VMware Cloud Foundation auf NetApp

NetApp virtualization solutions

NetApp
August 24, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html on August 24, 2025. Always check docs.netapp.com for the latest.

Inhalt

VMware Cloud Foundation auf NetApp . . . 1
- Vereinfachen Sie die Hybrid Cloud-Erfahrung mit VMware Cloud Foundation und ONTAP . . . 1
- Einführung . . . 1
  - Einführung in NetApp ONTAP . . . 1
  - Einführung in VMware Cloud Foundation . . . 1
  - VCF-Domänen . . . 2
  - Speicherung mit VCF . . . 3
  - Warum ONTAP für VCF . . . 3
  - Weitere Informationen: . . . 4
  - Zusammenfassung . . . 5
  - Dokumentationsressourcen . . . 5
- Designoptionen mit VMware Cloud Foundation und ONTAP . . . 6
  - Speicheroptionen . . . 6
  - Blaupausen . . . 6
- Einrichten privater Cloud-Umgebungen mit VMware Cloud Foundation und ONTAP . . . 11
  - Bereitstellen einer neuen VCF 9-Instanz . . . 11
  - Konvergieren Sie vorhandene Komponenten in VCF 9 . . . 13
  - Aktualisieren Sie eine vorhandene VCF-Umgebung auf VCF 9 . . . 14
- Implementierung von Disaster Recovery mit NetApp SnapMirror und BlueXP DRaaS . . . 14
  - Erste Schritte . . . 15
  - BlueXP disaster recovery . . . 17
  - Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array . . . 17
  - So richten Sie es für VMware Disaster Recovery ein . . . 18
  - Was kann BlueXP disaster recovery für Sie tun? . . . 18
  - Testen des Failovers . . . 23
  - Bereinigungs-Failover-Testvorgang . . . 25
  - Geplante Migration und Failover . . . 26
  - Failback . . . 27
  - Überwachung und Dashboard . . . 29
- Konvertieren Sie vorhandene vSphere-Cluster in VCF . . . 30
  - Erfahren Sie mehr über die Konvertierung einer vSphere-Umgebung mit vorhandenen Datenspeichern in VCF . . . 30
  - Konvertieren Sie die vCenter-Serverinstanz in eine VCF-Verwaltungsdomäne (NFS-Datenspeicher). . . . 30
  - Konvertieren Sie die vCenter-Serverinstanz in eine VCF-Verwaltungsdomäne (FC-Datenspeicher). . . . 44
- Bereitstellen von VCF mit Hauptspeicher . . . 58
  - Stellen Sie eine VCF-Umgebung mit ONTAP als primäre Speicherlösung bereit . . . 58
  - Verwenden Sie einen FC-basierten VMFS-Datenspeicher auf ONTAP als Hauptspeicher für die VCF-Verwaltungsdomäne . . . 59
  - Verwenden Sie einen NFS-Datenspeicher auf ONTAP als Hauptspeicher für die VCF-Verwaltungsdomäne . . . 60
  - Verwenden Sie einen FC-basierten VMFS-Datenspeicher auf ONTAP als Hauptspeicher für eine VI-Workload-Domäne . . . 62
  - Verwenden Sie einen NFS-Datenspeicher auf ONTAP als Hauptspeicher für eine VI-Workloaddomäne . . . 64

