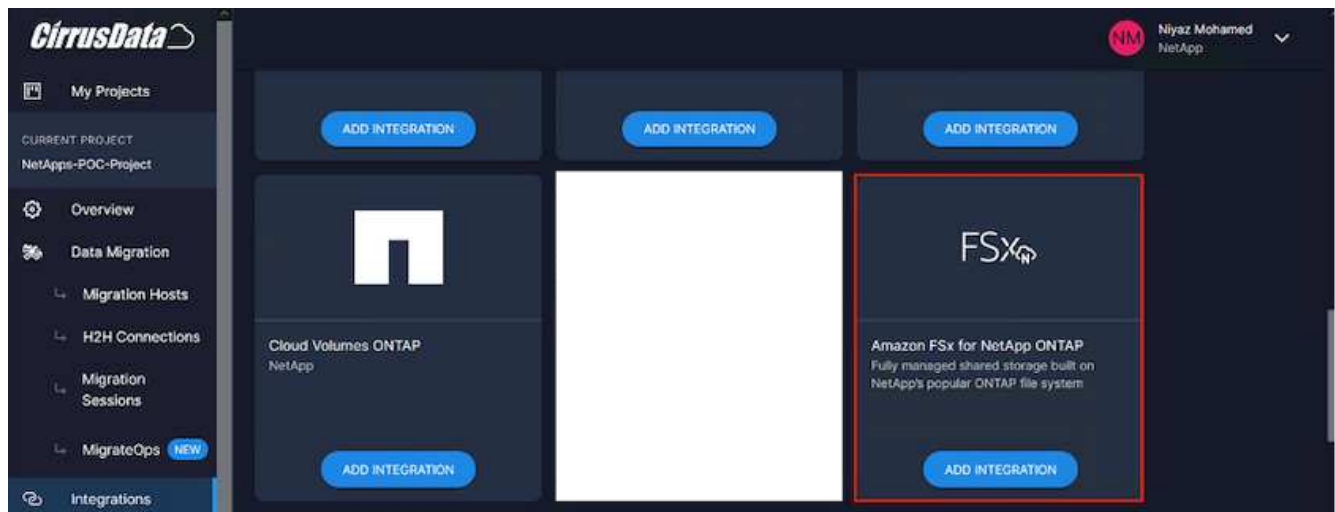
Hinweis: Eine Zielfestplatte im FSX ONTAP FS-Modell ist eine „LUN“, die auf einem „Volumen“ erstellt wird, das genug Kapazität hat, um die LUN zu enthalten plus eine angemessene Menge an Overhead für die Erleichterung von Snapshots und Metadaten. Die CMC-Automatisierung kümmert sich um all diese Details, um das entsprechende Volume und die LUN mit optionalen benutzerdefinierten Parametern zu erstellen.

- Erstellen Sie mit dem Host-Initiator-IQN Host-Entity (iGroups in FSX genannt)
- Ordnen Sie neu erstellte Volumes über Zuordnungen den entsprechenden Host-Einheiten zu
- Erstellen Sie alle anderen erforderlichen Konfigurationen

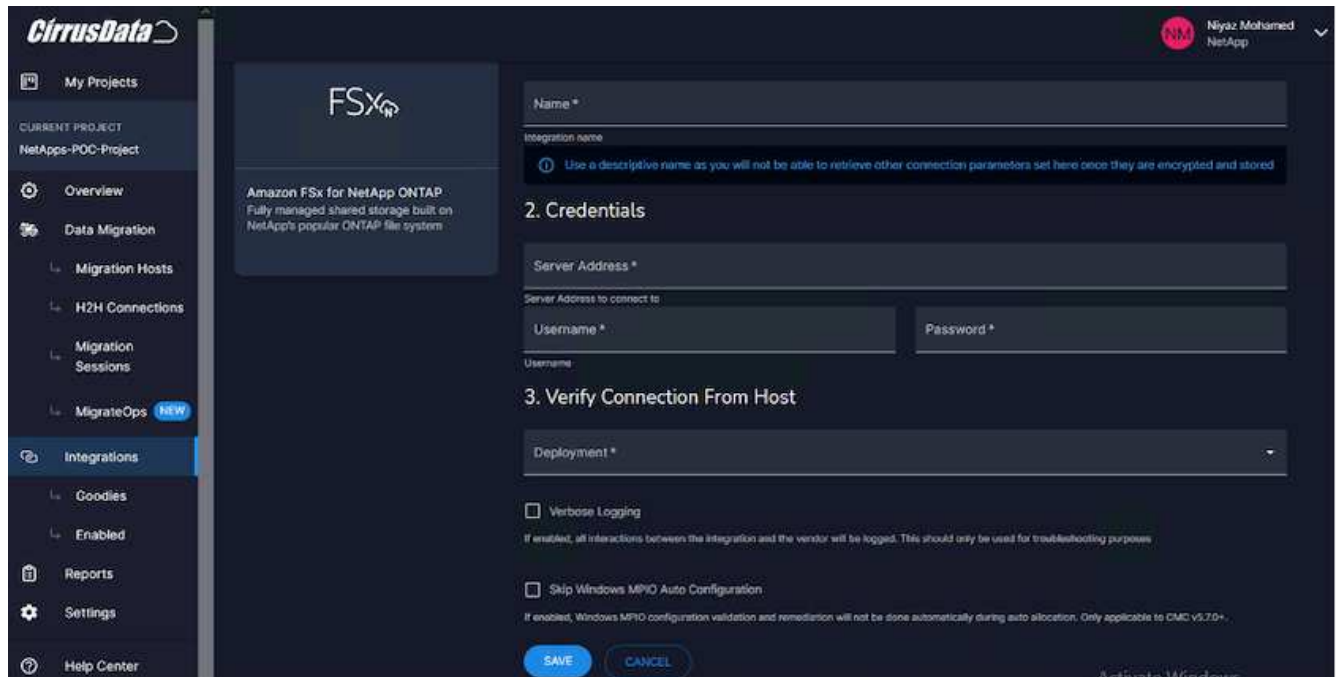
- Produktionshost für iSCSI-Verbindung vorbereiten:*
- Installieren und konfigurieren Sie ggf. die iSCSI-Funktion und richten Sie den Initiator ein.
- Falls erforderlich, installieren und konfigurieren Sie Multipath (MPIO für Windows) mit den richtigen Anbieterkennungen.
- Passen Sie ggf. Systemeinstellungen entsprechend den Best Practices des Herstellers an, z. B. mit udev-Einstellungen unter Linux.
- Erstellen und verwalten Sie iSCSI-Verbindungen, z. B. persistente/bevorzugte iSCSI-Ziele unter Windows.

So konfigurieren Sie die CMC-Integration für FSX ONTAP und AWS:

1. Melden Sie sich beim Cirrus Daten-Cloud-Portal an.
2. Öffnen Sie das Projekt, für das Sie die Integration aktivieren möchten.
3. Navigieren Sie zu Integrationen → Goodies.
4. Blättern Sie zu FSX ONTAP und klicken Sie auf INTEGRATION HINZUFÜGEN.



5. Geben Sie einen beschreibenden Namen (ausschließlich zu Anzeigezwecken) an, und fügen Sie die entsprechenden Anmeldeinformationen hinzu.



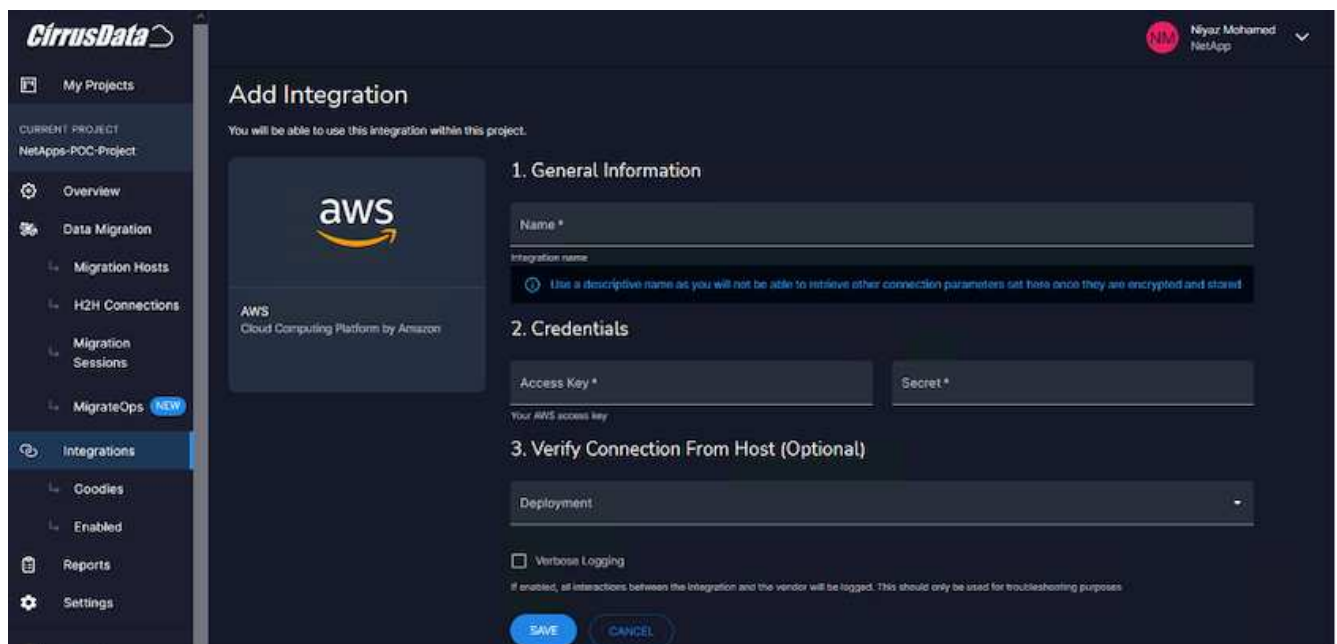
6. Sobald die Integration erstellt wurde, wählen Sie während der Erstellung einer neuen Migrationssitzung die Option Zielvolumen automatisch zuweisen aus, um automatisch neue Volumes auf FSX ONTAP zuzuweisen.

Hinweis: Neue LUNs werden mit der Größe des Quell-Volumes erstellt, es sei denn, für die Migration ist „in kleinere Volumes migrieren“ aktiviert.

Hinweis: Wenn eine Host-Entity (iGroup) nicht bereits existiert, wird eine neue erstellt. Alle Host-iSCSI-Initiator-IQNs werden dieser neuen Hosteinheit hinzugefügt.

Hinweis: Wenn eine vorhandene Hosteinheit mit einem der iSCSI-Initiatoren bereits existiert, wird sie erneut verwendet.

7. Sobald Sie fertig sind, fügen Sie die Integration für AWS, folgen Sie den Schritten auf dem Bildschirm.



Hinweis: Diese Integration wird bei der Migration von Virtual Machines vom lokalen Storage zu AWS zusammen mit der FSX ONTAP-Integration verwendet.

Hinweis: Verwenden Sie Managementrelais, um mit Cirrus Data Cloud zu kommunizieren, wenn keine direkte ausgehende Verbindung für die zu migrierenden Produktionsinstanzen besteht.

Mit zusätzlichen Integrationen ist es an der Zeit, Hosts beim Projekt zu registrieren. Sehen wir uns dazu ein Beispielszenario an.

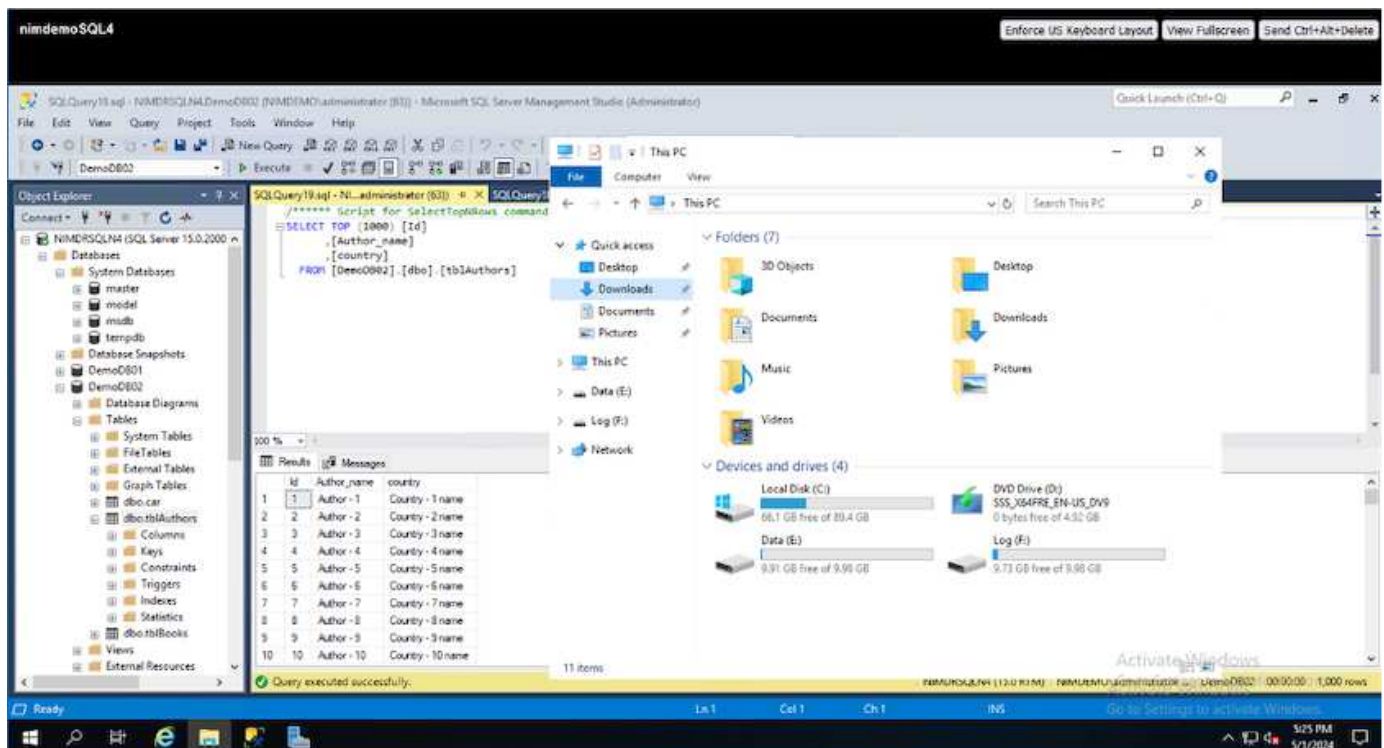
Szenario für die Hostregistrierung

VMware Gast-VMs in vCenter im lokalen Datacenter:

- Windows 2016 mit SQL Server mit drei VMDKs einschließlich Betriebssystem und Datenfestplatten. Er führt eine aktive Datenbank aus. Die Datenbank befindet sich auf einem Daten-Volume mit zwei VMDKs.

Hinweis: Da die Quelle eine VMware-Umgebung ist und VMDKs verwendet werden, ist die Windows iSCSI Initiator-Software derzeit nicht auf dieser Gast-VM konfiguriert. Um eine Verbindung zu unserem Ziel-Storage über iSCSI herzustellen, müssen sowohl iSCSI als auch MPIO installiert und konfiguriert werden. Die Integration von Cirrus Data Cloud führt diese Installation während des Vorgangs automatisch durch.

