NFS Reference Guide für vSphere 8

NetApp Solutions

NetApp
December 19, 2024

Inhalt

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-Datastores 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 Datastores 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 VVVVF 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:

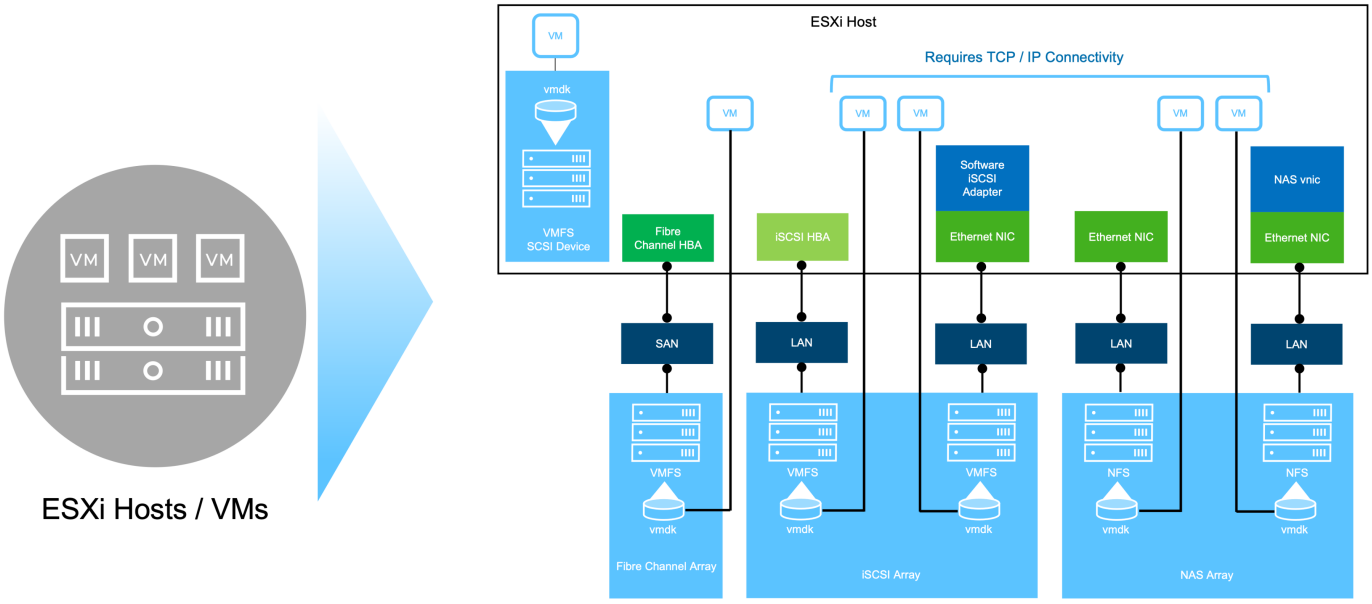
- VMware vSphere
- VMware vSAN
- Aria Standard
- VMware Tanzu Kubernetes Grid Service für vSphere
- VSphere Distributed Switch

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.

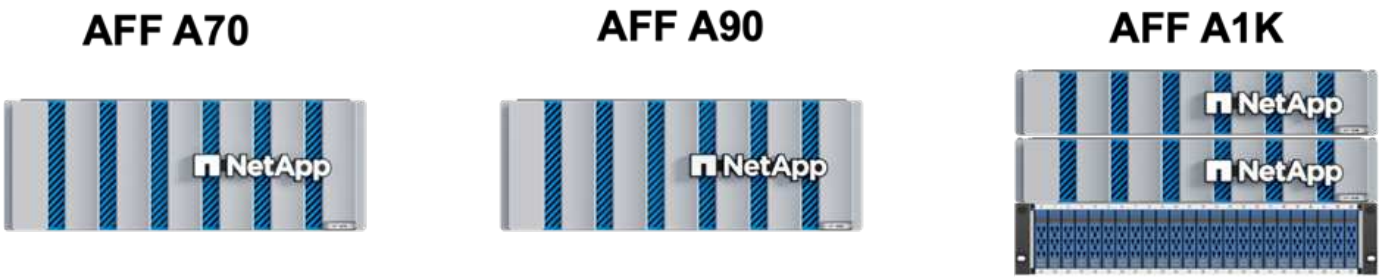
Die Kombination von ONTAP und vSphere ermöglicht Kosteneinsparungen für Host-Hardware und VMware Software. Schützen Sie Ihre Daten außerdem zu geringeren Kosten mit konstant hoher Performance. Da virtualisierte Workloads mobil sind, können Sie mit Storage vMotion verschiedene Ansätze nutzen, um VMs auf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

Rein Flash-basierte NetApp Arrays

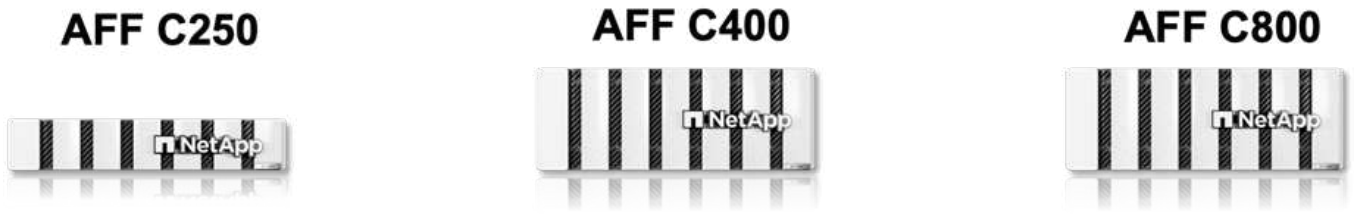
NetApp AFF (All Flash FAS) ist eine Produktreihe von All-Flash-Storage-Arrays. Es wurde für hochperformante Storage-Lösungen mit niedriger Latenz für Enterprise-Workloads entwickelt. Die AFF Series kombiniert die Vorteile der Flash-Technologie mit den Datenmanagementfunktionen von NetApp und bietet Unternehmen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



Unterstützte Storage-Protokolle

Die AFF unterstützen alle Standardprotokolle, die bei der Virtualisierung verwendet werden, sowohl für Datastores 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-Datastores. Mit dem NFS verbundene Datastores 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 Volumen: NetApp empfiehlt die Verwendung von **FlexVol** Volumen 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 Guarantee, 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

bekannten 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 NetApps Solutions an: "DR unter Verwendung von BlueXP DRaaS für NFS-Datastores"

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 Datastores 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-Datastore 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-Datastore auf demselben Host.
- Steigern Sie die Performance des NFS-Datastore.
- Sie können Services auf einem höheren Tier für VM- und Container-basierte Applikationen anbieten.

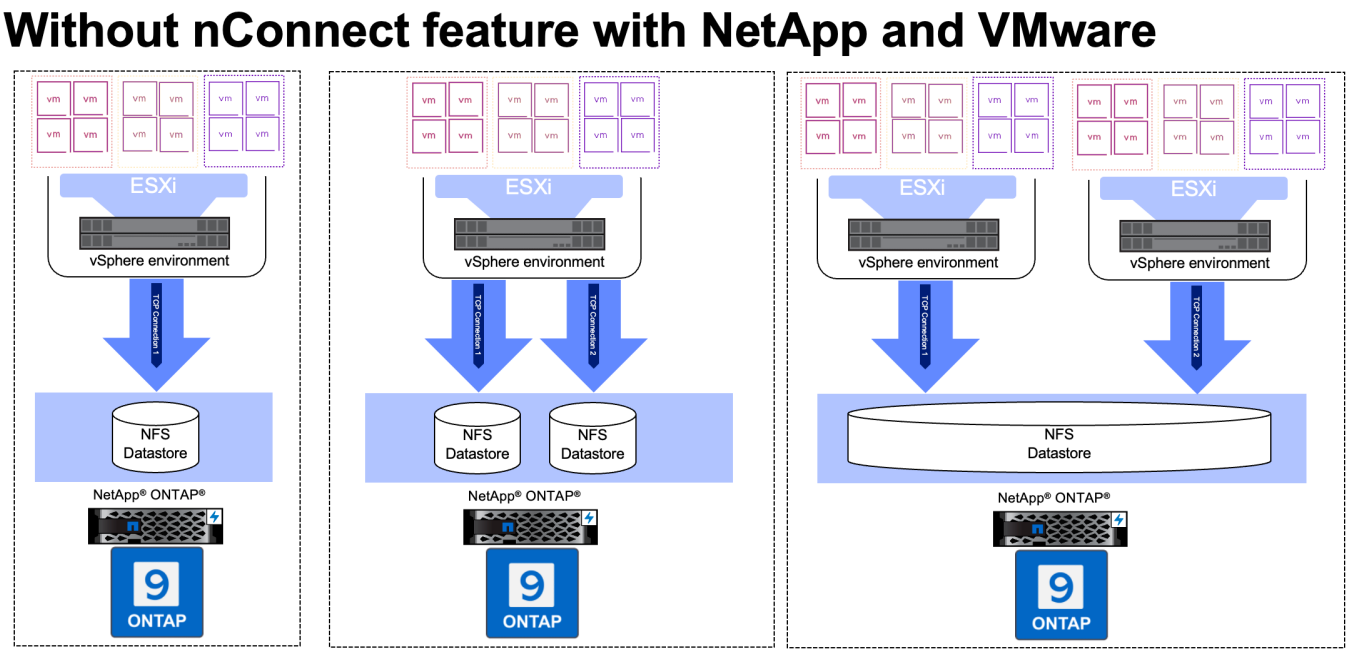
Technische Details

Der Zweck von nconnect besteht darin, mehrere TCP-Verbindungen pro NFS-Datastore auf einem vSphere-Host zur Verfügung zu stellen. Dadurch werden Parallelität und Performance von NFS-Datastores 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

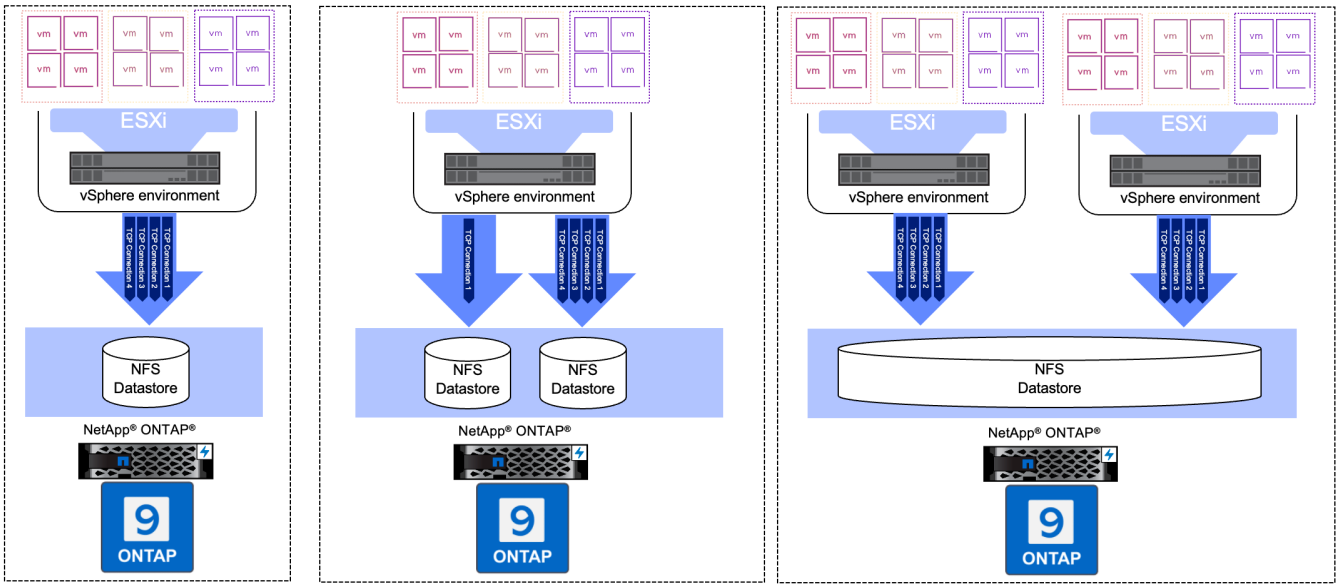
Um die Performance-Einschränkungen einer einzelnen Verbindung mit einem NFS-Datastore zu beheben, werden zusätzliche Datastores gemountet oder weitere Hosts hinzugefügt, um die Verbindung zu erhöhen.



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-Datastore 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
$nfsSpec = New-Object VMware.Vim.HostNasVolumeSpec
$nfsSpec.RemoteHost = "nfs_server.ontap.local"
$nfsSpec.RemotePath = "/DS01"
$nfsSpec.LocalPath = "DS01"
$nfsSpec.AccessMode = "readWrite"
$nfsSpec.Type = "NFS"
$nfsSpec.Connections = 4
$datastoreSys.CreateNasDatastore($nfsSpec)
```

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

```
$env.GOVC_URL = 'vcenter.vsphere.local'
$env.GOVC_USERNAME = 'administrator@vsphere.local'
$env.GOVC_PASSWORD = 'XXXXXXXXX'
$env.GOVC_Datastore = 'DS01'
# $env.GOVC_INSECURE = 1
$env.GOVC_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 Implementierungsleitfaden" 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.

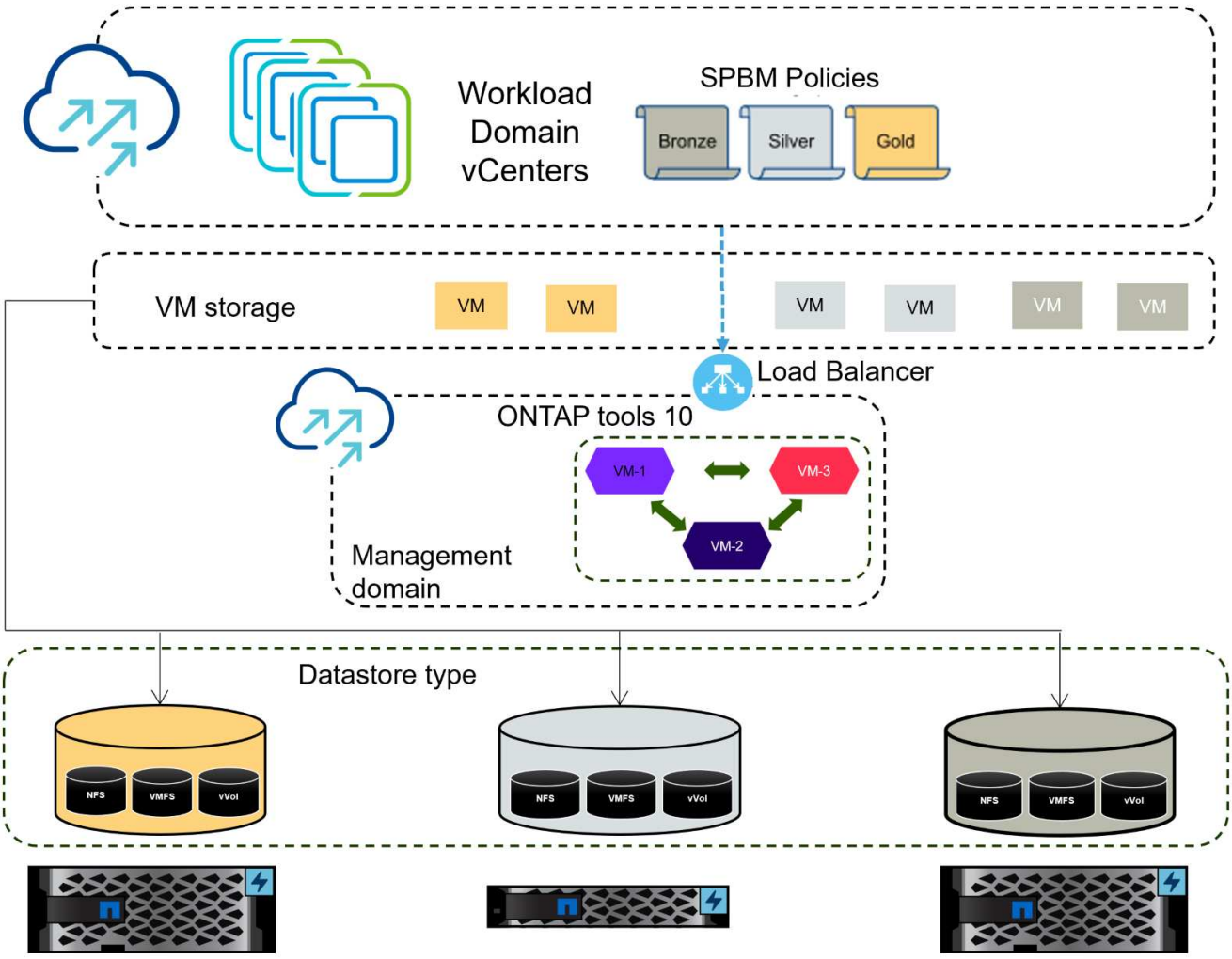
Lösungsüberblick

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-Datastore 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 Architekturanforderungen 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 "Netzwerkkonfiguration – 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:

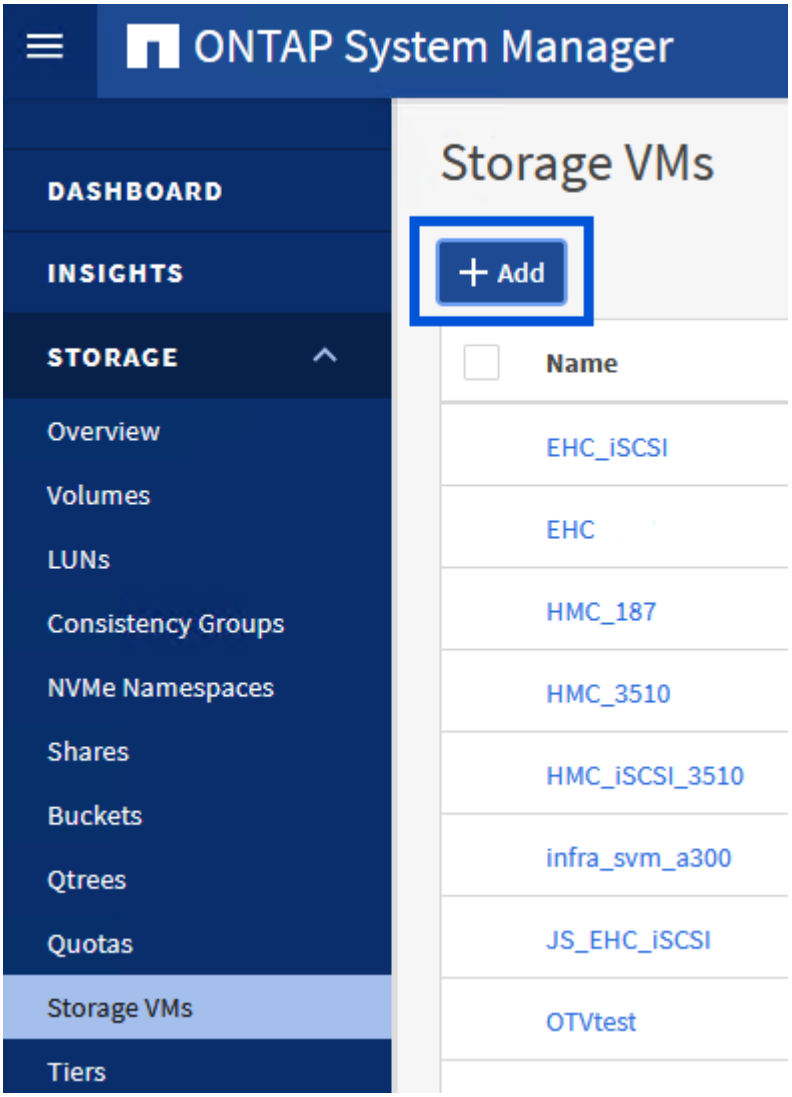
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

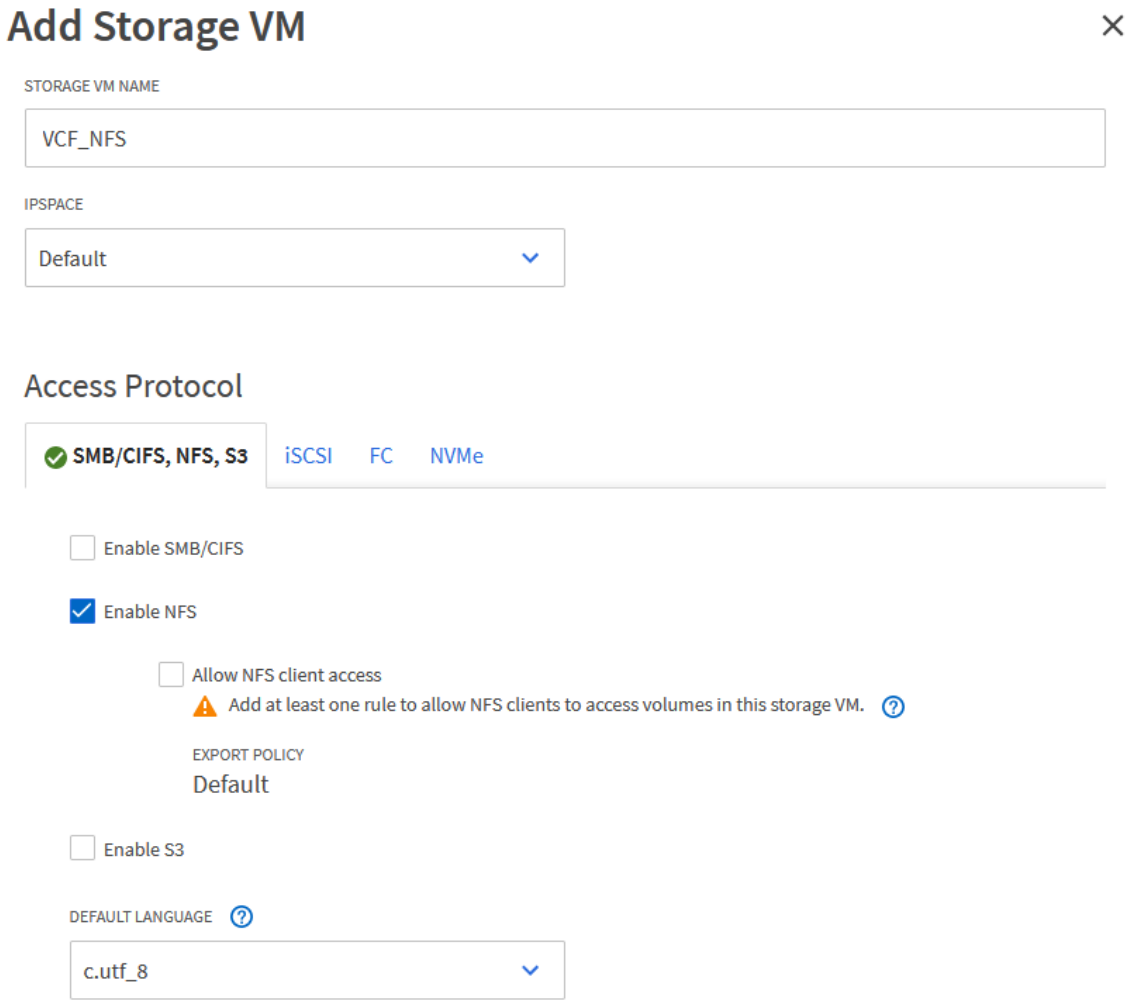
Storage-VM und LIFs erstellen

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.

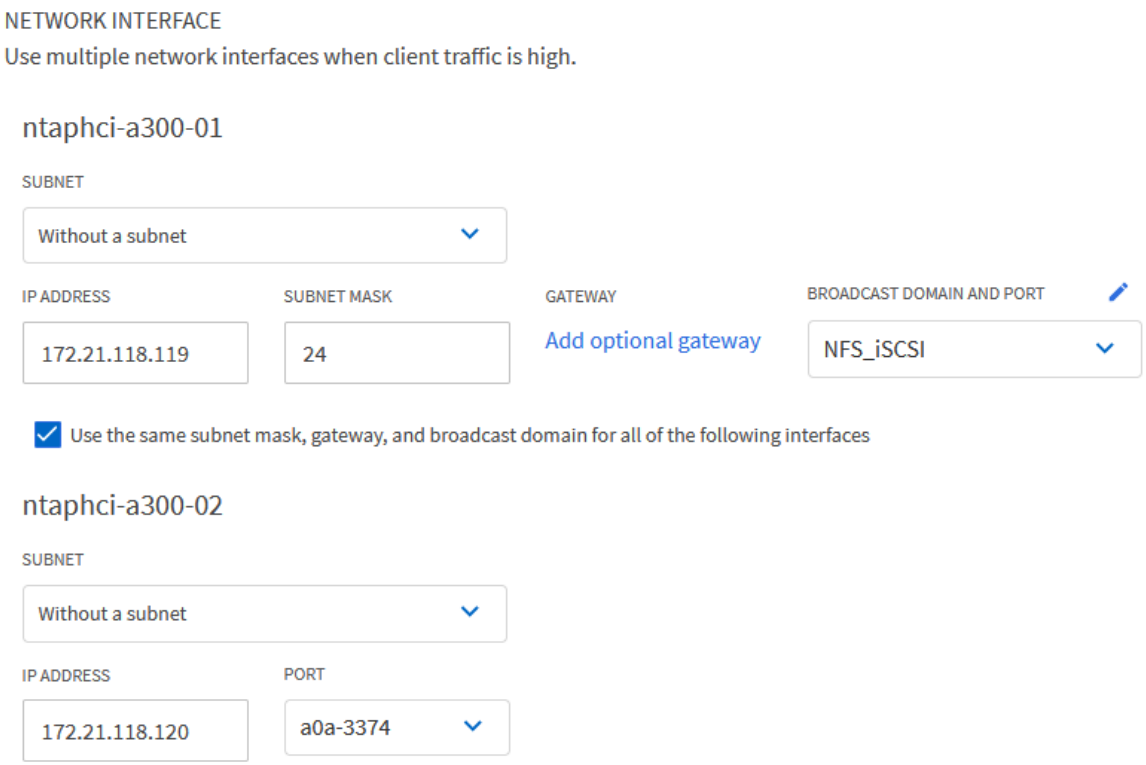


2. Im **Add Storage VM** Wizard geben Sie einen **Namen** für die SVM an, wählen Sie den **IP Space** aus und klicken dann unter **Access Protocol** auf die Registerkarte **SMB/CIFS, NFS, S3** und aktivieren Sie das Kontrollkästchen **enable NFS**.

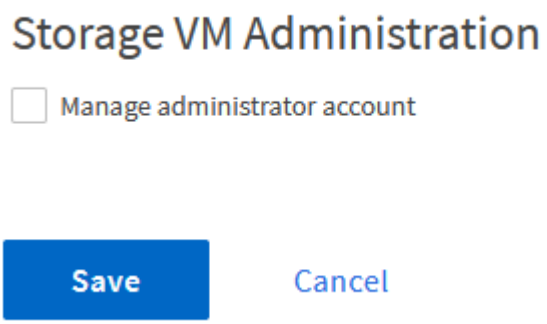


Es ist nicht notwendig, hier die Schaltfläche **NFS-Client-Zugriff zulassen** zu aktivieren, da ONTAP-Tools für VMware vSphere verwendet werden, um den Datastore-Bereitstellungsprozess zu automatisieren. Dazu gehört auch die Bereitstellung des Client-Zugriffs für die ESXi-Hosts.

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.



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.



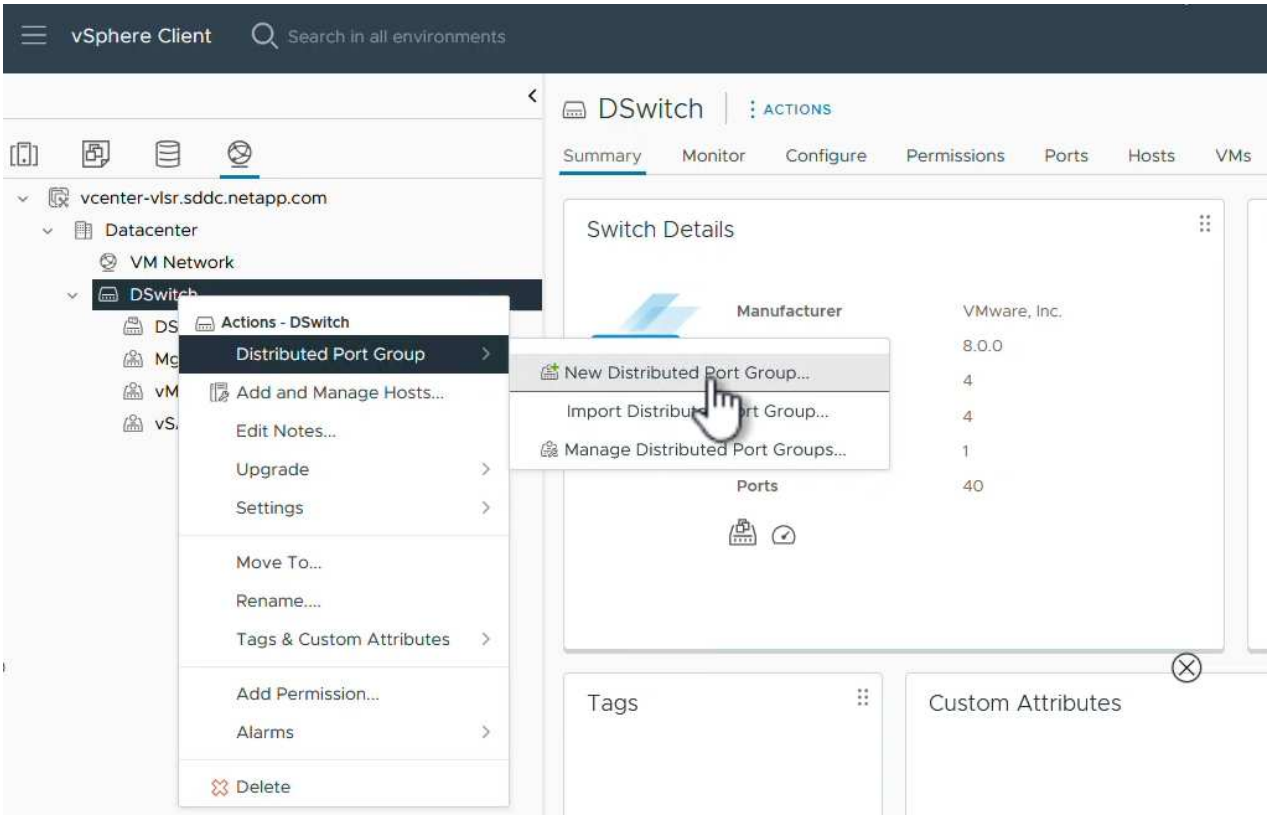
Richten Sie das Netzwerk für NFS auf ESXi-Hosts ein

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.