Erweitern Sie VCF mit zusätzlichem Speicher . . . 85
Erfahren Sie mehr über die Speichererweiterung für eine VCF-Umgebung mithilfe von zusätzlichem Speicher . . . 85
Fügen Sie mithilfe von ONTAP tools for VMware vSphere einen iSCSI-Datenspeicher als zusätzlichen Speicher für eine Verwaltungsdomäne hinzu . . . 85
Fügen Sie mithilfe von ONTAP tools for VMware vSphere einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher für eine Verwaltungsdomäne hinzu . . . 110
Fügen Sie vVols als zusätzlichen Speicher zu VI-Workload-Domänen hinzu, indem Sie ONTAP tools for VMware vSphere verwenden . . . 111
Fügen Sie mithilfe von ONTAP tools for VMware vSphere NFS und vVols als zusätzlichen Speicher zu VI-Workload-Domänen hinzu . . . 138
Fügen Sie NVMe über TCP als zusätzlichen Speicher zu VI-Workloaddomänen hinzu . . . 163
Fügen Sie einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher zu VI-Workload-Domänen hinzu . . . 187
Schützen Sie VCF mit SnapCenter . . . 188
Erfahren Sie mehr über den Schutz von VCF-Workload-Domänen mit dem SnapCenter -Plug-in für VMware vSphere . . . 188
Schützen Sie eine VCF-Workloaddomäne mit dem SnapCenter -Plug-in für VMware vSphere . . . 189
Schützen Sie VCF-Verwaltungs- und Workloaddomänen mit dem SnapCenter -Plug-in für VMware vSphere . . . 224
Schützen Sie VCF-Workload-Domänen mit NVMe über TCP-Speicher und SnapCenter -Plug-in für VMware vSphere . . . 237
Schützen Sie VMware-Datenspeicher mit BlueXP . . . 245
Erfahren Sie mehr über den Schutz von VMware-Datenspeichern mit BlueXP disaster recovery . . . 245
Konfigurieren Sie 3-2-1-Datenschutz für VMware mit dem SnapCenter -Plug-in für VMware vSphere und BlueXP backup and recovery . . . 245
Einrichten der Notfallwiederherstellung für VMFS-Datenspeicher mit BlueXP disaster recovery . . . 292
Einrichten der Notfallwiederherstellung für NFS-Datenspeicher mit BlueXP disaster recovery . . . 310
Schützen Sie Workloads mit vSphere Metro Storage Cluster . . . 331
Erfahren Sie mehr über die Integration der hohen Verfügbarkeit von ONTAP mit VMware vSphere Metro Storage Cluster (vMSC). . . . 331
Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne mit MetroCluster . . . 332
Konfigurieren eines Stretch-Clusters für eine VI-Workloaddomäne mit MetroCluster . . . 343
Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne mit SnapMirror Active Sync . . . 355
Konfigurieren eines Stretch-Clusters für eine VI-Workloaddomäne mit SnapMirror Active Sync . . . 357
Migrieren Sie VMs von VMware vSphere zu ONTAP -Datenspeichern . . . 359
Netzwerkanforderungen . . . 360
VM-Migrationsszenarien . . . 362
Szenarien für die Migration von VM-Vorlagen . . . 387
Anwendungsfälle . . . 395
Weitere Ressourcen . . . 396
Autonomer Ransomware-Schutz für NFS-Speicher . . . 396
Überwachen Sie den lokalen Speicher mit Data Infrastructure Insights . . . 406
Überwachung des lokalen Speichers mit Data Infrastructure Insights . . . 406
Übersicht über die Lösungsbereitstellung . . . 407

Voraussetzungen 407
Lösungsbereitstellung 407
Abschluss 424
Weitere Informationen 424

VMware Cloud Foundation auf NetApp

Vereinfachen Sie die Hybrid Cloud-Erfahrung mit VMware Cloud Foundation und ONTAP

NetApp ONTAP lässt sich in VMware Cloud Foundation (VCF) integrieren, um eine einheitliche Speicherlösung bereitzustellen, die sowohl Block- als auch Dateiprotokolle unterstützt. Diese Integration vereinfacht die Bereitstellung hybrider Clouds, verbessert die Datenverwaltung und -leistung und gewährleistet konsistente Datendienste in lokalen und Cloud-Umgebungen.

Einführung

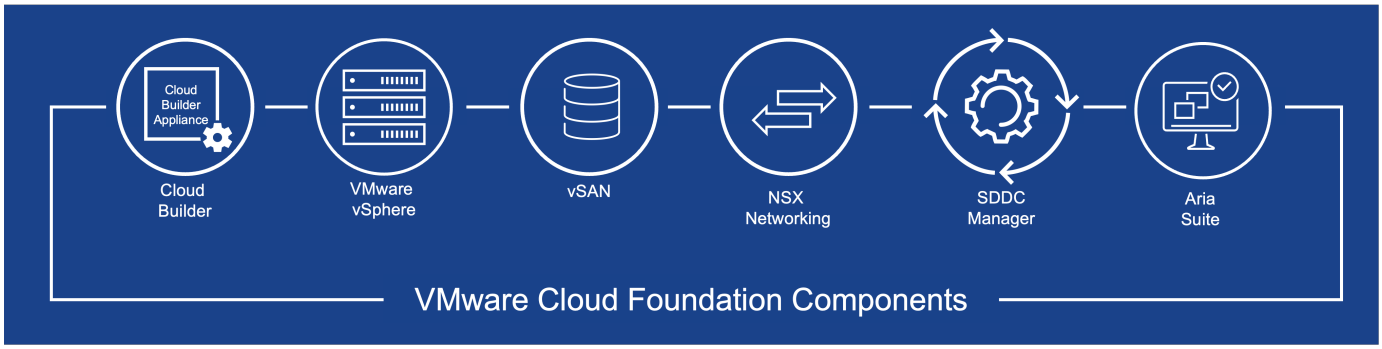
Die Verwendung von NetApp mit VCF verbessert die Datenverwaltung und Speichereffizienz durch die erweiterten Funktionen von NetApp wie Deduplizierung, Komprimierung und Snapshots. Diese Kombination bietet nahtlose Integration, hohe Leistung und Skalierbarkeit für virtualisierte Umgebungen. Darüber hinaus vereinfacht es die Bereitstellung hybrider Clouds, indem es konsistente Datendienste und -verwaltung über lokale und Cloud-Infrastrukturen hinweg ermöglicht.