Hinweis: Die im vorherigen Abschnitt konfigurierte Integration automatisiert die Konfiguration des neuen Zielspeichers bei der Erstellung der neuen Laufwerke, bei der Einrichtung der Hosteinheiten und ihrer IQNs und sogar bei der Wiederherstellung der Anwendungs-VM (Host) für iSCSI- und Multipath-Konfigurationen.



Bei dieser Demonstration werden die Applikations-VMDKs von jeder VM auf ein automatisch bereitgestelltes und zugeordnetes iSCSI-Volume von FSX ONTAP migriert. Die OS VMDK wird in diesem Fall zu einem Amazon EBS Volume migriert, da Amazon EC2 Instanzen diesen Amazon EBS nur als Boot-Disk unterstützen.

Hinweis: Der Skalierungsfaktor bei diesem Migrationsansatz ist die Netzwerkbandbreite und die Leitung, die On-Premises mit der AWS VPC verbindet. Da jede VM 1:1 Hostsitzungen konfiguriert hat, hängt die Gesamtmigrations-Performance von zwei Faktoren ab:

- Netzwerkbandbreite
- Typ der Zielinstanz und ENI-Bandbreite

Die Migrationsschritte sind wie folgt:

1. Installieren Sie den CMC-Agent auf jedem Host (Windows und Linux), der für die Migrationswelle bestimmt ist. Dies kann durch Ausführen eines einzeilige Installationsbefehls erfolgen.

Hierzu klicken Sie auf Data Migration > Migration Hosts > Klicken Sie auf „Deploy Cirrus Migrate Cloud“ und wählen Sie „Windows“ aus.

Kopieren Sie anschließend die `ieX` Befehl an den Host und führen Sie es mit PowerShell aus. Sobald die Bereitstellung des Agenten erfolgreich war, wird der Host unter „Migrationshosts“ zum Projekt hinzugefügt.

The screenshot shows the CirrusData console interface. On the left, the 'Migration Hosts' menu item is highlighted with a red box. A modal dialog box titled 'Deploy Cirrus Migrate Cloud' is open, showing the 'WINDOWS' tab. The dialog contains the following content:

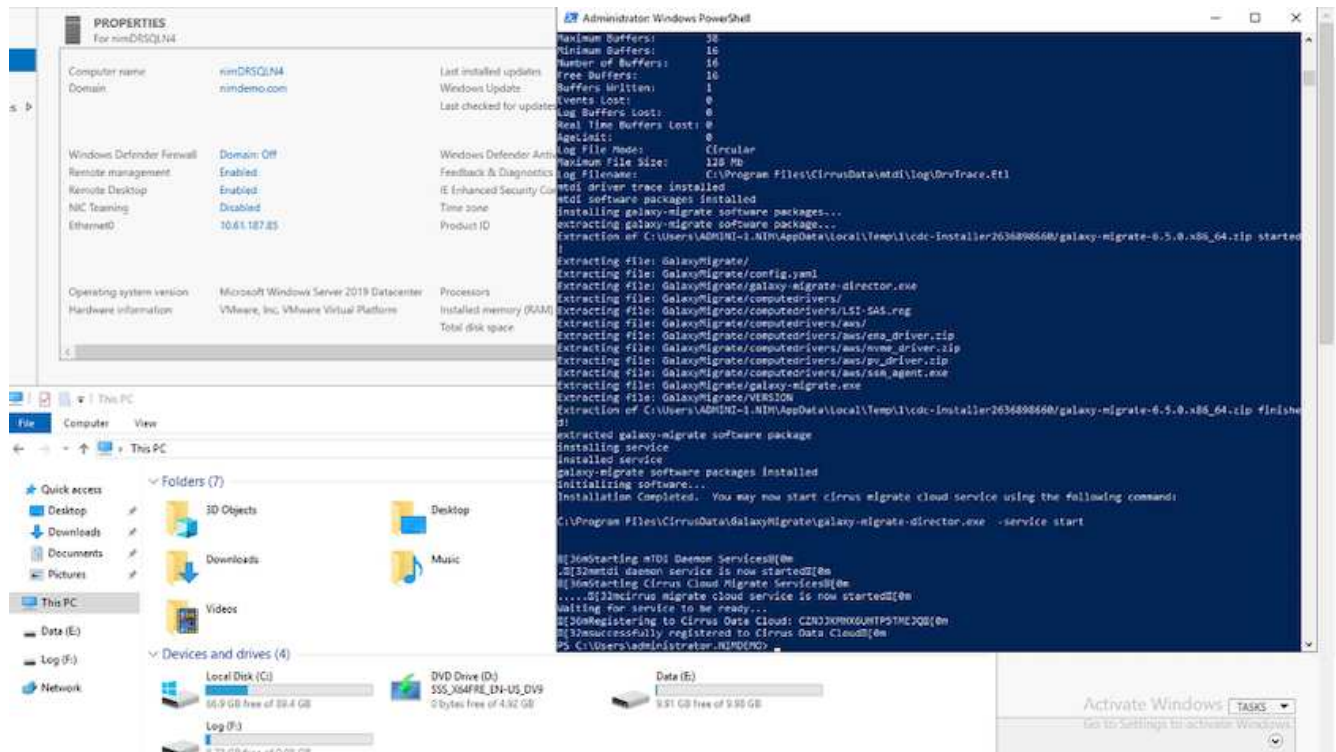
Installation - Windows
 In your Windows administrator account, run the following command in powershell to install Cirrus Migrate Cloud:

```
ieX * ($irm https://get.cirrusdata.cloud/install-cmc-win) -rjc C7N.LJKMHXBUHTP5TMEJQ*
```

Uninstall - Windows
 Run the following Command to uninstall Cirrus Migrate Cloud after migration is completed:

```
ieX * ($irm https://get.cirrusdata.cloud/install-cmc-win) -uninstall*
```

The background shows a table of 'Hosts Deployed' with columns for Name, Check-In, Latency, Labels, and Actions. The table lists several hosts with their respective check-in times and latencies.



2. Bereiten Sie die YAML für jede virtuelle Maschine vor.

Hinweis: Es ist ein wichtiger Schritt, eine YAML für jede VM zu haben, die das notwendige Rezept oder Blaupause für die Migrationsaufgabe angibt.

Die YAML liefert den Operationsnamen, Notizen (Beschreibung) zusammen mit dem Rezeptnamen als MIGRATEOPS_AWS_COMPUTE`Der Hostname (`system_name) Und Name der Integration (integration_name) Und der Quell- und Zielkonfiguration. Benutzerdefinierte Skripte können vor und nach der Umstellung als aktiv angegeben werden.

```
operations:
  - name: Win2016 SQL server to AWS
    notes: Migrate OS to AWS with EBS and Data to FSx ONTAP
    recipe: MIGRATEOPS_AWS_COMPUTE
    config:
      system_name: Win2016-123
      integration_name: NimAWSHybrid
      migrateops_aws_compute:
        region: us-west-2
        compute:
          instance_type: t3.medium
          availability_zone: us-west-2b
        network:
          vpc_id: vpc-05596abe79cb653b7
          subnet_id: subnet-070aeb9d6b1b804dd
          security_group_names:
            - default
      destination:
```

```

        default_volume_params:
            volume_type: GP2
        iscsi_data_storage:
            integration_name: DemoDRaaS
        default_volume_params:
            netapp:
                qos_policy_name: ""
    migration:
        session_description: Migrate OS to AWS with EBS and
Data to FSx ONTAP
        qos_level: MODERATE
    cutover:
        stop_applications:
            - os_shell:
                script:
                    - stop-service -name 'MSSQLSERVER'
-Force
                    - Start-Sleep -Seconds 5
                    - Set-Service -Name 'MSSQLSERVER'
-StartupType Disabled
                    - write-output "SQL service stopped
and disabled"
            - storage_unmount:
                mountpoint: e
            - storage_unmount:
                mountpoint: f
        after_cutover:
            - os_shell:
                script:
                    - stop-service -name 'MSSQLSERVER'
-Force
                    - write-output "Waiting 90 seconds to
mount disks..." > log.txt
                    - Start-Sleep -Seconds 90
                    - write-output "Now re-mounting disks
E and F for SQL..." >>log.txt
            - storage_unmount:
                mountpoint: e
            - storage_unmount:
                mountpoint: f
            - storage_mount_all: {}
            - os_shell:
                script:
                    - write-output "Waiting 60 seconds to
restart SQL Services..." >>log.txt

```

```

-Force

>>log.txt

-StartupType Automatic

- Start-Sleep -Seconds 60
- stop-service -name 'MSSQLSERVER'

- Start-Sleep -Seconds 3
- write-output "Start SQL Services..."

- Set-Service -Name 'MSSQLSERVER'

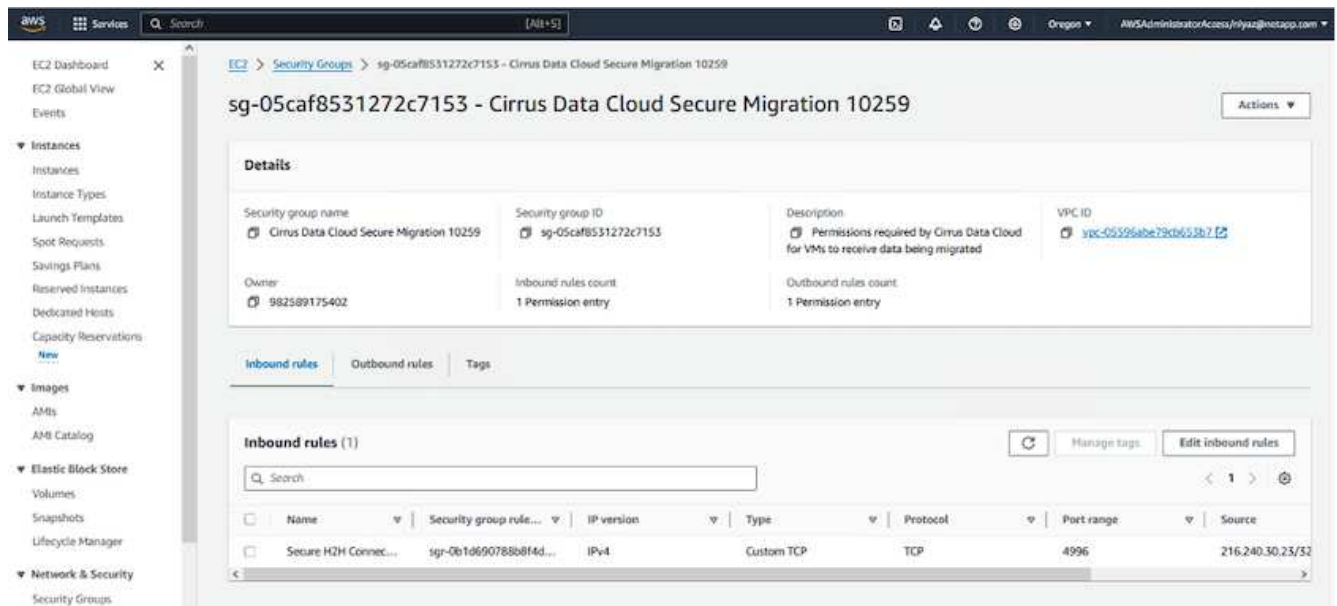
- start-service -name 'MSSQLSERVER'
- write-output "SQL started" >>log.txt

```

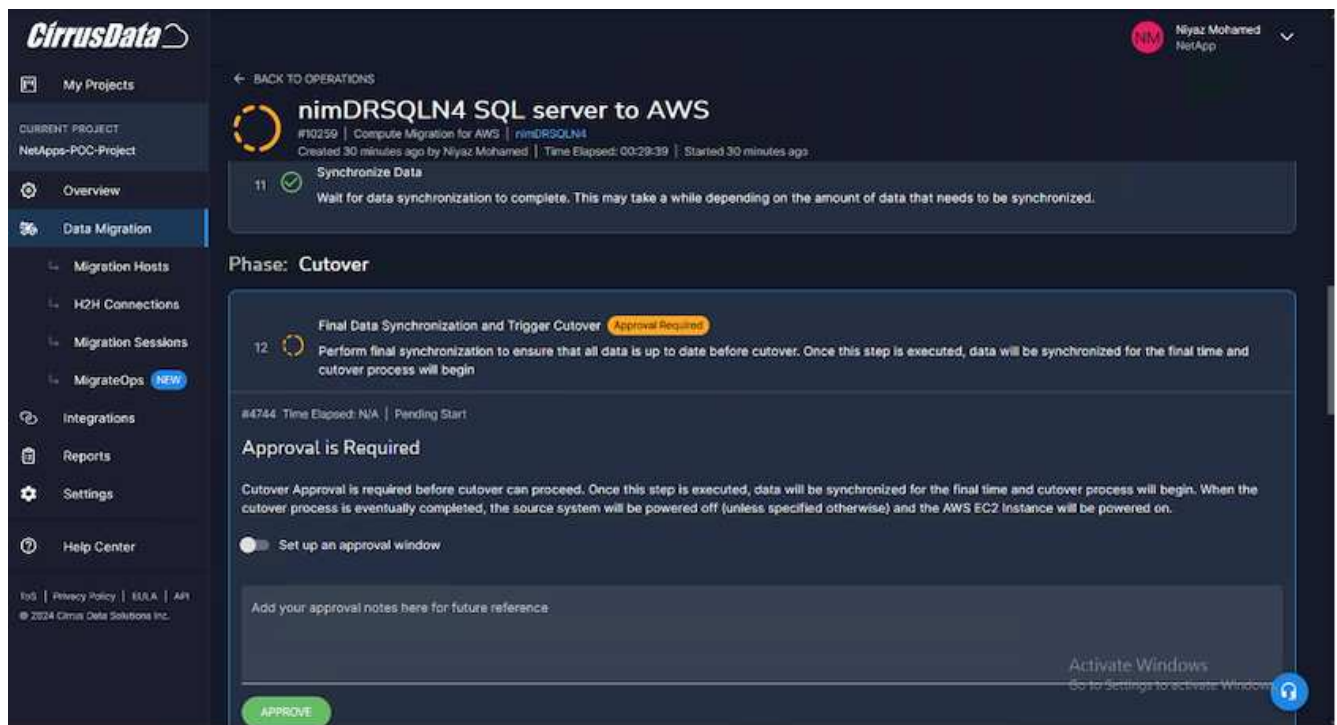
- Sobald die YAMLs eingerichtet sind, erstellen Sie die MigrateOps-Konfiguration. Gehen Sie dazu zu Data Migration > MigrateOps, klicken Sie auf „Start New Operation“ und geben Sie die Konfiguration im gültigen YAML-Format ein.
 - Klicken Sie auf „Create Operation“.
- Hinweis:** Um Parallelität zu erreichen, muss jeder Host eine YAML-Datei angeben und konfigurieren.
- Sofern nicht `scheduled_start_time` Feld wird in der Konfiguration angegeben, der Vorgang wird sofort gestartet.
 - Der Vorgang wird jetzt ausgeführt und fortgesetzt. Über die Benutzeroberfläche von Cirrus Data Cloud können Sie den Fortschritt mit detaillierten Meldungen überwachen. Diese Schritte umfassen automatisch Aufgaben, die normalerweise manuell ausgeführt werden, z. B. die automatische Zuweisung und das Erstellen von Migrationssitzungen.