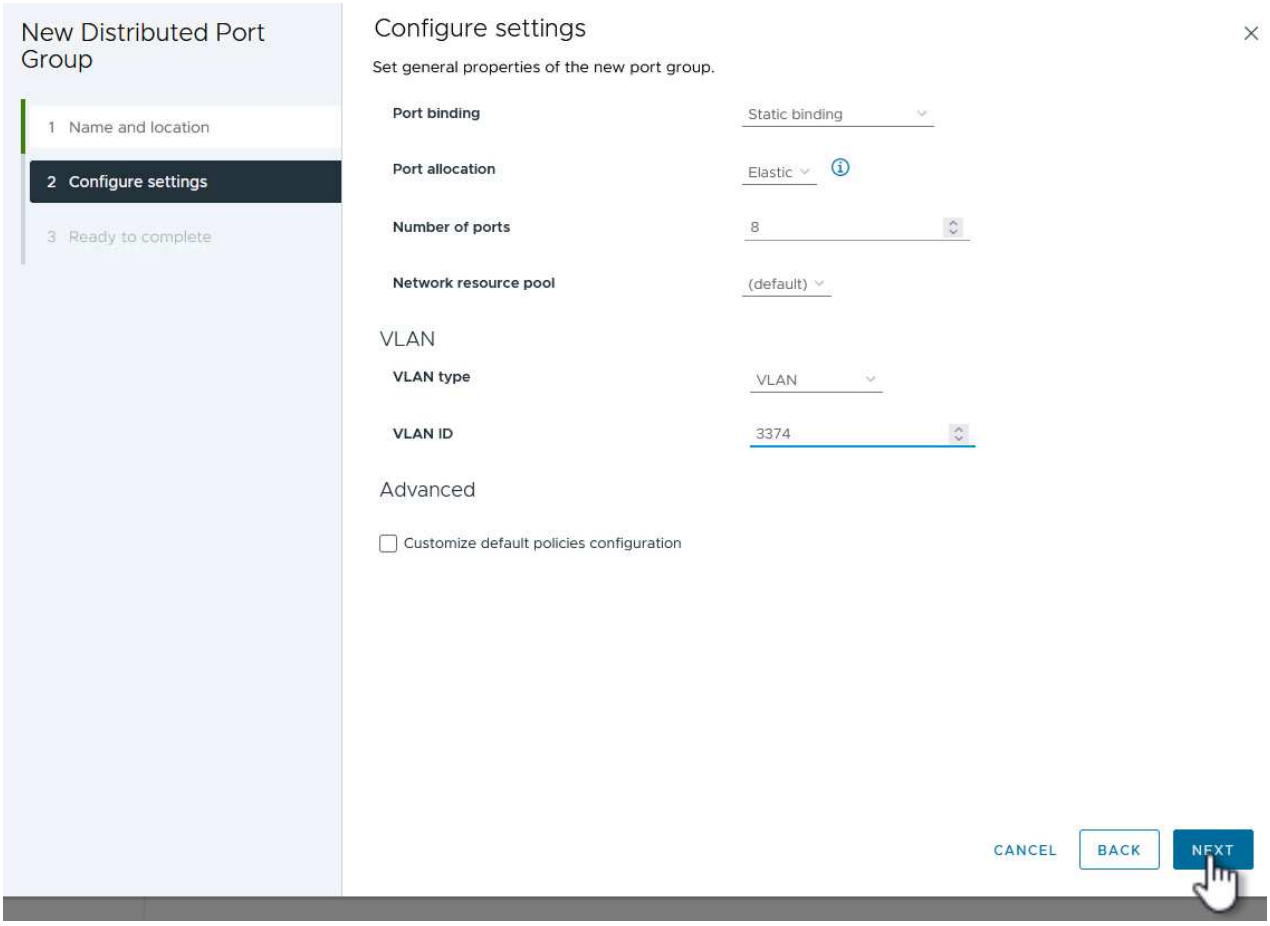
Erstellen Sie eine verteilte Portgruppe für NFS-Datenverkehr

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

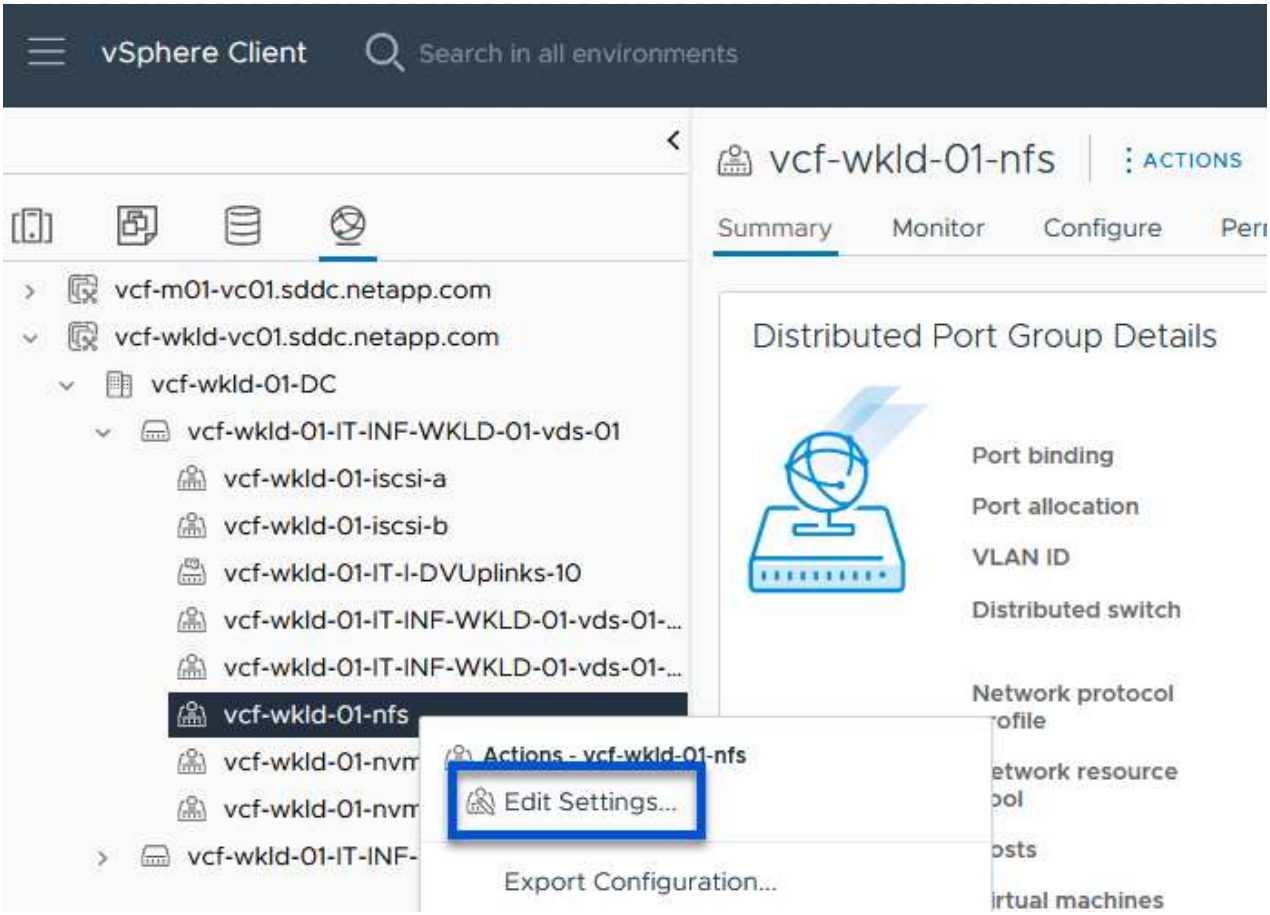
1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workload-Domäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen von **New Distributed Port Group…** aus.



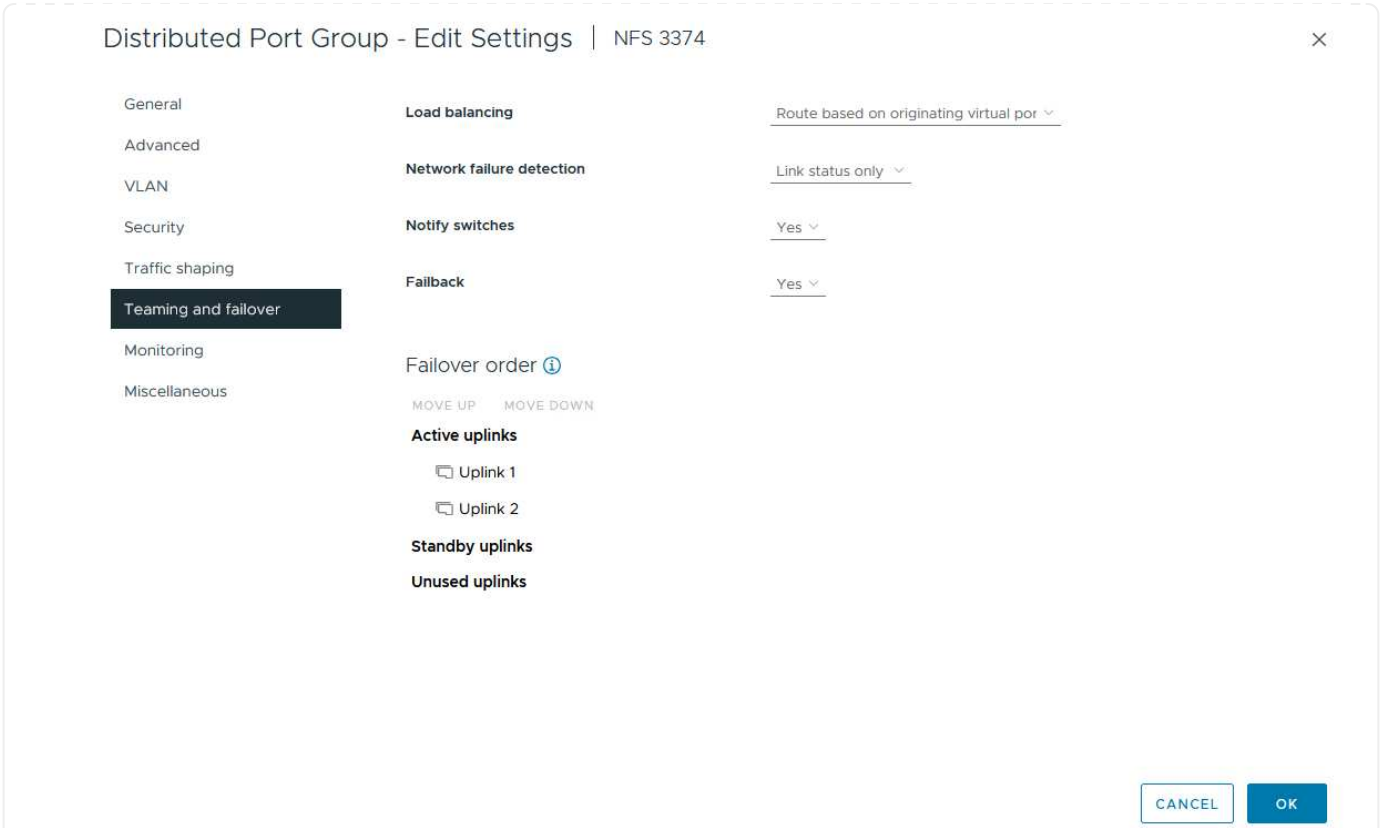
2. Geben Sie im Assistenten **New Distributed Port Group** einen Namen für die neue Portgruppe ein und klicken Sie auf **Next**, um fortzufahren.
3. Füllen Sie auf der Seite **Configure settings** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige VLAN-ID angeben.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



4. Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
5. 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**.

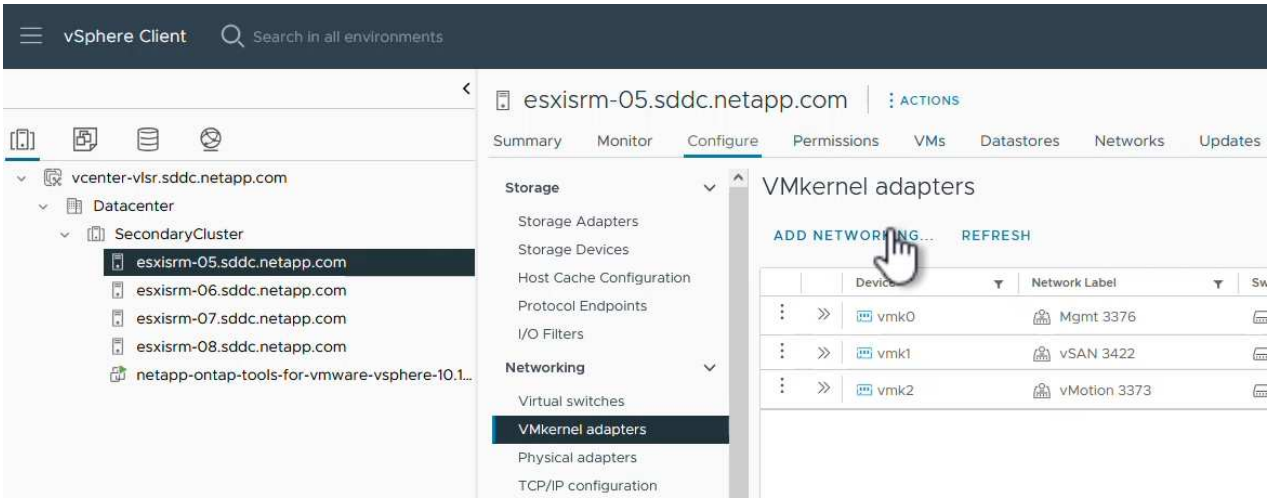


7. Wiederholen Sie diesen Vorgang für jeden ESXi-Host im Cluster.

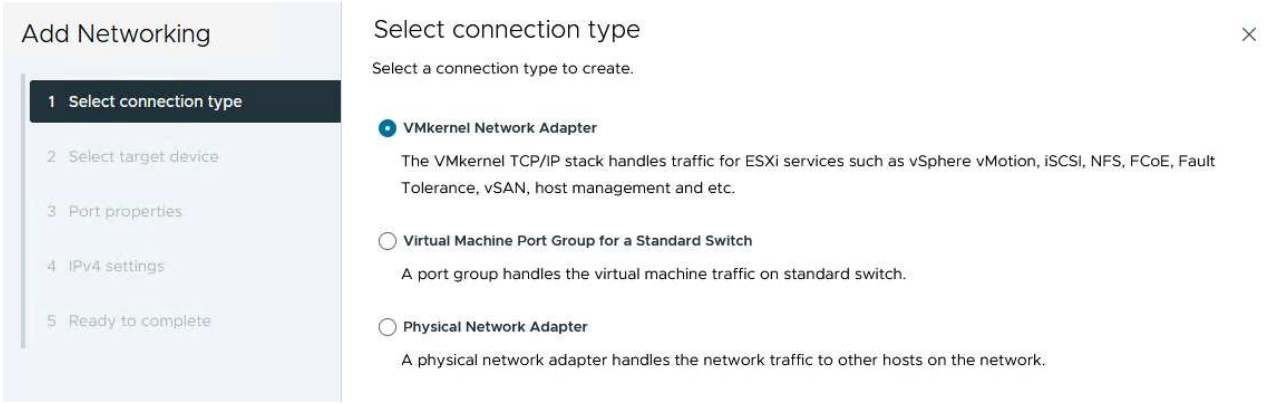
Erstellen Sie auf jedem ESXi-Host einen VMkernel-Adapter

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

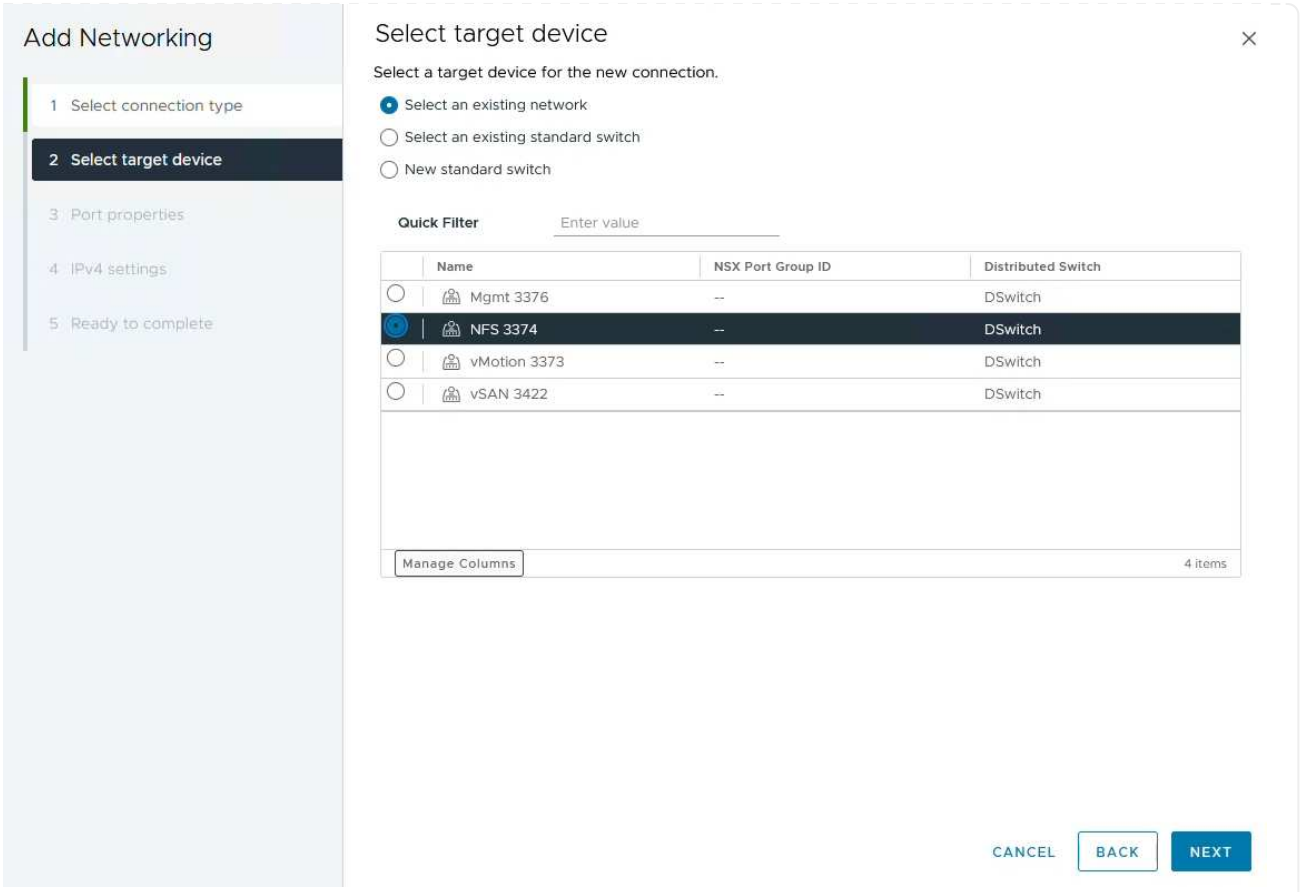
1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts in der Workload-Domäneninventarisierung. Wählen Sie auf der Registerkarte **Configure VMkernel Adapter** und klicken Sie auf **Add Networking…**, um zu starten.



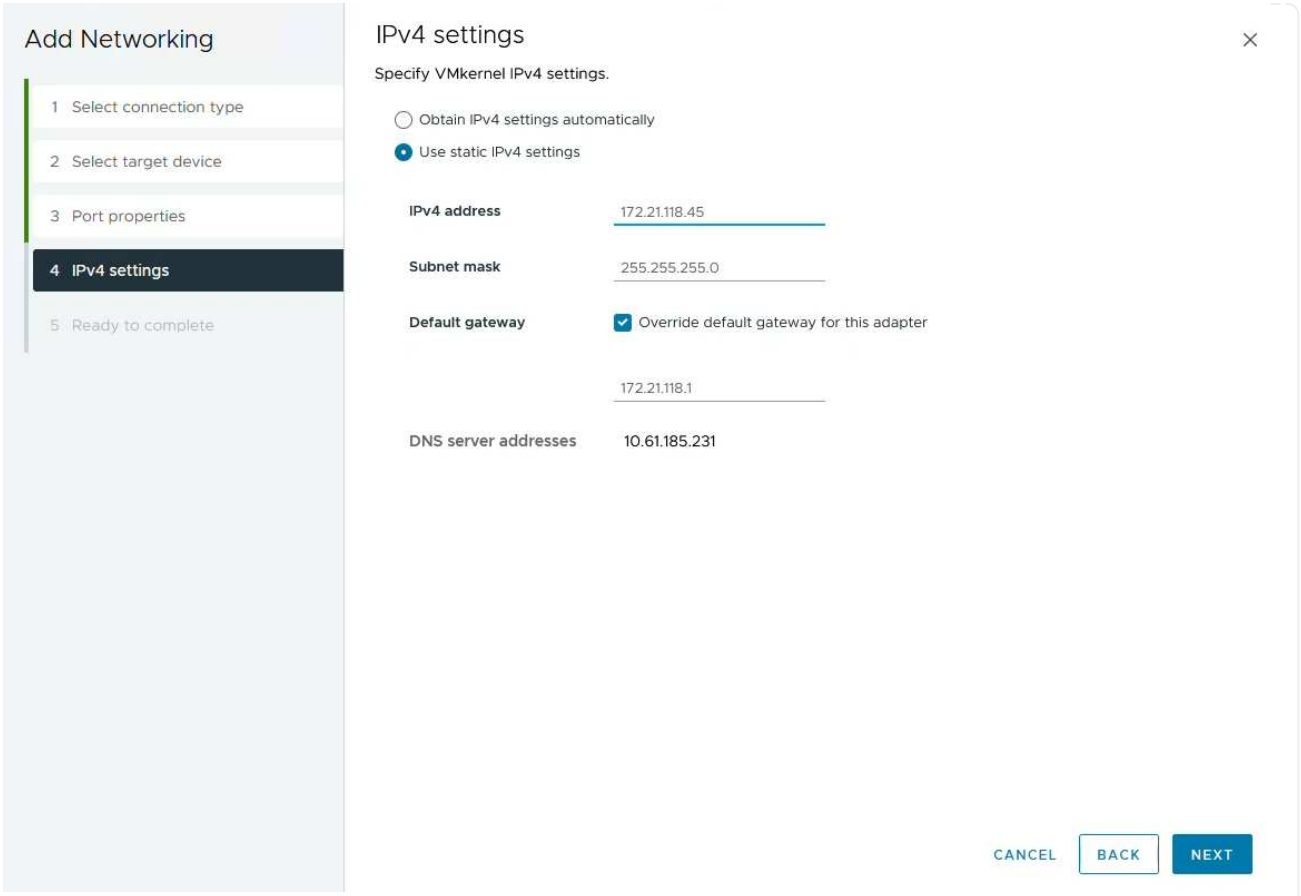
2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



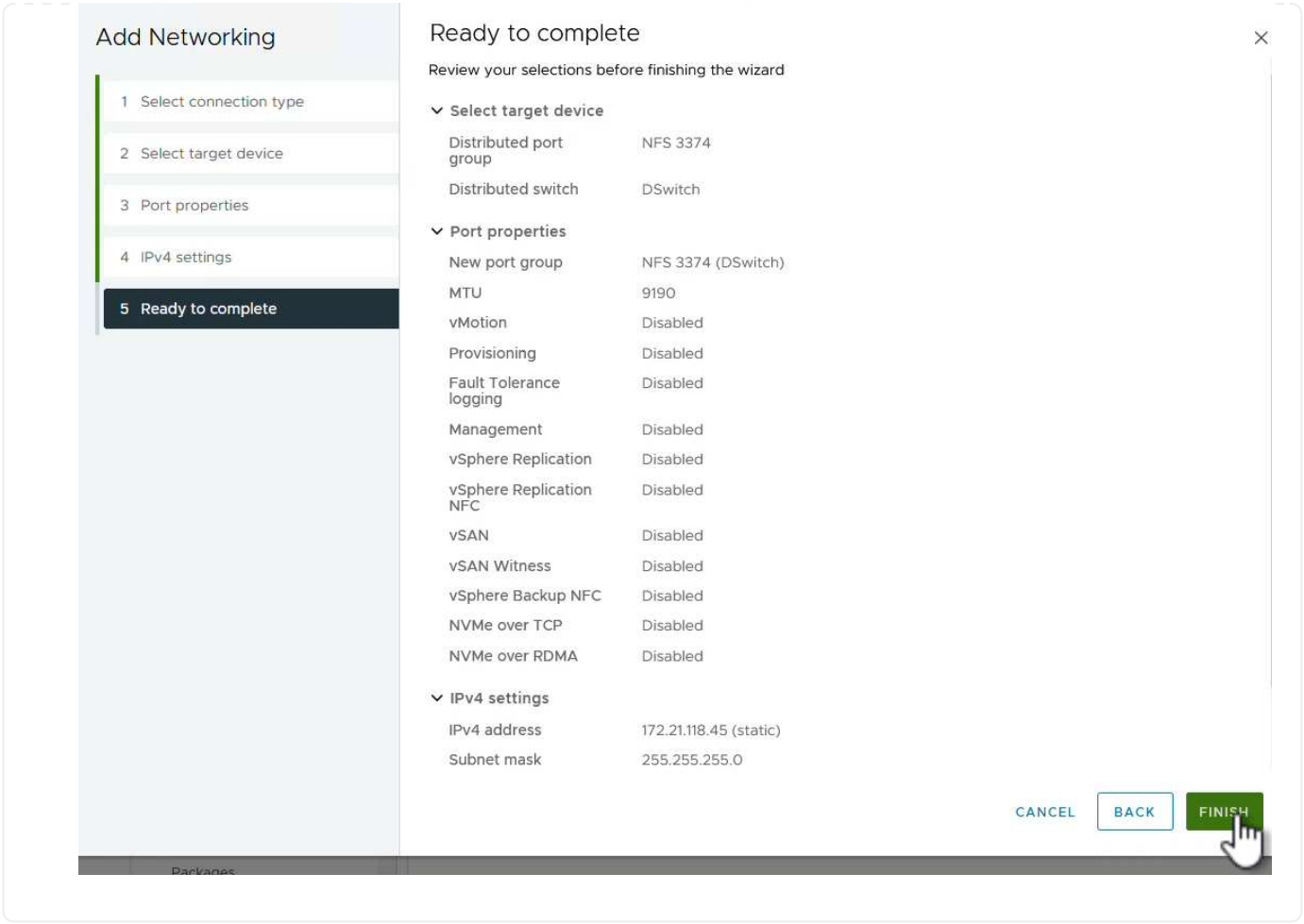
3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für NFS aus.



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.



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".

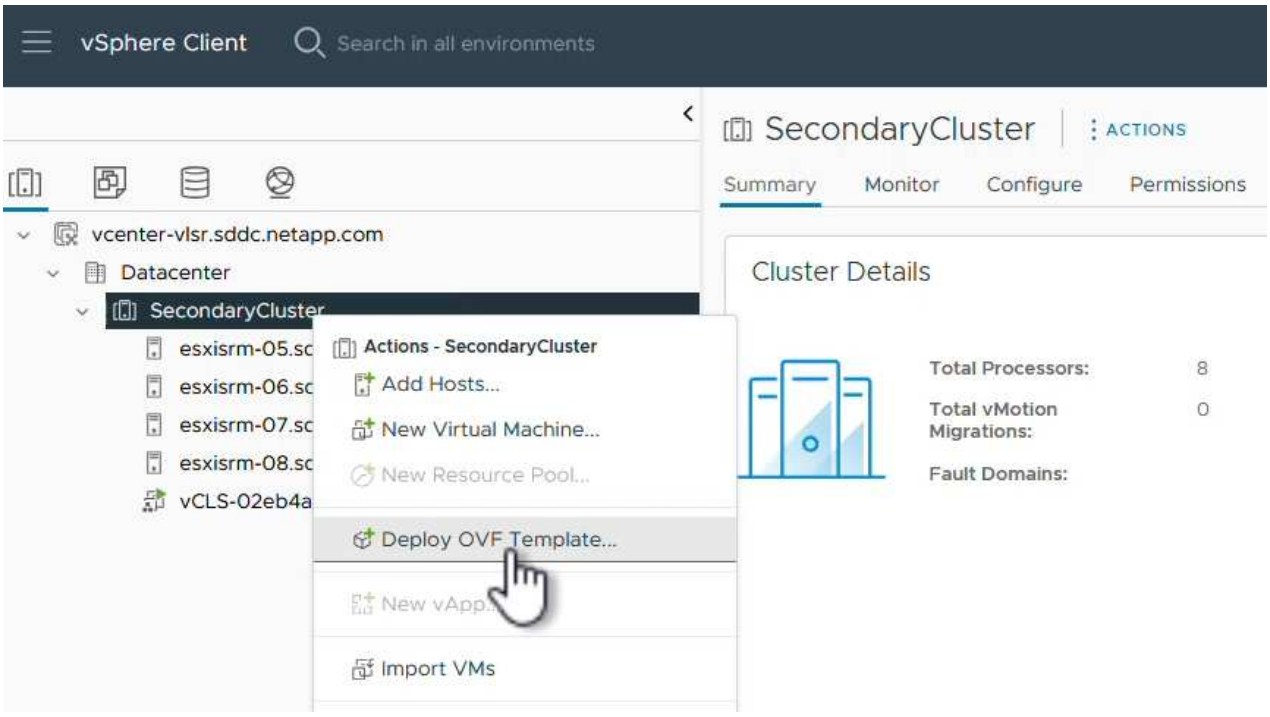
Implementieren Sie ONTAP-Tools für VMware vSphere 10

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.

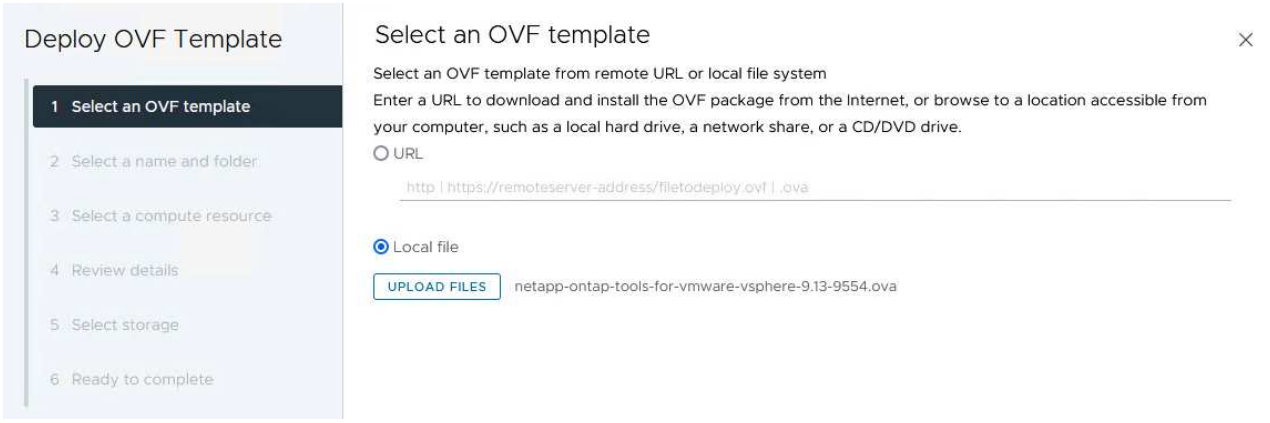
> In einem Szenario ohne Hochverfügbarkeit sind drei verfügbare IP-Adressen erforderlich. Dem Load Balancer wird eine IP-Adresse zugewiesen, eine weitere für die Kubernetes-Kontrollebene und die verbleibende Adresse für den Node. In einer HA-Implementierung sind zusätzlich zu den ersten drei für den 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:

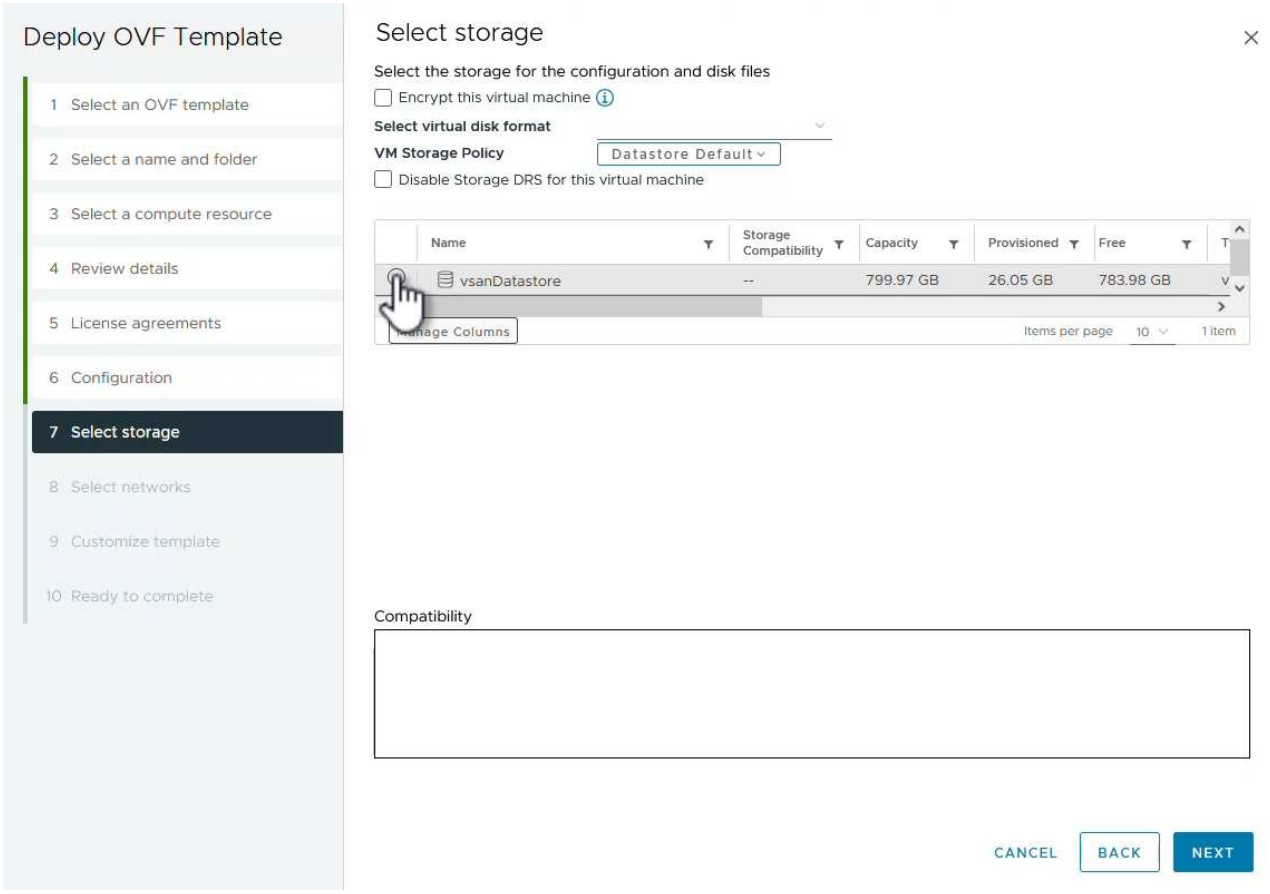
1. Rufen Sie das OVA-Image der ONTAP-Tools auf"NetApp Support Website", und laden Sie es in einen lokalen Ordner herunter.
2. Melden Sie sich bei der vCenter Appliance für den vSphere 8-Cluster an.
3. Klicken Sie in der vCenter-Appliance-Oberfläche mit der rechten Maustaste auf den Management-Cluster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



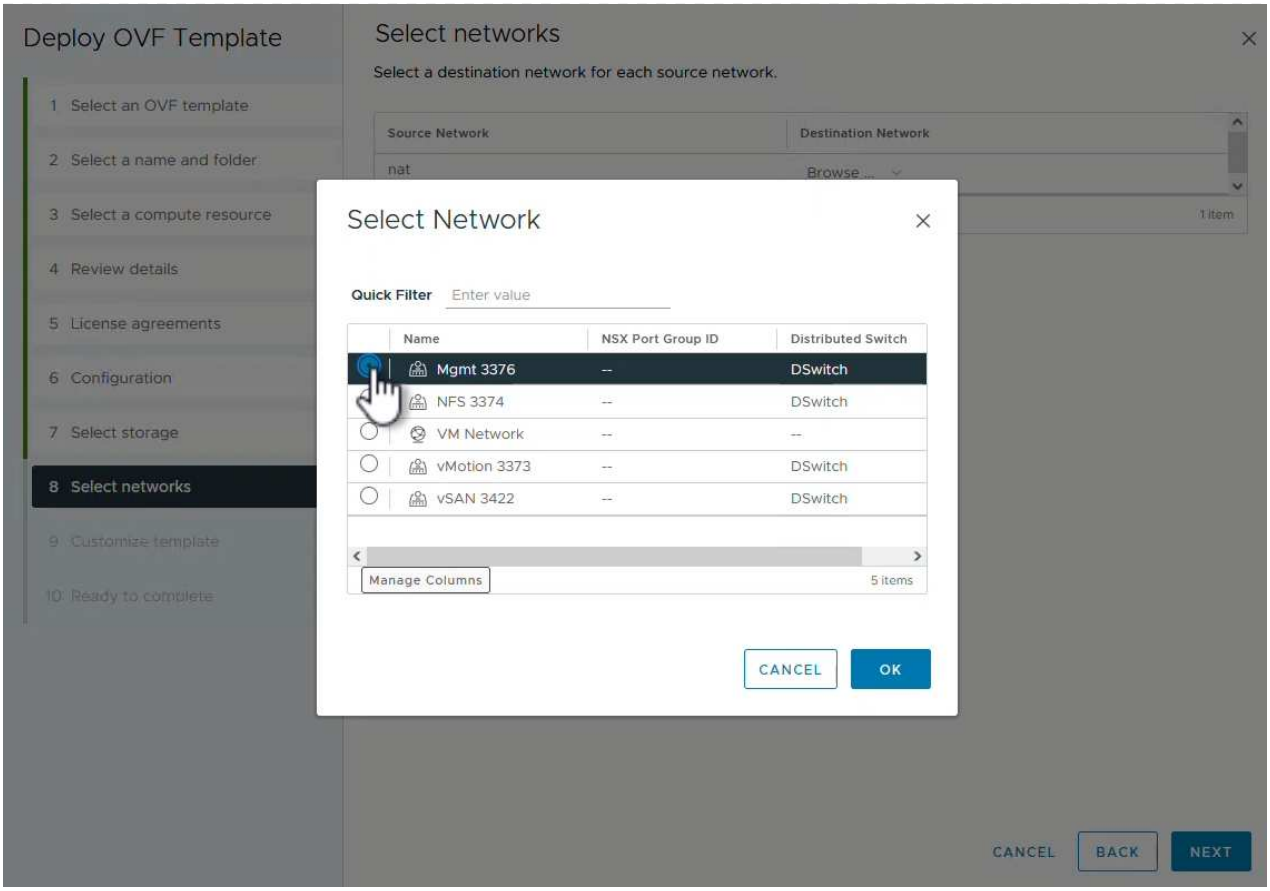
4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei für ONTAP-Tools aus.