Einführung in NetApp ONTAP

NetApp ONTAP ist eine umfassende Datenverwaltungssoftware, die erweiterte Speicherfunktionen für eine breite Produktlinie bietet. ONTAP ist als softwaredefinierter Speicher, als First-Party-Service über die großen Cloud-Anbieter und als Speicherbetriebssystem für NetApp ASA (All San Array), AFF (All-Flash FAS) und FAS Plattformen (Fabric-Attached Storage) verfügbar. ONTAP bietet hohe Leistung und geringe Latenz für eine Vielzahl von Anwendungsfällen, einschließlich VMware-Virtualisierung, ohne Silos zu erstellen.

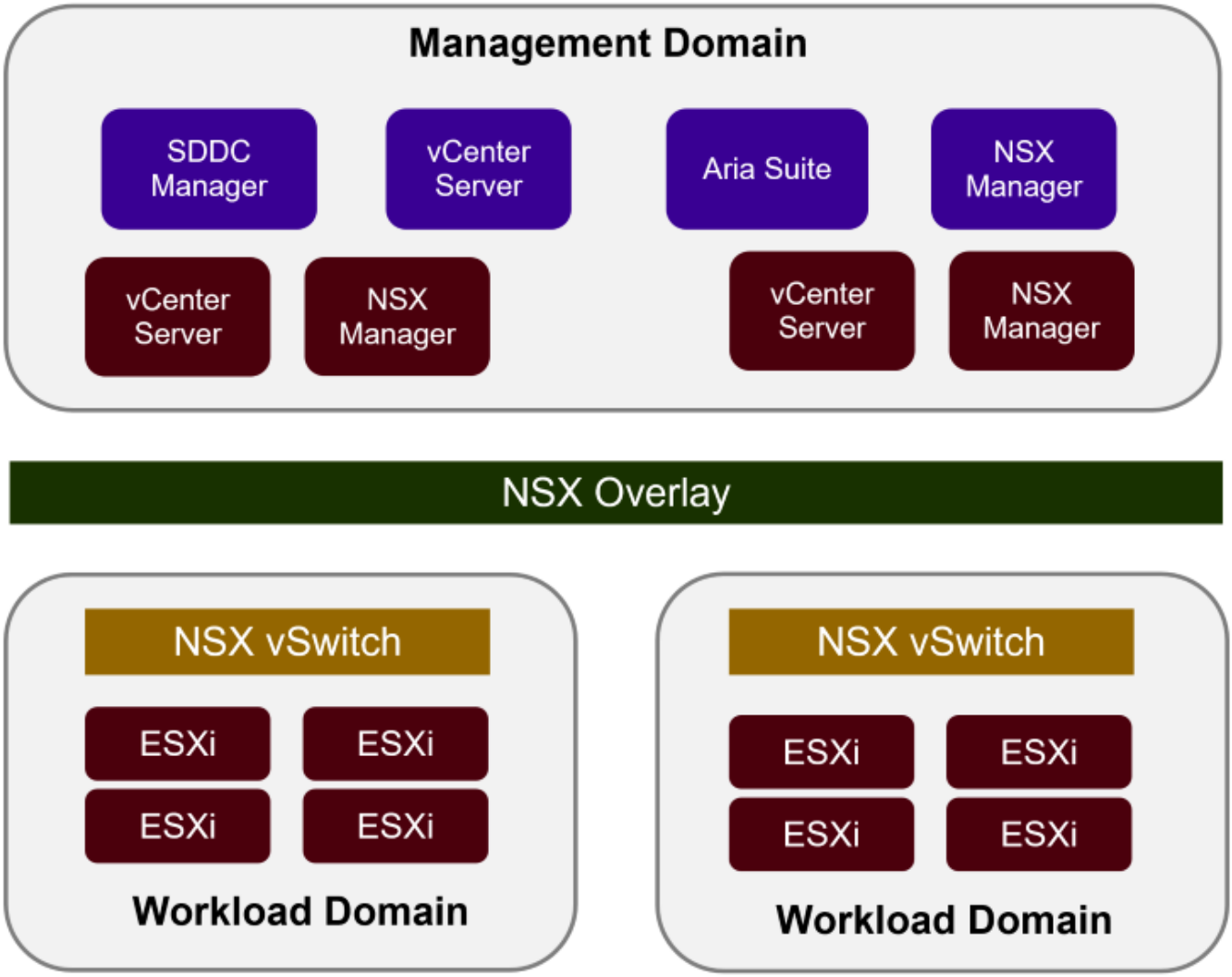
Einführung in VMware Cloud Foundation

VCF integriert Rechen-, Netzwerk- und Speicherangebote mit VMware-Produkten und Integrationen von Drittanbietern und ermöglicht so sowohl native Kubernetes- als auch auf virtuellen Maschinen basierende Workloads. Diese Softwareplattform umfasst Schlüsselkomponenten wie VMware vSphere, NSX, Aria Suite Enterprise, Tanzu Kubernetes Grid, HCX Enterprise, SDDC Manager und Speicherkapazität, die über vSAN mit Host-CPU-Kernen verbunden ist. NetApp ONTAP lässt sich nahtlos in eine Vielzahl von VCF-Bereitstellungsmodellen sowohl vor Ort als auch in der öffentlichen Cloud integrieren.



VCF-Domänen

Domänen sind ein grundlegendes Konstrukt innerhalb von VCF, das die Organisation von Ressourcen in eindeutige, unabhängige Gruppierungen ermöglicht. Domänen helfen dabei, die Infrastruktur effektiver zu organisieren und sicherzustellen, dass die Ressourcen effizient genutzt werden. Jede Domäne wird mit ihren eigenen Rechen-, Netzwerk- und Speicherelementen bereitgestellt.