Hinweis: Während der Host-zu-Host-Migration wird eine zusätzliche Sicherheitsgruppe mit einer Regel erstellt, die Inbound 4996-Port zulässt, die den erforderlichen Port für die Kommunikation ermöglicht und nach Abschluss der Synchronisierung automatisch gelöscht wird.



7. Während diese Migrationssitzung synchronisiert wird, gibt es in Phase 3 (Umstellung) einen zukünftigen Schritt mit dem Label „Genehmigung erforderlich“. Nach einem MigrateOps-Rezept müssen kritische Aufgaben (wie beispielsweise Migration-Umstellungen) vor der Ausführung erst genehmigt werden. Projektoperatoren oder Administratoren können diese Aufgaben über die Benutzeroberfläche genehmigen. Es kann auch ein zukünftiges Genehmigungsfenster erstellt werden.



8. Nach der Genehmigung wird der MigrateOps-Vorgang mit der Umstellung fortgesetzt.
 9. Nach einem kurzen Moment wird der Vorgang abgeschlossen.



Hinweis: Mit Hilfe der Cirrus Data cmotion™ Technologie wurde der Zielspeicher mit allen aktuellen Änderungen auf dem neuesten Stand gehalten. Daher dauert es nach Genehmigung nur eine Minute, bis der gesamte endgültige Umstellungsprozess abgeschlossen ist.

Verifizierung nach der Migration

Sehen wir uns die migrierte Amazon EC2 Instanz an, auf der das Windows Server-Betriebssystem ausgeführt wird, und die folgenden Schritte, die abgeschlossen sind:

1. Windows SQL Services werden jetzt gestartet.
2. Die Datenbank ist wieder online und verwendet Speicher vom iSCSI-Multipath-Gerät.
3. Alle neuen Datenbankeinträge, die während der Migration hinzugefügt wurden, sind in der neu migrierten Datenbank zu finden.
4. Der alte Speicher ist jetzt offline.

Hinweis: Mit nur einem Klick, um den Datenmobilitätsvorgang als Code zu übermitteln, und einem Klick, um die Umstellung zu genehmigen, hat die VM erfolgreich von lokalen VMware-Systemen auf eine Amazon EC2-Instanz mithilfe von FSX ONTAP und seinen iSCSI-Funktionen migriert.

Hinweis: Aufgrund der AWS API Beschränkung würden die konvertierten VMs als „Ubuntu“ angezeigt. Dies ist streng ein Anzeigeproblem und hat keinen Einfluss auf die Funktionalität der migrierten Instanz. In einer kommenden Version wird dieses Problem behoben.

Hinweis: Der Zugriff auf die migrierten Amazon EC2-Instanzen erfolgt über die Zugangsdaten, die auf der On-Premises-Seite verwendet wurden.

Migrieren Sie VMs zu Amazon EC2 und profitieren Sie von Amazon FSX for ONTAP – weitere Möglichkeiten und Schlussfolgerungen

In diesem Artikel werden weitere Möglichkeiten für diese Migrationslösung sowie der Abschluss des Themas hervorgehoben.

Andere Möglichkeiten

Derselbe Ansatz kann auch für die Migration von VMs unter Verwendung von in-Guest Storage auf lokalen

VMs erweitert werden. Die BS-VMDK kann mithilfe von CMC migriert werden, und die in-Guest iSCSI-LUNs können mit SnapMirror repliziert werden. Der Prozess erfordert, dass die Spiegelung gebrochen und die LUN an die neu migrierte Amazon EC2 Instanz angehängt wird, wie in der Abbildung unten dargestellt.



Schlussfolgerung

Dieses Dokument bietet eine vollständige Einführung in die Verwendung der Migrationsfunktion des CMC zur Migration von Daten, die in lokalen VMware-Repositories unter Verwendung von Amazon EC2-Instanzen und FSX ONTAP gespeichert sind.

Das folgende Video zeigt den Migrationsprozess von Anfang bis Ende:

[Migration von VMware VMs zu Amazon EC2](#)

Sehen Sie sich das GUI und die grundlegende lokale Migration von Amazon EBS to FSX ONTAP an:



Local Migration with
MigrateOps

Migration auf jeden skalierbaren Storage mit Cirrus Migrate Cloud

NetApp Hybrid-Multi-Cloud mit VMware Lösungen

Anwendungsfälle für die VMware Hybrid-Multi-Cloud

Anwendungsfälle für NetApp Hybrid-Multi-Cloud mit VMware

Ein Überblick über die Anwendungsfälle, die für DIE IT-Abteilung bei der Planung von Hybrid-Cloud- oder Cloud-First-Implementierungen von Bedeutung sind

Gängige Anwendungsfälle

Anwendungsfälle:

- Disaster Recovery,
- Hosting von Workloads während der Rechenzentrumswartung, * schneller Burst, in dem zusätzliche Ressourcen über die im lokalen Rechenzentrum bereitgestellten Ressourcen erforderlich sind,
- VMware-Site-Erweiterung,
- Schnelle Migration in die Cloud,
- Entwicklung/Test und
- Modernisierung von Applikationen mithilfe von zusätzlichen Cloud-Technologien

In der gesamten Dokumentation werden die Referenzen für Cloud-Workloads anhand der VMware Anwendungsfälle detailliert beschrieben. Anwendungsfälle sind:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)

- Migrieren
- Erweitern

In DER IT-Entwicklung

Die meisten Unternehmen befinden sich auf dem Weg zur Transformation und Modernisierung. Im Rahmen dieses Prozesses versuchen Unternehmen, ihre vorhandenen VMware Investitionen zu nutzen und gleichzeitig von den Vorteilen der Cloud zu profitieren und Möglichkeiten für eine nahtlose Migration zu entdecken. Durch diesen Ansatz würde sich ihre Modernisierungsbemühungen sehr vereinfachen, da sich die Daten bereits in der Cloud befinden.

Die einfachste Antwort auf dieses Szenario sind die Angebote von VMware in jedem Hyperscaler. Wie bei NetApp Cloud Volumes bietet VMware eine Möglichkeit, lokale VMware Umgebungen in jede Cloud zu verschieben oder zu erweitern. So können Sie vorhandene Ressourcen, Fachkenntnisse und Tools weiterhin nutzen, während Sie Workloads nativ in der Cloud ausführen. Das verringert die Risiken, da keine Serviceunterbrechungen oder IP-Änderungen erforderlich sind. Das IT-Team kann so unter Verwendung vorhandener Fachkenntnisse und Tools vor Ort Verfahren. Dies ermöglicht beschleunigte Cloud-Migrationen und einen viel reibungsloseren Übergang zu einer Hybrid Multi Cloud Architektur.

Bedeutung von zusätzlichen NFS-Storage-Optionen

Während VMware in jeder Cloud seinen Kunden einzigartige Hybrid-Funktionen bietet, haben begrenzte zusätzliche NFS-Storage-Optionen den Nutzen für Unternehmen mit Storage-lastigen Workloads eingeschränkt. Da Storage direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung von Storage darin, weitere Hosts hinzuzufügen. Die Kosten können bei Storage-intensiven Workloads um 35 bis 40 % oder mehr gesenkt werden. Diese Workloads erfordern nur zusätzlichen Storage und keine zusätzliche Leistung. Aber das bedeutet, dass zusätzliche Hosts bezahlt werden.

Betrachten wir das folgende Szenario:

Ein Kunde benötigt nur fünf Hosts für CPU und Arbeitsspeicher, hat aber hohe Storage-Anforderungen und benötigt 12 Hosts, um die Storage-Anforderungen zu erfüllen. Diese Anforderung kippt letztlich in Richtung Finanzskalierung, indem sie zusätzliche Leistung kaufen müssen, wenn sie nur den Storage erhöhen müssen.

Wenn Sie Cloud-Einführung und -Migrationen planen, ist es immer wichtig, den besten Ansatz zu bewerten und den einfachsten Weg zu gehen, der die Gesamtinvestitionen reduziert. Der gängigste und einfachste Ansatz für jede Applikationsmigration besteht in Rehosting (auch bekannt als „Lift and Shift“), in dem keine Virtual Machine (VM) oder Datenkonvertierung vorhanden ist. NetApp Cloud Volumes mit dem softwaredefinierten Datacenter (SDDC) von VMware und ergänzen vSAN und bieten eine einfache „Lift-and-Shift“-Option.

VMware vSphere Automation

Einführung in die Automatisierung für ONTAP und vSphere

Auf dieser Seite werden die Vorteile der Automatisierung der grundlegenden ONTAP Funktionen in einer VMware vSphere Umgebung beschrieben.

VMware Automatisierung

Seit den ersten Tagen von VMware ESX ist die Automatisierung ein integraler Bestandteil des Managements von VMware Umgebungen. Die Möglichkeit, Infrastruktur als Code zu implementieren und Verfahren auf private Cloud-Vorgänge auszuweiten, um Bedenken hinsichtlich Skalierbarkeit, Flexibilität, Self-Provisioning

und Effizienz zu zerstreuen.

Die Automatisierung kann in die folgenden Kategorien eingeteilt werden:

- * Bereitstellung virtueller Infrastrukturen*
- **Betrieb der Gastmaschine**
- **Cloud-Betrieb**

Administratoren stehen im Hinblick auf die Automatisierung ihrer Infrastruktur viele Optionen zur Verfügung. Ob durch die Nutzung nativer vSphere Funktionen wie Host-Profile oder Anpassungsspezifikationen für Virtual Machines über verfügbare APIs auf den VMware Software-Komponenten, Betriebssystemen und NetApp Storage-Systemen verfügen - hier sind umfangreiche Dokumentationen und Anleitungen verfügbar.

Data ONTAP 8.0.1 und höher unterstützt bestimmte VMware vSphere APIs for Array Integration (VAAI)-Funktionen, wenn der ESX-Host ESX 4.1 oder höher ausführt. VAAI ist eine Reihe von APIs für die Kommunikation zwischen VMware vSphere ESXi Hosts und Storage-Geräten. Diese Funktionen helfen, Vorgänge vom ESX Host zum Storage-System zu verlagern und den Netzwerkdurchsatz zu steigern. Der ESX-Host aktiviert die Funktionen automatisch in der richtigen Umgebung. Sie können bestimmen, in welchem Umfang Ihr System VAAI-Funktionen verwendet, indem Sie die Statistiken in den VAAI-Zählern prüfen.

Der häufigste Ausgangspunkt für die Automatisierung der Implementierung einer VMware-Umgebung ist die Bereitstellung von Block- oder dateibasierten Datastores. Vor der Entwicklung der entsprechenden Automatisierung ist es wichtig, die Anforderungen der eigentlichen Aufgaben abzubilden.

Weitere Informationen zur Automatisierung von VMware-Umgebungen finden Sie in den folgenden Ressourcen:

- ["„NetApp Pub“"](#). NetApp Konfigurationsmanagement und Automatisierung:
- ["Ansible Galaxy Community für VMware"](#). Eine Sammlung von Ansible-Ressourcen für VMware.
- ["VMware {Code} Ressourcen"](#). Ressourcen, die zum entwickeln von Lösungen für das softwaredefinierte Datacenter erforderlich sind, einschließlich Foren, Designstandards, Beispielcode und Entwickler-Tools

Herkömmliche Bereitstellung Von Block Storage

VSphere herkömmliche Block-Storage-Bereitstellung mit ONTAP

VMware vSphere unterstützt die folgenden VMFS-Datstore-Optionen, wobei die Unterstützung für das ONTAP-SAN-Protokoll angegeben ist.

VMFS-Datenspeicher-Optionen	Unterstützte ONTAP SAN-Protokolle
"Fibre Channel (FC)"	ja
"Fibre Channel over Ethernet (FCoE)"	ja
"ISCSI"	ja
ISCSI-Erweiterungen für RDMA (iSER)	Nein
"NVMe over Fabric mit FC (NVMe/FC)"	ja

VMFS-Datenspeicher-Optionen	Unterstützte ONTAP SAN-Protokolle
NVMe over Fabric mit RDMA over Converged Ethernet (NVMe/RoCE)	Nein



Wenn iSER- oder NVMe/RoCE-VMFS erforderlich ist, prüfen Sie SANtricity-basierte Storage-Systeme.

VMware VMFS Datastore – Fibre-Channel-Storage-Back-End mit ONTAP

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit ONTAP Fibre Channel (FC)-Storage behandelt.

Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- ONTAP Storage-Systeme (FAS/AFF/CVO/ONTAP Select/ASA) mit {ontap_Version}
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ONTAP WWPN von Host-, Ziel- und SVM- sowie LUN-Informationen
- ["Das ausgefüllte FC-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- Informationen zu vSphere Hosts
 - {vsphere_Version}
- Fabric Switch(e)
 - Mit verbundenen ONTAP FC-Daten-Ports und vSphere-Hosts
 - Bei aktivierter N_Port ID Virtualization (NPIV)
 - Erstellen Sie einen einzelnen Initiator-Zielbereich.
 - Erstellen Sie für jeden Initiator eine Zone (einzelne Initiatorzone).
 - Geben Sie für jede Zone ein Ziel an, das die logische ONTAP FC-Schnittstelle (WWPN) für die SVMs ist. Es sollten mindestens zwei logische Schnittstellen pro Node pro SVM vorhanden sein. Verwenden Sie den WWPN der physischen Ports nicht.
- Ein ONTAP Tool für Implementierung, Konfiguration und Einsatzbereitschaft von VMware vSphere

Bereitstellung eines VMFS-Datenspeichers

Gehen Sie wie folgt vor, um einen VMFS-Datenspeicher bereitzustellen:

1. Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#)
2. Überprüfen Sie das ["FCP-Konfiguration wird unterstützt"](#).

ONTAP Aufgaben

1. ["Vergewissern Sie sich, dass Sie eine ONTAP-Lizenz für FCP haben."](#)
 - a. Verwenden Sie die `system license show` Befehl zum Überprüfen, ob FCP aufgeführt ist.
 - b. Nutzung `license add -license-code <license code>` Um die Lizenz hinzuzufügen.

2. Vergewissern Sie sich, dass das FCP-Protokoll auf der SVM aktiviert ist.
 - a. ["Überprüfen Sie das FCP auf einer vorhandenen SVM."](#)
 - b. ["Konfigurieren Sie das FCP für eine vorhandene SVM."](#)
 - c. ["Erstellen Sie mit dem FCP eine neue SVM."](#)
3. Stellen Sie sicher, dass auf einer SVM logische FCP-Schnittstellen verfügbar sind.
 - a. Nutzung `Network Interface show` Um den FCP-Adapter zu überprüfen.
 - b. Wird mit der GUI eine SVM erstellt, gehören zu diesem Prozess logische Schnittstellen.
 - c. Verwenden Sie zum Umbenennen von Netzwerkschnittstellen `Network Interface modify`.
4. ["Erstellen und Zuordnen einer LUN."](#) Überspringen Sie diesen Schritt, wenn Sie ONTAP-Tools für VMware vSphere verwenden.