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.

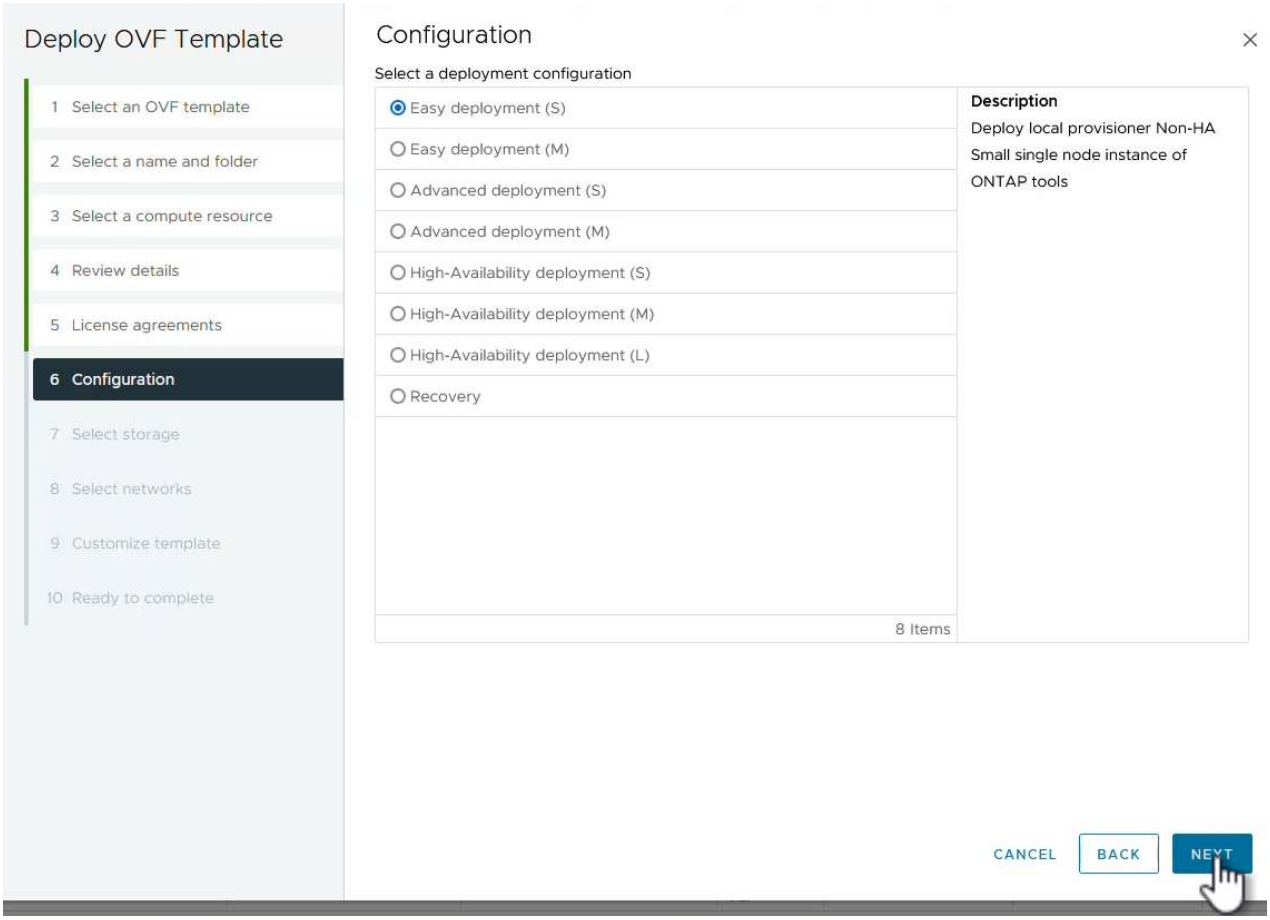


7. Wählen Sie auf der Seite Netzwerk auswählen das Netzwerk aus, das für den Verwaltungsdatenverkehr verwendet wird.



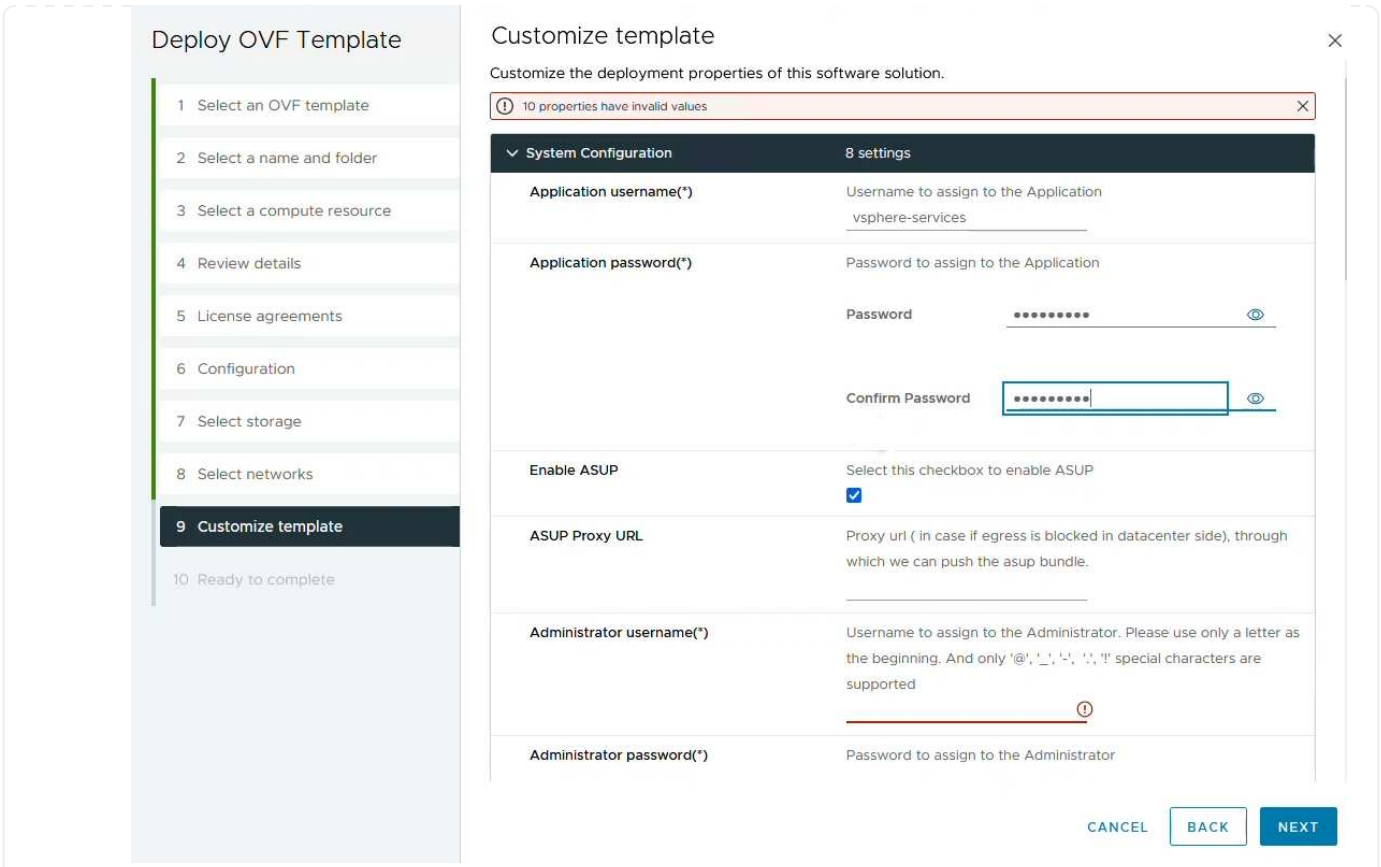
8. Wählen Sie auf der Konfigurationsseite die zu verwendende Bereitstellungskonfiguration aus. In diesem Szenario wird die einfache Bereitstellungsmethode verwendet.

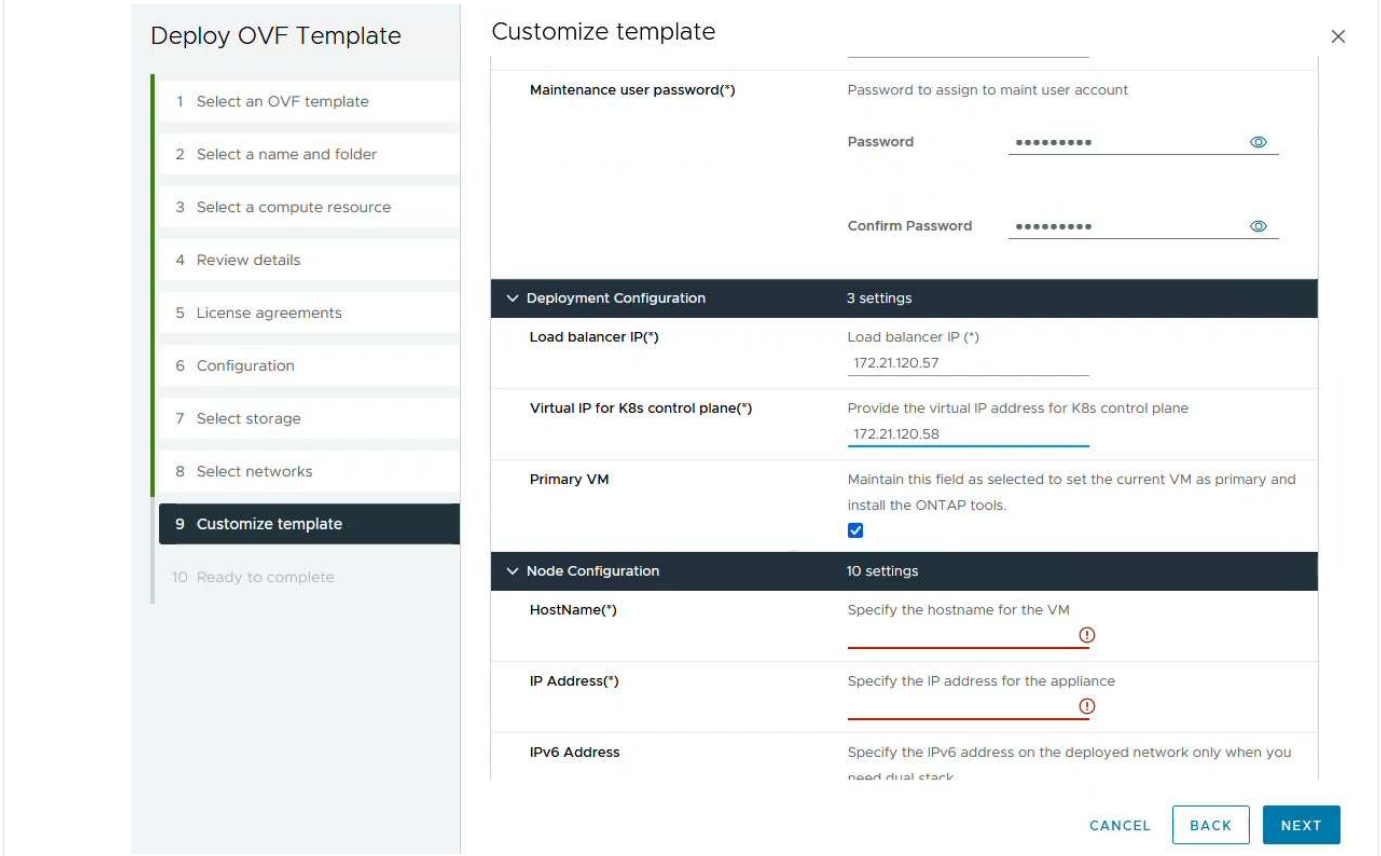
> ONTAP Tools 10 umfasst verschiedene Implementierungskonfigurationen, einschließlich Hochverfügbarkeitsimplementierungen mit mehreren Nodes. Dokumentation zu allen Bereitstellungskonfigurationen und -Voraussetzungen finden Sie unter "Voraussetzungen für die Bereitstellung von ONTAP-Tools für VMware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



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.
   - Wartungsbenutzerpasswort 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
System Configuration
8 settings
Application username(*)
Username to assign to the Application
vsphere-services
Application password(*)
Password to assign to the Application
Password
Confirm Password
Enable ASUP
Select this checkbox to enable ASUP
ASUP Proxy URL
Proxy url (in case if egress is blocked in datacenter side), through which we can push the asup bundle.
Administrator username(*)
Username to assign to the Administrator. Please use only a letter as the beginning. And only '@', '_', '-', '.', '!' special characters are supported
Administrator password(*)
Password to assign to the Administrator
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
Password
Confirm Password
Deployment Configuration
3 settings
Load balancer IP(*)
Load balancer IP (*)
172.21.120.57
Virtual IP for K8s control plane(*)
Provide the virtual IP address for K8s control plane
172.21.120.58
Primary VM
Maintain this field as selected to set the current VM as primary and install the ONTAP tools.
Node Configuration
10 settings
HostName(*)
Specify the hostname for the VM
IP Address(*)
Specify the IP address for the appliance
IPv6 Address
Specify the IPv6 address on the deployed network only when you
CANCEL
BACK
NEXT

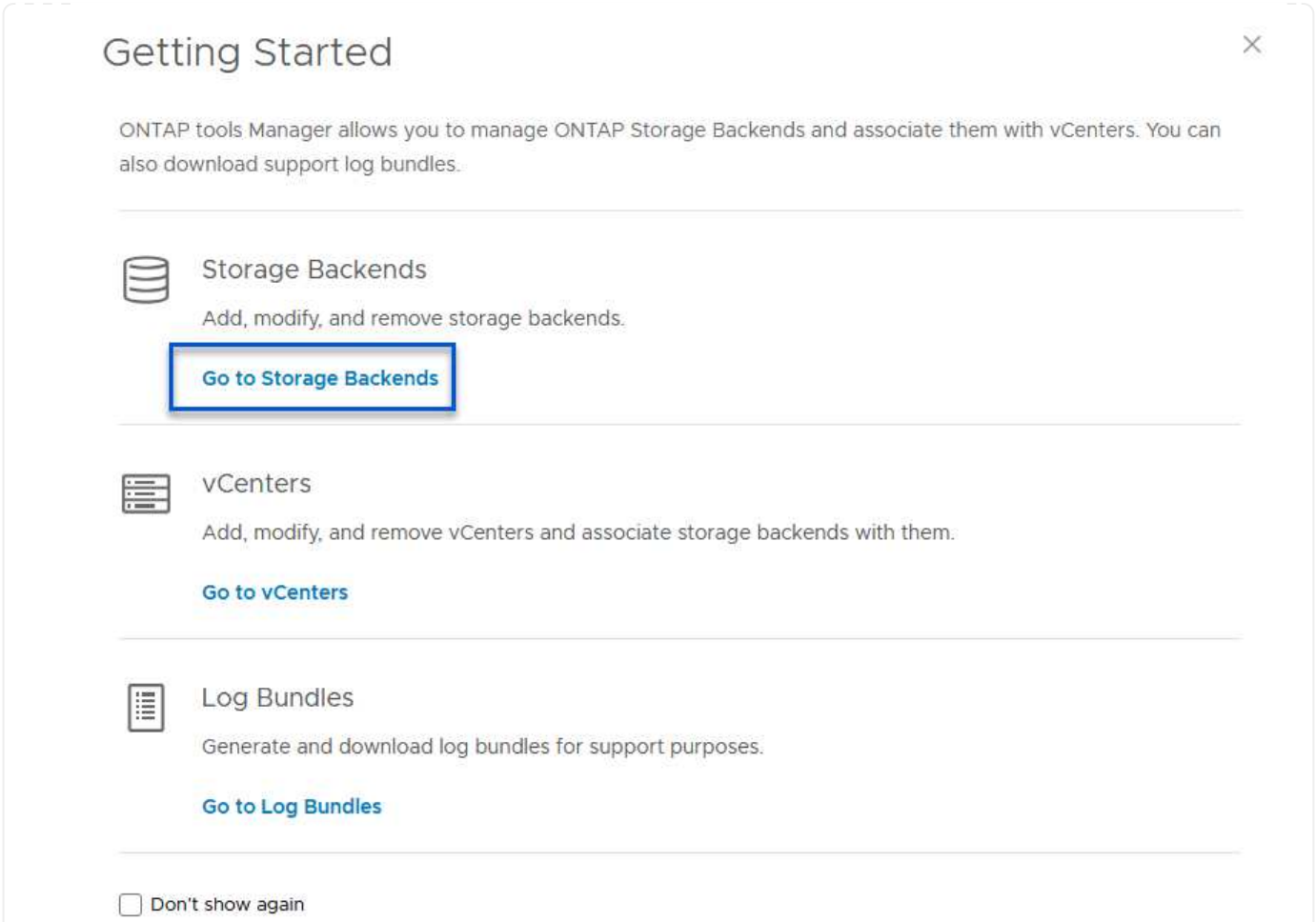
10. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der ONTAP Tools Appliance zu beginnen.

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

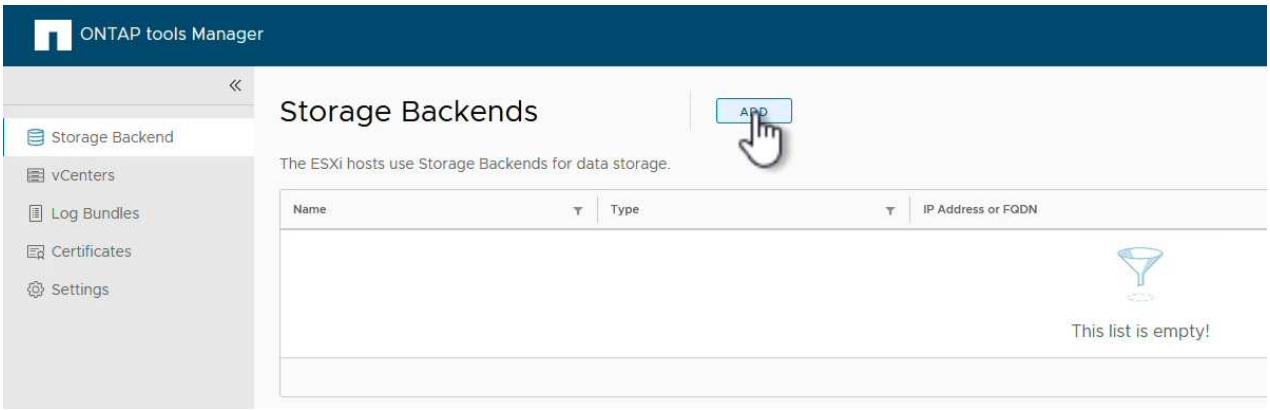
Der ONTAP-Tools-Manager wird verwendet, um globale Einstellungen für ONTAP-Tools 10 zu konfigurieren.

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.

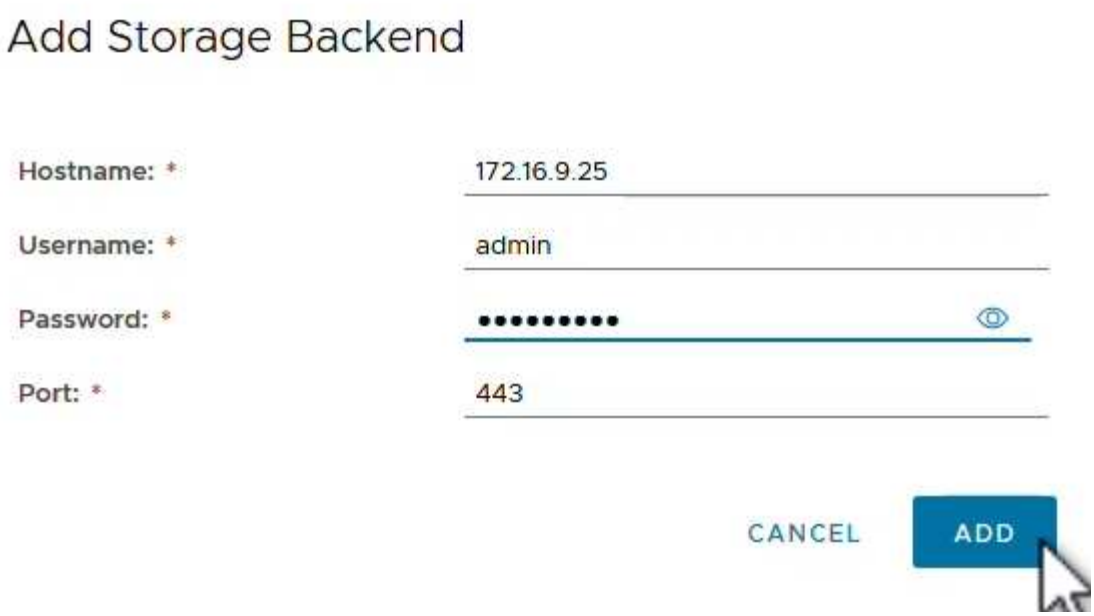
2. Klicken Sie auf der Seite **erste Schritte** auf **Gehe zu Speicher-Backends**.



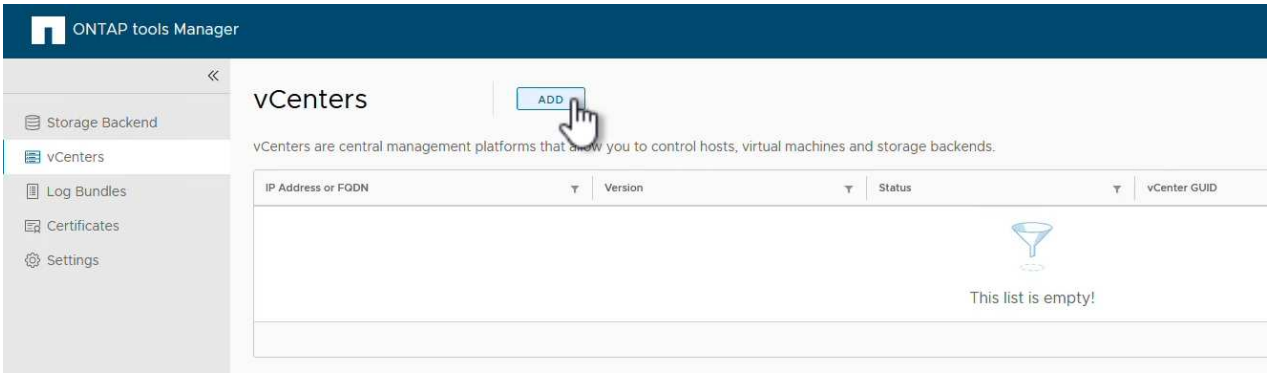
3. Klicken Sie auf der Seite **Speicher-Backends** auf **ADD**, um die Zugangsdaten eines ONTAP-Speichersystems einzugeben, das mit den ONTAP-Tools 10 registriert werden soll.



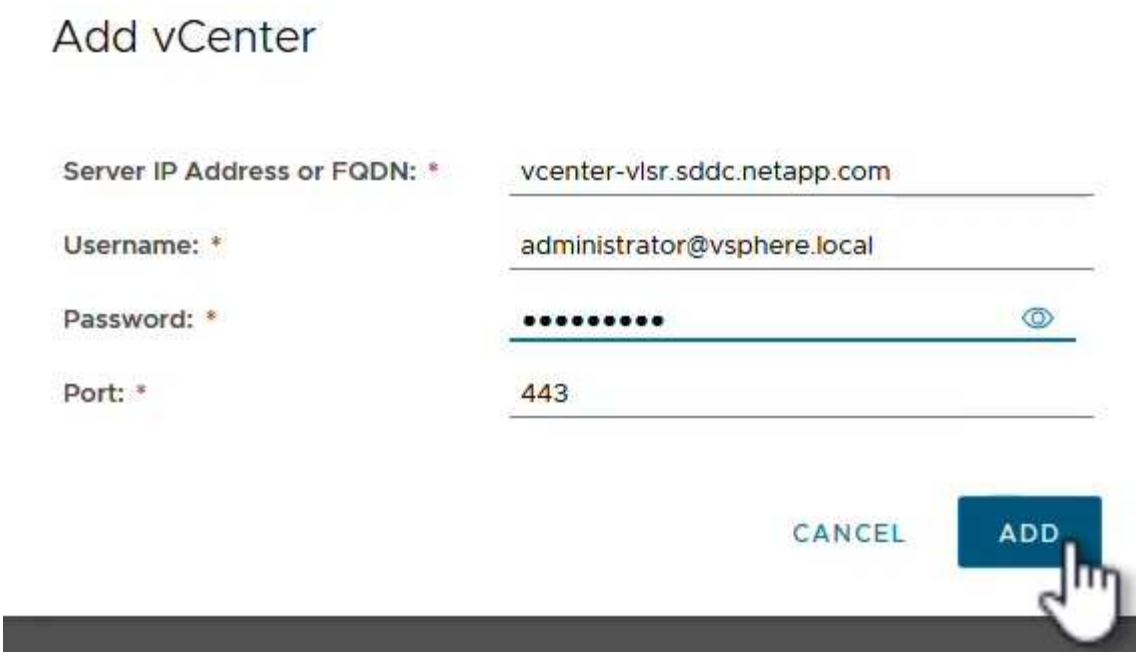
4. Geben Sie im Feld **Speicher-Backend hinzufügen** die Anmeldeinformationen für das ONTAP-Speichersystem ein.



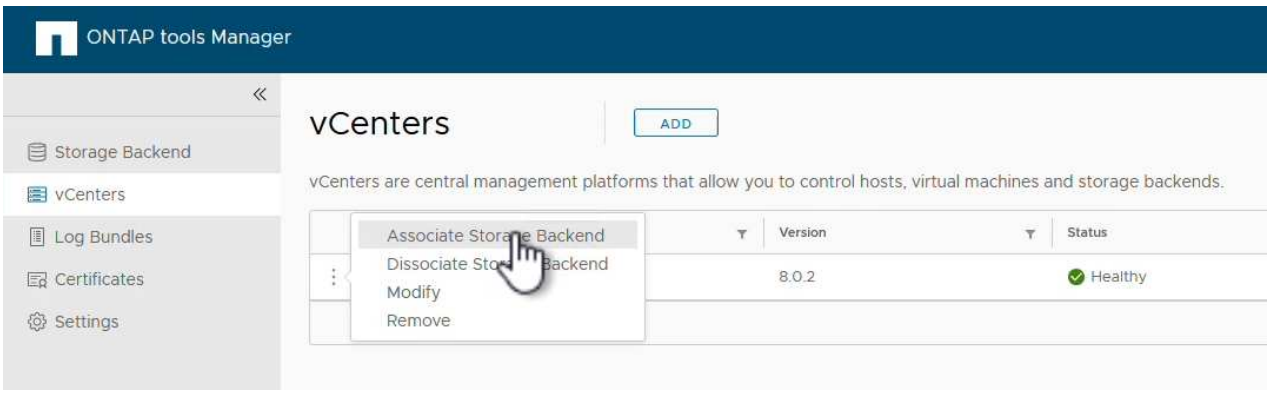
5. Klicken Sie im linken Menü auf **vCenters** und dann auf **ADD**, um die Zugangsdaten eines vCenter-Servers einzugeben, der mit den ONTAP-Tools 10 registriert werden soll.



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

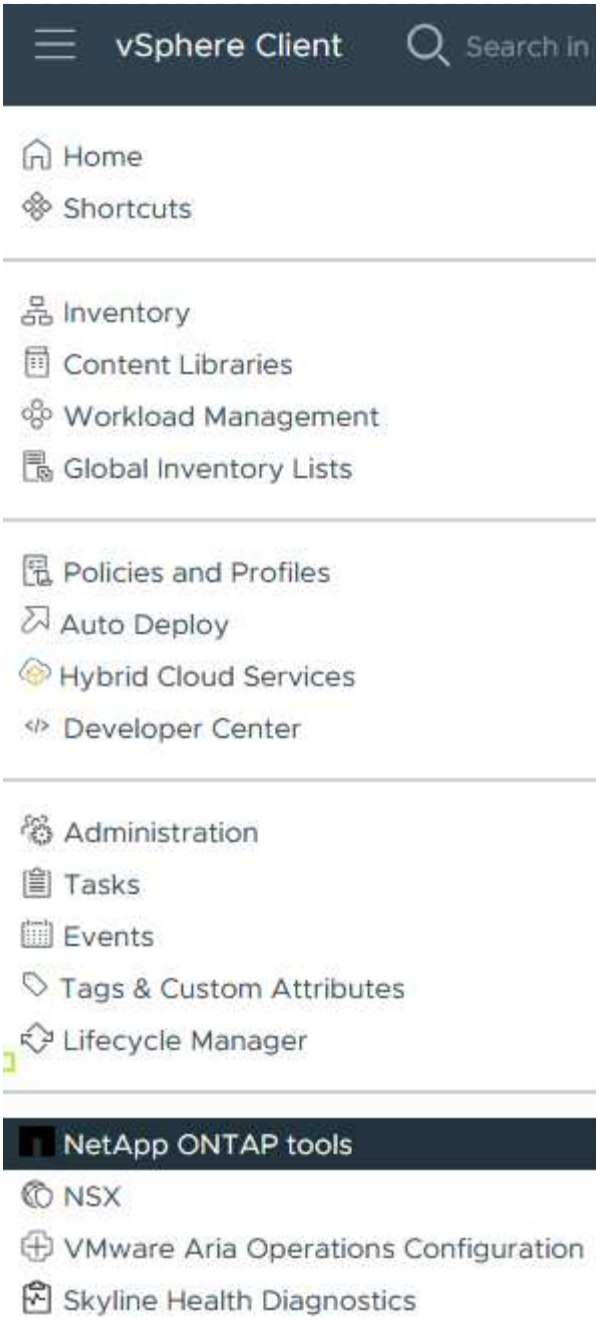


7. Wählen Sie im vertikalen drei-Punkt-Menü für den neu ermittelten vCenter-Server **Speicher-Backend zuordnen** aus.

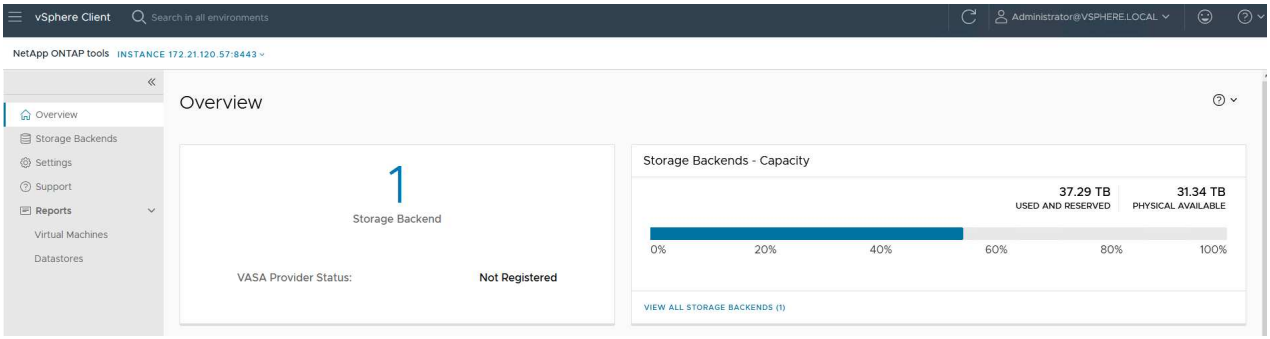


8. Wählen Sie im Feld **Speicher-Backend zuordnen** das ONTAP-Speichersystem aus, das dem vCenter-Server zugeordnet ist, und klicken Sie auf **Associate**, um die Aktion abzuschließen.