Es gibt zwei Haupttypen von Domänen mit VCF:

- **Verwaltungsdomäne** – Die Verwaltungsdomäne umfasst Komponenten, die für die Kernfunktionen der VCF-Umgebung verantwortlich sind. Die Komponenten übernehmen wichtige Aufgaben wie Ressourcenbereitstellung, Überwachung und Wartung und umfassen Plug-In-Integrationen von Drittanbietern wie NetApp ONTAP Tools für VMware. Um die Einhaltung bewährter Methoden sicherzustellen, können Verwaltungsdomänen mithilfe der Cloud Builder Appliance bereitgestellt oder eine vorhandene vCenter-Umgebung in eine VCF-Verwaltungsdomäne umgewandelt werden.
- **Virtual Infrastructure Workload Domain** – Virtual Infrastructure Workload Domains sind als Ressourcenpools konzipiert, die einem bestimmten Betriebsbedarf, einer bestimmten Arbeitslast oder Organisation gewidmet sind. Workload-Domänen lassen sich problemlos über den SDDC Manager bereitstellen und tragen so zur Automatisierung einer Reihe komplexer Aufgaben bei. Innerhalb einer VCF-Umgebung können bis zu 24 Workload-Domänen bereitgestellt werden, wobei jede eine Einheit anwendungsbereiter Infrastruktur darstellt.

Speicherung mit VCF

Der von ihnen verbrauchte Speicherplatz ist für die Funktionalität von Domänen von zentraler Bedeutung. Während VCF CPU-Core-basierte vSAN-Kapazität für hyperkonvergente Anwendungsfälle umfasst, unterstützt es auch eine breite Palette externer Speicherlösungen. Diese Flexibilität ist entscheidend für Unternehmen, die erheblich in vorhandene Speicher-Arrays investiert haben oder Protokolle unterstützen müssen, die über die Möglichkeiten von vSAN hinausgehen. VMware unterstützt mit VCF mehrere Speichertypen.