Aufgaben für VMware vSphere

1. Die HBA-Treiber sind installiert. Von VMware unterstützte HBAs verfügen über Out-of-the-Box-Treiber, die im sichtbar sein sollten ["Informationen Zum Storage-Adapter"](#).
2. ["Stellen Sie einen VMFS-Datenspeicher mit ONTAP Tools bereit"](#).

VSphere VMFS Datenspeicher – Fibre Channel over Ethernet Storage-Protokoll mit ONTAP

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit dem FCoE-Transportprotokoll (Fibre Channel over Ethernet) zu ONTAP Storage behandelt.

Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- ONTAP Storage-System (FAS/AFF/CVO/ONTAP Select) mit {ontap_Version}
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ["Eine unterstützte FCoE-Kombination"](#)
- ["Ein ausgefülltes Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- Informationen zu vSphere Hosts
 - {vsphere_Version}
- Fabric Switch(e)
 - Mit ONTAP FC-Daten-Ports oder vSphere-Hosts verbunden
 - Bei aktivierter N_Port ID Virtualization (NPIV)
 - Erstellen Sie einen einzelnen Initiator-Zielbereich.
 - ["FC/FCoE-Zoning konfiguriert"](#)
- Netzwerk-Switch(e)
 - FCoE-Support
 - DCB-Support
 - ["Jumbo Frames für FCoE"](#)

- ONTAP Tool für VMware vSphere – implementiert, konfiguriert und betriebsbereit

Bereitstellung eines VMFS-Datenspeichers

- Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#).
- ["Vergewissern Sie sich, dass die FCoE-Konfiguration unterstützt wird"](#).

ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für FCP."](#)
 - a. Verwenden Sie die `system license show` Befehl zum Überprüfen, ob das FCP aufgeführt ist.
 - b. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. Vergewissern Sie sich, dass das FCP-Protokoll auf der SVM aktiviert ist.
 - a. ["Überprüfen Sie das FCP auf einer vorhandenen SVM."](#)
 - b. ["Konfigurieren Sie das FCP für eine vorhandene SVM."](#)
 - c. ["Erstellen Sie eine neue SVM mit dem FCP."](#)
3. Vergewissern Sie sich, dass auf der SVM logische FCP-Schnittstellen verfügbar sind.
 - a. Nutzung `Network Interface show` Um den FCP-Adapter zu überprüfen.
 - b. Wird mit der GUI eine SVM erstellt, sind logische Schnittstellen Teil dieses Prozesses.
 - c. Verwenden Sie zum Umbenennen der Netzwerkschnittstelle `Network Interface modify`.
4. ["Erstellen und Zuordnen einer LUN"](#); überspringen Sie diesen Schritt, wenn Sie ONTAP-Tools für VMware vSphere nutzen.

Aufgaben für VMware vSphere

1. Vergewissern Sie sich, dass die HBA-Treiber installiert sind. Bei den von VMware unterstützten HBAs sind die Treiber Out-of-the-Box implementiert und sollten im sichtbar sein ["Informationen zu Storage-Adapttern"](#).
2. ["Stellen Sie einen VMFS-Datenspeicher mit ONTAP Tools bereit"](#).

VSphere VMFS Datenspeicher – iSCSI-Storage-Back-End mit ONTAP

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit ONTAP iSCSI-Speicher behandelt.

Verwenden Sie für die automatische Bereitstellung das folgende Skript: [\[Ansible\]](#).

Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- ONTAP Storage-Systeme (FAS/AFF/CVO/ONTAP Select/ASA) mit {ontap_Version}
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ONTAP Netzwerkport, SVM und LUN-Informationen für iSCSI
- ["Ein ausgefülltes iSCSI-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- Informationen zu vSphere Hosts

- {vsphere_Version}
- IP-Informationen zum iSCSI VMkernel Adapter
- Netzwerk-Switch(e)
 - Mit Netzwerk-Daten-Ports des ONTAP Systems und verbundenen vSphere Hosts
 - Für iSCSI konfigurierte VLANs
 - (Optional) Link Aggregation konfiguriert für ONTAP Netzwerkdatenports
- ONTAP Tool für VMware vSphere – implementiert, konfiguriert und betriebsbereit

Schritte

1. Prüfen Sie die Kompatibilität mit dem "[Interoperabilitäts-Matrix-Tool \(IMT\)](#)".
2. "[Vergewissern Sie sich, dass die iSCSI-Konfiguration unterstützt wird.](#)"
3. Führen Sie die folgenden Aufgaben für ONTAP und vSphere aus.

ONTAP Aufgaben

1. "[Überprüfen Sie die ONTAP Lizenz für iSCSI](#)".
 - a. Verwenden Sie die `system license show` Befehl, um zu überprüfen, ob iSCSI aufgeführt ist.
 - b. Nutzung `license add -license-code <license code>` Um die Lizenz hinzuzufügen.
2. "[Vergewissern Sie sich, dass das iSCSI-Protokoll auf der SVM aktiviert ist.](#)"
3. Vergewissern Sie sich, dass auf der SVM logische iSCSI-Netzwerk-Schnittstellen verfügbar sind.



Wenn über die GUI eine SVM erstellt wird, werden auch iSCSI-Netzwerkschnittstellen erstellt.

4. Verwenden Sie die `network interface` Befehl zum Anzeigen oder Ändern der Netzwerkschnittstelle.



Es werden zwei iSCSI-Netzwerkschnittstellen pro Node empfohlen.

5. "[Erstellen Sie eine iSCSI-Netzwerkschnittstelle.](#)" Sie können die Service-Richtlinie für Standarddatenblöcke verwenden.
6. "[Überprüfen Sie, ob der Daten-iscsi-Service in der Service-Richtlinie enthalten ist.](#)" Verwenden Sie können `network interface service-policy show` Zu überprüfen.
7. "[Vergewissern Sie sich, dass Jumbo Frames aktiviert sind.](#)"
8. "[Erstellen und Zuordnen der LUN.](#)" Überspringen Sie diesen Schritt, wenn Sie ONTAP-Tools für VMware vSphere verwenden. Wiederholen Sie diesen Schritt für jede LUN.

Aufgaben für VMware vSphere

1. Stellen Sie sicher, dass mindestens eine NIC für das iSCSI-VLAN verfügbar ist. Zwei NICs werden bevorzugt, um eine bessere Performance und Fehlertoleranz zu schaffen.
2. "[Ermitteln Sie die Anzahl der physischen NICs, die auf dem vSphere-Host verfügbar sind.](#)"
3. "[Konfigurieren Sie den iSCSI-Initiator.](#)" Ein typischer Anwendungsfall ist ein Software-iSCSI-Initiator.
4. "[Stellen Sie sicher, dass der TCP/IP-Stack für iSCSI verfügbar ist.](#)"

5. "Vergewissern Sie sich, dass iSCSI-Portgruppen verfügbar sind".
 - In der Regel verwenden wir einen einzelnen virtuellen Switch mit mehreren Uplink-Ports.
 - Verwenden Sie 1:1-Adapterzuordnung.
6. Vergewissern Sie sich, dass die iSCSI-VMkernel-Adapter für die Anzahl der NICs aktiviert sind und IP-Adressen zugewiesen sind.
7. "Binden Sie den iSCSI-Software-Adapter an die iSCSI-VMkernel-Adapter."
8. "Stellen Sie den VMFS-Datenspeicher mit ONTAP Tools bereit". Wiederholen Sie diesen Schritt für alle Datenspeicher.
9. "Prüfen Sie, ob die Hardware-Beschleunigung unterstützt wird."

Was kommt als Nächstes?

Nach Abschluss dieser Aufgaben kann der VMFS-Datenspeicher für die Bereitstellung von Virtual Machines genutzt werden.

Ansible Playbook

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
        password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
        register: vclogin

    # Generate Session ID for ONTAP tools with vCenter
    - name: Generate a Session ID for ONTAP tools with vCenter
      uri:
        url: "https://{{ ontap_tools_ip
        }}:8143/api/rest/2.0/security/user/login"
        validate_certs: false
        method: POST
        return_content: yes
        body_format: json
        body:
```

```

    vcenterUserName: "{{ vcenter_username }}"
    vcenterPassword: "{{ vcenter_password }}"
register: login

# Get existing registered ONTAP Cluster info with ONTAP tools
- name: Get ONTAP Cluster info from ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
    validate_certs: false
    method: Get
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
    validate_certs: false
    method: GET
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
      cluster-id: "{{ ontap_svm_id }}"
  when: ontap_svm_id != ''
  register: aggrinfo

- name: Select Aggregate with max free capacity
  set_fact:

```

```

    aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
vars:
    aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB
  set_fact:
    datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

- name: Get vSphere Cluster Info
  uri:
    url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
    validate_certs: false
    method: GET
    return_content: yes
    body_format: json
    headers:
      vmware-api-session-id: "{{ vclgin.json.value }}"
  when: vsphere_cluster != ''
  register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
    validate_certs: false
    method: POST
    return_content: yes
    status_code: [200]
    body_format: json
    body:
      traditionalDatastoreRequest:
        name: "{{ iscsi_datastore_name }}"
        datastoreType: VMFS
        protocol: ISCSI
        spaceReserve: Thin
        clusterID: "{{ ontap_cluster_id }}"
        svmID: "{{ ontap_svm_id }}"
        targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
        datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
        vmfsFileSystem: VMFS6
        aggrName: "{{ aggr_name }}"
        existingFlexVolName: ""
        volumeStyle: FLEXVOL

```