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



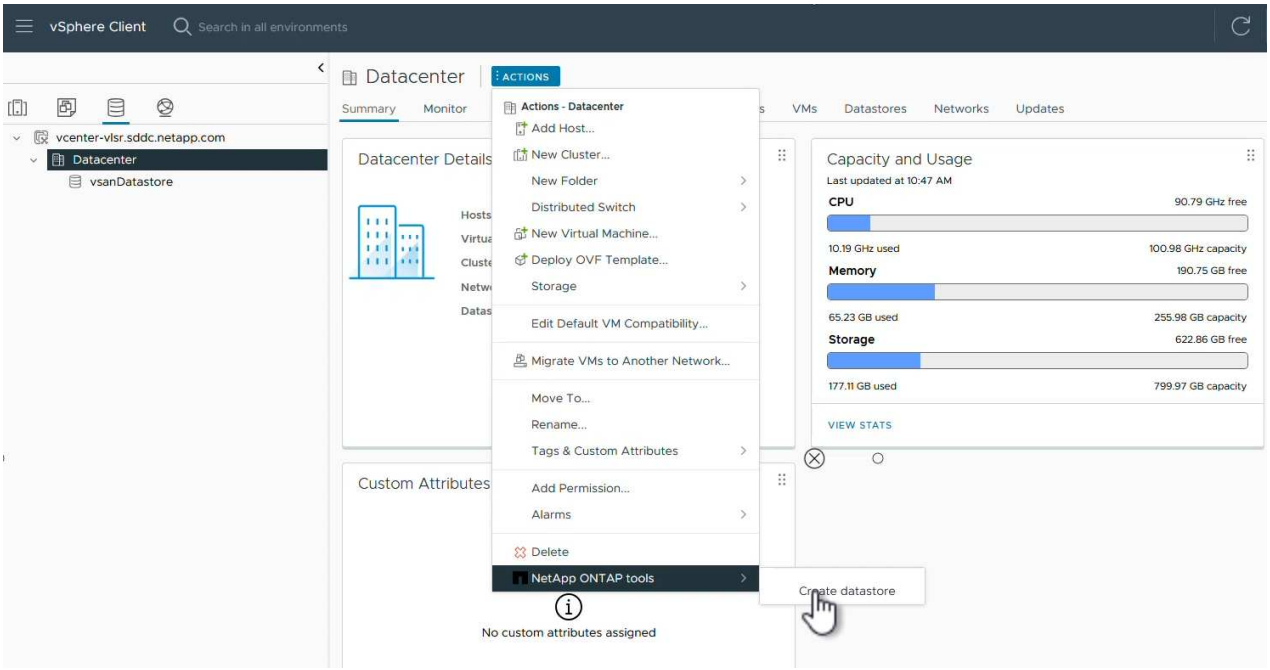
10. Im Dashboard der ONTAP-Tools sollten Sie sehen, dass ein Speicher-Back-End mit dem vCenter Server verknüpft war.



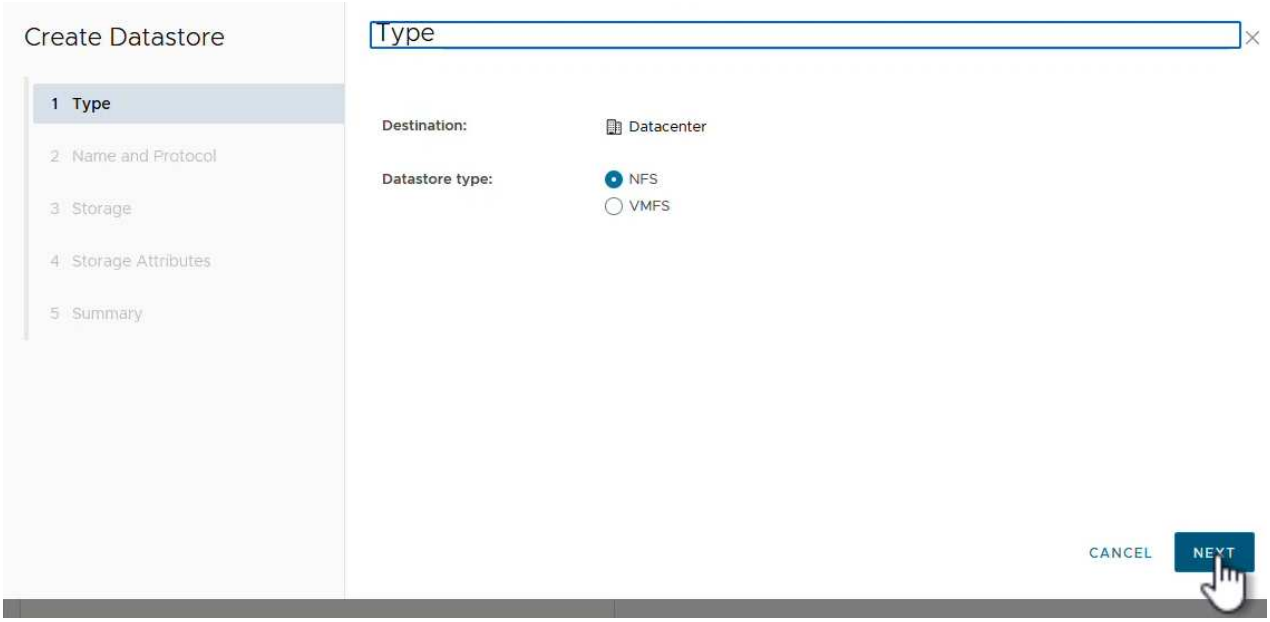
Erstellen Sie einen NFS-Datastore mit ONTAP-Tools 10

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

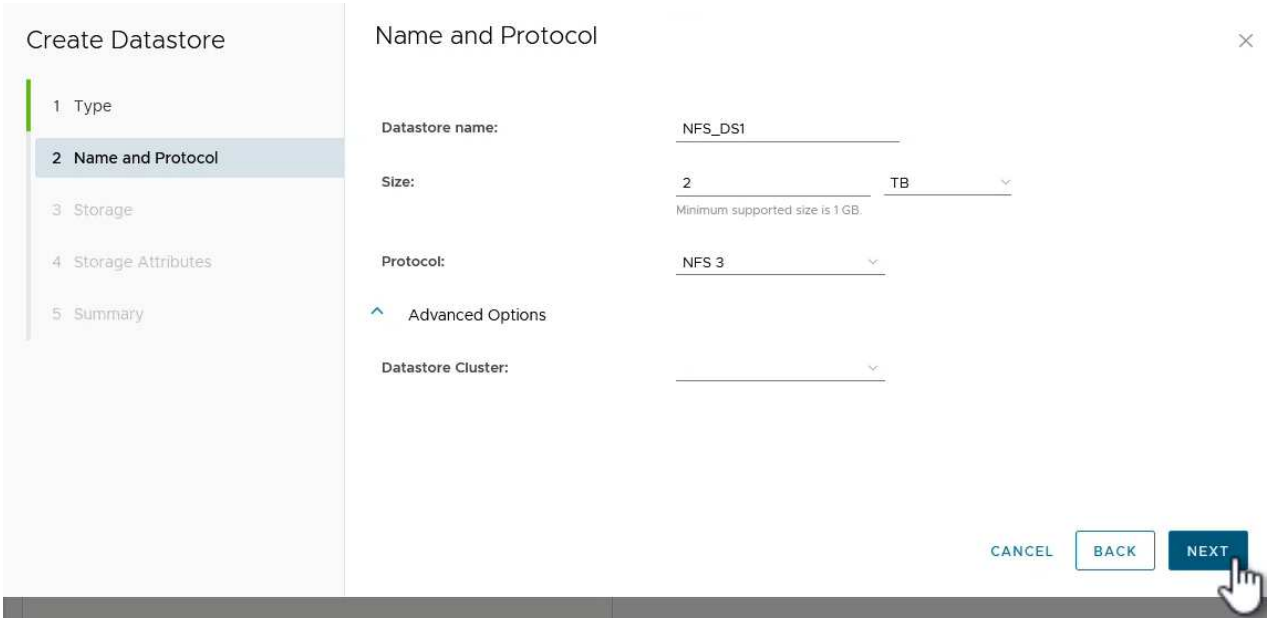
1. Navigieren Sie im vSphere-Client zum Speicherbestand. Wählen Sie im Menü **ACTIONS** die Option **NetApp ONTAP Tools > Datastore erstellen**.



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

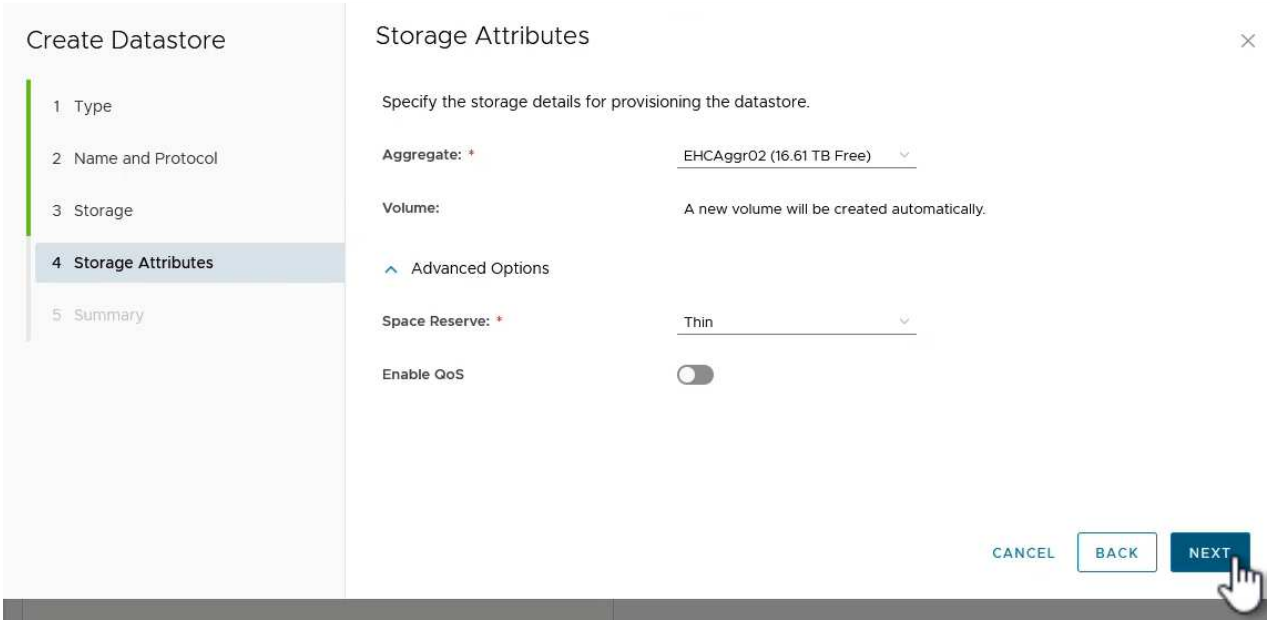


3. Geben Sie auf der Seite **Name und Protokoll** den Namen, die Größe und das Protokoll für den Datastore ein. Klicken Sie auf **Weiter**, um fortzufahren.

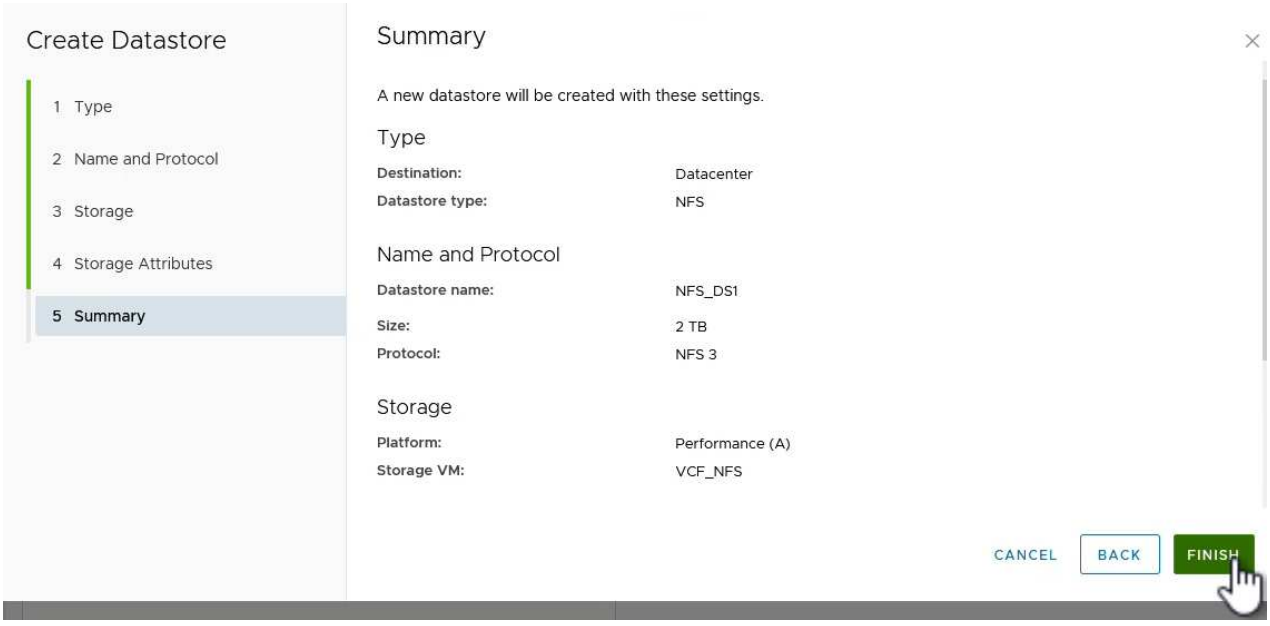


4. Wählen Sie auf der Seite **Storage** eine Plattform (filtert das Speichersystem nach Typ) und eine Speicher-VM für das Volume aus. Wählen Sie optional eine benutzerdefinierte Exportrichtlinie aus. Klicken Sie auf **Weiter**, um fortzufahren.

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.



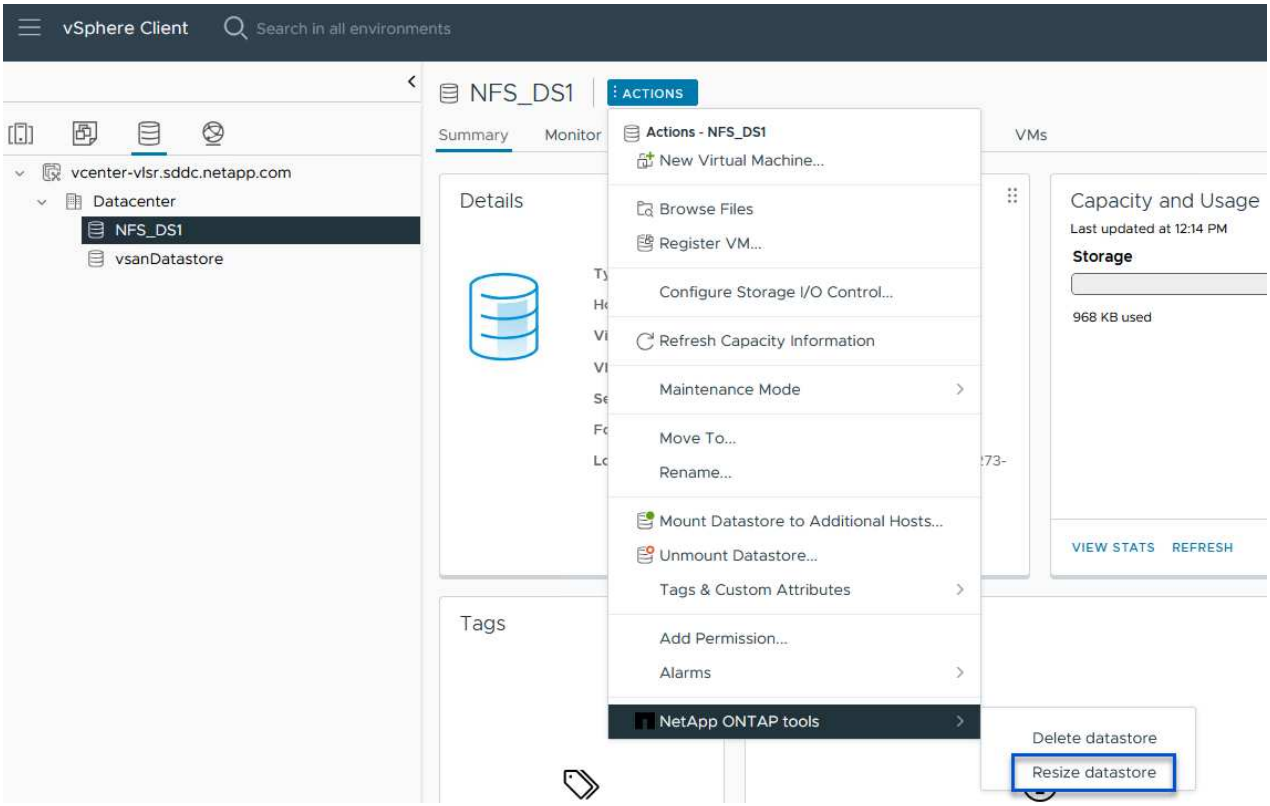
6. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf Fertig stellen, um mit der Erstellung des NFS-Datastore zu beginnen.



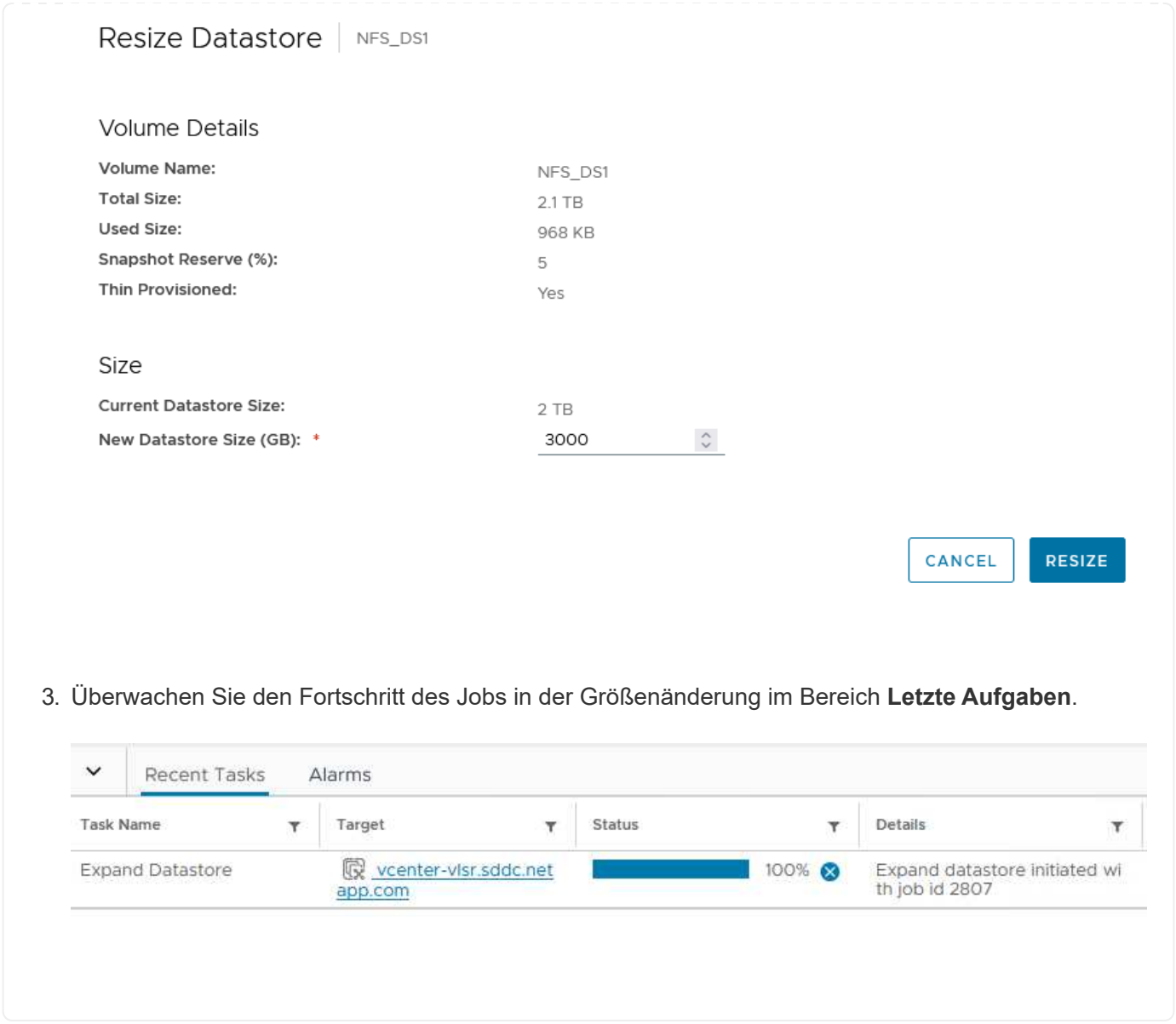
Größe eines NFS-Datenspeichers mit ONTAP-Tools ändern 10

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.



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

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.

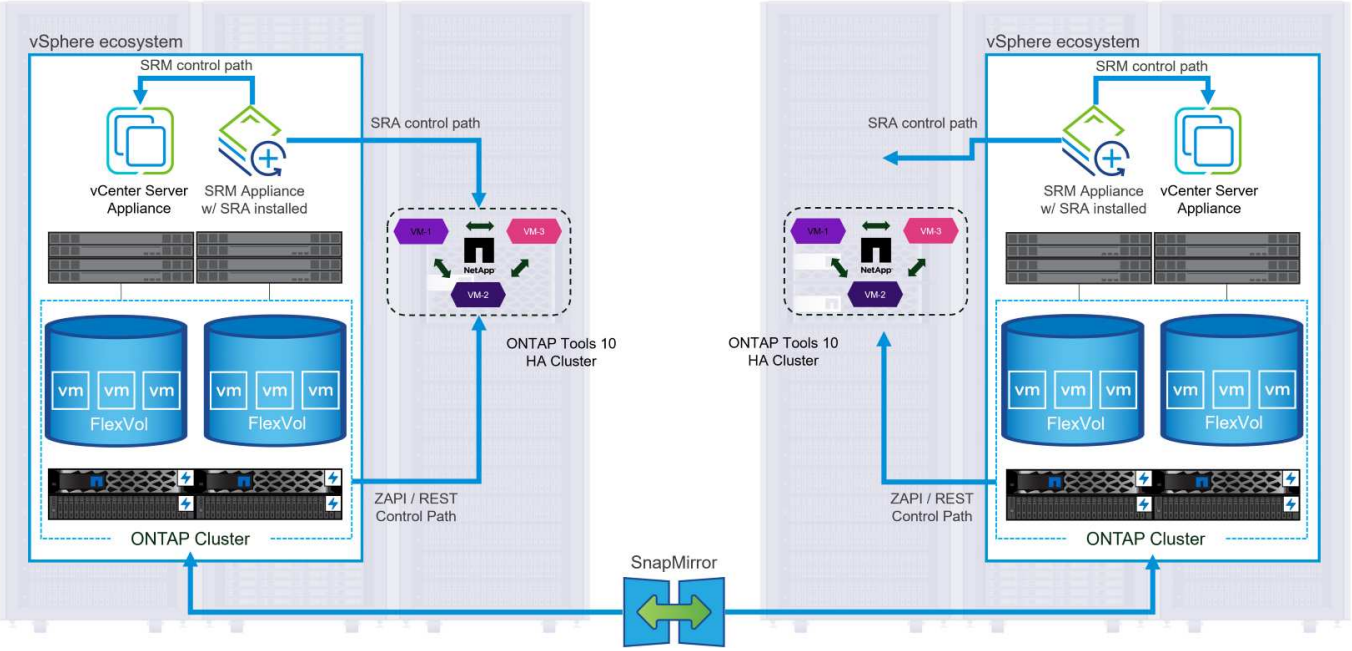
Szenarioübersicht

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 Replication 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 Architekturanforderungen 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 "Netzwerkkonfiguration – 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.

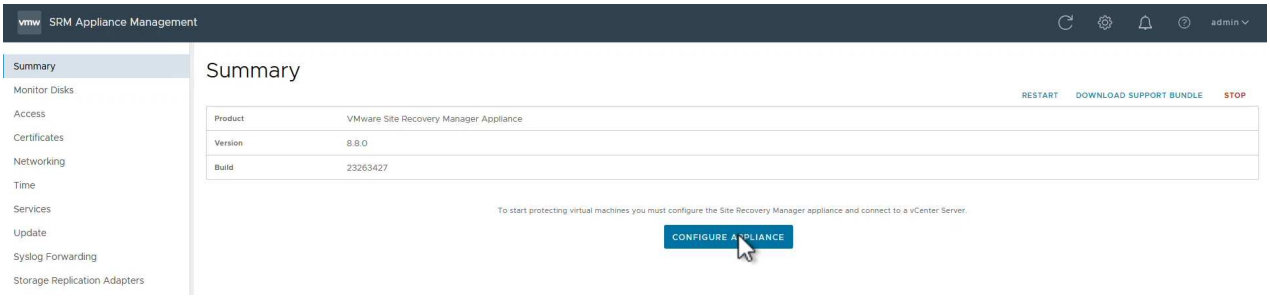
Konfigurieren Sie die SRM-Appliance

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

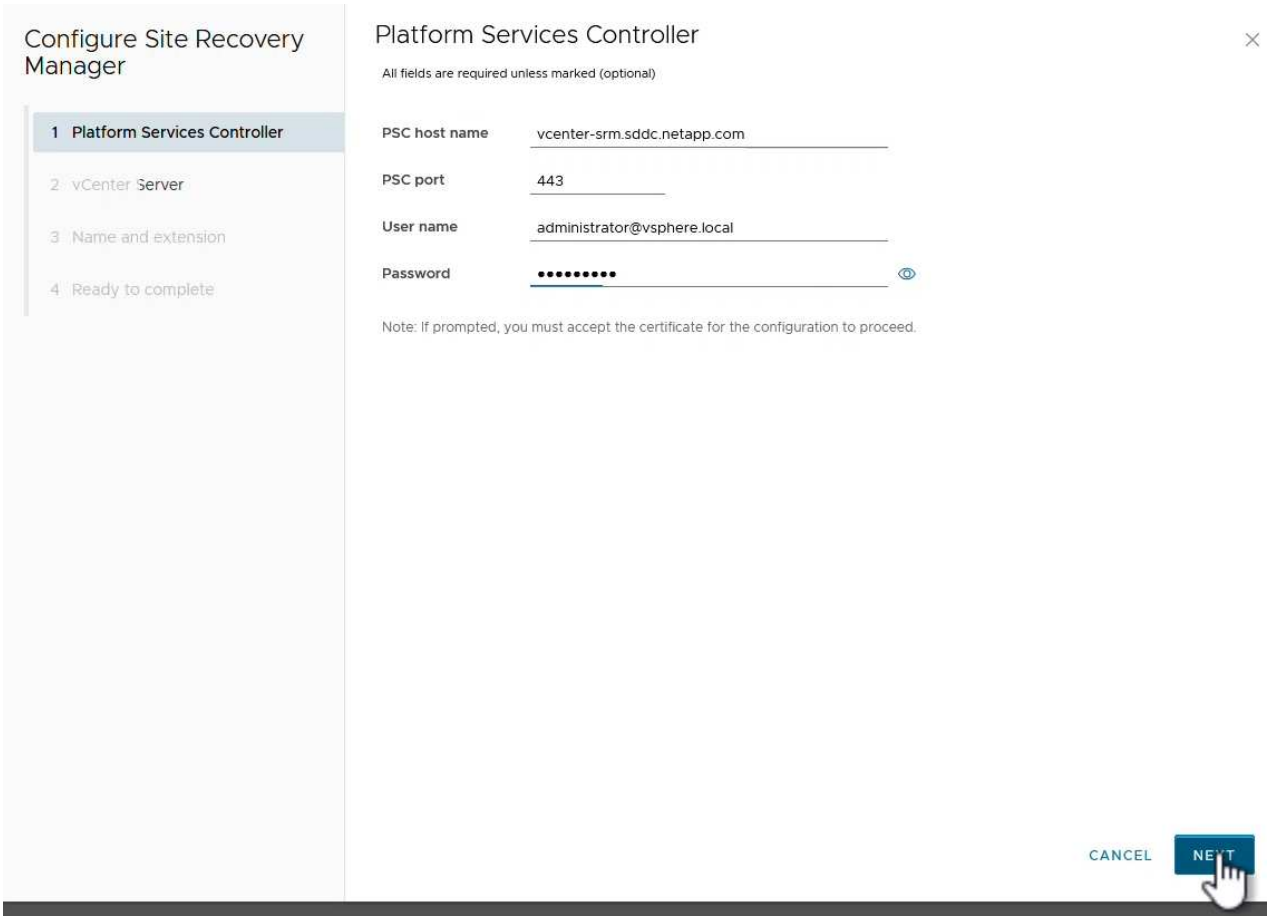
Verbinden Sie die SRM-Appliance für primäre und sekundäre Standorte

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.



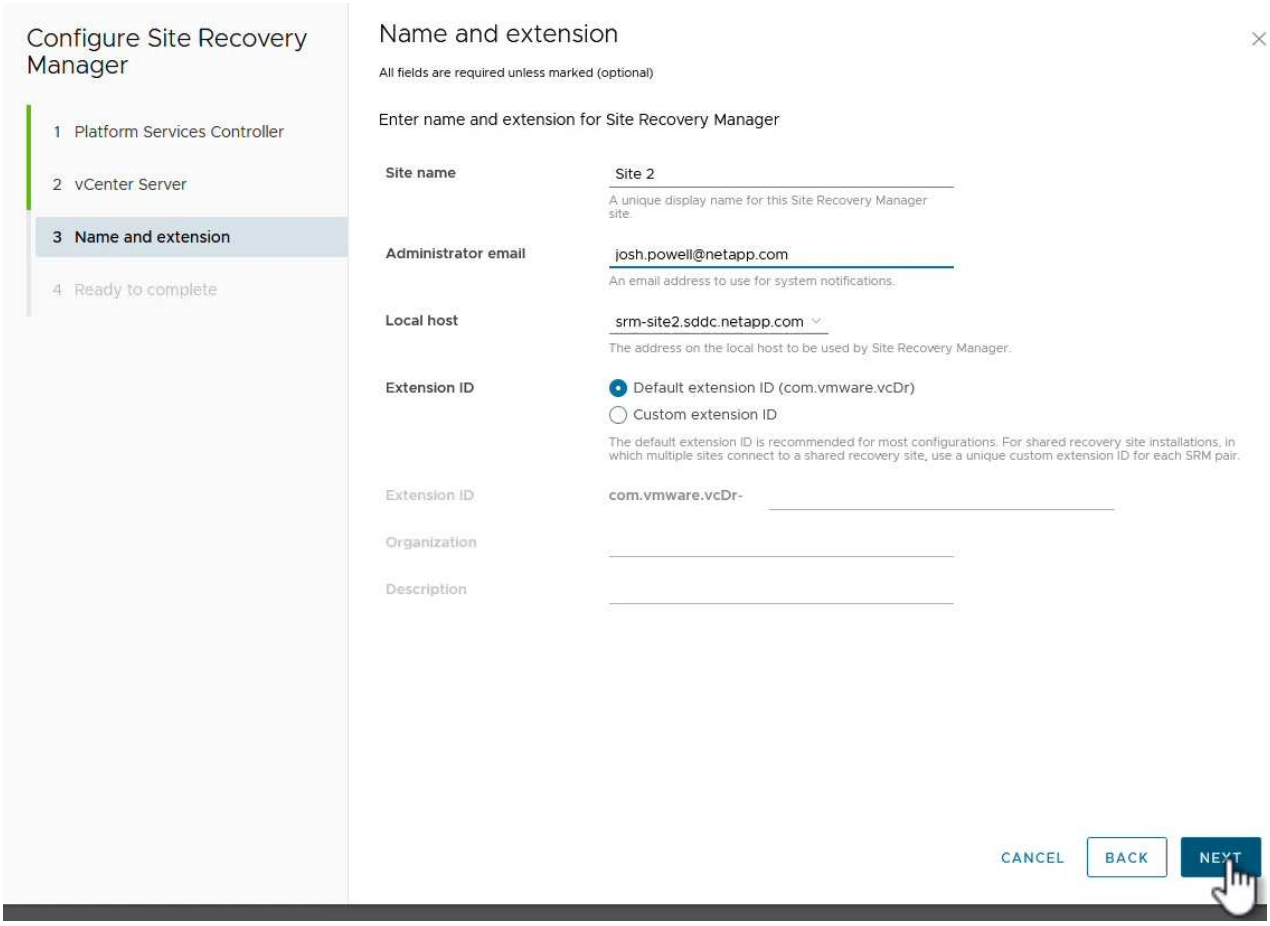
2. Geben Sie auf der Seite **Platform Services Controller** des Assistenten Site Recovery Manager konfigurieren die Anmeldeinformationen des vCenter-Servers ein, für den SRM registriert wird. Klicken Sie auf **Weiter**, um fortzufahren.



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.

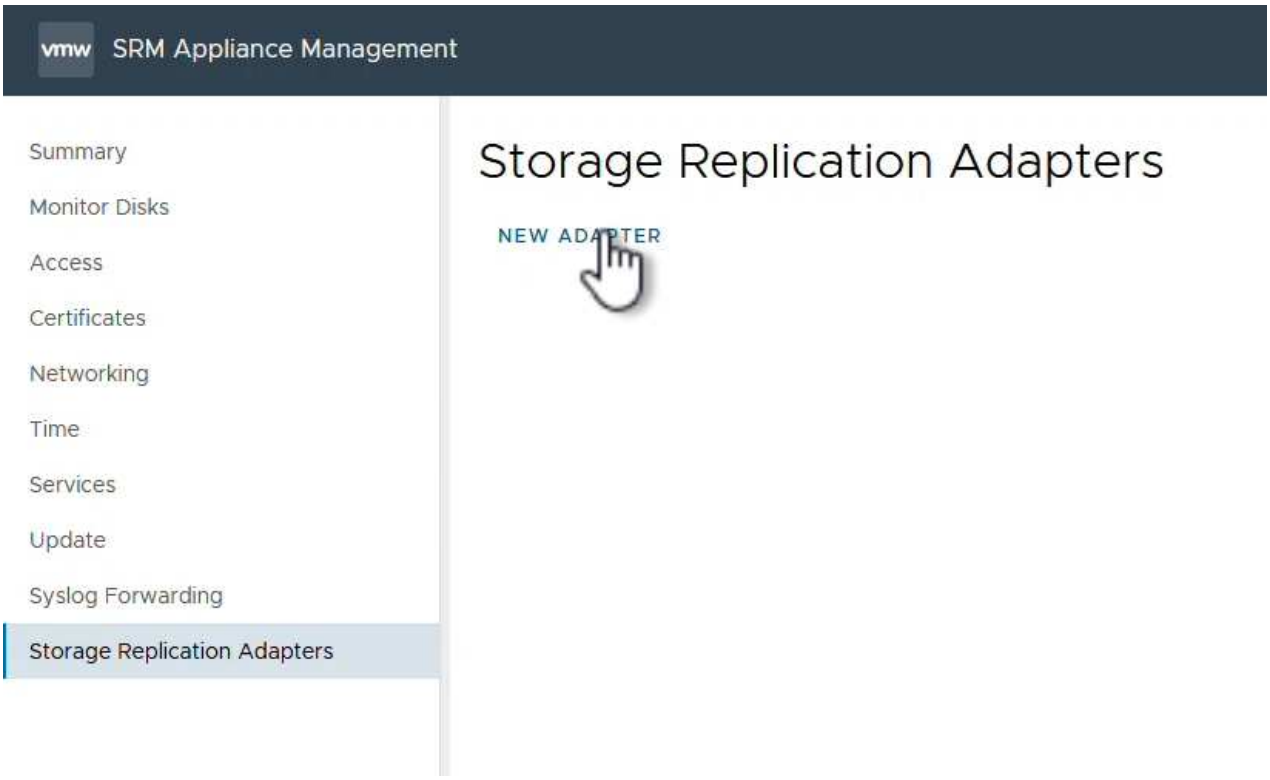


5. Überprüfen Sie auf der Seite **Ready to Complete** die Zusammenfassung der Änderungen

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.