Es gibt zwei Hauptspeichertypen mit VCF:

- **Hauptspeicher** – Dieser Speichertyp wird bei der ersten Erstellung der Domäne zugewiesen. Für Verwaltungsdomänen beherbergt dieser Speicher die Verwaltungs- und Betriebskomponenten von VCF. Bei Workload-Domänen ist dieser Speicher darauf ausgelegt, die Workloads, VMs oder Container zu unterstützen, für die die Domäne bereitgestellt wurde.
- **Zusätzlicher Speicher** – Nach der Bereitstellung kann jeder Workloaddomäne zusätzlicher Speicher hinzugefügt werden. Dieser Speichertyp hilft Unternehmen, vorhandene Investitionen in die Speicherinfrastruktur zu nutzen und verschiedene Speichertechnologien zu integrieren, um Leistung, Skalierbarkeit und Kosteneffizienz zu optimieren.

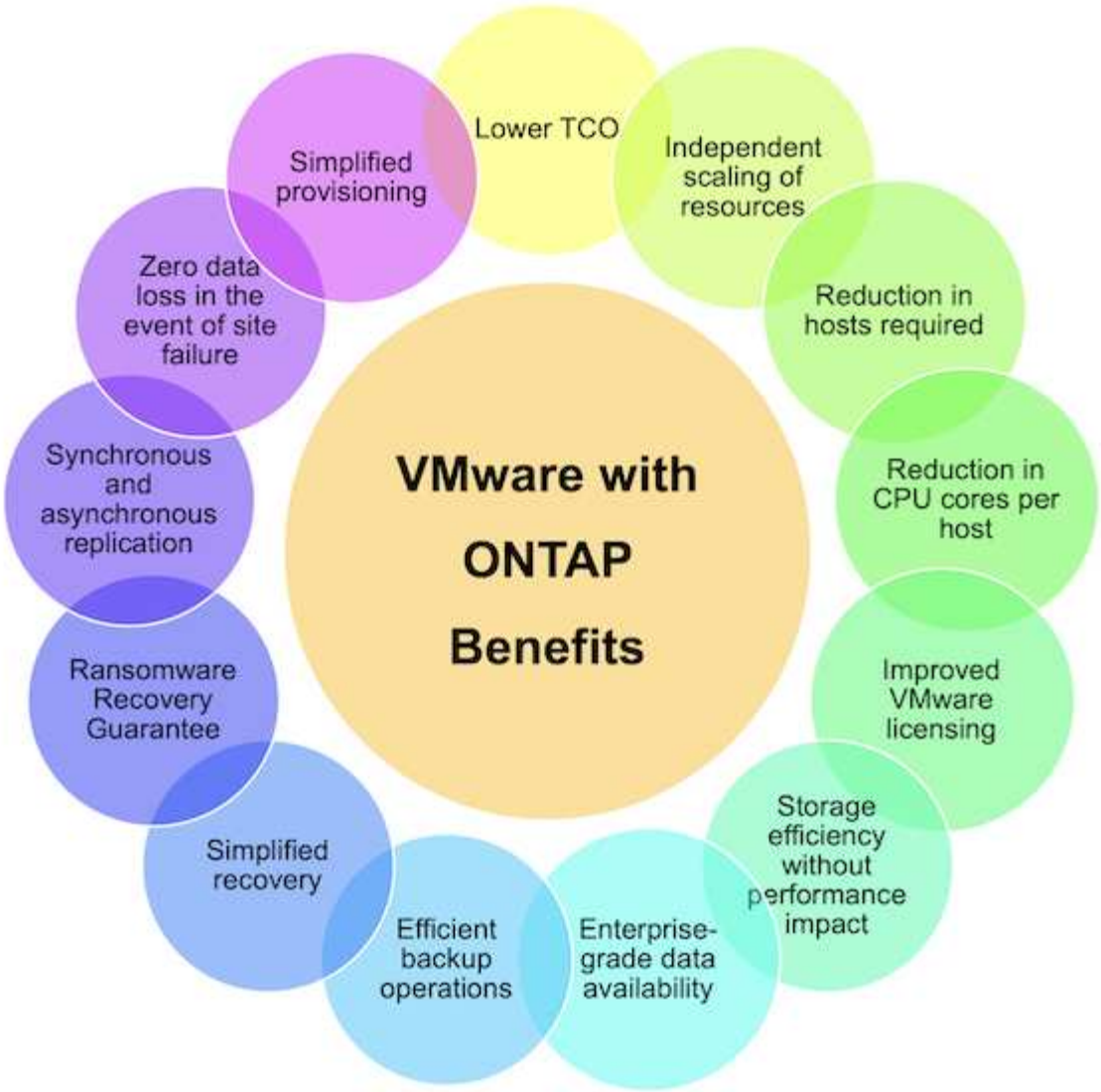
Unterstützt VCF-Speichertypen

Domänentyp	Hauptspeicher	Zusätzlicher Speicher
Verwaltungsdomäne	vSAN FC* NFS*	vVols (FC, iSCSI oder NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA
Arbeitslastdomäne der virtuellen Infrastruktur	vSAN vVols (FC, iSCSI oder NFS) FC NFS	vVols (FC, iSCSI oder NFS) FC NFS iSCSI NVMe/TCP NVMe/FC NVMe/RDMA

Hinweis: * Spezifische Protokollunterstützung wird bei Verwendung des VCF-Importtools mit vorhandenen vSphere-Umgebungen bereitgestellt.

Warum ONTAP für VCF

Neben Anwendungsfällen, die Investitionsschutz und Multiprotokollunterstützung beinhalten, gibt es viele weitere Gründe, die Vorteile externer gemeinsam genutzter Speicher innerhalb einer VCF-Workloaddomäne zu nutzen. Es kann davon ausgegangen werden, dass der für eine Workload-Domäne bereitgestellte Speicher lediglich ein Repository zum Hosten von VMs und Containern ist. Die Anforderungen der Organisation übersteigen jedoch häufig die Möglichkeiten der lizenzierten Kapazität und erfordern Unternehmensspeicher. Der von ONTAP bereitgestellte Speicher, der Domänen innerhalb von VCF zugewiesen ist, lässt sich einfach bereitstellen und bietet eine zukunftssichere Shared-Storage-Lösung.