```
datastoreClusterMoref: ""
headers:
  vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
register: result
changed_when: result.status == 200
```

VSphere VMFS Datastore – NVMe/FC mit ONTAP

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit ONTAP-Storage mithilfe von NVMe/FC beschrieben.

Was Sie brauchen

- Erforderliche Grundkenntnisse für das Management von vSphere Umgebungen und ONTAP
- ["Grundkenntnisse von NVMe/FC"](#).
- Ein ONTAP-Storage-System (FAS/AFF/CVO/ONTAP Select/ASA) mit {ontap_Version}
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ONTAP WWPN für Host-, Ziel- und SVMs- sowie LUN-Informationen
- ["Ein ausgefülltes FC-Konfigurationsarbeitsblatt"](#)
- VCenter Server
- Informationen zu vSphere-Host(s) ({vsphere_Version})
- Fabric Switch(e)
 - Mit ONTAP FC-Daten-Ports und vSphere-Hosts verbunden.
 - Bei aktivierter N_Port ID Virtualization (NPIV).
 - Erstellen einer Zielzone für einen einzelnen Initiator
 - Erstellen Sie für jeden Initiator eine Zone (einzelne Initiatorzone).
 - Geben Sie für jede Zone ein Ziel an, das die logische ONTAP FC-Schnittstelle (WWPN) für die SVMs ist. Es sollten mindestens zwei logische Schnittstellen pro Node pro SVM vorhanden sein. Verwenden Sie den WWPN von physischen Ports nicht.

Bereitstellung von VMFS-Datenspeichern

1. Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#).
2. ["Vergewissern Sie sich, dass die NVMe/FC-Konfiguration unterstützt wird."](#)

ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für FCP."](#) Überprüfen Sie mit dem `system license show` Befehl, ob NVMe_of aufgeführt ist. Mit `license add -license-code <license code>` können Sie eine Lizenz hinzufügen.
2. Vergewissern Sie sich, dass das NVMe-Protokoll auf der SVM aktiviert ist.
 - a. ["Konfigurieren Sie SVMs für NVMe."](#)

3. Stellen Sie sicher, dass auf den SVMs logische NVMe/FC-Schnittstellen verfügbar sind.
 - a. Nutzung `Network Interface show` Um den FCP-Adapter zu überprüfen.
 - b. Wird mit der GUI eine SVM erstellt, gehören zu diesem Prozess logische Schnittstellen.
 - c. Verwenden Sie zum Umbenennen der Netzwerkschnittstelle den Befehl `Network Interface modify`.
4. ["NVMe Namespace und Subsystem erstellen"](#)

Aufgaben für VMware vSphere

1. Vergewissern Sie sich, dass die HBA-Treiber installiert sind. Die von VMware unterstützten HBAs verfügen über die Out-of-the-Box-Treiber und sollten sichtbar sein ["Informationen Zum Storage-Adapter"](#)
2. ["Führen Sie die Installation des vSphere Host-NVMe-Treibers und Validierungsaufgaben durch"](#)
3. ["Erstellen eines VMFS-Datenspeichers"](#)

Herkömmliche File Storage-Provisionierung

vSphere herkömmliche File Storage-Bereitstellung mit ONTAP

VMware vSphere unterstützt folgende NFS-Protokolle: Beide unterstützen ONTAP.

- ["NFS-Version 3"](#)
- ["NFS-Version 4.1"](#)

Wenn Sie Hilfe bei der Auswahl der richtigen NFS-Version für vSphere benötigen, prüfen Sie die Version ["Diesen Vergleich der NFS Client-Versionen"](#).

Referenz

["vSphere Datastore- und Protokollfunktionen: NFS"](#)

vSphere NFS Datastore - Version 3 mit ONTAP

Erstellung von NFS-Data-Version-3-Datenspeichern mit ONTAP-NAS-Storage

Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und ONTAP
- Ein ONTAP Storage-System (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) mit {ONTAP_Version}
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID, Passwort)
- ONTAP Netzwerkport, SVM und LUN-Informationen für NFS
 - ["Ein ausgefülltes NFS-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- vSphere-Host(s)-Informationen für {vsphere_Version}
- IP-Informationen für den NFS VMkernel Adapter
- Netzwerk-Switch(e)
 - Mit Netzwerk-Daten-Ports des ONTAP Systems und verbundenen vSphere Hosts

- Für NFS konfigurierte VLANs
- (Optional) Link Aggregation konfiguriert für ONTAP Netzwerkdatenports
- ONTAP Tool für VMware vSphere – implementiert, konfiguriert und betriebsbereit

Schritte

- Prüfen Sie die Kompatibilität mit dem "[Interoperabilitäts-Matrix-Tool \(IMT\)](#)"
 - "[Vergewissern Sie sich, dass die NFS-Konfiguration unterstützt wird.](#)"
- Führen Sie die folgenden Aufgaben für ONTAP und vSphere aus.

ONTAP Aufgaben

1. "[Überprüfen Sie die ONTAP Lizenz für NFS.](#)"
 - a. Verwenden Sie die `system license show` Führen Sie einen Befehl aus und überprüfen Sie, ob NFS aufgelistet ist.
 - b. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. "[Folgen Sie dem NFS-Konfigurations-Workflow.](#)"

Aufgaben für VMware vSphere

["Folgen Sie dem Workflow der NFS Client-Konfiguration für vSphere."](#)

Referenz

["vSphere Datastore- und Protokollfunktionen: NFS"](#)

Was kommt als Nächstes?

Nach Abschluss dieser Aufgaben kann der NFS-Datenspeicher zur Bereitstellung von Virtual Machines genutzt werden.

vSphere NFS Datastore - Version 4.1 mit ONTAP

In diesem Abschnitt wird die Erstellung eines NFS-Version 4.1-Datenspeichers mit ONTAP-NAS-Speicher beschrieben.

Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- ONTAP Storage-System (FAS/AFF/CVO/ONTAP Select/Cloud Volume Service/Azure NetApp Files) mit {ontap_Version}
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID, Passwort)
- ONTAP Netzwerkport, SVM und LUN-Informationen für NFS
- "[Ein ausgefülltes NFS-Konfigurationsarbeitsblatt](#)"
- Anmeldedaten für vCenter Server
- Informationen zu vSphere-Hosts {vsphere_Version}
- IP-Informationen für den NFS VMkernel Adapter

- Netzwerk-Switch(e)
 - Mit ONTAP System-Netzwerk-Daten-Ports, vSphere-Hosts und verbunden
 - Für NFS konfigurierte VLANs
 - (Optional) Link Aggregation konfiguriert für ONTAP Netzwerkdatenports
- ONTAP Tools für VMware vSphere Implementierung, Konfiguration und Einsatzbereitschaft

Schritte

- Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\):"](#)
 - ["Vergewissern Sie sich, dass die NFS-Konfiguration unterstützt wird."](#)
- Führen Sie die im Folgenden aufgeführten ONTAP- und vSphere-Aufgaben aus.

ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für NFS"](#)
 - a. Einsatz `the system license show` Befehl zum Überprüfen, ob NFS aufgelistet ist.
 - b. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. ["Folgen Sie dem NFS-Konfigurations-Workflow"](#)

Aufgaben für VMware vSphere

["Folgen Sie dem NFS Client Configuration für vSphere Workflow."](#)

Was kommt als Nächstes?

Nach Abschluss dieser Aufgaben kann der NFS-Datenspeicher zur Bereitstellung von Virtual Machines genutzt werden.

Virtual Machine Data Collector (VMDC)

Der Virtual Machine Data Collector (VMDC) ist ein kostenloses, leichtes und einfaches GUI-basiertes Toolkit für VMware-Umgebungen, mit dem Benutzer detaillierte Inventarinformationen über ihre virtuellen Maschinen (VMs), Hosts, Speicher und Netzwerke sammeln können.

Überblick

Die Hauptfunktion von VMDC besteht in der Erstellung von Berichten zur Konfiguration von vCenter, ESXi-Servern und den Virtual Machines (VMs) in einer vSphere Umgebung, einschließlich Clusterkonfigurations-, Netzwerk-, Storage- und Performancedaten. Sobald umfassende Umgebungsdaten erfasst wurden, können daraus aufschlussreiche Informationen über die Infrastruktur gewonnen werden. Die Anzeige der Berichtsausgabe ist eine grafische Benutzeroberfläche im Tabellenformat mit mehreren Registerkarten für die verschiedenen Abschnitte. Er bietet leicht verständliche Berichte, hilft bei der Optimierung der Ressourcenauslastung und Kapazitätsplanung.