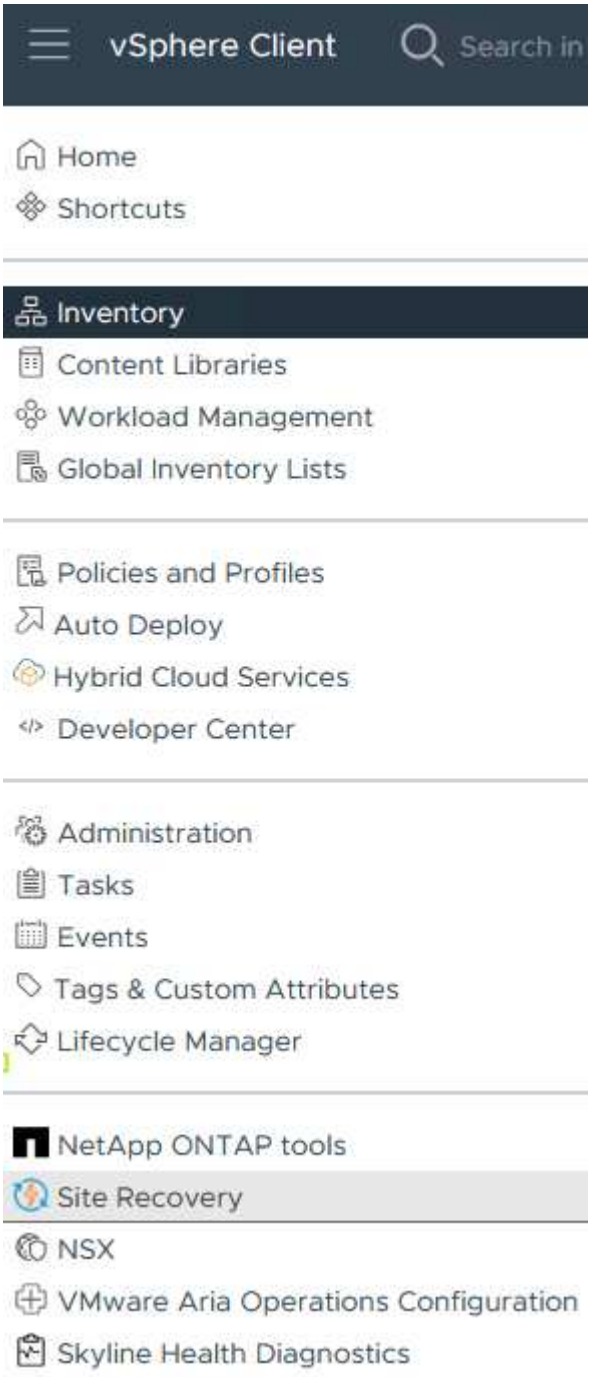
Konfigurieren Sie Site Recovery für SRM

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

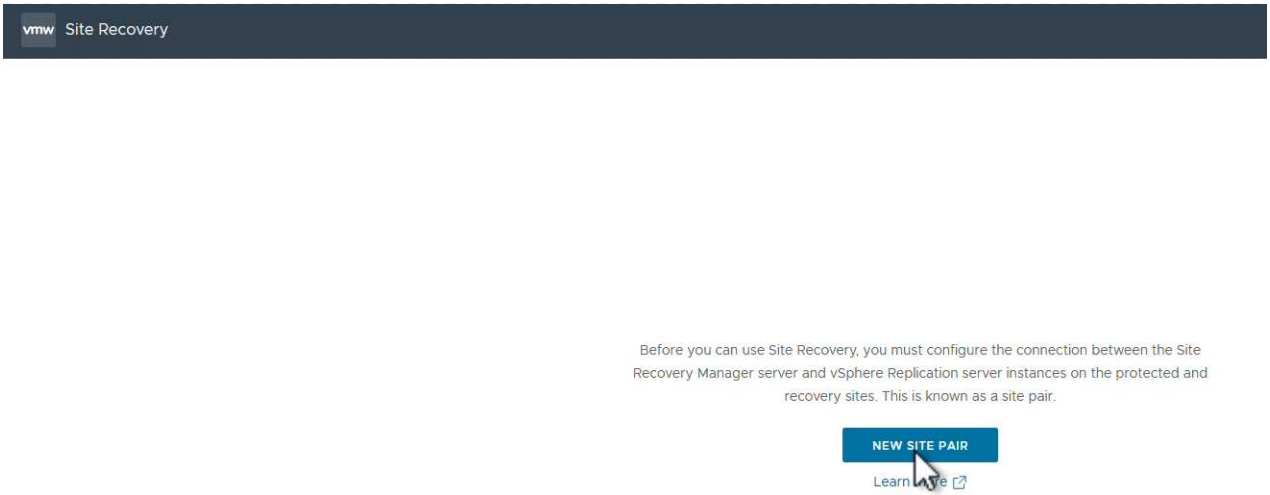
Konfigurieren Sie die Standortanpairing für SRM

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

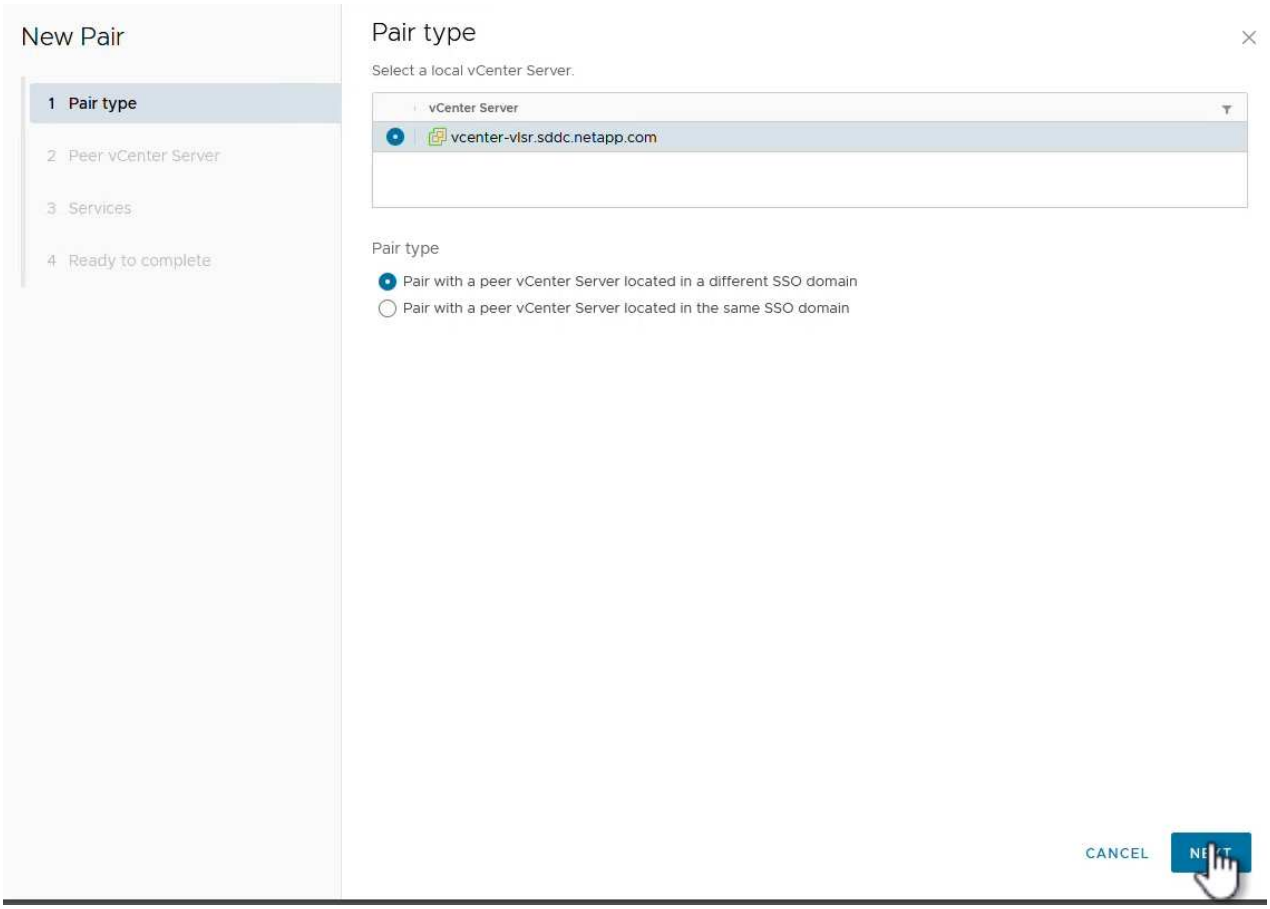
1. Klicken Sie im vSphere-Client im linken Menü auf **Site Recovery**. Ein neues Browserfenster wird für die SRM-Management-UI am primären Standort geöffnet.



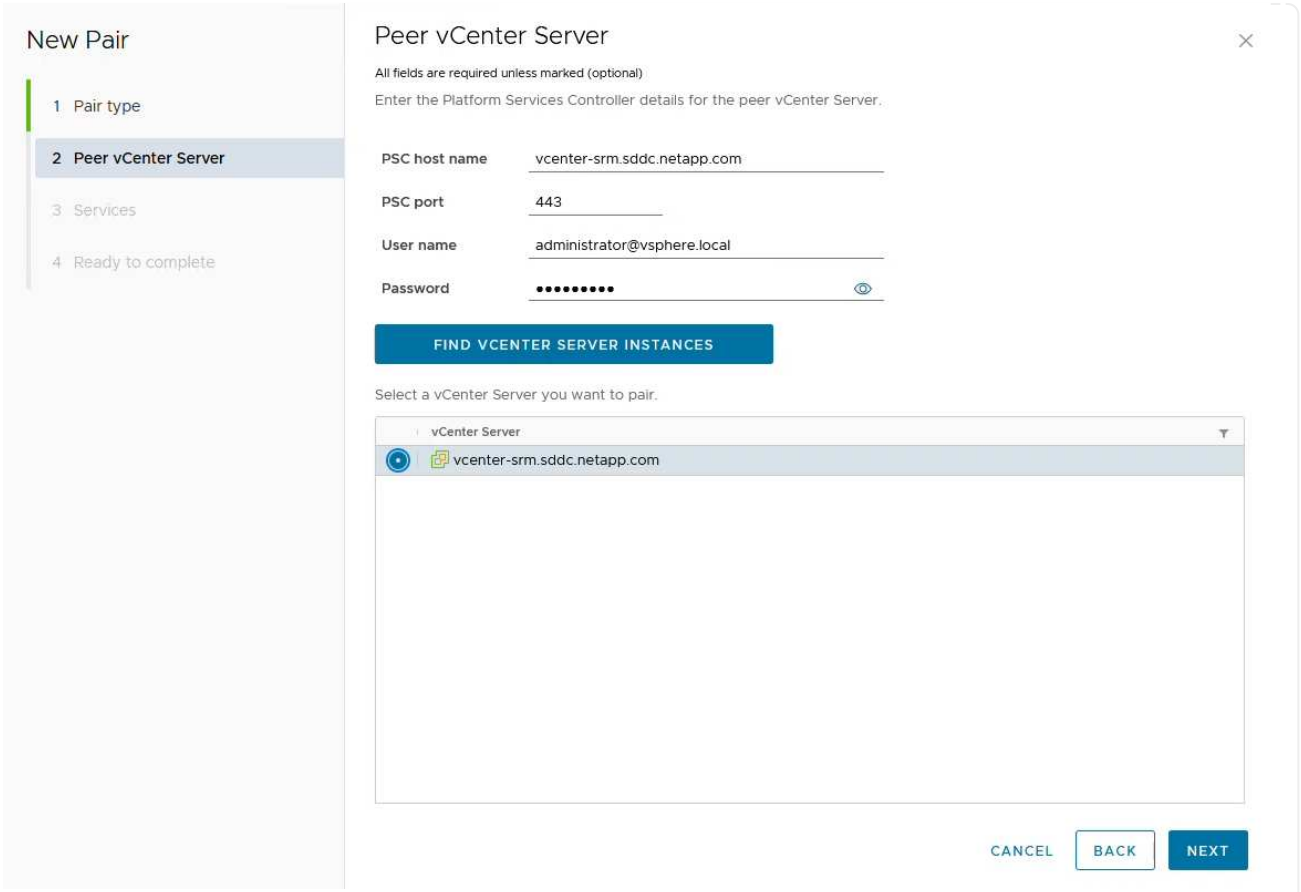
2. Klicken Sie auf der Seite **STANDORTWIEDERHERSTELLUNG** auf **NEUES STANDORTPAAR**.



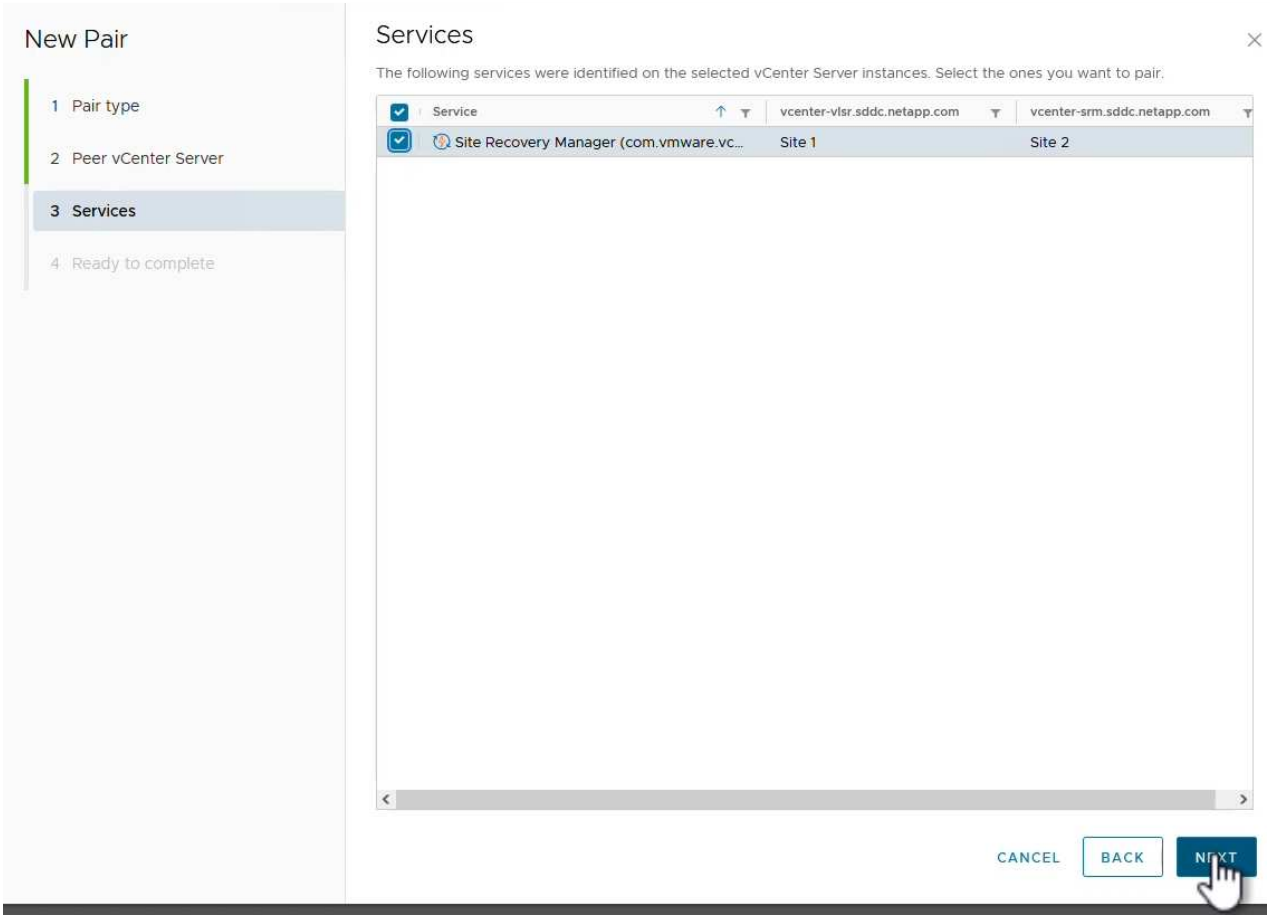
3. Überprüfen Sie auf der Seite **Pair type** des **New Pair Wizard**, ob der lokale vCenter Server ausgewählt ist, und wählen Sie den **Pair Typ** aus. Klicken Sie auf **Weiter**, um fortzufahren.



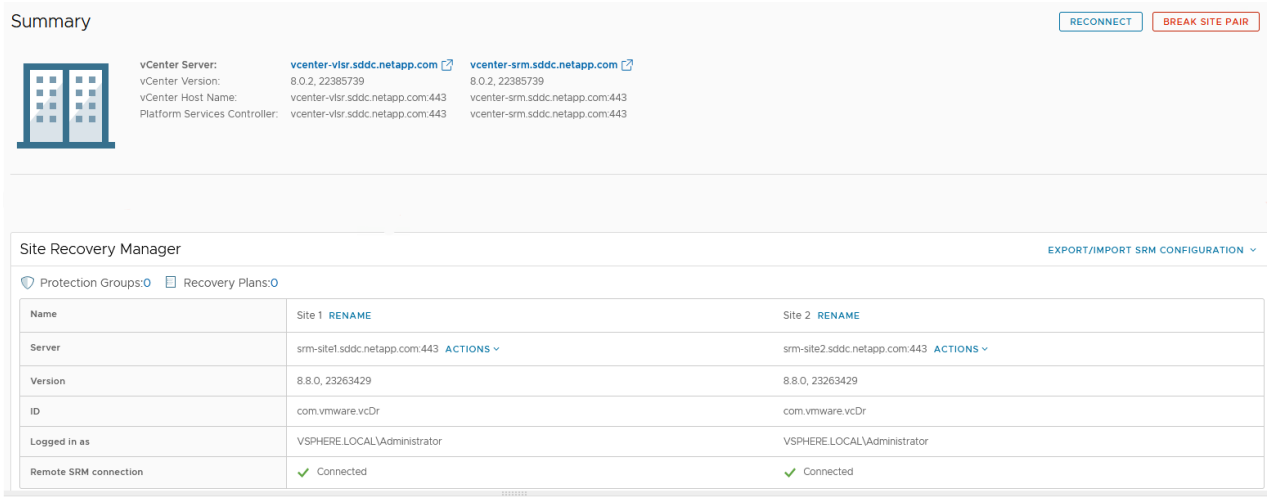
4. Geben Sie auf der Seite **Peer vCenter** die Zugangsdaten des vCenter am sekundären Standort ein und klicken Sie auf **Find vCenter Instances**. Überprüfen Sie, ob die vCenter-Instanz erkannt wurde, und klicken Sie auf **Weiter**, um fortzufahren.



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



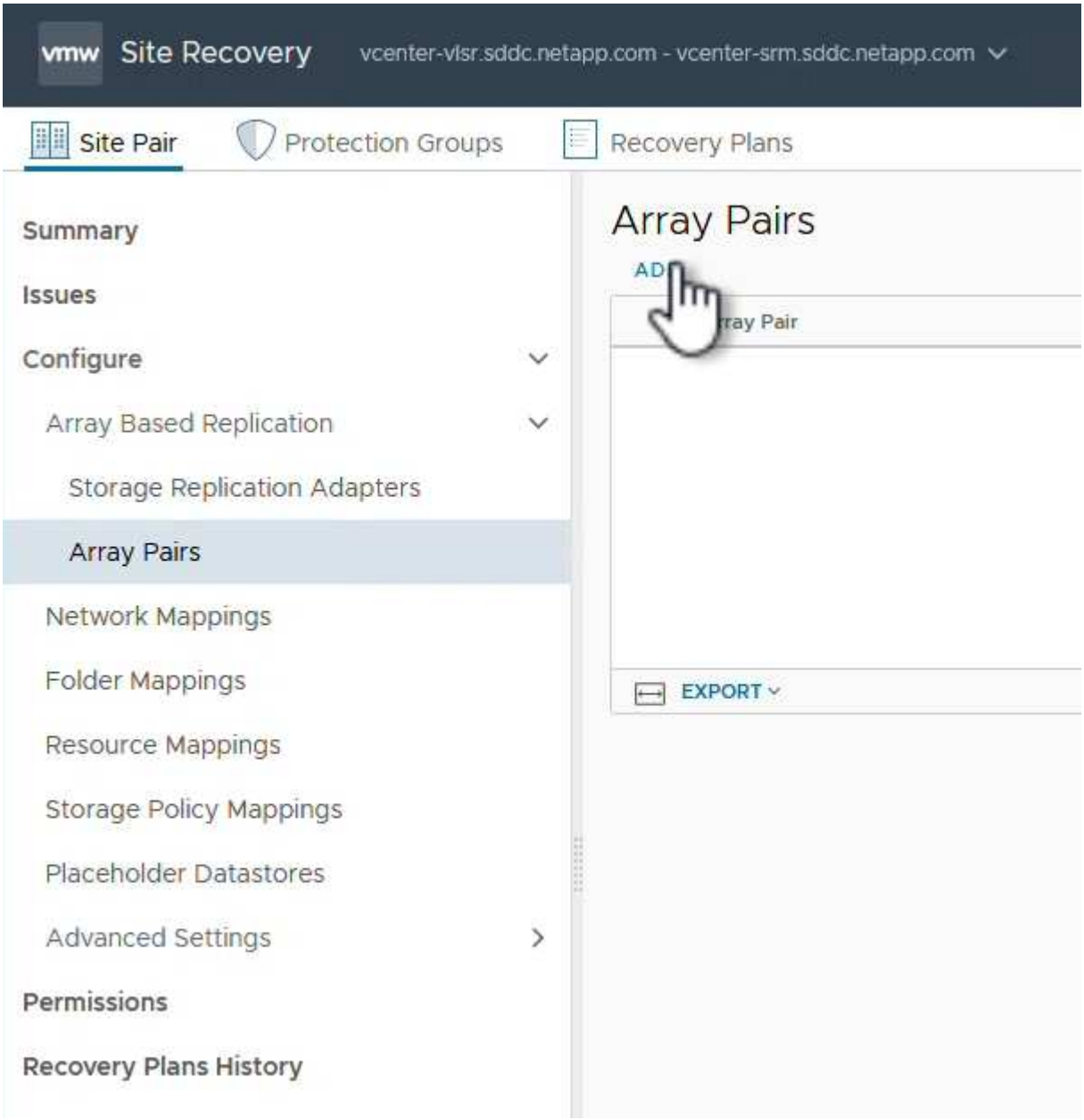
6. Überprüfen Sie auf der Seite **Ready to Complete** die vorgeschlagene Konfiguration und klicken Sie dann auf die Schaltfläche **Finish**, um die Standortanordnung zu erstellen
7. Das neue Standortpaar und seine Zusammenfassung können auf der Übersichtsseite angezeigt werden.



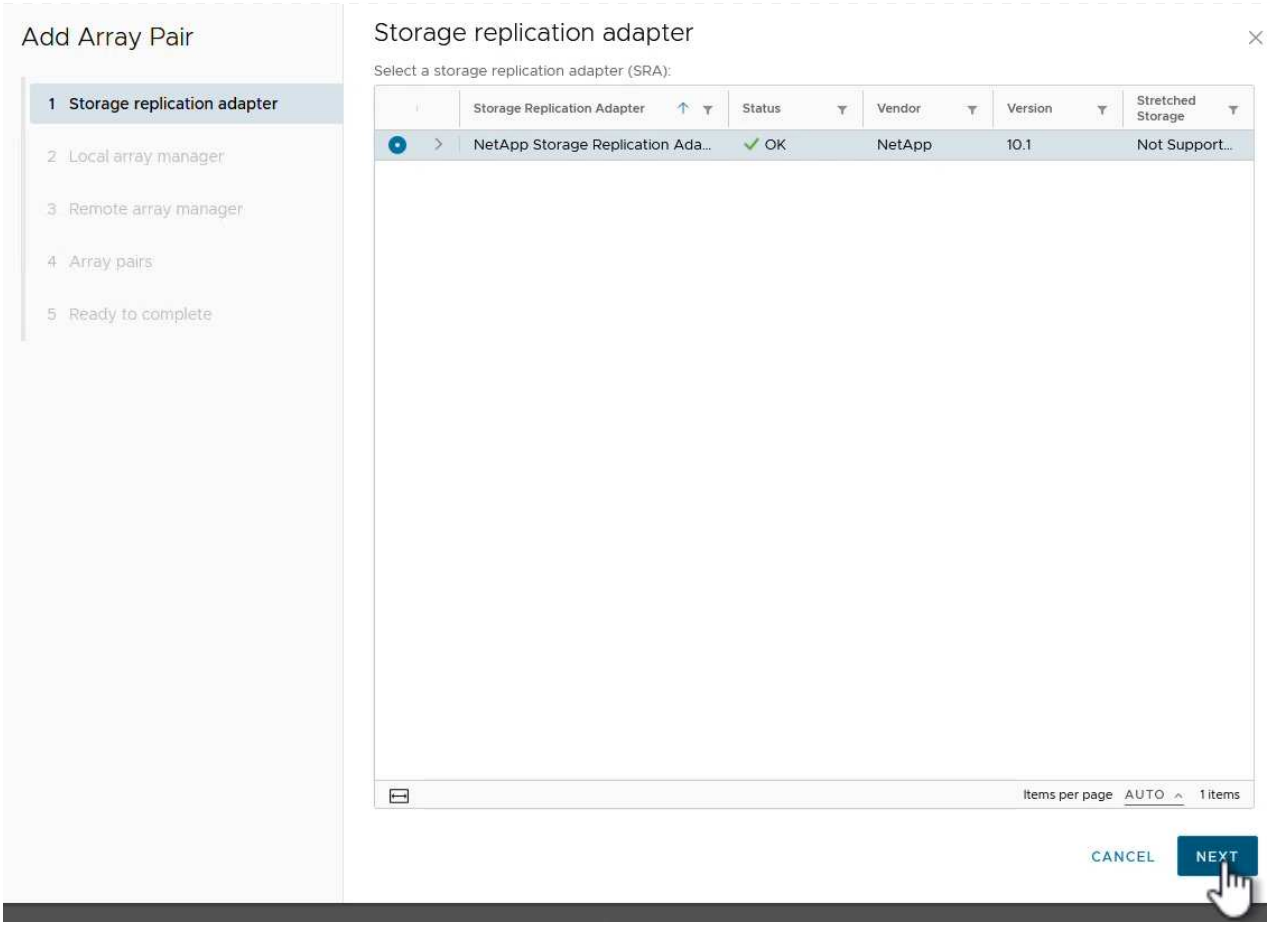
Fügen Sie ein Array-Paar für SRM hinzu

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

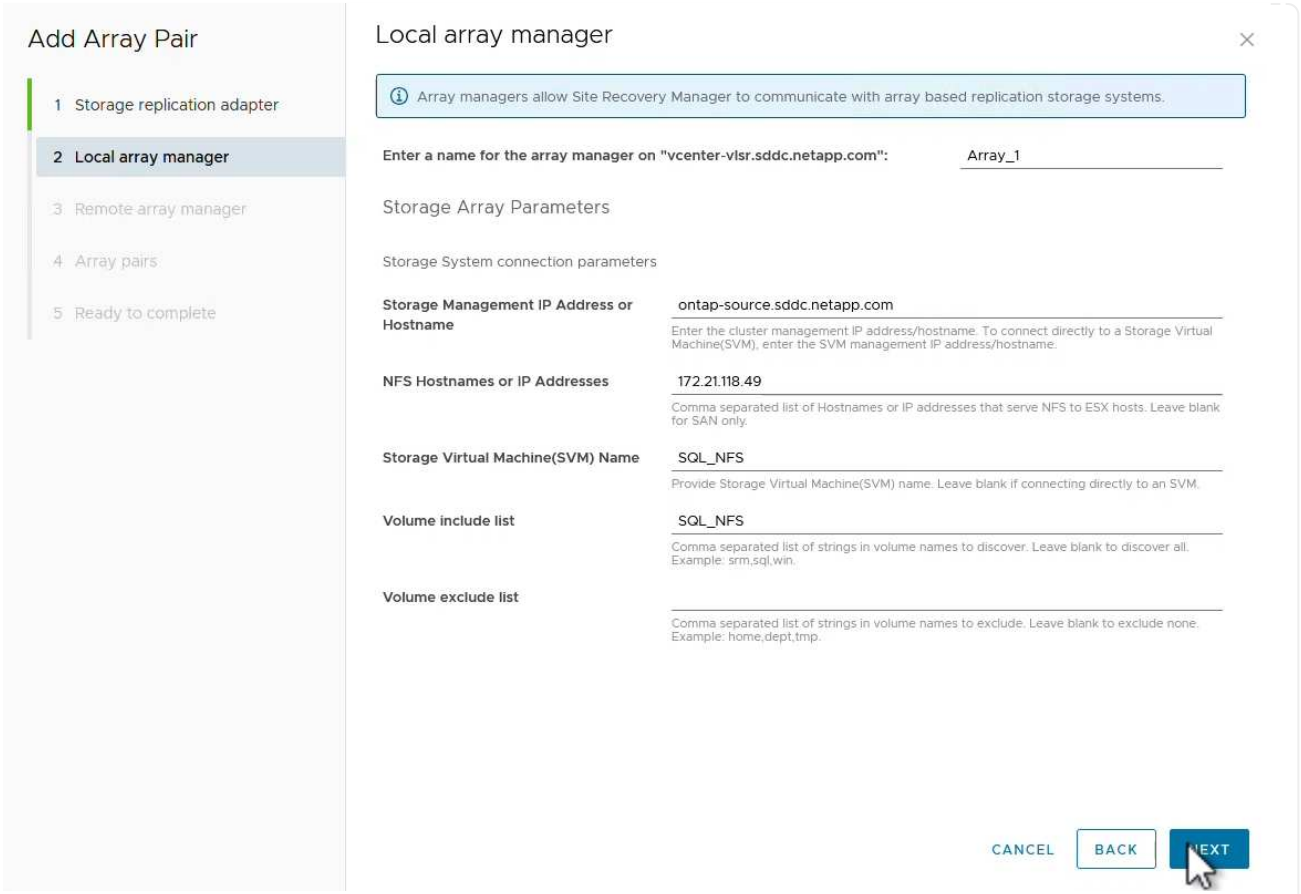
1. Navigieren Sie in der Benutzeroberfläche für die Standortwiederherstellung im linken Menü zu **Konfigurieren > Array-basierte Replikation > Array Pairs**. Klicken Sie auf **ADD**, um zu beginnen.



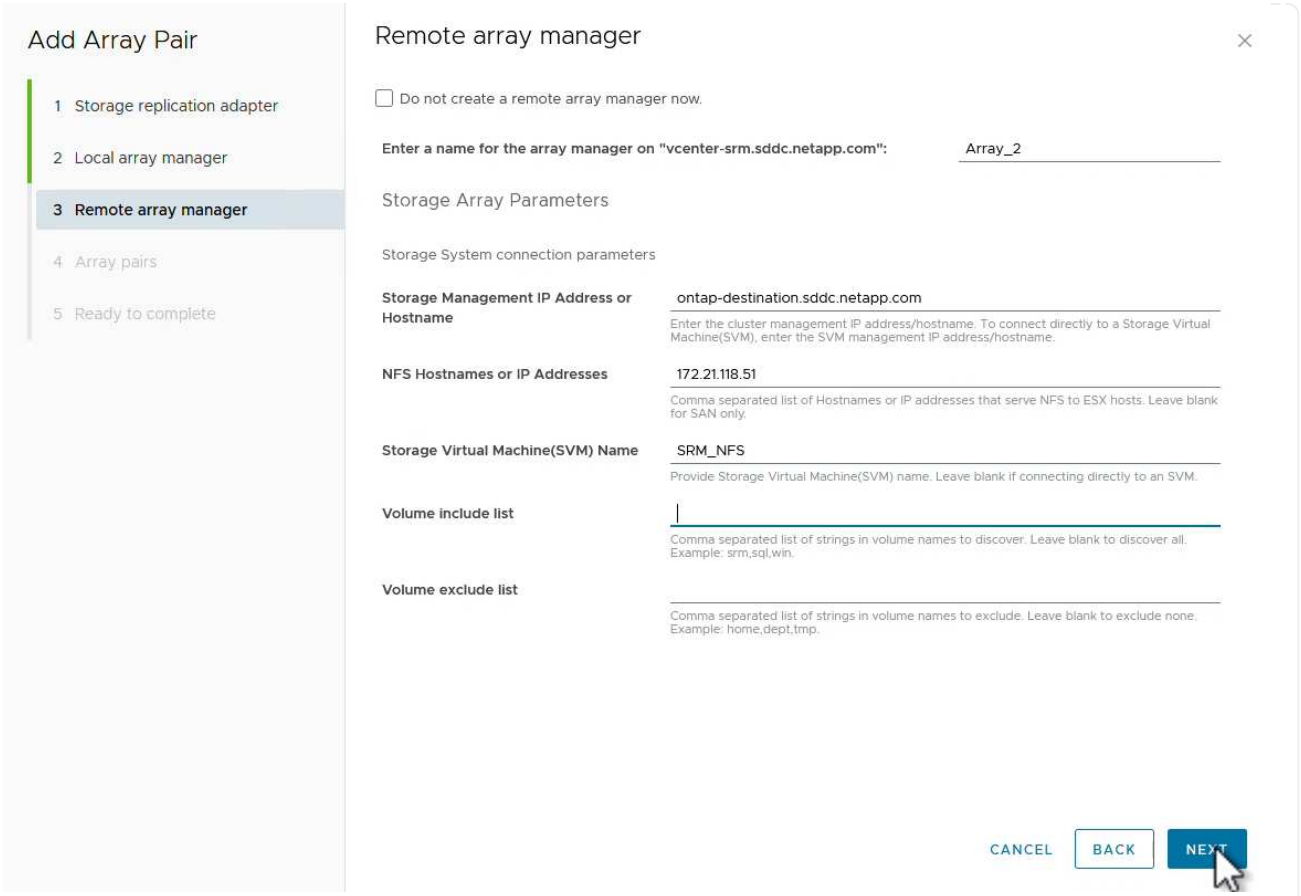
2. Überprüfen Sie auf der Seite **Speicherreplikationsadapter** des Assistenten **Array Pair hinzufügen**, ob der SRA-Adapter für den primären Standort vorhanden ist, und klicken Sie auf **Weiter**, um fortzufahren.