Weitere Informationen zu den wichtigsten ONTAP Vorteilen für VMware VCF finden Sie unten unter"Warum ONTAP für VMware" .

- Flexibilität ab dem ersten Tag und bei der Skalierung
- Lagern Sie Speicheraufgaben auf ONTAP aus
- Klassenbeste Speichereffizienz
- Datenverfügbarkeit auf Unternehmensniveau
- Effiziente Backup- und Wiederherstellungsvorgänge
- Ganzheitliche Geschäftskontinuitätsfunktionen

Weitere Informationen:

- "NetApp Storage-Optionen"
- "Unterstützung für vSphere Metro Storage Cluster (vMSC)"
- "ONTAP Tools für VMware vSphere"
- "VMware-Automatisierung mit ONTAP"

- "NetApp SnapCenter"
- "Hybrid Multicloud mit VMware und NetApp"
- "Sicherheit und Ransomware-Schutz"
- "Einfache Migration von VMware-Workloads zu NetApp"
- "BlueXP Notfallwiederherstellung"
- "Einblicke in die Dateninfrastruktur"
- "VM-Datensammler"

Zusammenfassung

ONTAP bietet eine Plattform, die alle Workload-Anforderungen erfüllt und maßgeschneiderte Blockspeicherlösungen sowie einheitliche Angebote bietet, um schnellere Ergebnisse für VMs und Anwendungen auf zuverlässige und sichere Weise zu ermöglichen. ONTAP umfasst erweiterte Techniken zur Datenreduzierung und -verschiebung, um den Platzbedarf des Rechenzentrums zu minimieren und gleichzeitig eine Verfügbarkeit auf Unternehmensebene sicherzustellen, damit kritische Workloads online bleiben. Darüber hinaus unterstützen AWS, Azure und Google im Rahmen ihrer VMware-in-the-Cloud-Angebote externen Speicher auf NetApp-Basis, um den vSAN-Speicher in Cloud-basierten VMware-Clustern zu verbessern. Insgesamt ist NetApp aufgrund seiner überlegenen Funktionen eine effektivere Wahl für VMware Cloud Foundation-Bereitstellungen.