VMDC ist nur ein Sprungbrett, um schnelle und sofortige Statistiken für die Projektion von Optimierungsmöglichkeiten für VMware-Core-Lizenzierung zusammen mit vCPU und RAM zu sammeln. ["Einblicke in die NetApp Dateninfrastruktur"](#) Was die Installation von aus und Datensammler erfordert, sollte der naheliegendste nächste Schritt sein, um die detaillierte VM-Topologie zu verstehen, VMs zu gruppieren,

die Annotation verwenden, um die richtige Größe der Workloads festzulegen und die Infrastruktur zukunftssicher zu machen.

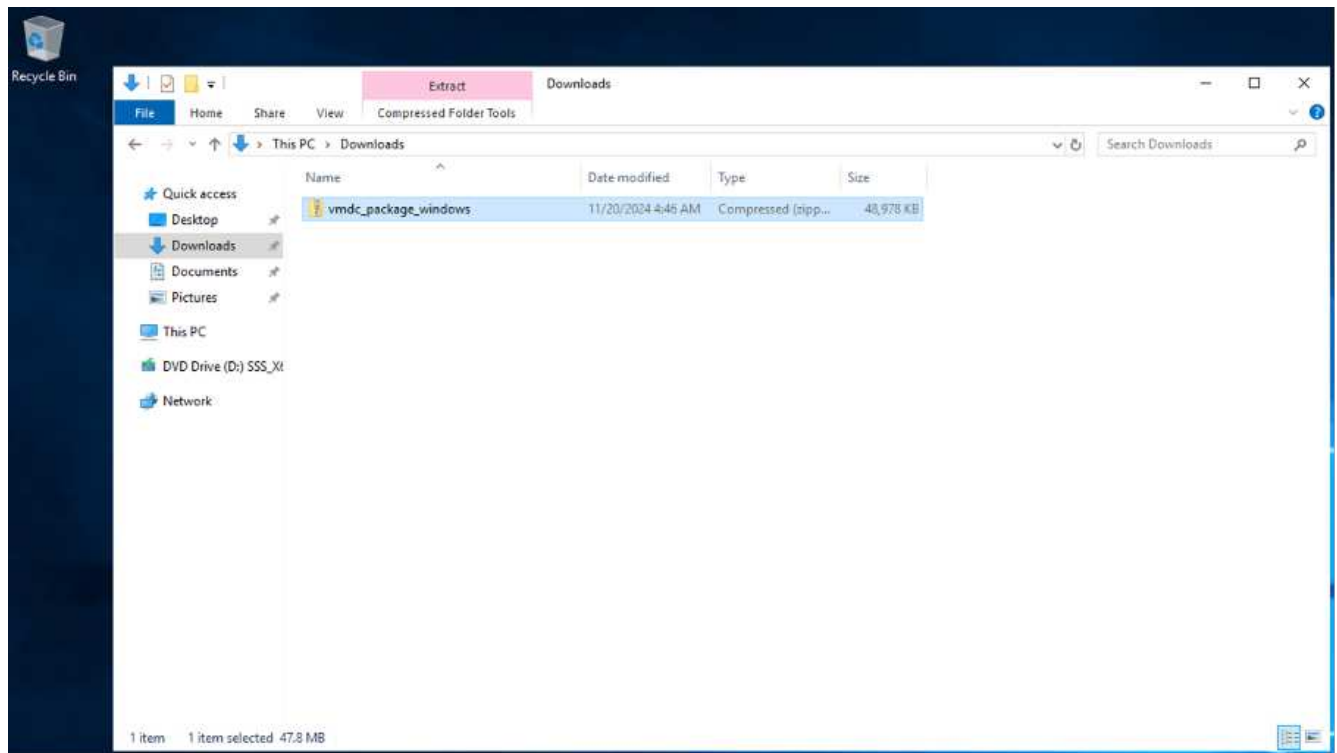
VMDC kann heruntergeladen werden ["Hier"](#) und ist nur für Windows-Systeme verfügbar.

Installieren und Einrichten von VMDC

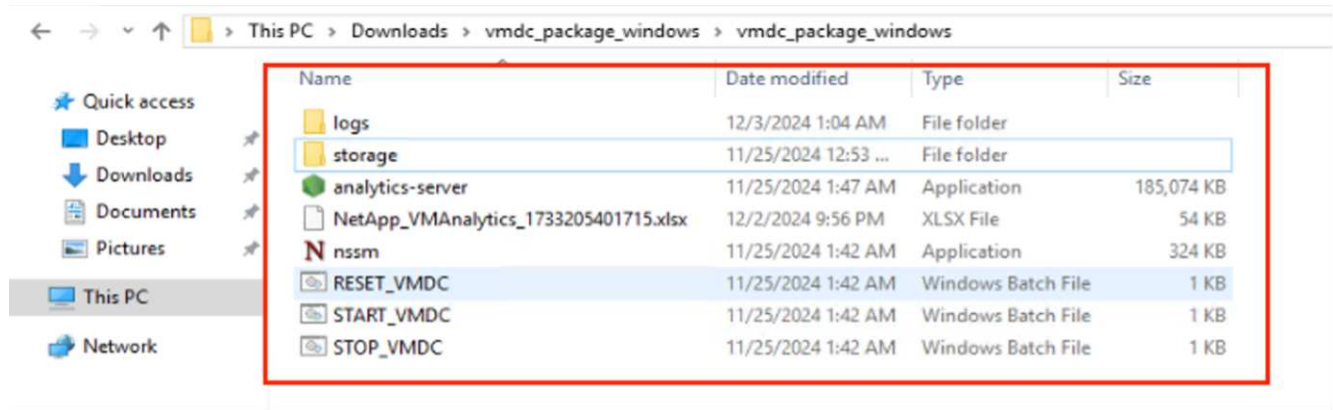
VMDC kann unter Windows 2019, 2022 Version ausgeführt werden. Voraussetzung ist die Netzwerkverbindung von der VMDC-Instanz zu den designierten vCenter-Servern. Laden Sie nach der Überprüfung das VMDC-Paket von [herunter](#), entpacken Sie das Paket, und führen Sie die Batch-Datei aus ["NetApp Toolchest"](#), um den Dienst zu installieren und zu starten.

Sobald VMDC installiert wurde, greifen Sie über die bei der Installation angegebene IP-Adresse auf die Benutzeroberfläche zu. Dadurch wird die VMDC-Anmeldeschnittstelle aufgerufen, wo die vCenter durch Eingabe der IP-Adresse oder des DNS-Namens und der Anmeldeinformationen eines vCenter-Servers hinzugefügt werden können.

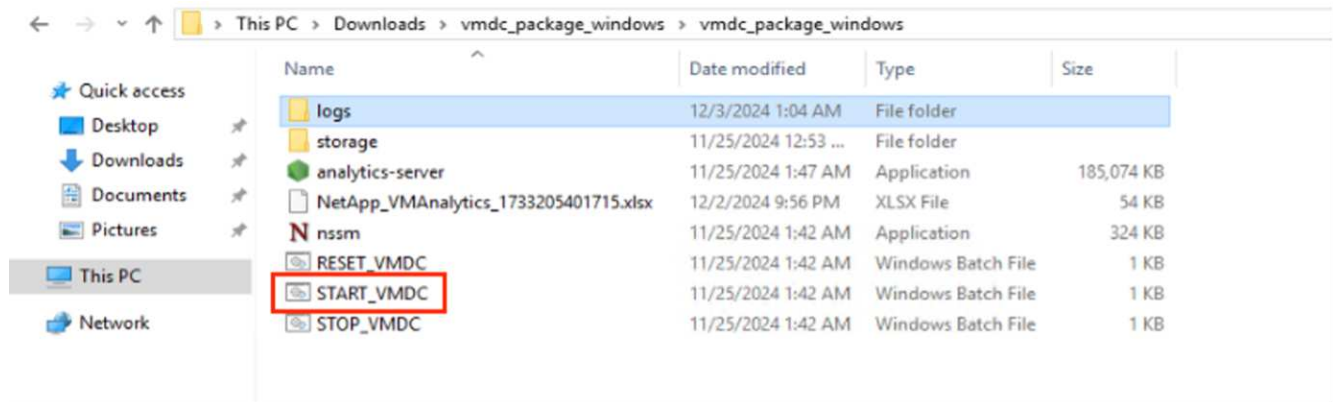
1. Herunterladen ["VMDC-Paket"](#).



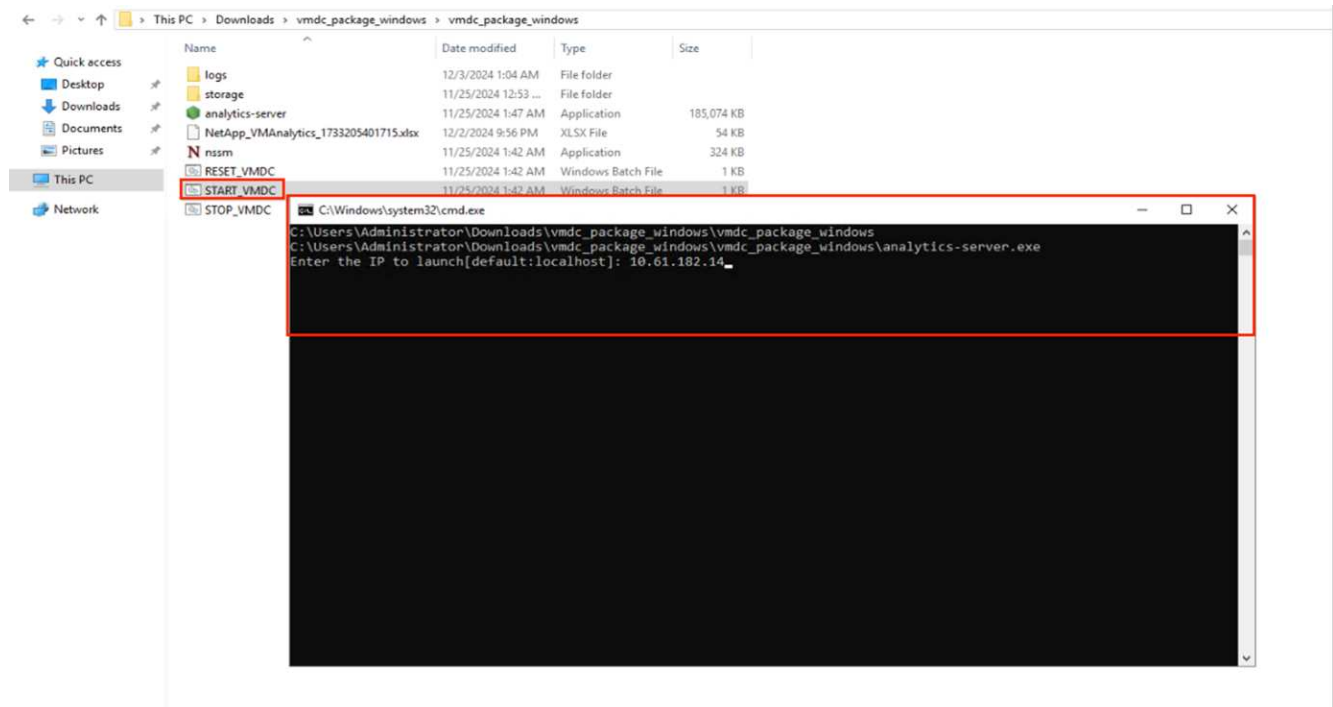
2. Extrahieren Sie das Paket in den angegebenen Ordner.

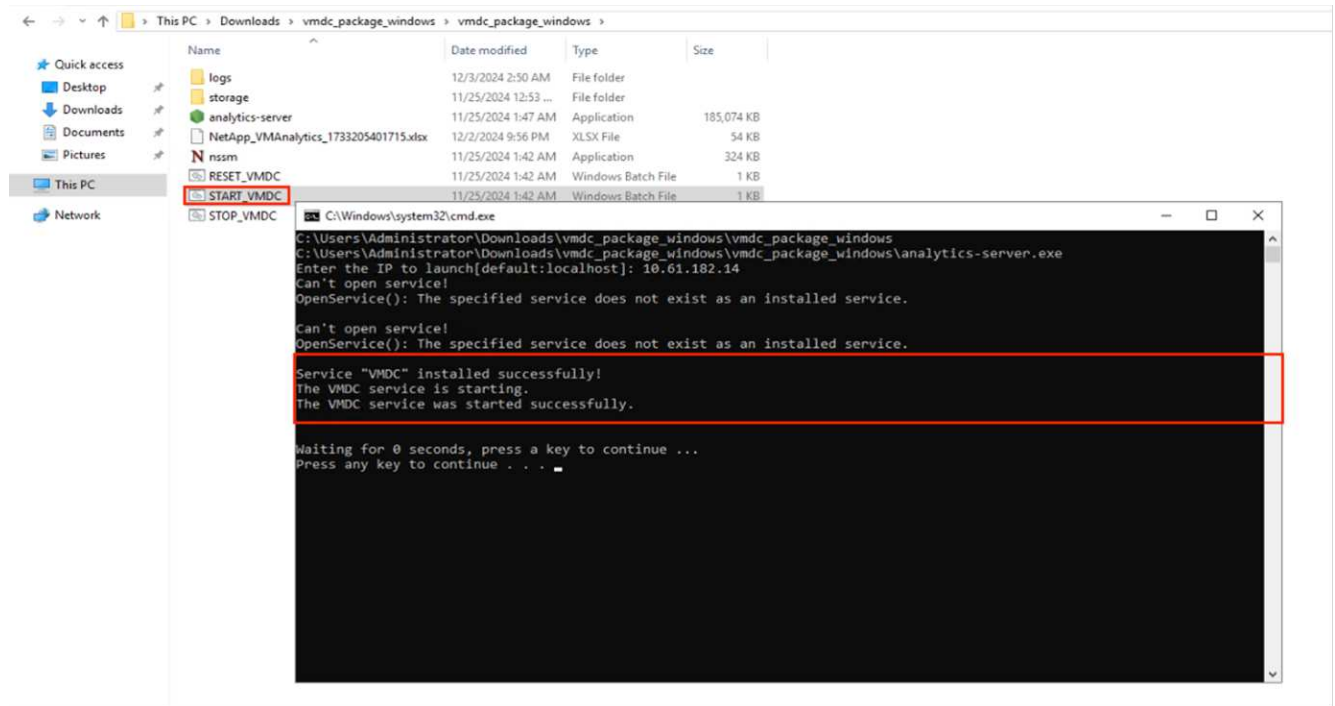


3. Führen Sie das VMDC-Paket aus, indem Sie auf Start_VMDC Batch-Datei klicken. Dadurch wird die Eingabeaufforderung geöffnet und die IP-Adresse eingegeben.

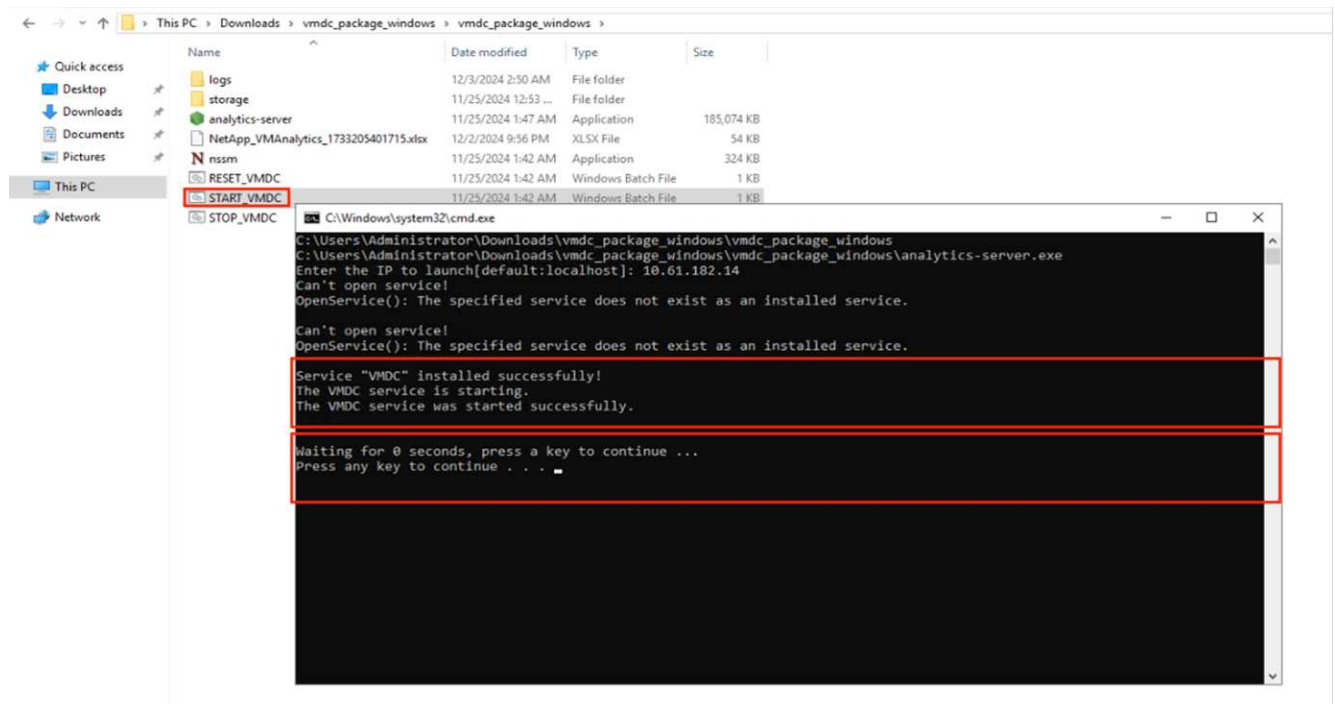


4. Das Installationsprogramm startet den Installationsprozess und startet den VMDC-Dienst.





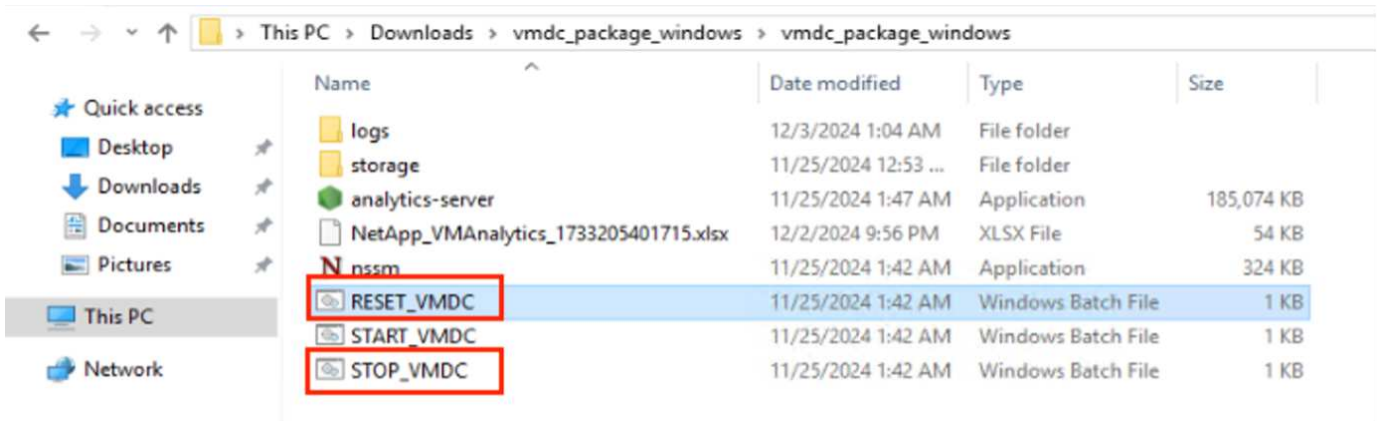
5. Sobald Sie fertig sind, „Drücken Sie eine beliebige Taste, um fortzufahren“, um die Eingabeaufforderung zu schließen.



Um die Datenerfassung zu beenden, klicken Sie auf Stop_VMDC Batch-Datei.



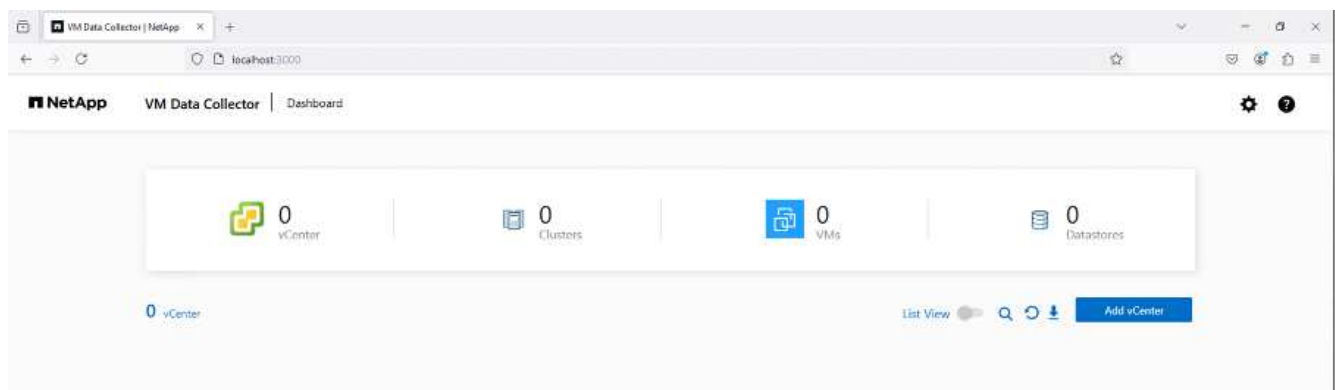
Um die erfassten Daten zu entfernen und VMDC zurückzusetzen, führen Sie die Batch-Datei RESET_VMDC aus. Denken Sie daran, wenn Sie die RESET bat-Datei ausführen, werden alle vorhandenen Daten gelöscht und von Grund auf neu gestartet.



Verwenden des GUI

Führen Sie VMDC aus

- Greifen Sie über den Browser auf die VMDC-Benutzeroberfläche zu



- Fügen Sie das angegebene vCenter mit der Option „Add vCenter“ hinzu
 - VCenter Name: Geben Sie einen Namen für vCenter ein
 - Endpunkt: Geben Sie die IP-Adresse oder den FQDN des vCenter-Servers ein
 - Benutzername: Benutzername für den Zugriff auf vCenter (im UPN-Format: `username@domain.com`)
 - Passwort
- Ändern Sie die „Additional Details“ gemäß den Anforderungen
 - Datenintervallzeit – gibt den Zeitbereich für die Probenaggregation an. Der Standardwert beträgt 5 Minuten, kann jedoch nach Bedarf auf 30 Sekunden oder 1 Minute geändert werden.
 - Datenaufbewahrung – gibt die Aufbewahrungsfrist an, in der die historischen Kennzahlen gespeichert werden sollen.
 - Erfassen von Performance-Metriken: Wenn diese Option aktiviert ist, werden die Performance-Metriken für jede VM erfasst. Wenn nicht ausgewählt, bietet VMDC Funktionen wie RVTools, indem nur die Details zu VM, Host und Datastore bereitgestellt werden.
- Klicken Sie anschließend auf „Add vCenter“.

The screenshot shows the 'Add New vCenter' configuration page in the NetApp VM Data Collector. The form is titled 'vCenter Details' and contains the following fields and options:

- vCenter Name:** vCenter-WK LDA
- Endpoint:** 172.21.255.141
- Username:** administrator@ehudc.com
- Password:** [Masked]
- Accept self-signed certificates**
- Additional Details:**
 - Data Interval:** 5 min
 - Data Retention:** 7 Days
 - Collect Performance Metrics**

An 'Add vCenter' button is located at the bottom of the form.



Die Datenerfassung beginnt sofort, sobald das vCenter hinzugefügt wird. Es muss keine Zeit für die Erfassung eingeplant werden, da der Prozess die in der vCenter-Datenbank verfügbaren Daten abrufen und diese basierend auf der angegebenen „Daten-Intervall-Zeit“ aggregieren würde.

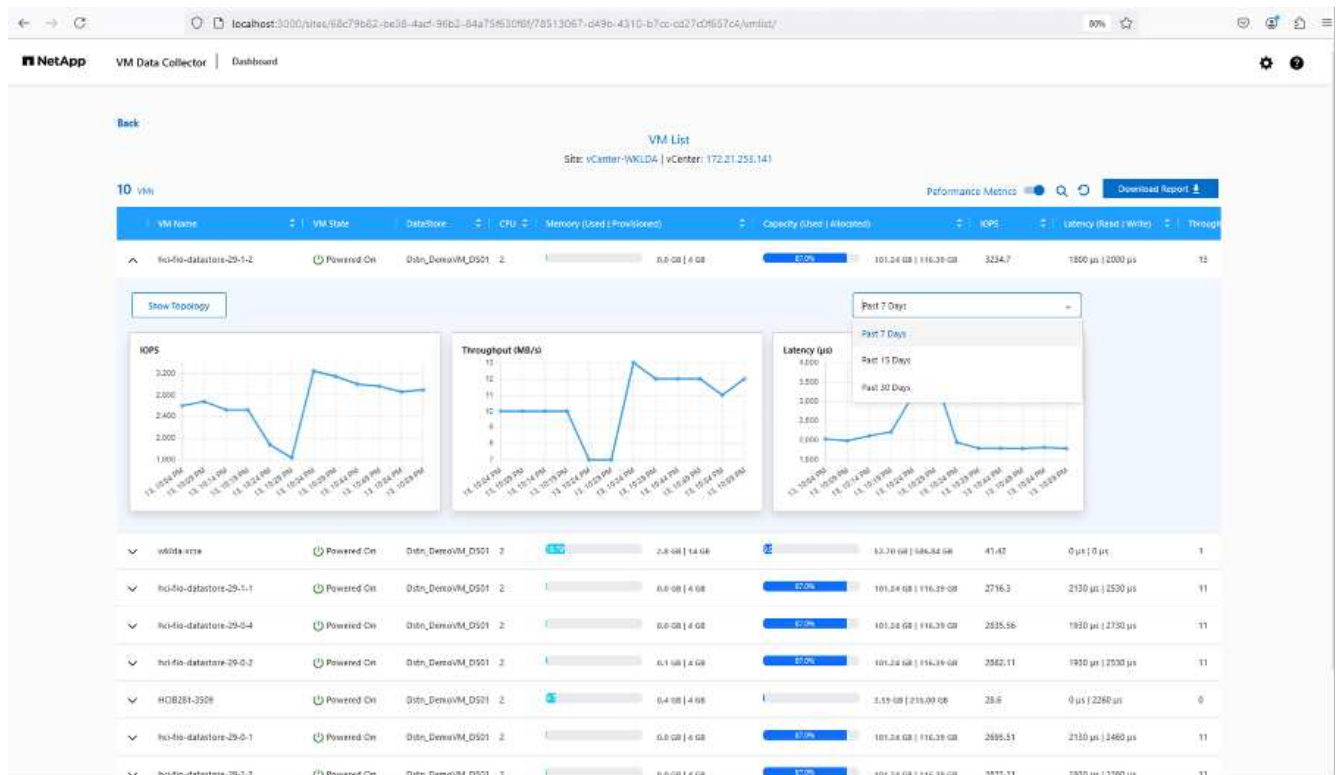
Zum Anzeigen der Daten für ein bestimmtes vCenter öffnen Sie das Dashboard und klicken unter dem entsprechenden vCenter Namen auf „View Inventory“. Auf der Seite wird der VM-Bestand zusammen mit den VM-Attributen angezeigt. Standardmäßig ist „Performance Metrics“ in der UI deaktiviert, kann aber mithilfe der Umschaltoption AKTIVIERT werden. Sobald Performance-Metriken aktiviert sind, werden die Performance-Daten für jede VM angezeigt. Um Informationen zur Live-Performance anzuzeigen, klicken Sie auf die Schaltfläche Aktualisieren.

Zeigen Sie die VM-Topologie an

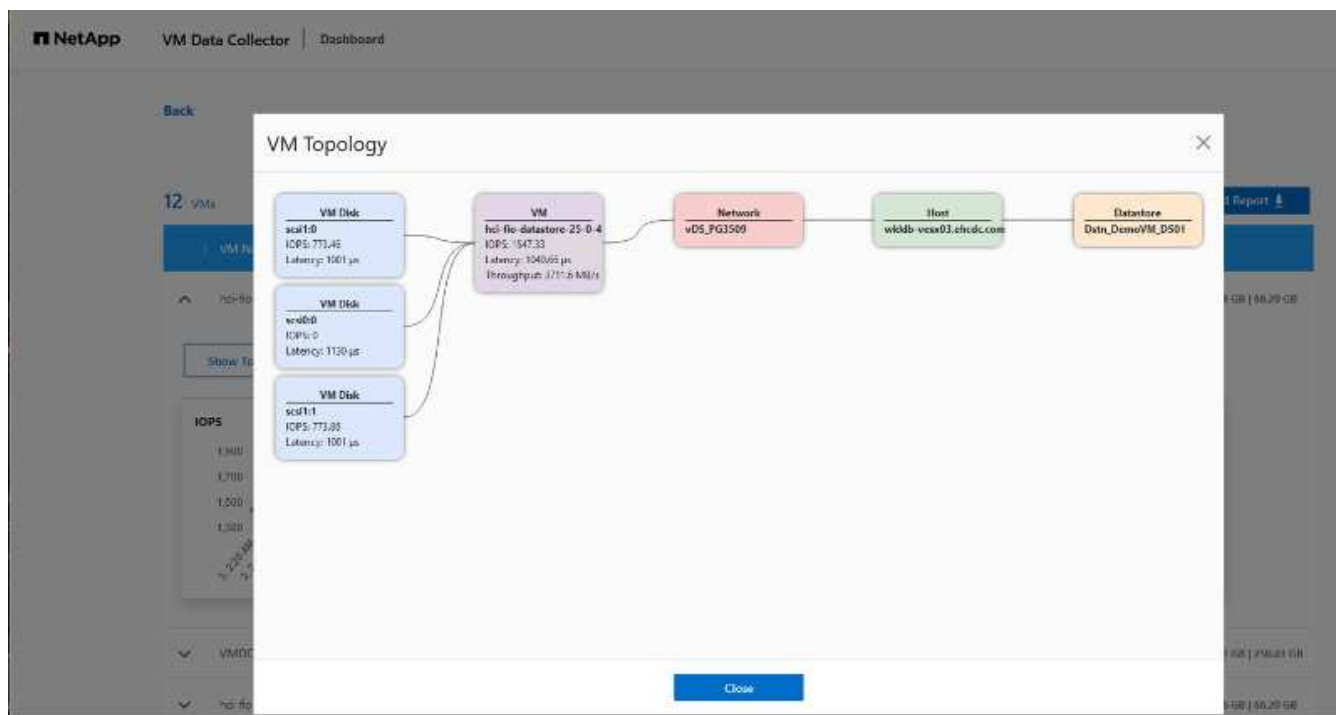
VMDC bietet die Option „Topologie anzeigen“ für jede VM, die eine interaktive Schnittstelle bietet, um Ressourcen und ihre Beziehungen zwischen VM-Festplatte, VM, ESXi-Host, Datastores und Netzwerken anzuzeigen. Es hilft, anhand von Erkenntnissen aus den erfassten Performance-Daten zu managen und zu überwachen. Mithilfe der Topologie können Sie grundlegende Diagnosen durchführen und Probleme mithilfe der aktuellen Daten beheben. Für eine detaillierte Fehlerbehebung und eine schnelle MTTR verwenden ["Einblicke in die NetApp Dateninfrastruktur"](#), die eine detaillierte Topologieansicht mit End-to-End-Abhängigkeitszuordnung bietet.

Gehen Sie wie folgt vor, um auf die Topologieansicht zuzugreifen:

- Rufen Sie das VMDC-Dashboard auf.
- Wählen Sie den vCenter Namen aus und klicken Sie auf „View Inventory“.



- Wählen Sie die VM aus und klicken Sie auf „Show Topology“.

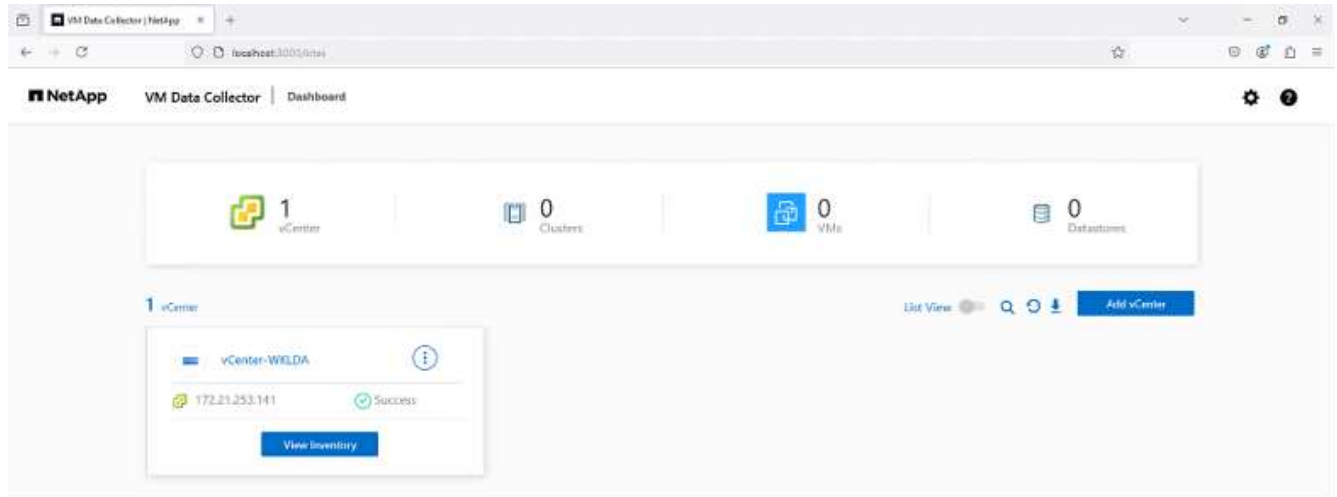


Export nach Excel

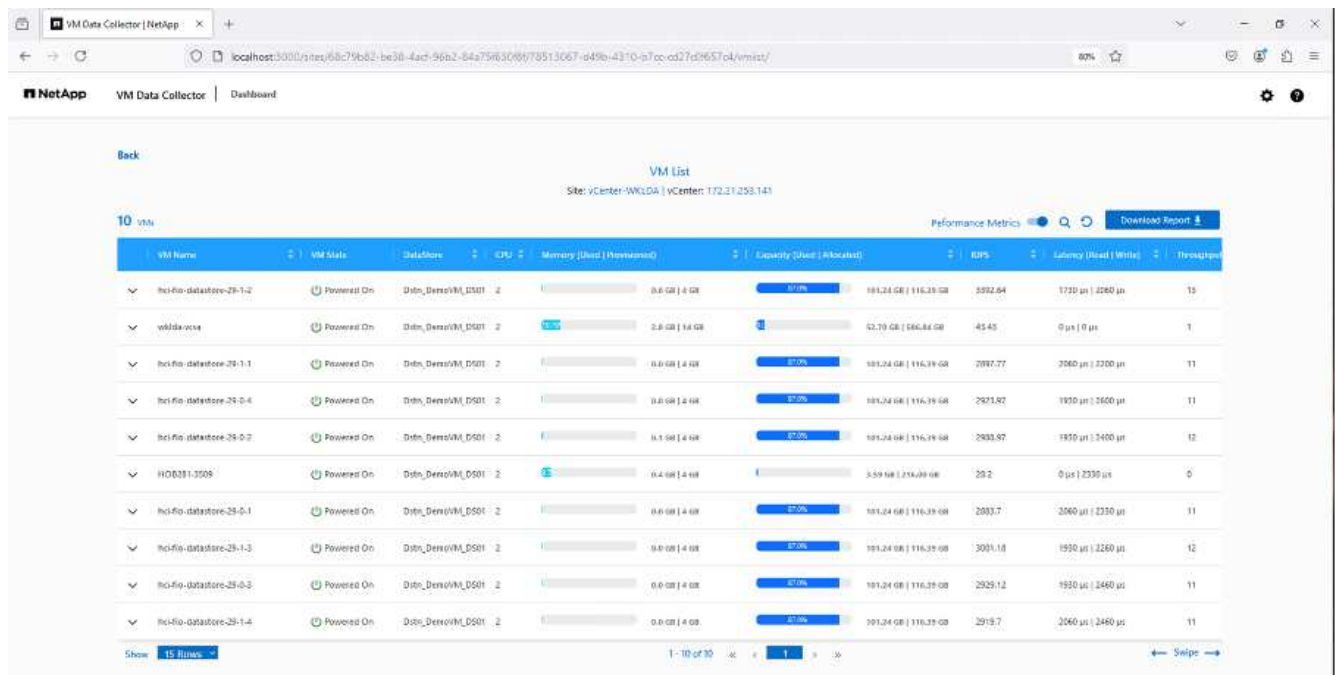
Um die gesammelten in einem nutzbaren Format zu erfassen, verwenden Sie die Option "Download Report", um die XLSX-Datei herunterzuladen.

Gehen Sie wie folgt vor, um den Bericht herunterzuladen:

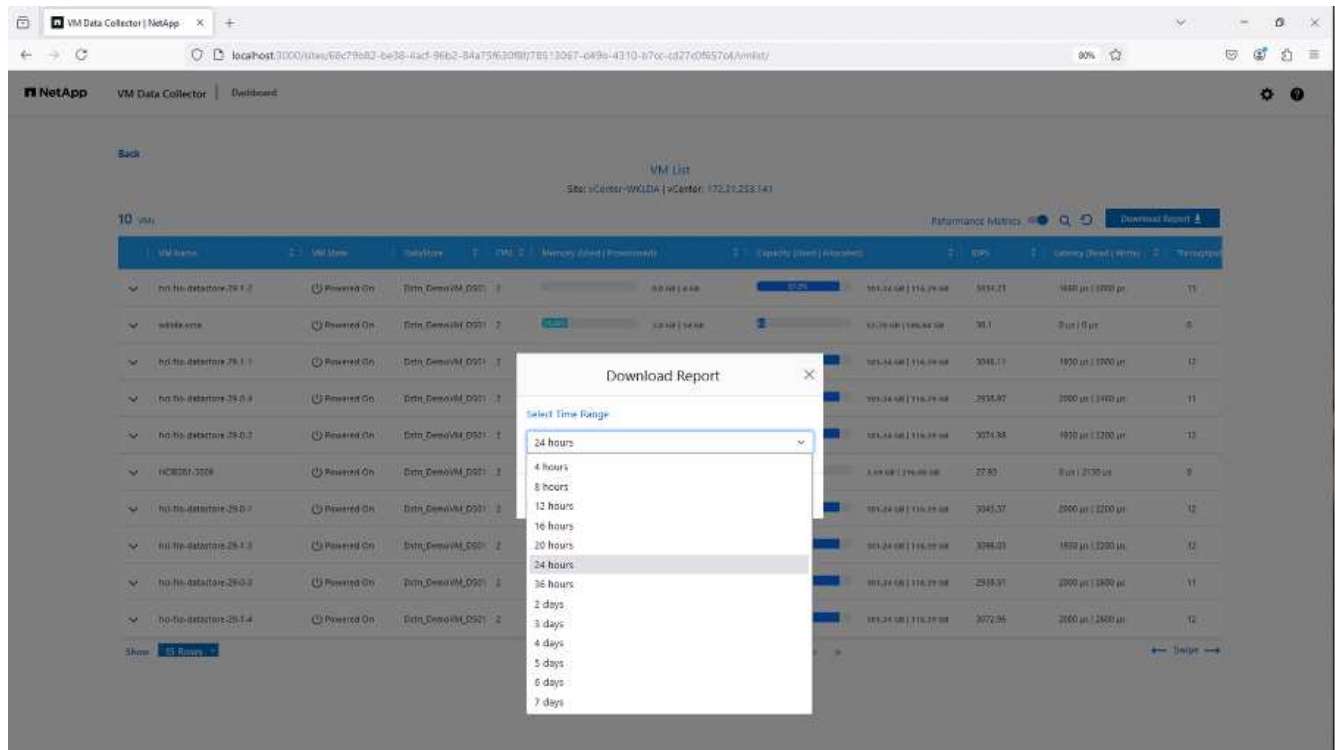
- Rufen Sie das VMDC-Dashboard auf.
- Wählen Sie den vCenter Namen aus und klicken Sie auf „View Inventory“.



- Wählen Sie die Option „Bericht herunterladen“ aus



- Wählen Sie den Zeitbereich aus. Der Zeitbereich bietet mehrere Optionen von 4 Stunden bis 7 Tagen.



Wenn die erforderlichen Daten beispielsweise für die letzten 4 Stunden verwendet werden, wählen Sie 4 oder wählen Sie den entsprechenden Wert aus, um die Daten für den angegebenen Zeitraum zu erfassen. Die erzeugten Daten werden kontinuierlich aggregiert. Wählen Sie also den Zeitraum aus, um sicherzustellen, dass der erstellte Bericht die erforderlichen Workload-Statistiken erfasst.