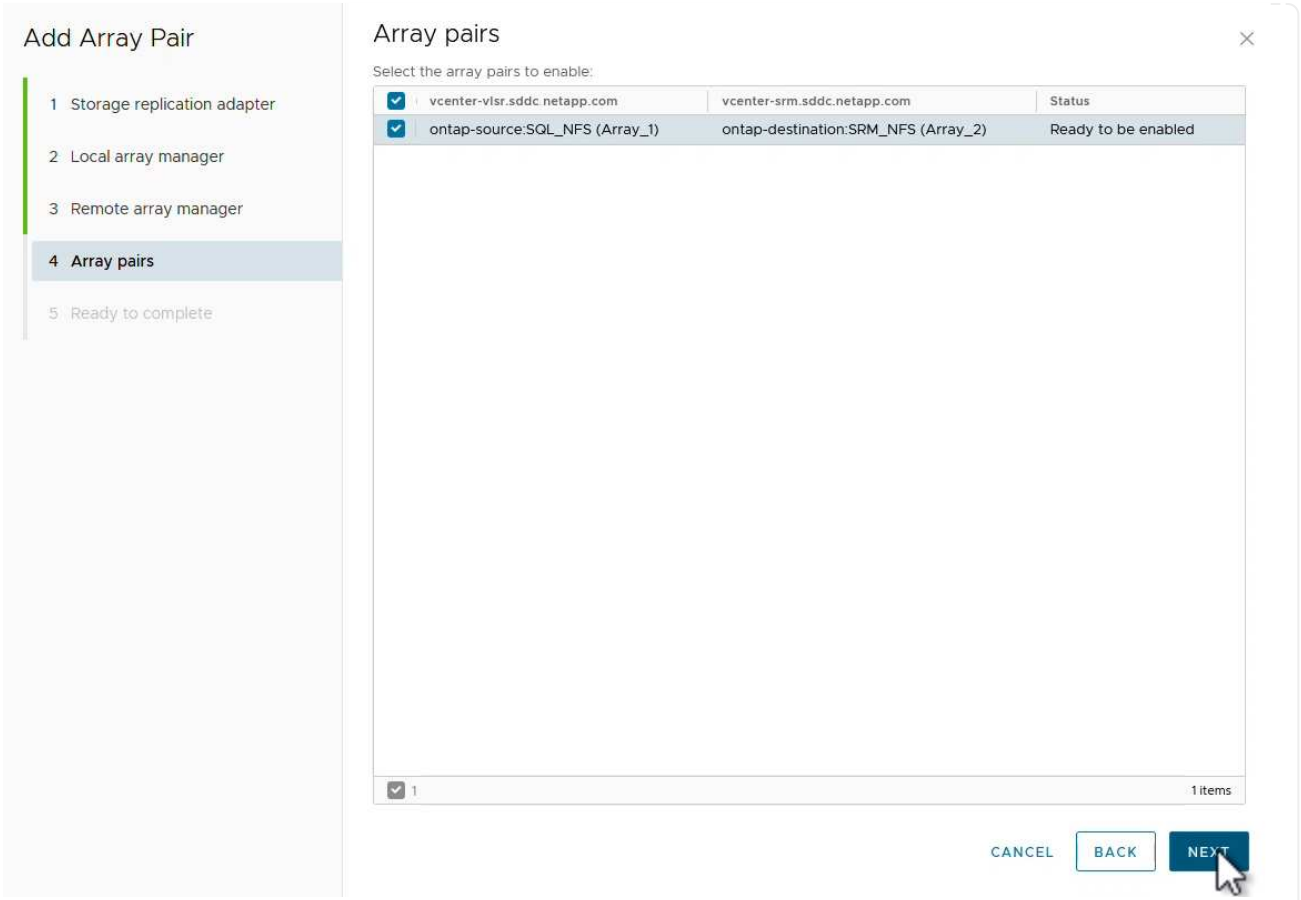
3. Geben Sie auf der Seite **Local Array Manager** einen Namen für das Array am primären Standort, den FQDN des Speichersystems, die SVM-IP-Adressen, die NFS bereitstellen, und optional die Namen bestimmter Volumes ein, die ermittelt werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.



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



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

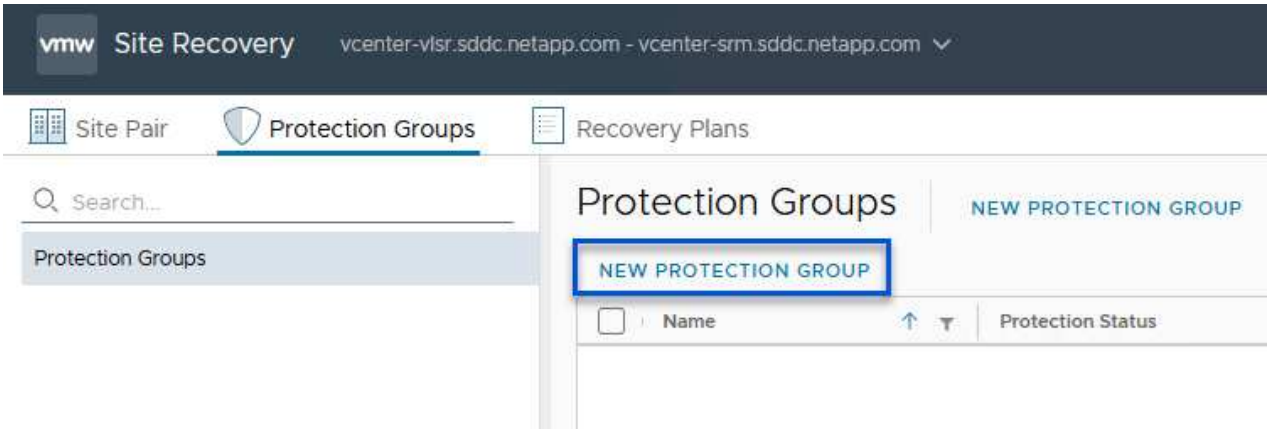


6. Überprüfen Sie die Informationen auf der Seite **Ready to Complete** und klicken Sie auf **Finish**, um das Array-Paar zu erstellen.

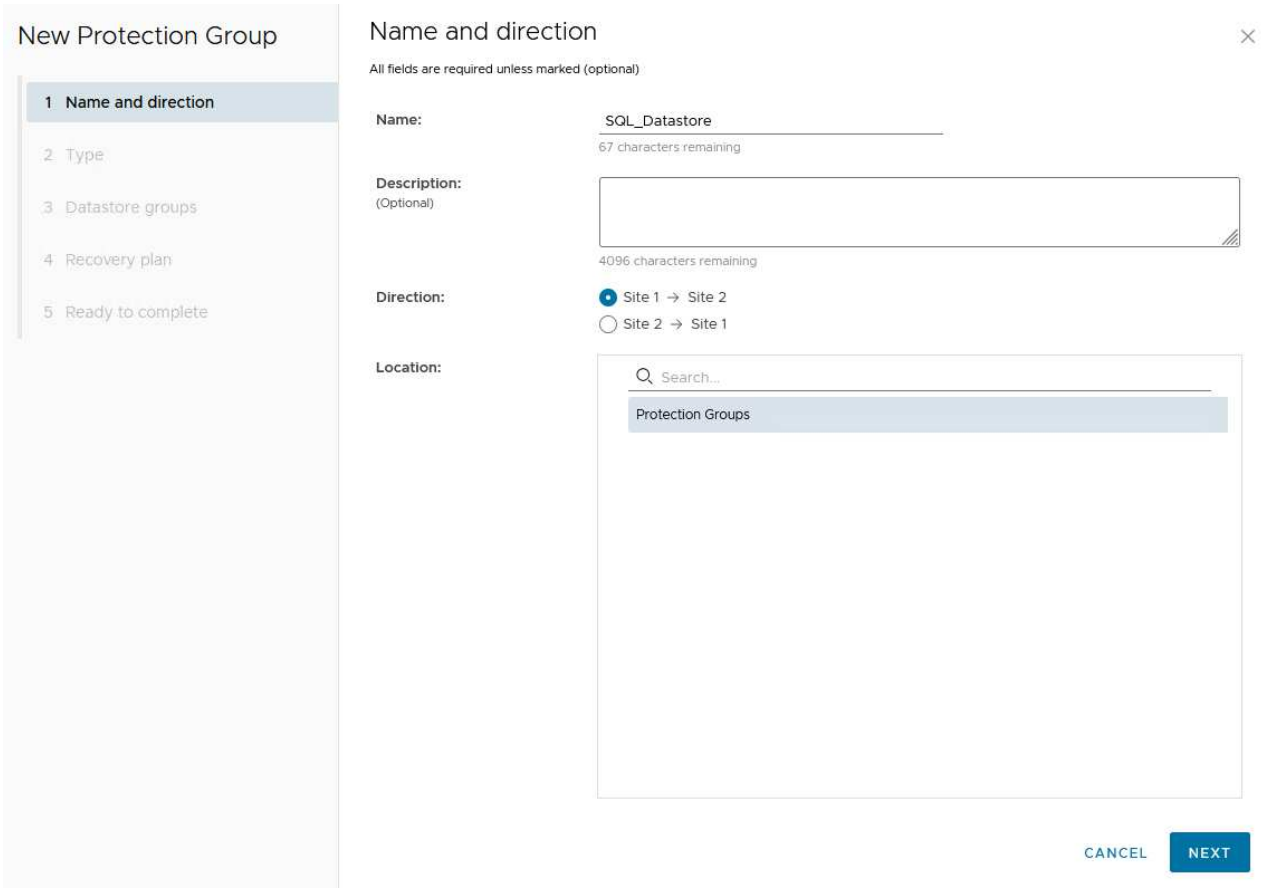
Konfigurieren Sie Schutzgruppen für SRM

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

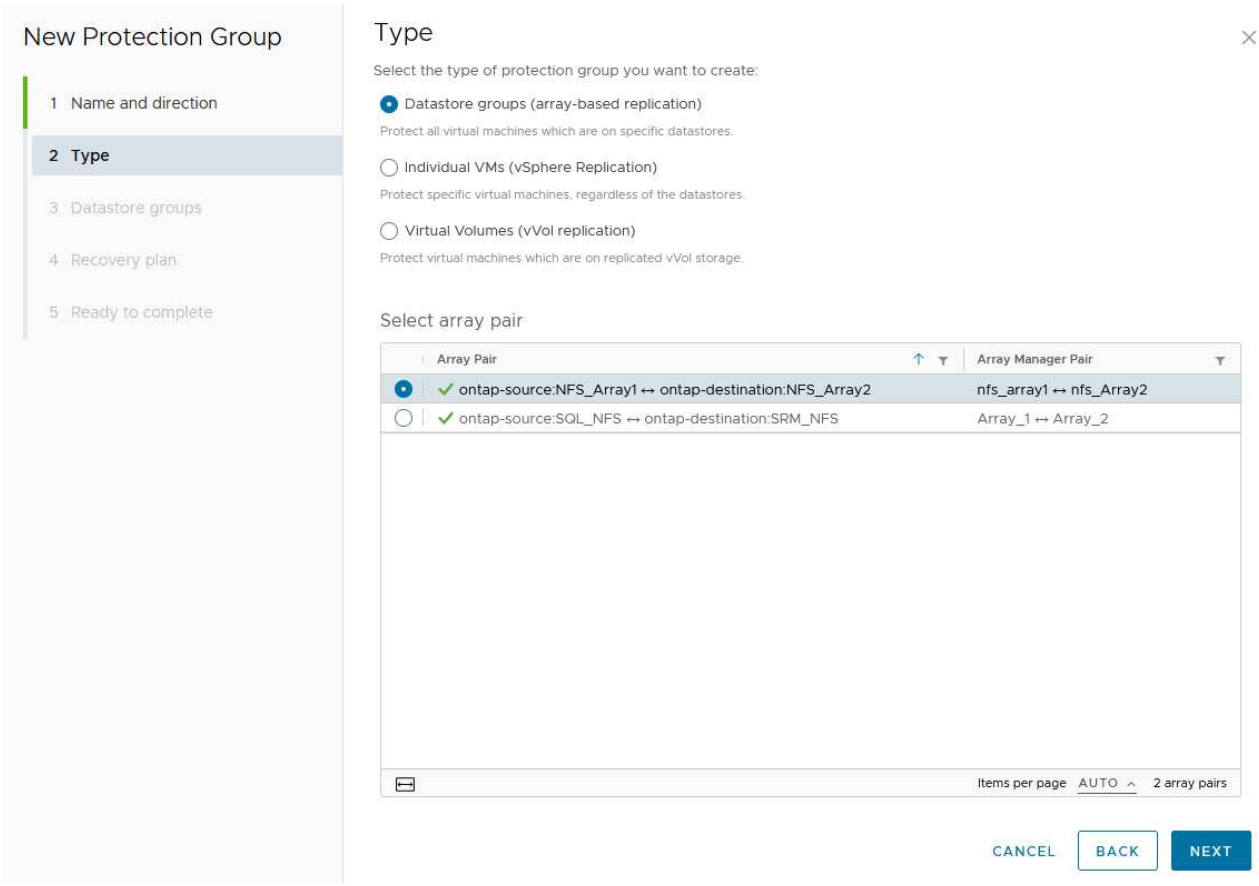
1. Klicken Sie in der Site Recovery Oberfläche auf die Registerkarte **Schutzgruppen** und dann auf **Neue Schutzgruppe**, um zu beginnen.



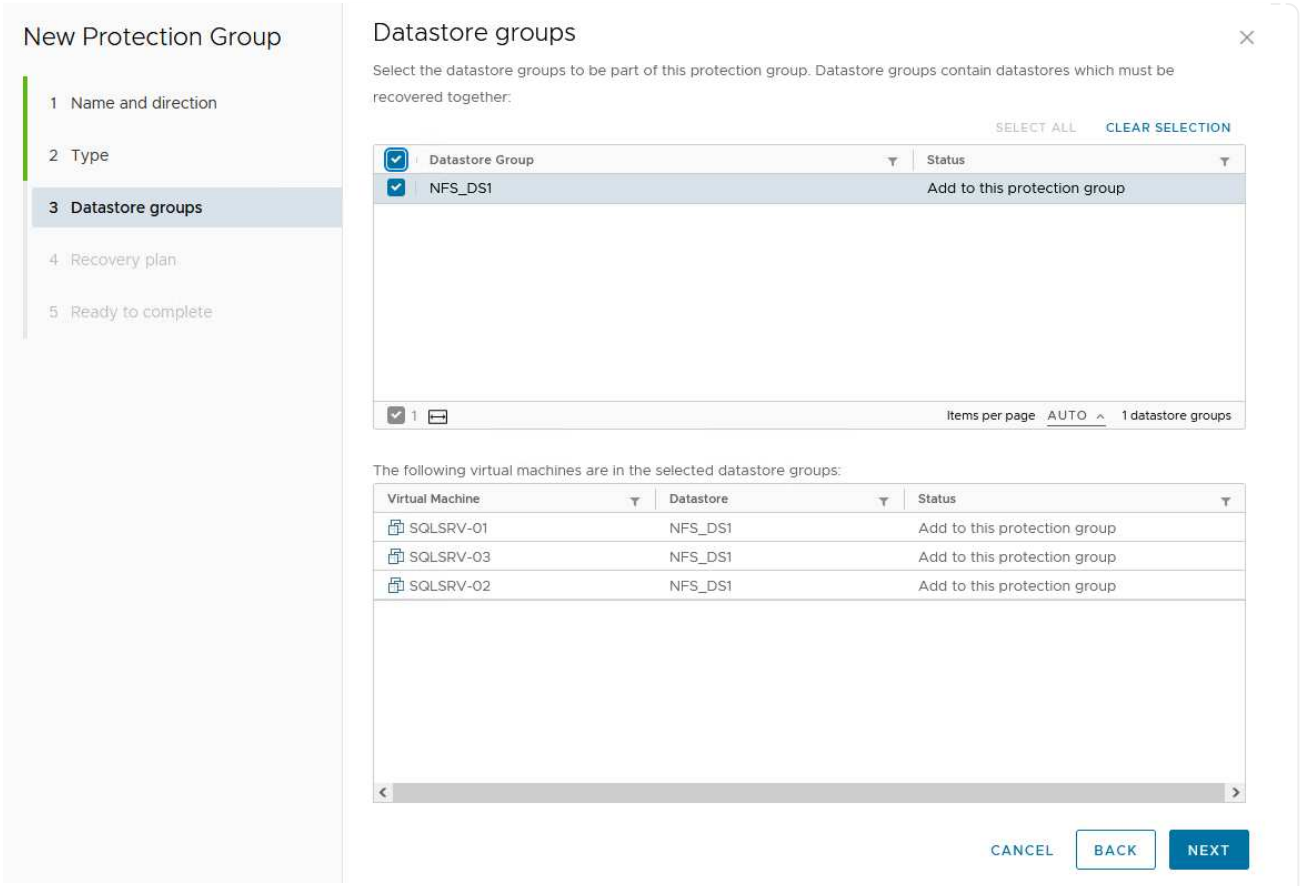
2. Geben Sie auf der Seite **Name und Richtung** des **New Protection Group**-Assistenten einen Namen für die Gruppe ein und wählen Sie die Standortrichtung zum Schutz der Daten aus.



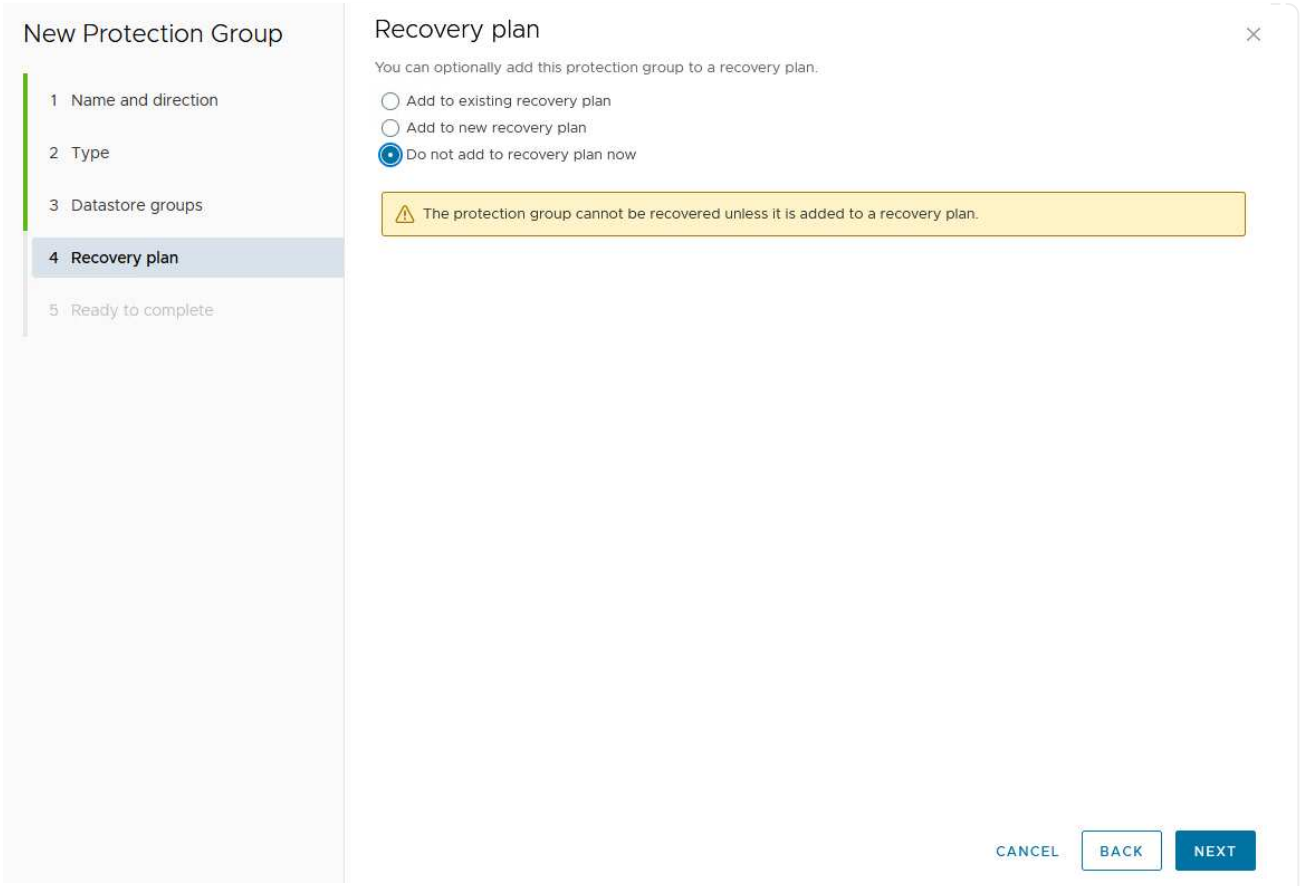
3. Wählen Sie auf der Seite **Typ** den Typ der Schutzgruppe (Datastore, VM oder vVol) aus und wählen Sie das Array-Paar aus. Klicken Sie auf **Weiter**, um fortzufahren.



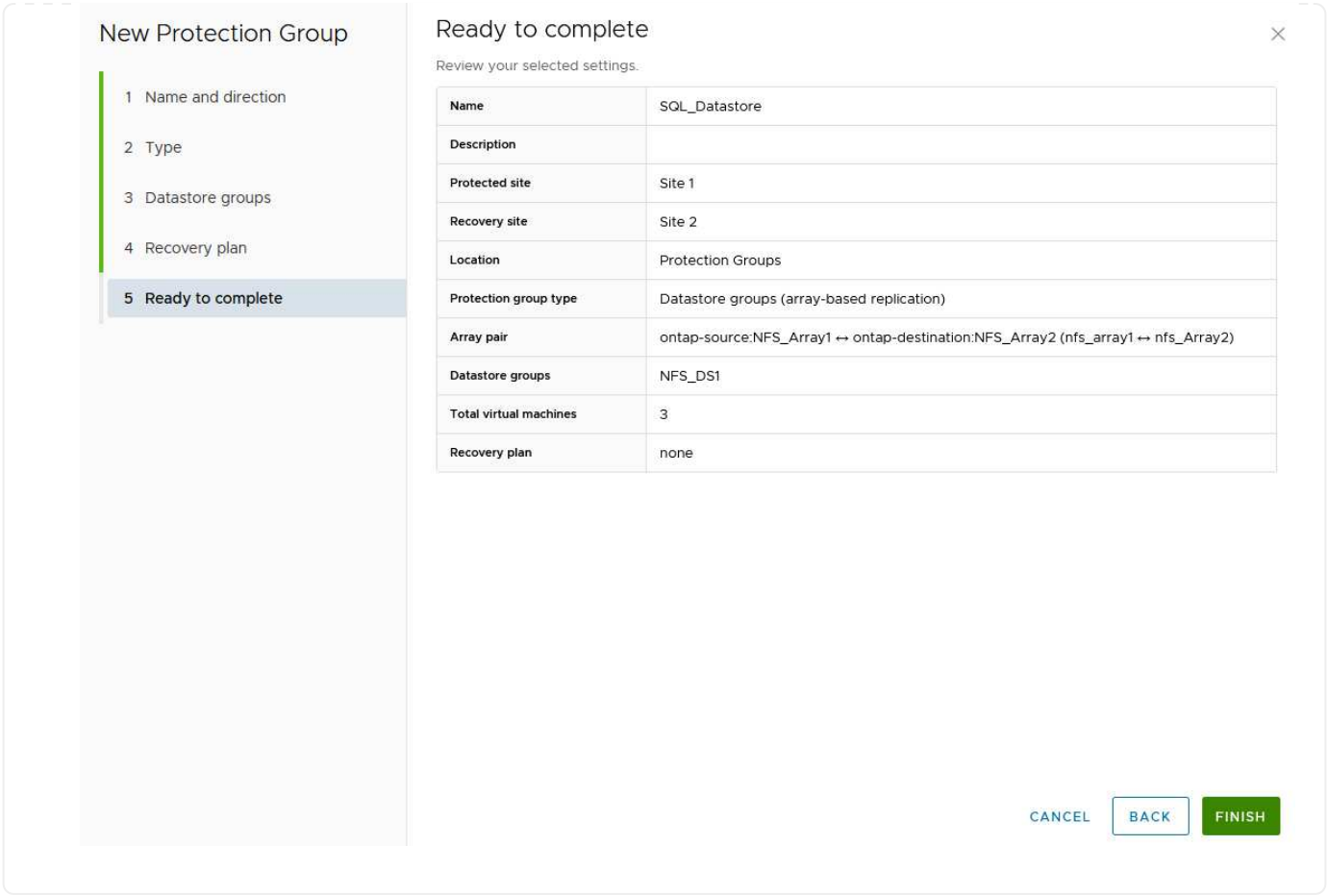
4. Wählen Sie auf der Seite **Datastore groups** die Datastores aus, die in die Schutzgruppe aufgenommen werden sollen. VMs, die sich derzeit auf dem Datenspeicher befinden, werden für jeden ausgewählten Datenspeicher angezeigt. Klicken Sie auf **Weiter**, um fortzufahren.



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.



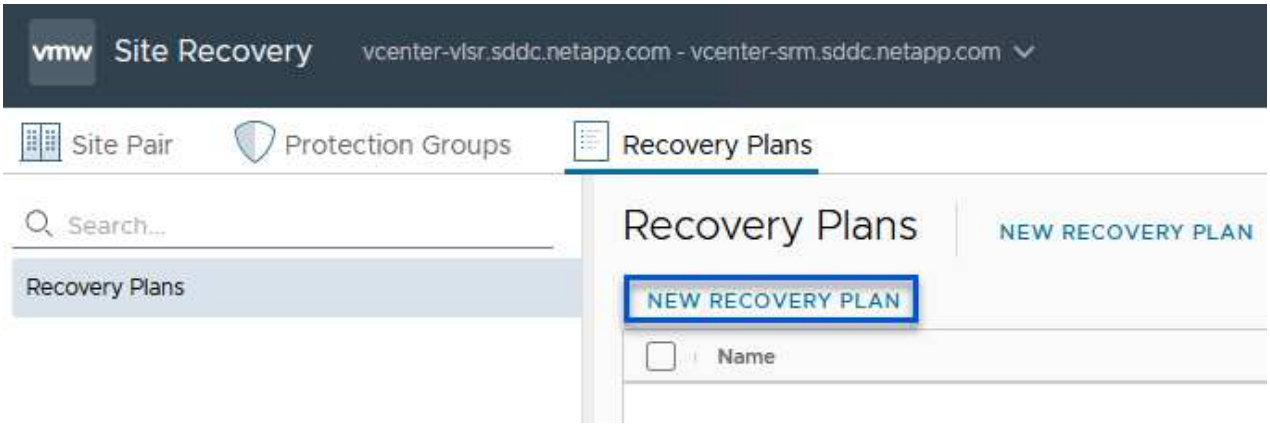
6. Überprüfen Sie auf der Seite **Ready to Complete** die neuen Parameter der Schutzgruppe und klicken Sie auf **Finish**, um die Gruppe zu erstellen.


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

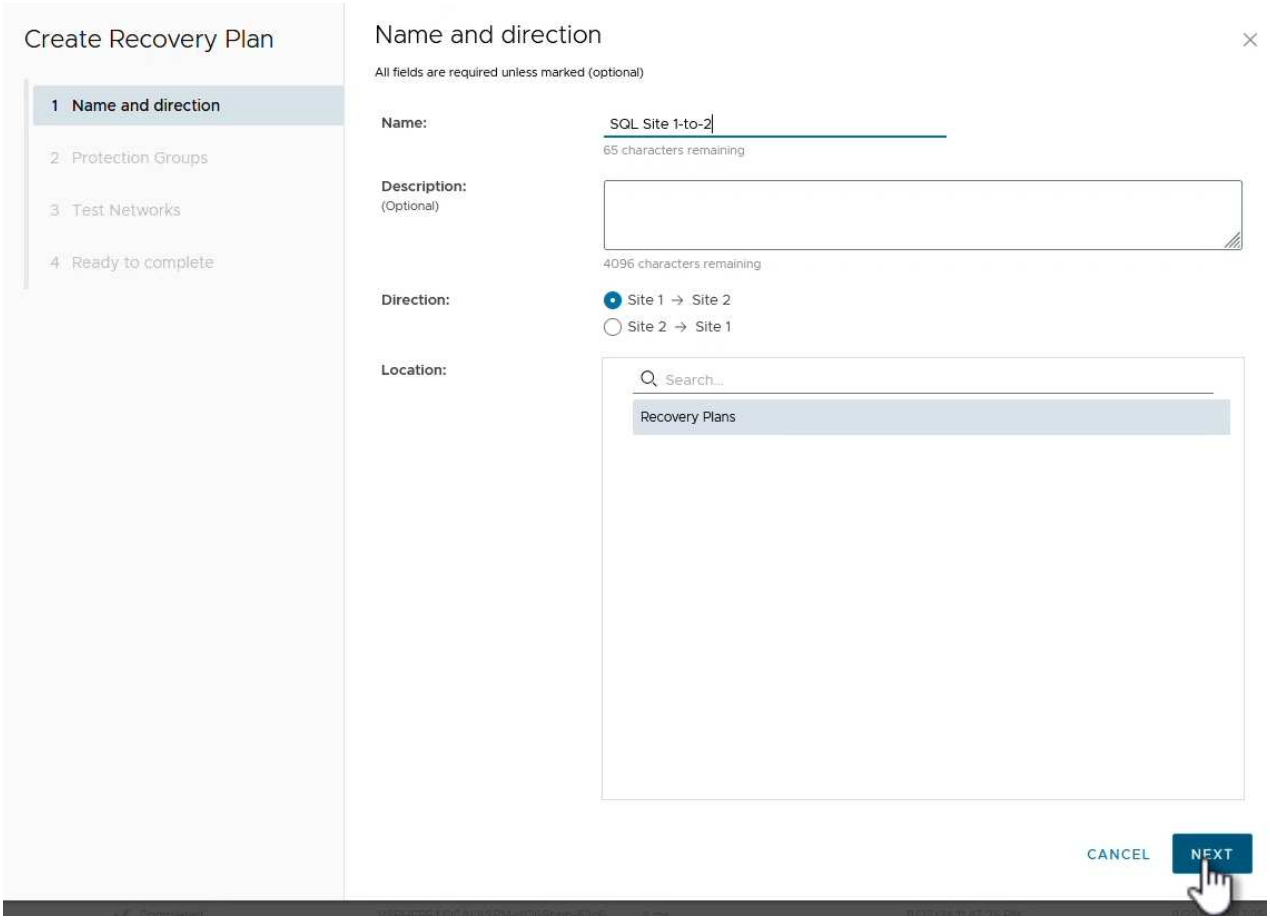
Konfiguration des Recovery-Plans für SRM

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

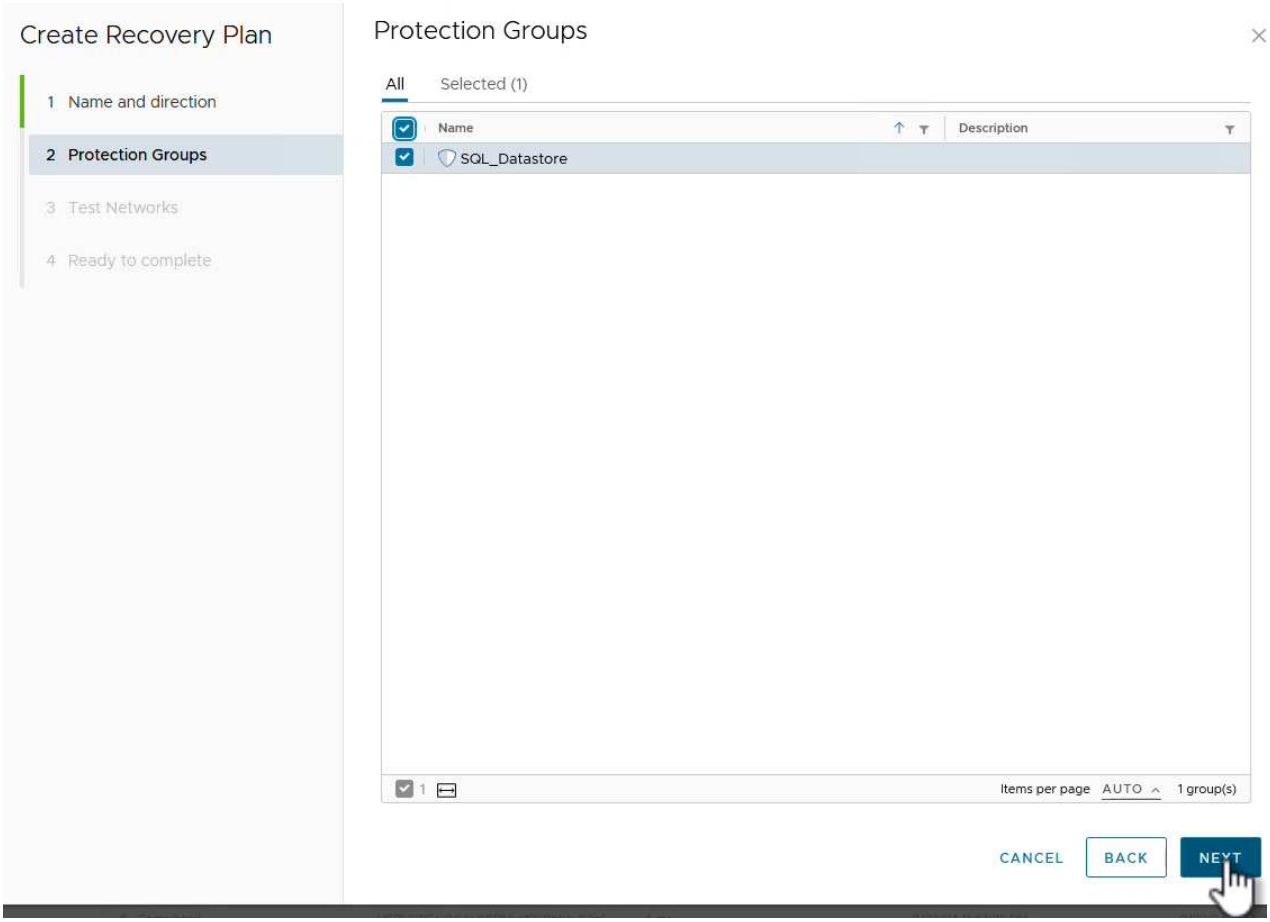
1. Klicken Sie in der Benutzeroberfläche der Standortwiederherstellung auf die Registerkarte **Wiederherstellungsplan** und dann auf **Neuer Wiederherstellungsplan**, um zu beginnen.