Dokumentationsressourcen

Ausführliche Informationen zu den NetApp -Angeboten für VMware Cloud Foundation finden Sie hier:

VMware Cloud Foundation-Dokumentation

- "VMware Cloud Foundation-Dokumentation"

Vier (4)-teilige Blogserie zu VCF mit NetApp

- "NetApp und VMware Cloud Foundation leicht gemacht Teil 1: Erste Schritte"
- "NetApp und VMware Cloud Foundation leicht gemacht Teil 2: VCF und ONTAP Principal Storage"
- "NetApp und VMware Cloud Foundation leicht gemacht Teil 3: VCF und Element Principal Storage"
- "NetApp und VMware Cloud Foundation leicht gemacht – Teil 4: ONTAP Tools für VMware und zusätzlichen Speicher"

VMware Cloud Foundation mit NetApp All-Flash SAN-Arrays

- "VCF mit NetApp ASA Arrays, Einführung und Technologieübersicht"
- "Verwenden Sie ONTAP mit FC als Hauptspeicher für Verwaltungsdomänen"
- "Verwenden Sie ONTAP mit FC als Hauptspeicher für VI-Workload-Domänen"
- "Verwenden Sie Ontap Tools, um iSCSI-Datenspeicher in einer VCF-Verwaltungsdomäne bereitzustellen"
- "Verwenden Sie Ontap Tools, um FC-Datenspeicher in einer VCF-Verwaltungsdomäne bereitzustellen"
- "Verwenden Sie Ontap Tools, um vVols (iSCSI)-Datenspeicher in einer VI-Workload-Domäne bereitzustellen"
- "Konfigurieren Sie NVMe über TCP-Datenspeicher für die Verwendung in einer VI-Workloaddomäne"
- "Bereitstellen und Verwenden des SnapCenter Plug-in for VMware vSphere zum Schutz und zur

Wiederherstellung von VMs in einer VI-Workloaddomäne"

- "Stellen Sie das SnapCenter Plug-in for VMware vSphere bereit und verwenden Sie es, um VMs in einer VI-Workloaddomäne (NVMe/TCP-Datenspeicher) zu schützen und wiederherzustellen."

VMware Cloud Foundation mit NetApp All-Flash AFF -Arrays

- "VCF mit NetApp AFF Arrays, Einführung und Technologieübersicht"
- "Verwenden Sie ONTAP mit NFS als Hauptspeicher für Verwaltungsdomänen"
- "Verwenden Sie ONTAP mit NFS als Hauptspeicher für VI-Workloaddomänen"
- "Verwenden Sie ONTAP Tools, um vVols (NFS)-Datenspeicher in einer VI-Workload-Domäne bereitzustellen"
- NetApp FlexPod -Lösungen für VMware Cloud Foundation*
- "Erweiterung der FlexPod Hybrid Cloud mit VMware Cloud Foundation"
- "FlexPod als Workload-Domäne für VMware Cloud Foundation"
- "FlexPod als Workload-Domäne für VMware Cloud Foundation – Designhandbuch"

Designoptionen mit VMware Cloud Foundation und ONTAP

Sie können mit VCF 9 neu beginnen oder vorhandene Bereitstellungen wiederverwenden, um mit VCF 9 und ONTAP eine Private Cloud-Umgebung zu erstellen. Informieren Sie sich über beliebte Design-Blueprints für VCF 9 und erfahren Sie, wie NetApp -Produkte einen Mehrwert bieten.

Speicheroptionen

VMware Cloud Foundation mit ONTAP unterstützt eine Vielzahl von Speicherkonfigurationen, um unterschiedliche Anforderungen an Leistung, Skalierbarkeit und Verfügbarkeit zu erfüllen. In den folgenden Tabellen sind die wichtigsten und zusätzlichen Speicheroptionen zusammengefasst, die für Ihre Umgebung verfügbar sind.

Produktfamilie	VMFS auf FC	NFSv3
ASA A-Serie und C-Serie	Ja	Nein
AFF A-Serie und C-Serie	Ja	Ja
FAS	Ja	Ja

Produktfamilie	VMFS auf FC	VMFS auf iSCSI	VMFS auf NVMe-oF	NFSv3	NFSv4.1
ASA A-Serie und C-Serie	Ja	Ja	Ja	Nein	Nein
AFF A-Serie und C-Serie	Ja	Ja	Ja	Ja	Ja
FAS	Ja	Ja	Ja	Ja	Ja