VMDC-Datenzähler

Nach dem Herunterladen zeigt VMDC als erstes Blatt „VM Info“ an, ein Blatt, das Informationen zu den VMs enthält, die sich in der vSphere-Umgebung befinden. Hier werden allgemeine Informationen zu den virtuellen Maschinen angezeigt: VM-Name, Energiezustand, CPUs, bereitgestellter Arbeitsspeicher (MB), genutzter Speicher (MB), bereitgestellte Kapazität (GB), genutzte Kapazität (GB), Version der VMware-Tools, Betriebssystemversion, Umgebungstyp, Datacenter, Cluster, Host, Ordner, primärer Datenspeicher, Festplatten, NICs, VM-ID und VM-UUID.

Auf der Registerkarte „VM-Performance“ werden die Performance-Daten für jede VM erfasst, die auf der ausgewählten Intervallebene erfasst wird (Standardeinstellung sind 5 Minuten). Die Stichprobe jeder virtuellen Maschine umfasst: Durchschnittliche Lese-IOPS, durchschnittliche Schreib-IOPS, durchschnittliche IOPS-Werte insgesamt, IOPS mit Spitzenwerten bei Lesezugriffen, IOPS mit Spitzenwerten insgesamt, durchschnittlicher Lesedurchsatz (KB/s), durchschnittlicher Schreibdurchsatz (KB/s), durchschnittlicher Lesedurchsatz (KB/s), Spitzenleselatenz (KB/s), maximale Schreiblatenz (KB/s), maximaler Spitzendurchsatz (ms), maximale Leselatenz (ms), maximale Schreiblatenz (ms) (ms)

Die Registerkarte „ESXi Host Info“ erfasst für jeden Host: Datacenter, vCenter, Cluster, Betriebssystem, Hersteller, Modell, CPU Sockets, CPU-Cores, Net Clock Speed (GHz), CPU Clock Speed (GHz), CPU Threads, Arbeitsspeicher (GB), verwendeter Speicher (%), CPU-Auslastung (%), Gast-VM-Anzahl und Anzahl der NICs.

Nächste Schritte

Verwenden Sie die heruntergeladene XLSX-Datei für Optimierungsaufgaben und Refactoring-Aufgaben.

Beschreibung der VMDC-Attribute

Dieser Abschnitt des Dokuments enthält die Definition aller im Excel-Arbeitsblatt verwendeten Zähler.

VM-Infoblatt

Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
CPUs	The number of vCPUs provisioned on the Guest Virtual Machine
Memory Provisioned (MB)	The Memory Provisioned on the Guest Virtual Machine. Units MB
Memory Utilized (MB)	Active Memory Utilized by the Guest Virtual Machine during the phase of metrics collection. Units MB
Capacity Provisioned (GB)	Total Capacity of the Virtual Disks provisioned on the Guest Virtual Machine. Units GB
Capacity Utilized (GB)	Total Utilized Virtual Disks capacity on the Guest Virtual Machine. Units GB
VMware tools version	Version of the VMware Tools installed on the Guest Virtual machine
OS Version	The Operating System installed on the Guest Virtual Machine
Environment Type	
Datacenter	Name of the Datacenter containing the Guest Virtual Machine
Cluster	Name of the Cluster containing the Guest Virtual Machine
Host	Name of the ESXi Server on which the Guest Virtual Machine is hosted
Folder	Name of the folder under the VMs Tab containing the Guest Virtual Machine
Primary Datastore	Name of the Datastore on which the Guest Virtual Machine's disks reside
Disks	Number of Virtual Disks connected to the Guest Virtual Machine
NICs	Number of Virtual Network Interface connections to the Guest Virtual Machine
VM ID	The Guest Virtual Machine Identifier String within the scope of vCenter Server Monitoring
VM UUID	The Unique Identifier value for the Guest Virtual Machine

VM Performance Sheet

Counter Name	Counter Description
VM Name	Name of the Guest Virtual Machine as shown in vCenter
Power State	Guest Virtual Machine Power Status. One of these values: Powered On, Powered Off, or Suspended
Number of CPUs	Number of vCPUs provisioned on the Guest Virtual Machine
Average CPU (%)	Average vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Peak CPU (%)	Maximum vCPU usage of the Guest Virtual Machine presented as percentage within the selected time slot
Average Read IOPS	Average read IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Write IOPS	Average Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Average IOPS	Combined Average Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Read IOPS	Maximum Read IO operations per second for the Guest Virtual Machine to and from the storage attached
Peak Write IOPS	Maximum Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Total Peak IOPS	Combined Maximum Read & Write IO operations per second for the Guest Virtual Machine to and from the storage attached
Average Read Throughput (KB/s)	Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Write Throughput (KB/s)	Average rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Average Throughput (KB/s)	Combined Average rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Read Throughput (KB/s)	Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Peak Write Throughput (KB/s)	Peak rate of Write on Disk Data from the ESXi Host for the duration of metrics collected
Total Peak Throughput (KB/s)	Combined Peak rate of Read on Disk Data from the ESXi Host for the duration of metrics collected
Average Read Latency (ms)	Average Read latency for the Guest Virtual Machine. Units milliseconds
Average Write Latency (ms)	Average Write latency for the Guest Virtual Machine. Units milliseconds
Total Average Latency (ms)	Combined Average Read & Write latency for the Guest Virtual Machine. Units milliseconds
Peak Read Latency (ms)	Maximum Read latency for the Guest Virtual Machine. Units milliseconds
Peak Write Latency (ms)	Maximum Write latency for the Guest Virtual Machine. Units milliseconds
Total Peak Latency (ms)	Combined Maximum Read & Write latency for the Guest Virtual Machine. Units milliseconds

ESXi Host Info

Counter Name	Counter Description
Host	Hostname of the ESXi Hypervisor Server
Datacenter	Virtual DataCenter Name under which the ESXi Hypervisor Hosts exists
vCenter	Version of the VMware vCenter Server used to Manage & Monitor the ESXi Hosts
Cluster	Name of the Cluster under which the ESXi Hypervisor Hosts exists
OS	Version of VMware ESXi Hypervisor that is installed on the Host / Server
Manufacturer	Vendor Company name of the Physical Server of the Host
Model	Server Model / Model Number of the Physical Server
CPU Sockets	Total number of CPU Sockets installed on the Physical Server
CPU Cores	Total number of Cores across all CPU Sockets installed on the Physical Server
CPU Description	Vendor Company & Model Information of the CPU Type installed on the Physical Server
Net Clock Speed (GHz)	Sum of CPU Clock Speed of all CPU cores running on the Physical Server. Units GHz
CPU Clock Speed (GHz)	Clock Speed of each CPU core running on the Physical Server. Units GHz
CPU Threads	Total Number of threads supported for all Cores on the Physical Server
Memory (GB)	Total RAM installed on the Physical Server. Units GB
Memory Used (%)	Percentage of Memory Used on the Physical Server / Host
CPU usage (%)	Percentage of CPU Used on the Physical Server / Host
Guest VM Count	Total Number of Guest Virtual Machines running on the Physical Server / Host
Number of NICs	Total Number of Network Interface Connection Ports on the Physical Hypervisor Server / Host