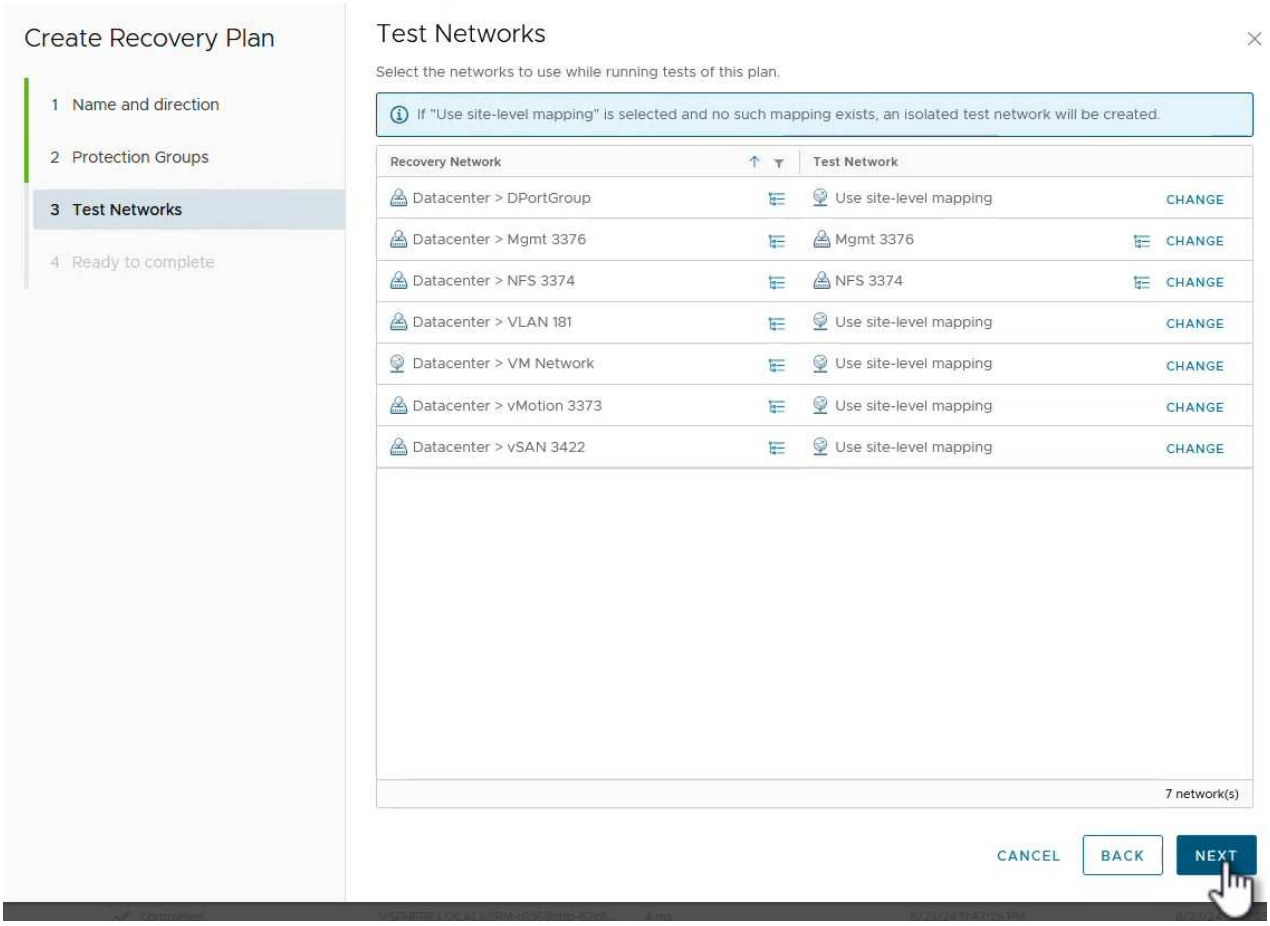
2. Geben Sie auf der Seite **Name und Richtung** des Assistenten **Wiederherstellungsplan erstellen** einen Namen für den Wiederherstellungsplan ein und wählen Sie die Richtung zwischen Quell- und Zielstandort aus. Klicken Sie auf **Weiter**, um fortzufahren.



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.



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.



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

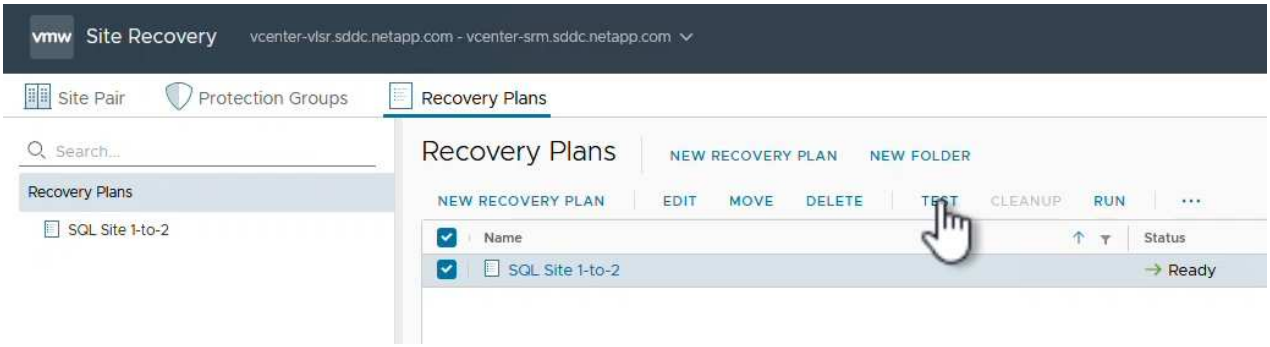
In diesem Abschnitt werden verschiedene Funktionen der Verwendung von Disaster Recovery mit SRM behandelt, darunter das Testen von Failover, das Durchführen von Failovers, das Durchführen von Datensicherung und Failback.

```
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.
```

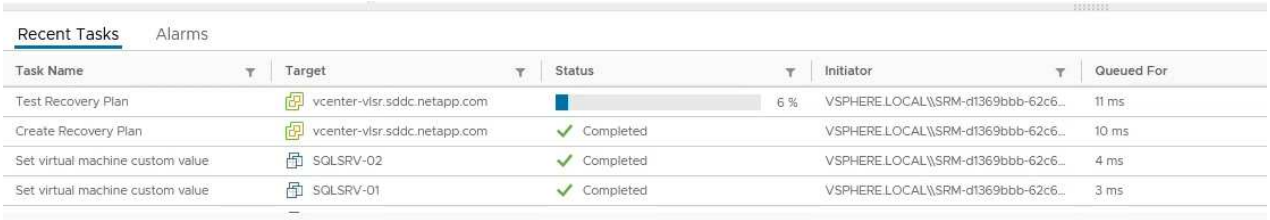
Testen des Failover mit SRM

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

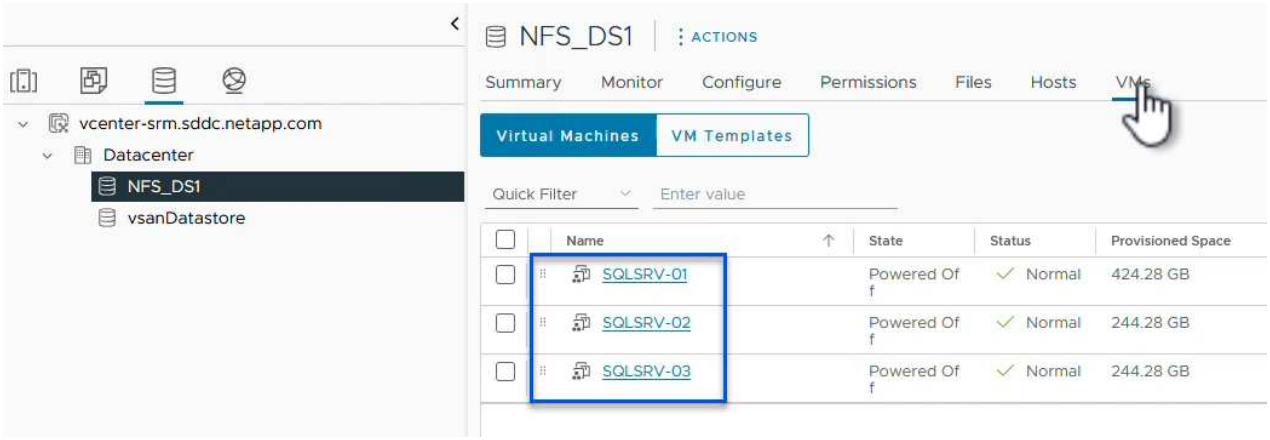
1. Klicken Sie in der Benutzeroberfläche für die Standortwiederherstellung auf die Registerkarte **Wiederherstellungsplan** und wählen Sie dann einen Wiederherstellungsplan aus. Klicken Sie auf die Schaltfläche **Test**, um den Failover zum sekundären Standort zu testen.



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

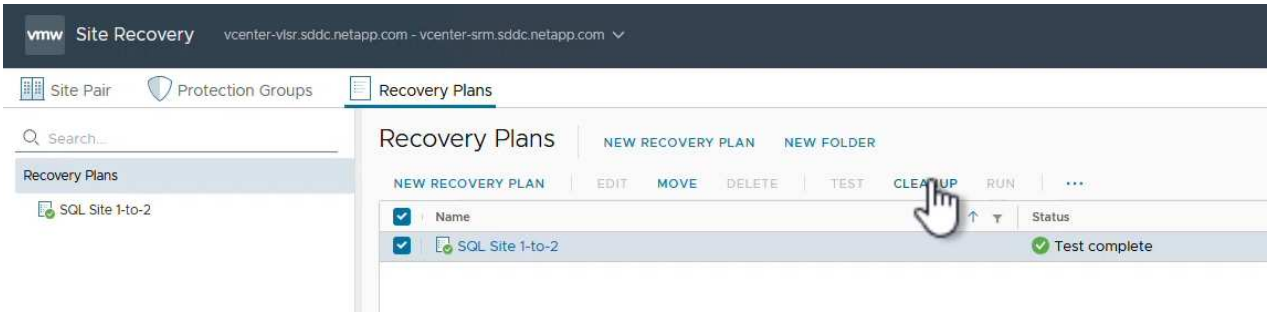


3. SRM sendet Befehle über den SRA an das sekundäre ONTAP Storage-System. Eine FlexClone des letzten Snapshots wird auf dem sekundären vSphere-Cluster erstellt und gemountet. Der neu gemountete Datastore kann im Storage Inventory angezeigt werden.



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

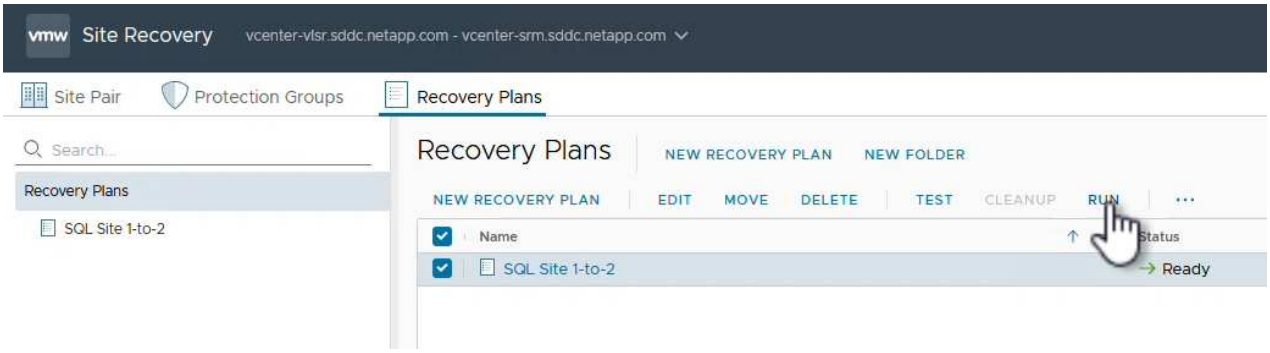
zur ursprünglichen Umgebung zurückzukehren.



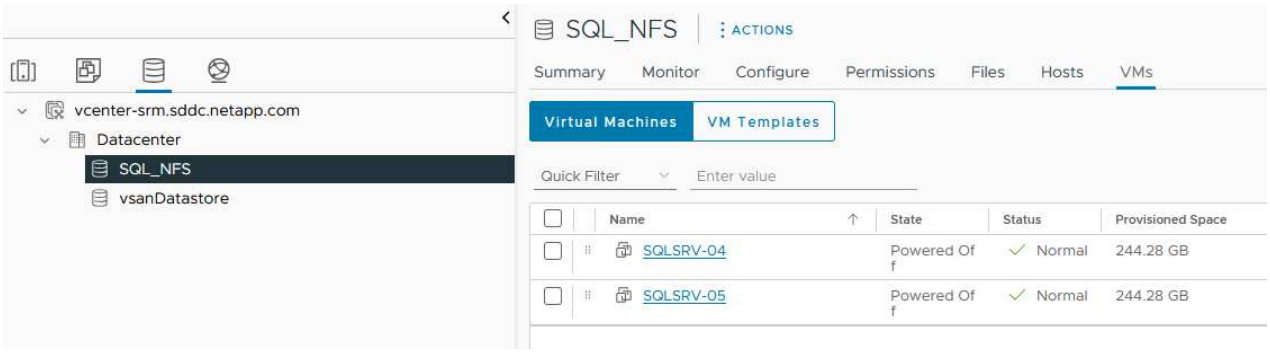
Ausführen des Recovery-Plans mit SRM

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"

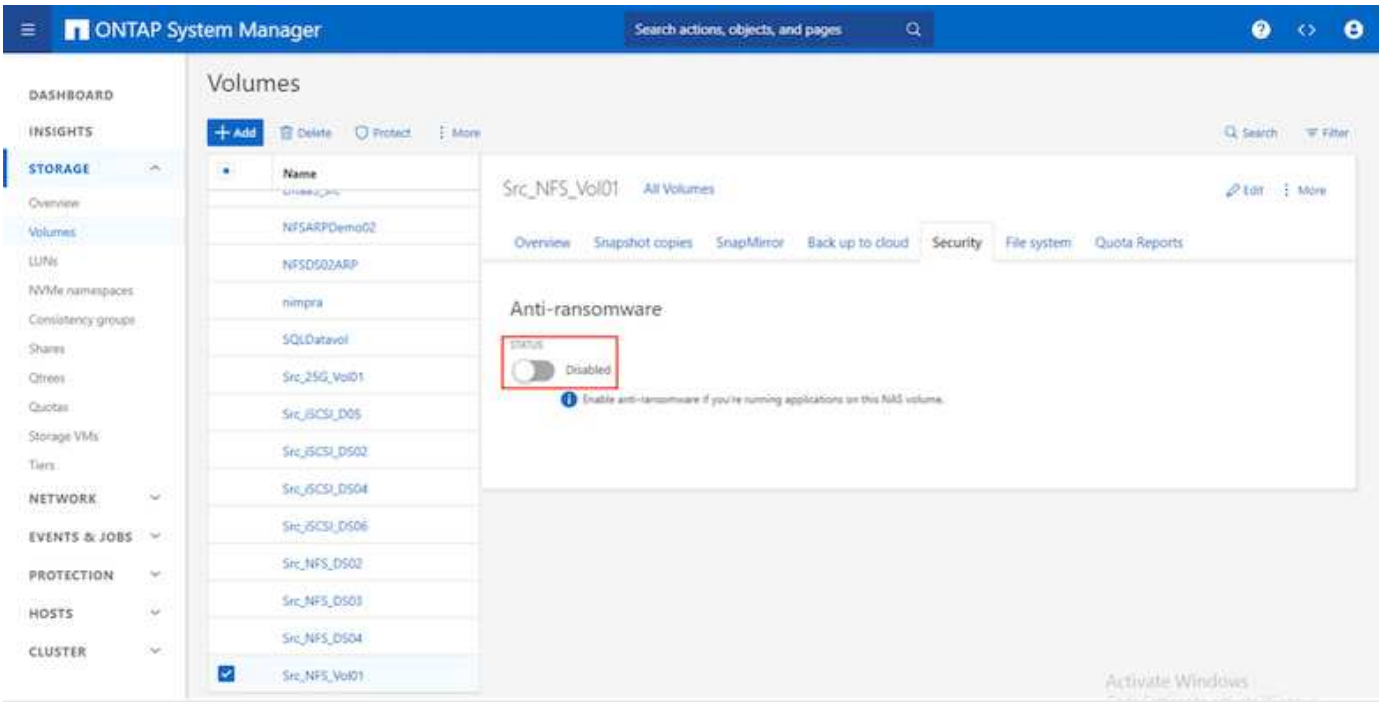
Informationen zum Konfigurieren von ONTAP-Speichersystemen finden Sie im "ONTAP 9-Dokumentation" Zentrieren.

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.

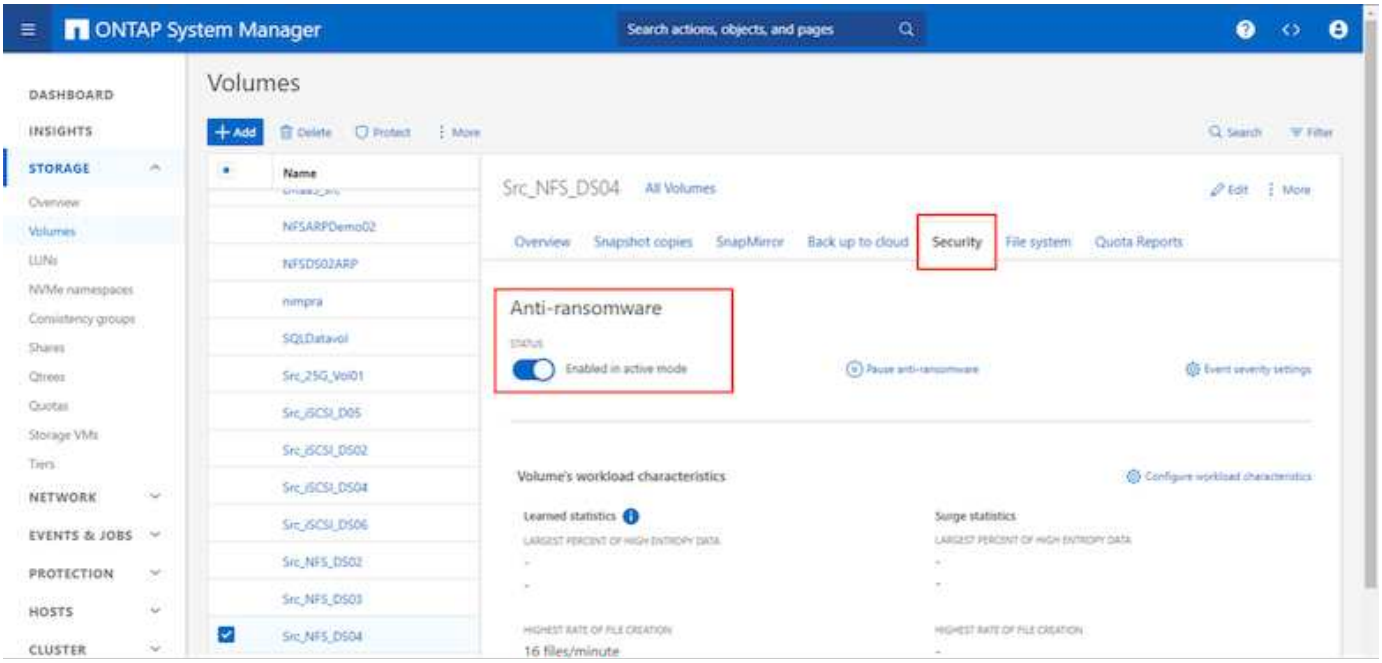
Sehen wir uns an, wie die oben genannten Funktionen mit VMware zusammenarbeiten, um Daten vor Ransomware zu schützen und wiederherzustellen. Um vSphere und Gast-VMs vor Angriffen zu schützen, müssen verschiedene Maßnahmen ergriffen werden, darunter Segmentierung, Einsatz von EDR/XDR/SIEM für Endpunkte und Installation von Sicherheitsupdates sowie Einhaltung der entsprechenden Härtungsrichtlinien. 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.

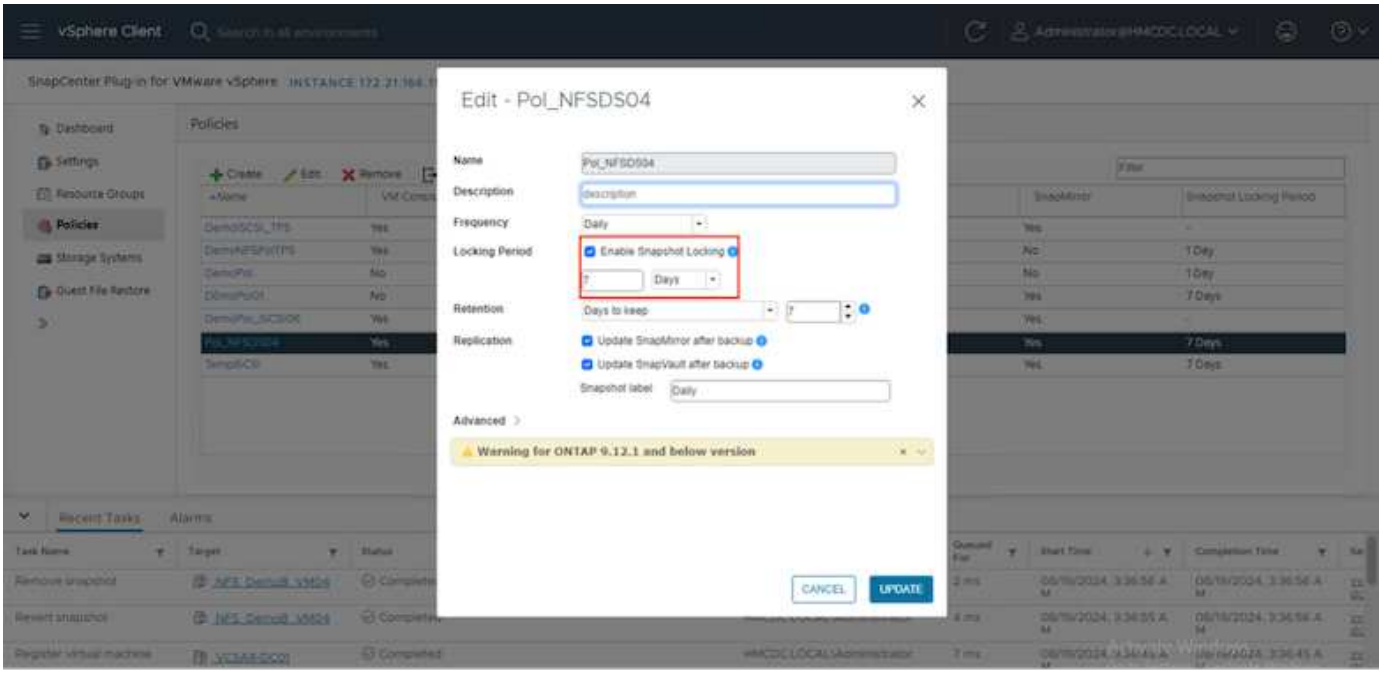
Im aktiven Modus wird nach der abnormalen Volume-Aktivität gesucht, die möglicherweise ein Ransomware-Angriff sein könnte. Wenn anormale Aktivitäten erkannt werden, wird sofort eine automatische Snapshot Kopie erstellt. Dadurch wird ein Wiederherstellungspunkt so nah wie möglich an der Infektion mit 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.



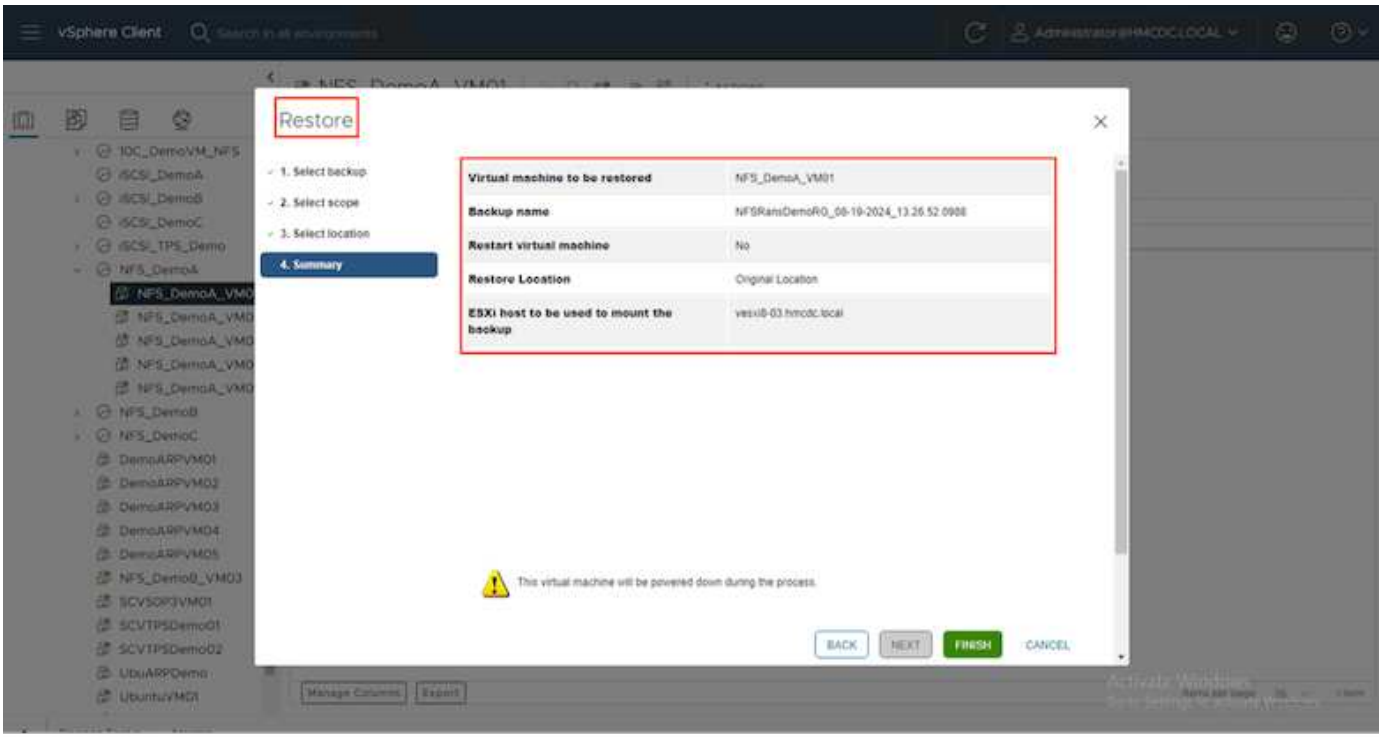
Wenn ein Ransomware-Angriff auf die virtuelle Maschine (VM) zielt und Dateien innerhalb der VM verändert, ohne Änderungen außerhalb der VM vorzunehmen, erkennt der Advanced Ransomware Protection (ARP) immer noch die Bedrohung, wenn die Standard-Entropie der VM niedrig ist, z. B. für Dateitypen wie .txt, .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.



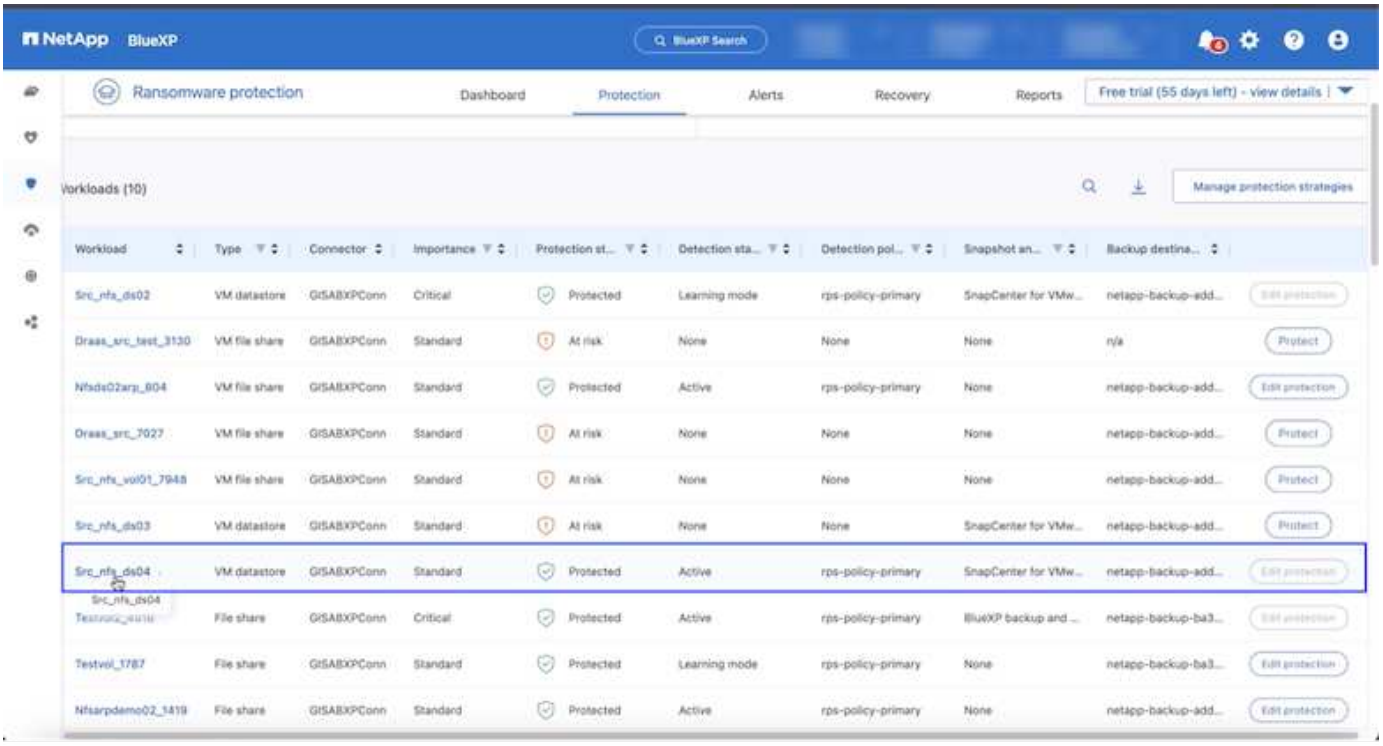
In der obigen Abbildung wird gezeigt, wie ONTAP Storage die vorhandenen Techniken um eine zusätzliche Schicht erweitert und so die Zukunftssicherheit der Umgebung verbessert.

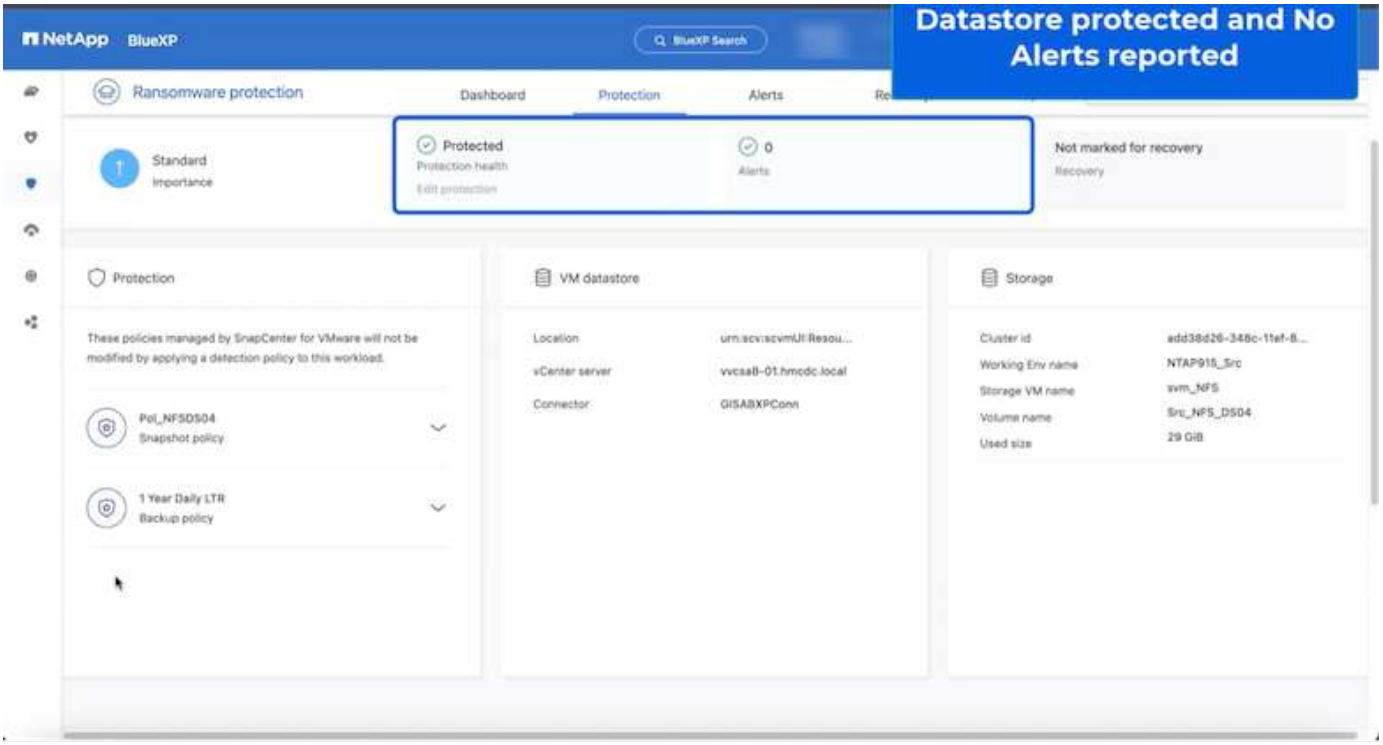
Weitere Informationen finden Sie in der Anleitung für "NetApp Lösungen für Ransomware".