Schlussfolgerung

Angesichts der bevorstehenden Lizenzierungsänderungen gehen Unternehmen proaktiv auf die potenzielle Erhöhung der Gesamtbetriebskosten (TCO) ein. Sie optimieren ihre VMware-Infrastruktur durch offensives Ressourcenmanagement und richtiges Sizing strategisch, um die Ressourcenauslastung zu verbessern und

die Kapazitätsplanung zu optimieren. Durch den effektiven Einsatz spezialisierter Tools können Unternehmen verschwendete Ressourcen effizient identifizieren und wieder nutzbar machen, wodurch die Anzahl der Kerne und die Lizenzierungskosten insgesamt reduziert werden. VMDC ermöglicht die schnelle Erfassung von VM-Daten, die geteilt werden können, um Berichte zu erstellen und die vorhandene Umgebung zu optimieren.

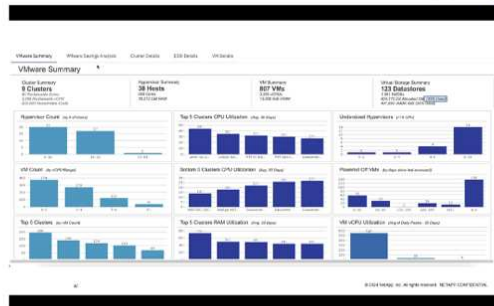
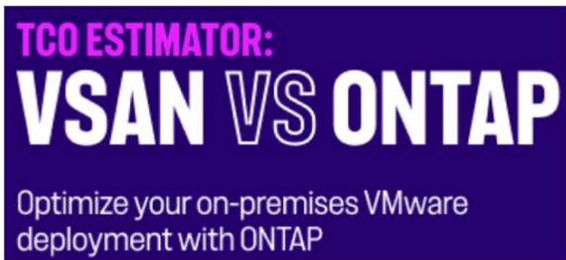
Führen Sie mithilfe von VMDC eine schnelle Bewertung durch, um nicht ausgelastete Ressourcen ausfindig zu machen, und verwenden Sie anschließend NetApp Dateninfrastrukturanalysen (DII), um detaillierte Analysen und Empfehlungen für die Rückgewinnung von VMs bereitzustellen. Dadurch können Kunden potenzielle Kosteneinsparungen und Optimierungen analysieren, während NetApp Dateninfrastrukturanalysen (DII) implementiert und konfiguriert werden. NetApp Einblicke in die Dateninfrastruktur (DII) bieten Unternehmen fundierte Entscheidungen zur Optimierung ihrer VM-Umgebung. Die Lösung kann ermitteln, wo Ressourcen zurückgewonnen oder Hosts stillgelegt werden können, ohne dass sich dies auf die Produktion auswirkt. So können Unternehmen die durch die Übernahme von VMware durch Broadcom vorgenommenen Änderungen auf durchdachte und strategische Weise bewältigen. Mit anderen Worten: VMDC und DII als detaillierter Analysemechanismus helfen Unternehmen, die Entscheidung ohne Emotionen zu treffen. Anstatt mit Panik oder Frustration auf die Veränderungen zu reagieren, können sie die Erkenntnisse dieser beiden Tools nutzen, um rationale, strategische Entscheidungen zu treffen, die Kostenoptimierung mit betrieblicher Effizienz und Produktivität in Einklang bringen.

Mit NetApp passen Sie die Größe Ihrer virtualisierten Umgebungen an und führen kostengünstige Flash-Storage-Performance ein sowie vereinfachtes Datenmanagement und Ransomware-Lösungen. So können Sie sicherstellen, dass Unternehmen auf ein neues Abonnementmodell vorbereitet sind und gleichzeitig die aktuellen IT-Ressourcen optimieren.

Optimize VMware core licensing

Optimize VMware core licensing and right-size workloads

25-50% optimization savings (based on VMDC reports showing CPU utilization of ~30% or less)



- Optimize:**
- VMware core licensing
 - VM CPU and memory



- NetApp® Data Infrastructure Insights**
- Understand topology
 - Drive density
 - Right-size workloads

Nächste Schritte

Laden Sie das VMDC-Paket herunter, und sammeln Sie die Daten und "VSAN TCO-Kalkulator" die Verwendung für eine einfache Projektion und verwenden Sie ES dann "DII", um kontinuierlich die Intelligenz bereitzustellen und SIE jetzt und in Zukunft zu beeinflussen, um sicherzustellen, dass es sich an neue Anforderungen anpassen kann.

Demos und Tutorials

Virtualisierungsvideos und -Demos

Sehen Sie sich die folgenden Videos und Demos an, in denen die spezifischen Funktionen von Hybrid Cloud-, Virtualisierungs- und Container-Lösungen vorgestellt werden.

NetApp ONTAP Tools für VMware vSphere

[ONTAP Tools für VMware - Übersicht](#)

[Bereitstellung von VMware iSCSI-Datenspeichern mit ONTAP](#)

[Bereitstellung von VMware NFS-Datenspeichern mit ONTAP](#)

SnapCenter Plug-in für VMware vSphere

Die NetApp SnapCenter Software ist eine unkomplizierte Enterprise-Plattform, die die Koordination und das Management der Datensicherung für alle Applikationen, Datenbanken und Filesysteme sicher gestaltet.

Das SnapCenter Plug-in für VMware vSphere ermöglicht Ihnen Backup-, Wiederherstellungs- und Anschlussvorgänge für VMs sowie Backup- und Mount-Vorgänge für Datastores, die bei SnapCenter direkt in VMware vCenter registriert sind.

Weitere Informationen zum NetApp SnapCenter Plug-in für VMware vSphere finden Sie im "[Überblick über NetApp SnapCenter Plug-in für VMware vSphere](#)".

[SnapCenter Plug-in für VMware vSphere – Voraussetzungen für eine Lösung](#)

[SnapCenter Plug-in für VMware vSphere – Implementierung](#)

[SnapCenter Plug-in für VMware vSphere – Backup-Workflow](#)

[SnapCenter Plug-in für VMware vSphere – Workflow wiederherstellen](#)

[SnapCenter - SQL Restore-Workflow](#)

3-2-1 Datensicherungslösungen

3-2-1-1 Datensicherungslösungen kombinieren primäre und sekundäre Backups vor Ort mithilfe von SnapMirror Technologie mit replizierten Kopien in Objekt-Storage mithilfe von BlueXP Backup und Recovery.

[3-2-1 Datensicherung für VMFS Datastores mit SnapCenter Plug-in für VMware vSphere und BlueXP Backup und Recovery für Virtual Machines](#)

VMware Cloud on AWS mit AWS FSX ONTAP

[Windows Guest Connected Storage mit FSX ONTAP über iSCSI](#)

[Linux Guest Connected Storage with FSX ONTAP Using NFS](#)

[TCO-Einsparungen mit VMware Cloud on AWS mit Amazon FSX ONTAP](#)

[Ergänzender Datastore für VMware Cloud on AWS mit Amazon FSX ONTAP](#)

[VMware HCX Deployment and Configuration Setup für VMC](#)

[VMotion Migration Demonstration mit VMware HCX für VMC und FSX ONTAP](#)

[Demo für kalte Migration mit VMware HCX für VMC und FSX ONTAP](#)

Azure VMware-Services auf Azure mit Azure NetApp Files (ANF)

[Übersicht über die Azure VMware Lösung zusätzlichen Datastore mit Azure NetApp Files](#)

[Azure VMware Lösung für DR mit Cloud Volumes ONTAP, SnapCenter und JetStream](#)

[Demonstration zur Cold-Migration mit VMware HCX für AVS und ANF](#)

[VMotion-Demo mit VMware HCX für AVS und ANF](#)

[Massenmigration mit VMware HCX für AVS und ANF](#)

VMware Cloud Foundation mit NetApp ONTAP

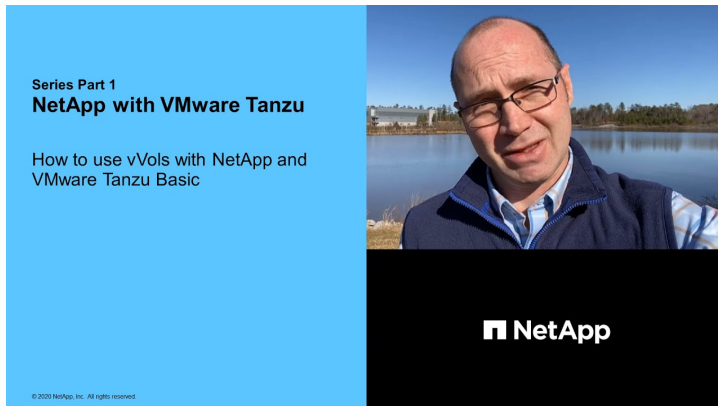
[NFS-Datenspeicher als Principal Storage für VCF Workload Domains](#)

[iSCSI-Datenspeicher als ergänzender Speicher für VCF-Management-Domänen](#)

NetApp mit VMware Tanzu

Mit VMware Tanzu können Kunden ihre Kubernetes-Umgebung über vSphere oder VMware Cloud Foundation implementieren, managen und managen. Mit diesem VMware Portfolio können Kunden alle relevanten Kubernetes Cluster über eine einzige Kontrollebene managen. Dazu wählen sie die für sie am besten geeignete VMware Tanzu Edition.

Weitere Informationen zu VMware Tanzu finden Sie im "[VMware Tanzu Overview](#)". Diese Überprüfung behandelt Anwendungsfälle, verfügbare Ergänzungen und mehr über VMware Tanzu.



Verwendung von VVols mit NetApp und VMware Tanzu Basic, Teil 1



Verwendung von VVols mit NetApp und VMware Tanzu Basic, Teil 2



Verwendung von VVols mit NetApp und VMware Tanzu Basic, Teil 3

NetApp Cloud Insights

NetApp Cloud Insights ist eine umfassende Monitoring- und Analyseplattform, die für Transparenz und Kontrolle der On-Premises- und Cloud-Infrastruktur konzipiert ist.

[NetApp Cloud Insights – Beobachtbarkeit für das moderne Datacenter](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.