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-Datastores und File Shares in lokalem NFS-Storage.

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

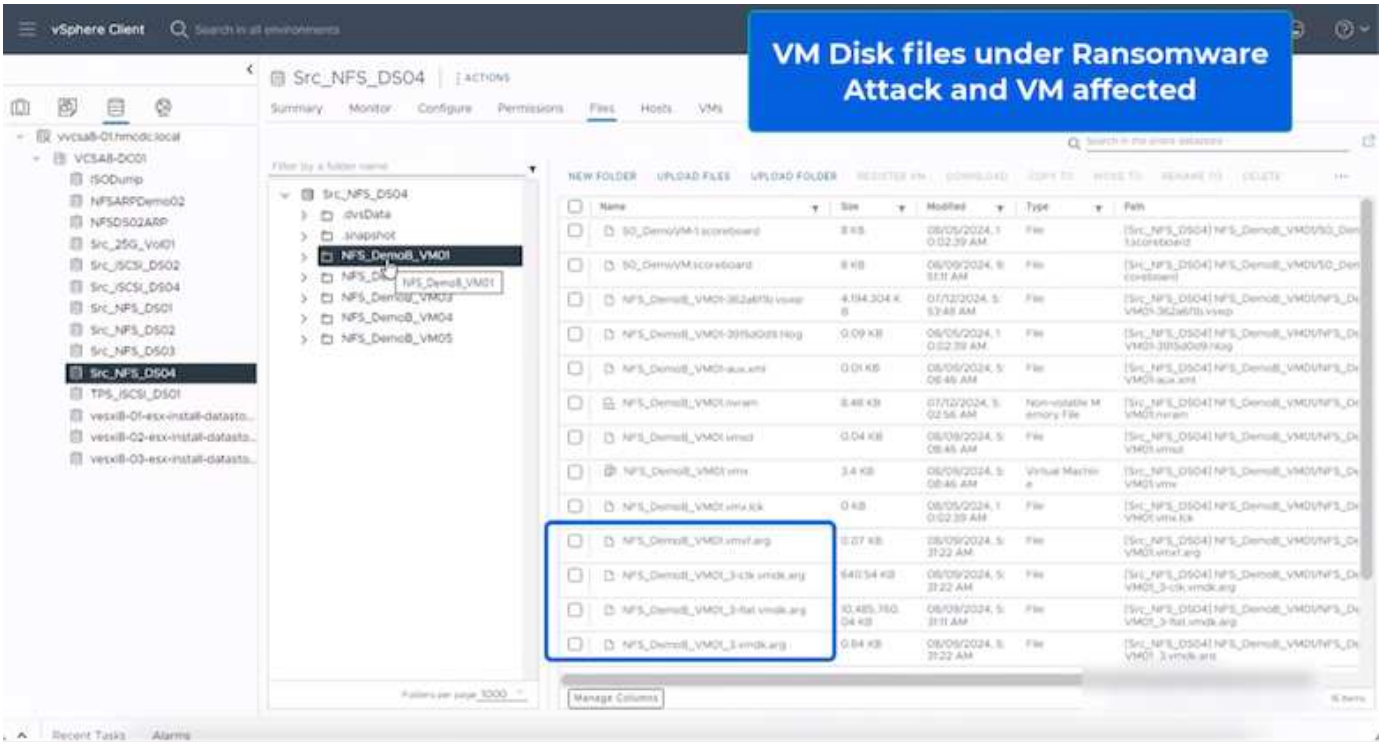




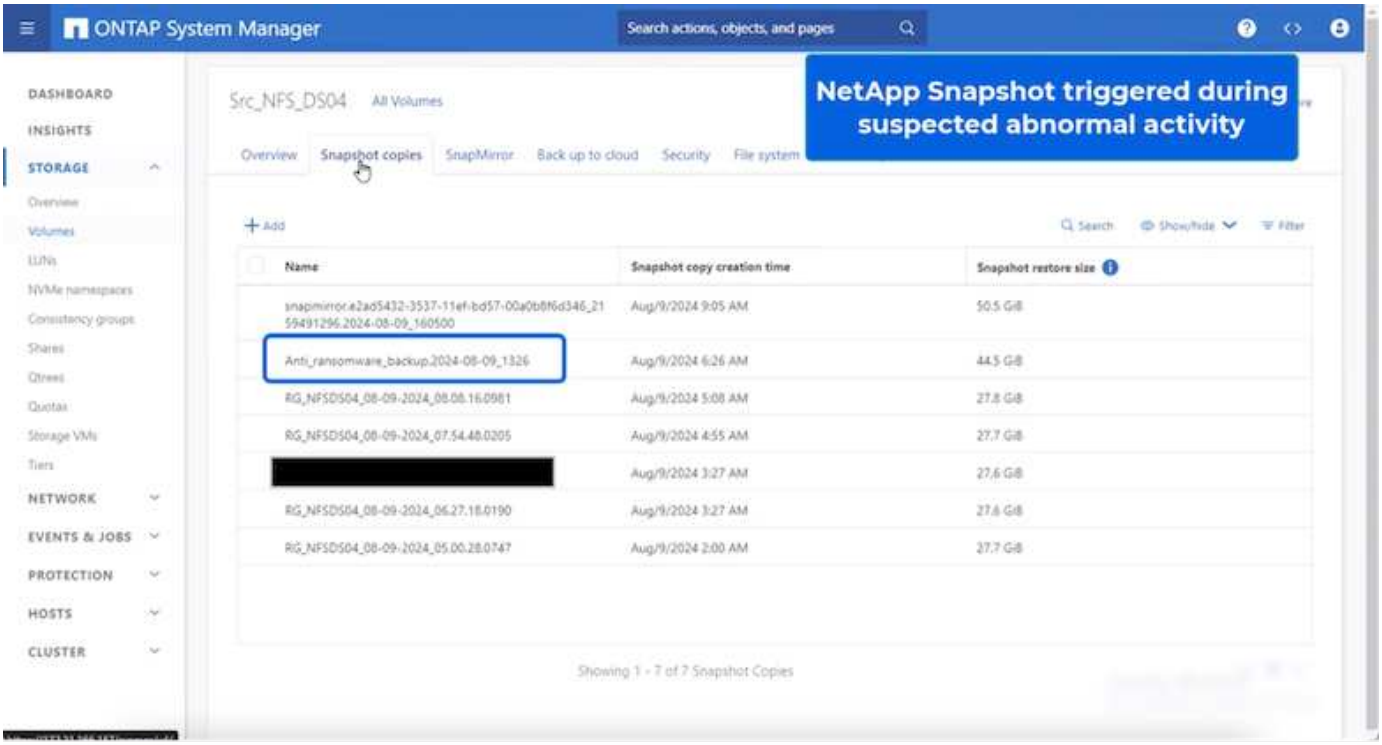
Ausführliche Informationen zum Konfigurieren von BlueXP -Ransomware-Schutz finden Sie unter "Einrichten des BlueXP Ransomware-Schutzes" und "Konfigurieren Sie BlueXP Ransomware-Schutzeinstellungen".

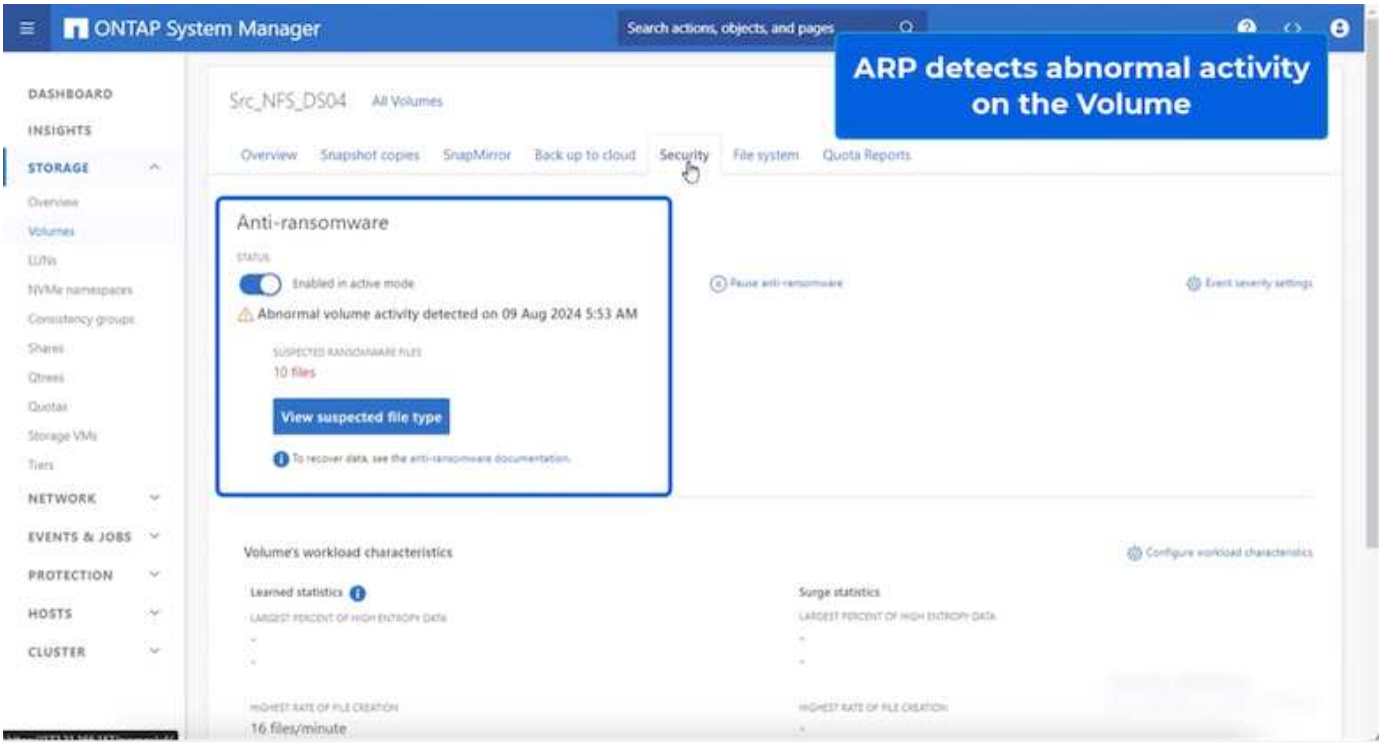
Es ist an der Zeit, dies anhand eines Beispiels zu erläutern. In dieser Anleitung ist der Datastore

„SRC_NFS_DS04“ betroffen.

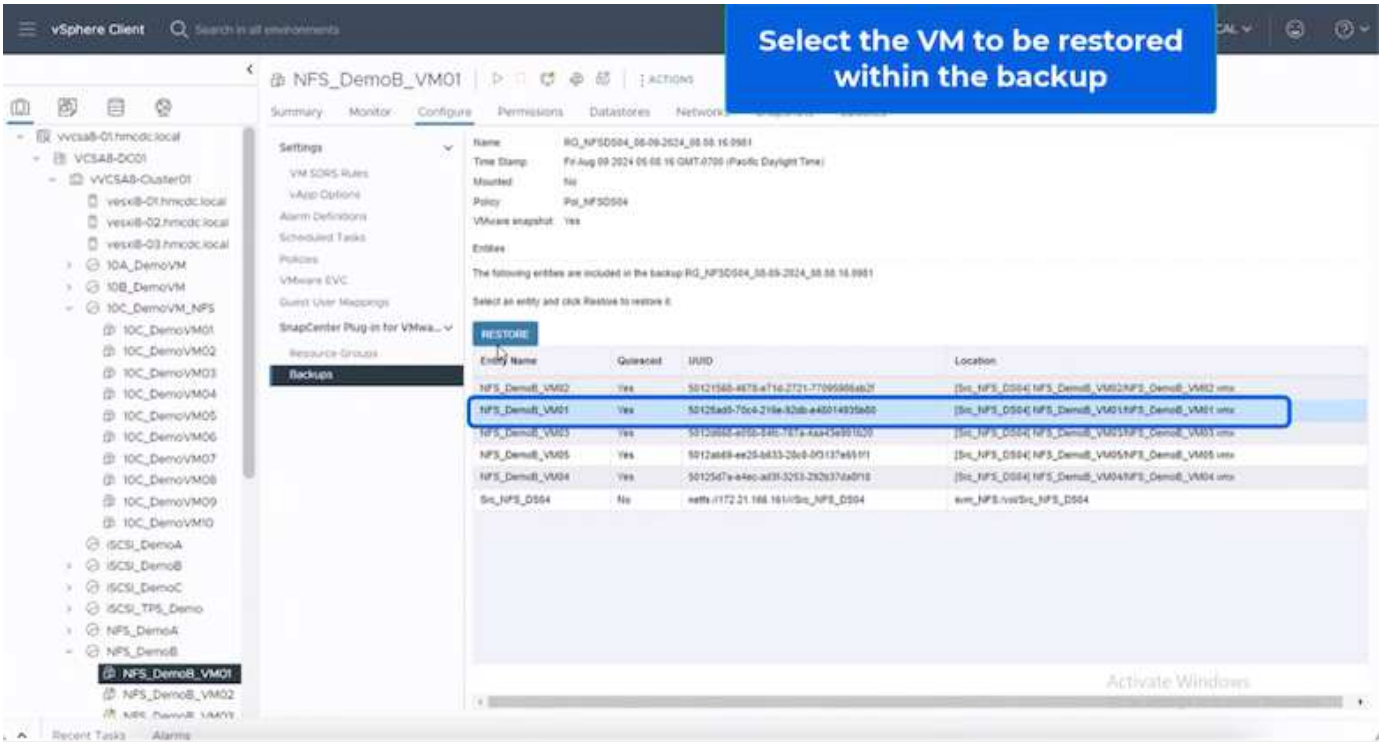


ARP hat bei der Erkennung sofort einen Snapshot auf dem Volume ausgelöst.





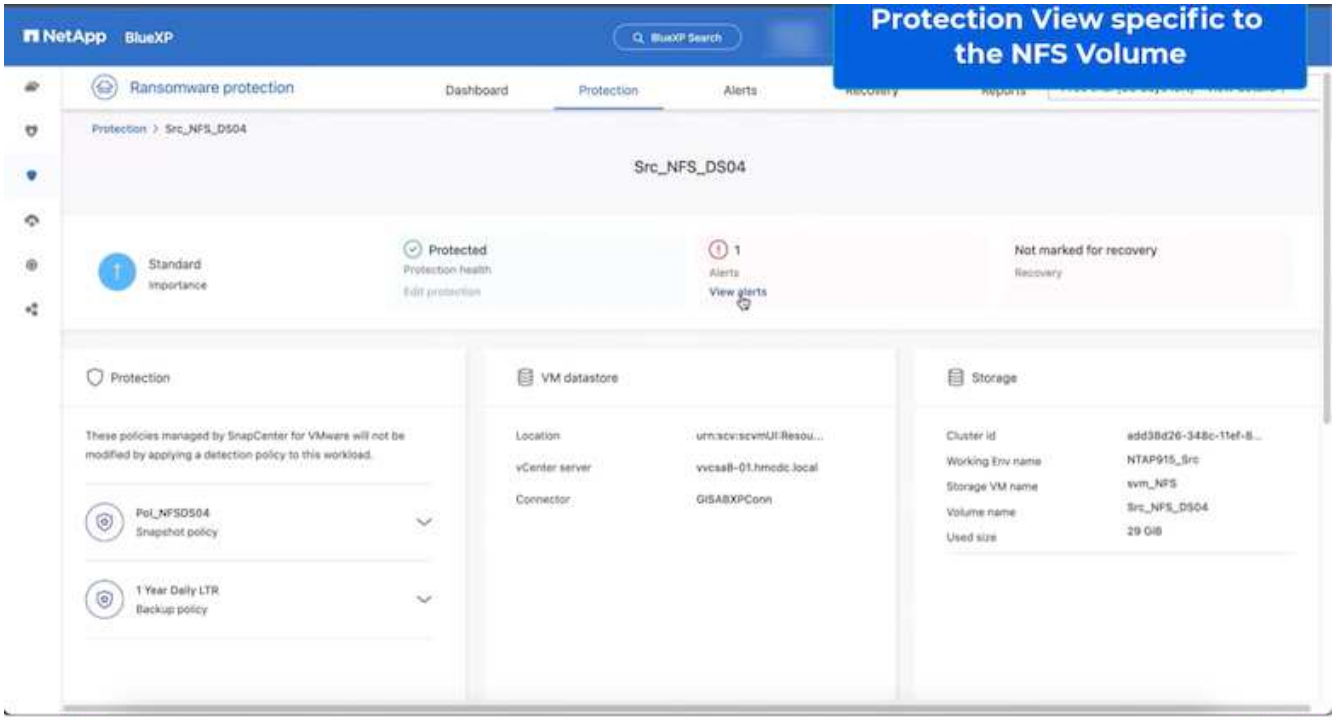
Sobald die forensische Analyse abgeschlossen ist, können die Wiederherstellungen mithilfe von SnapCenter oder BlueXP Ransomware-Schutz schnell und nahtlos durchgeführt werden. Wechseln Sie bei SnapCenter zu den betroffenen Virtual Machines, und wählen Sie den entsprechenden wiederherzustellenden Snapshot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



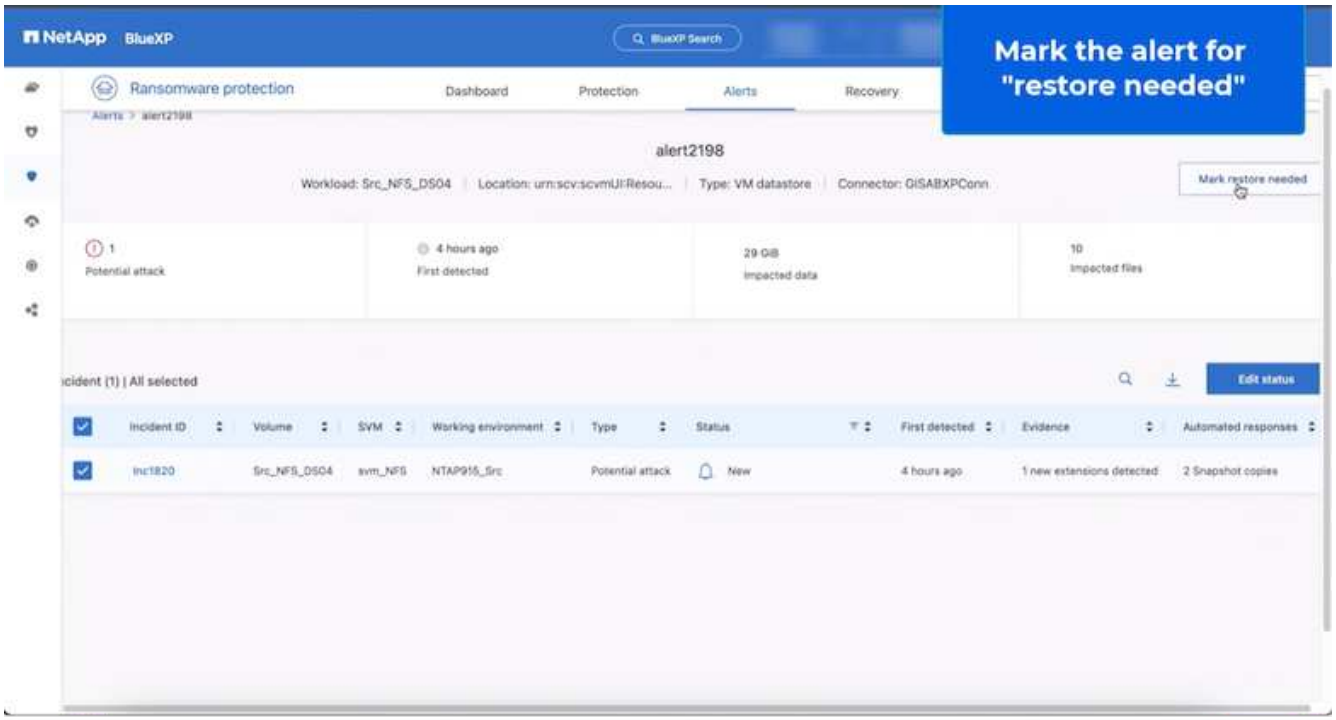
Dieser Abschnitt beschäftigt sich damit, wie der BlueXP Ransomware-Schutz die Recovery nach einem Ransomware-Vorfall orchestriert, bei dem die VM-Dateien verschlüsselt sind.

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

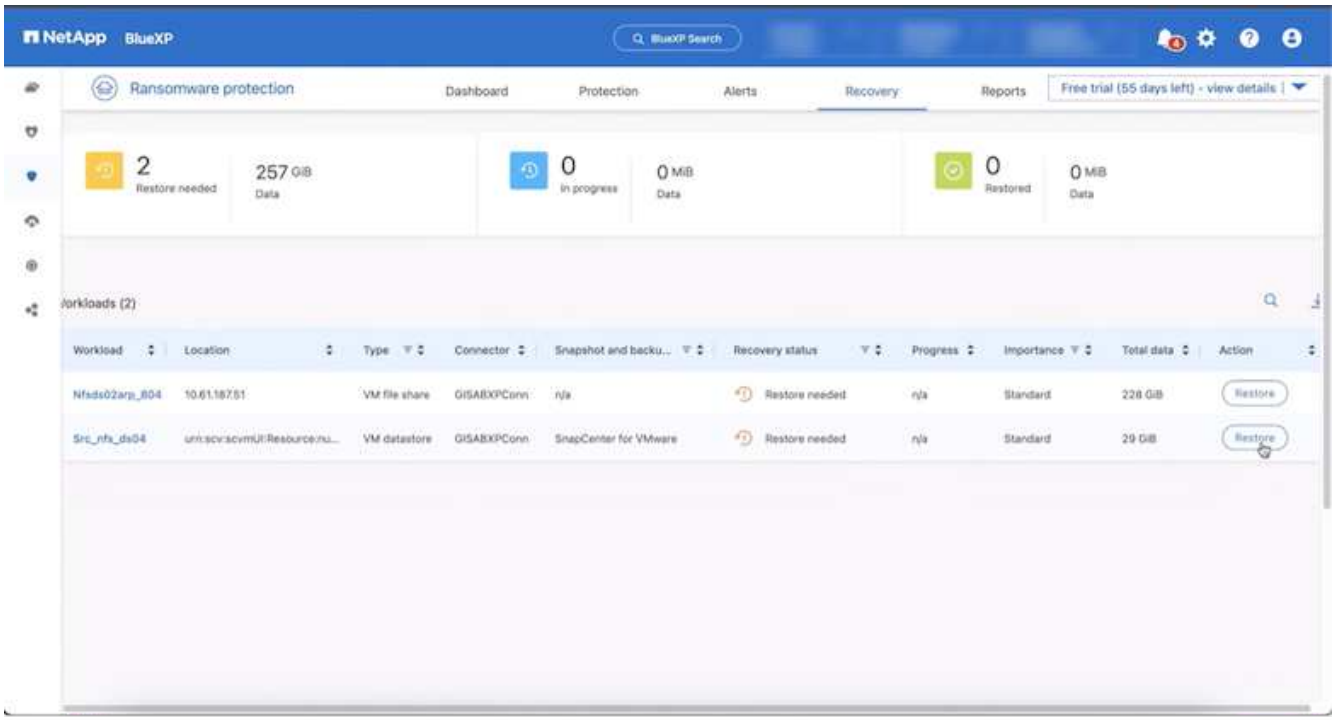


3. Markieren Sie den Ransomware-Vorfall als bereit für die Wiederherstellung (nach dem Neutralisieren von Vorfällen), indem Sie „Wiederherstellung erforderlich markieren“ auswählen.

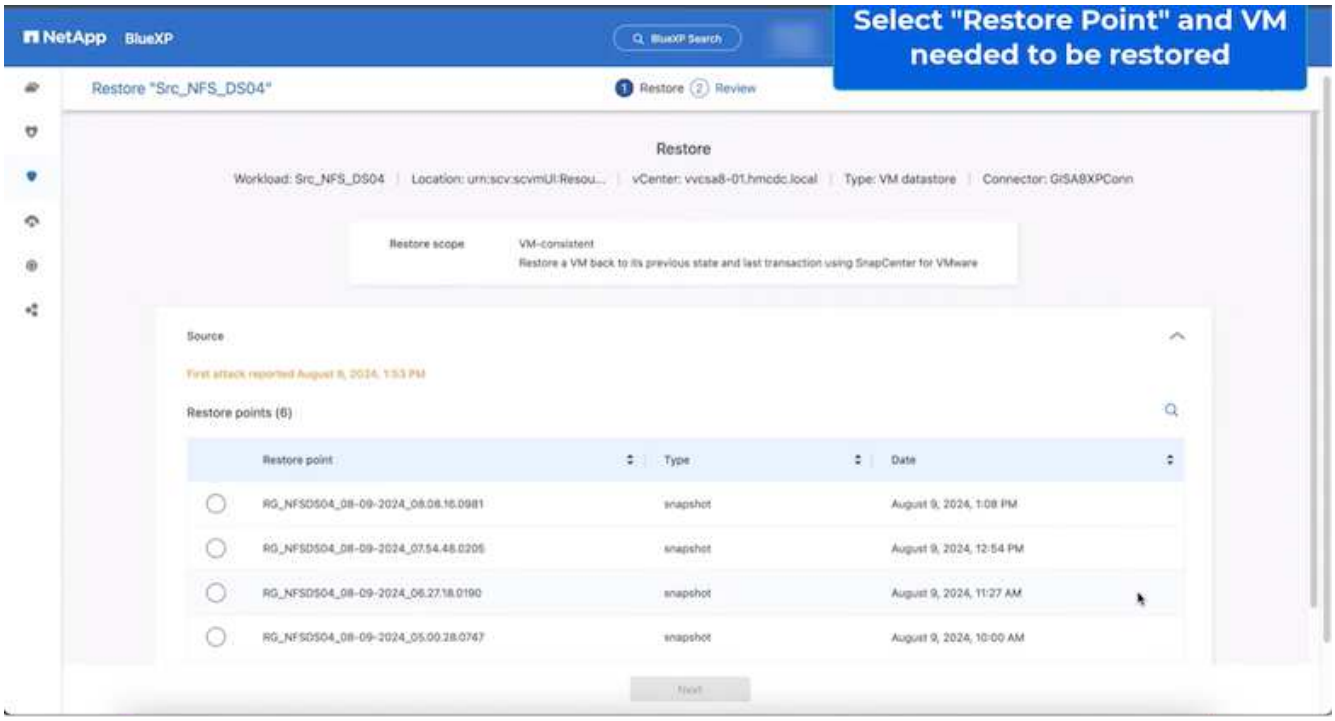


Die Warnung kann abgewiesen werden, wenn sich der Vorfall als falsch positiv herausstellt.

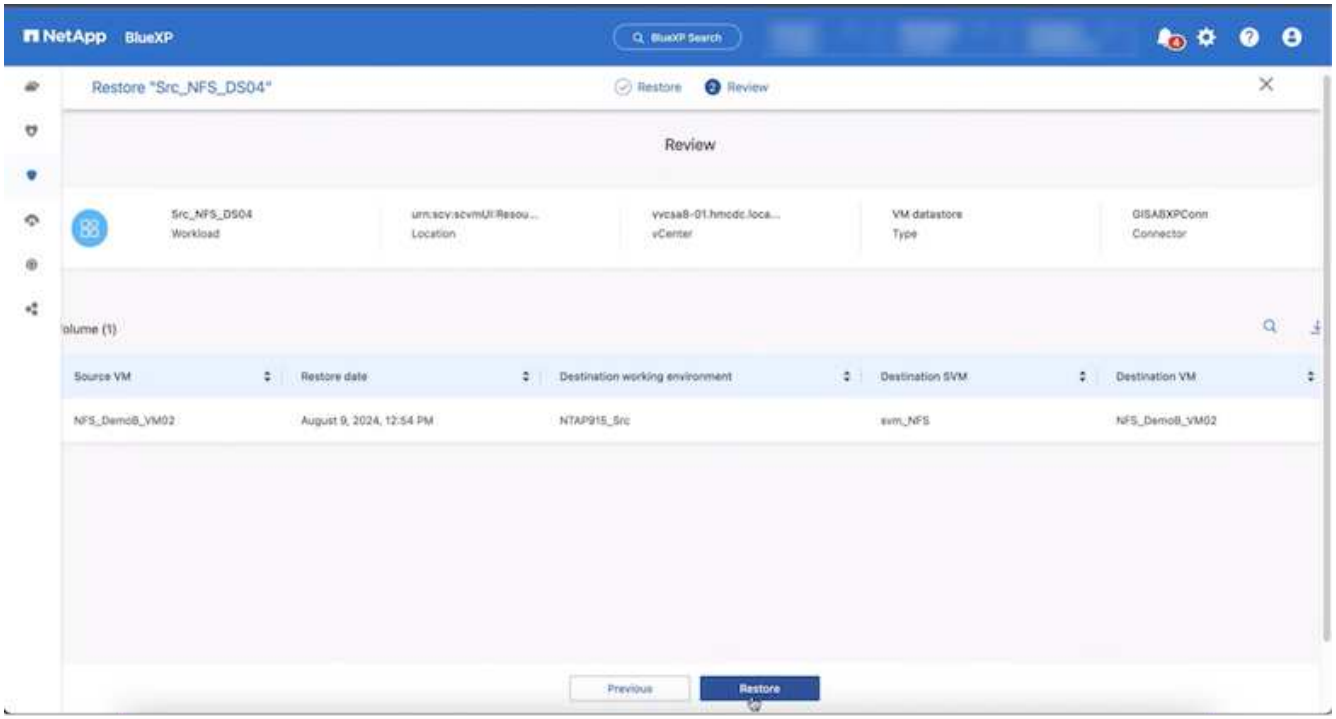
4. Ging zur Registerkarte Recovery und überprüfe die Workload-Informationen auf der Recovery Seite und wähle das Datastore-Volume aus, das sich im Status „Restore needed“ befindet, und wähle Restore aus.



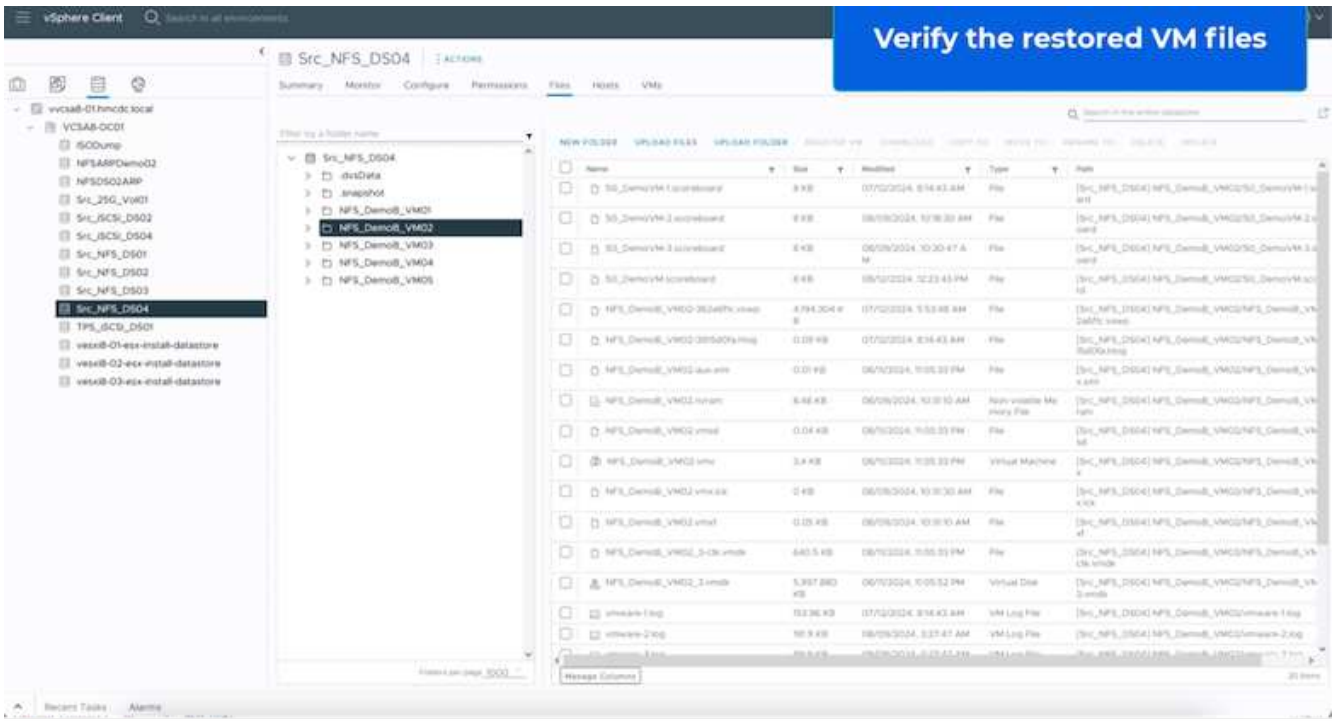
5. In diesem Fall ist der Umfang der Wiederherstellung „durch VM“ (für SnapCenter für VMs ist der Umfang der Wiederherstellung „durch VM“)



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



7. 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 Einsehnen, 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.