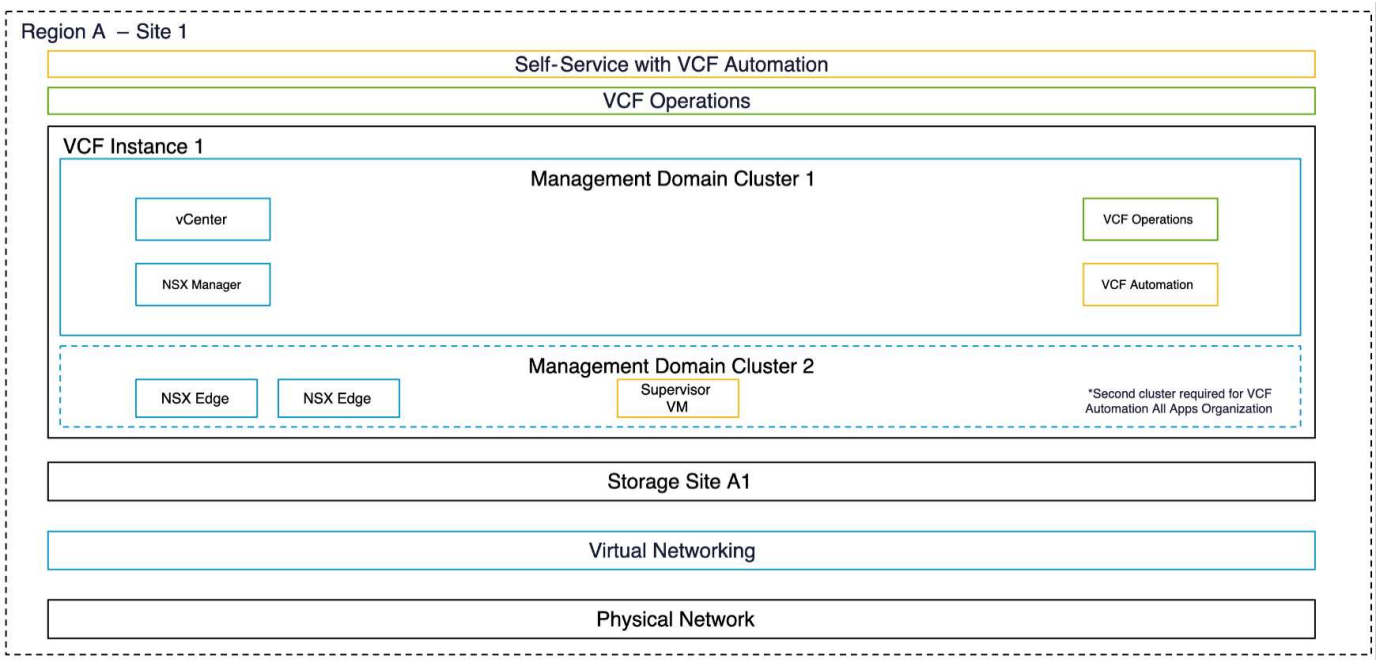
Blaupausen

Die folgenden Blueprints veranschaulichen gängige Bereitstellungsmodelle für VMware Cloud Foundation und

ONTAP in verschiedenen Site- und Ressourcenszenarien.

VCF-Flotte an einem einzigen Standort mit minimalem Platzbedarf

Dieser Entwurf dient der Bereitstellung von Management- und Workload-Komponenten in einem einzelnen vSphere-Cluster mit minimalen Ressourcen. Es unterstützt VMFS- und NFSv3-Principal-Datastores und eine einfache Bereitstellungsoption mit einer Zwei-Knoten-Konfiguration. Wenn Sie VCF Automation mit dem All Apps Organization-Modell verwenden möchten, benötigen Sie einen zweiten Cluster, um vSphere Supervisor- und NSX Edge-Knoten bereitzustellen.



Um den Ressourcenverbrauch zu minimieren, verwenden Sie nach Möglichkeit eine vorhandene ONTAP -Tools-Instanz. Falls nicht verfügbar, ist ein einzelner Knoten mit einem kleinen Profil geeignet. Das SnapCenter Plug-in for VMware vSphere schützt virtuelle Maschinen und Datenspeicher mithilfe nativer Snapshots und Replikation auf ein anderes ONTAP -Speicherarray.

> Wenn Ihnen die Ressourcen fehlen, um VCF zu erkunden, bieten viele Cloud-Anbieter VCF als Service an und ONTAP ist als First-Party-Service von Cloud-Anbietern verfügbar.

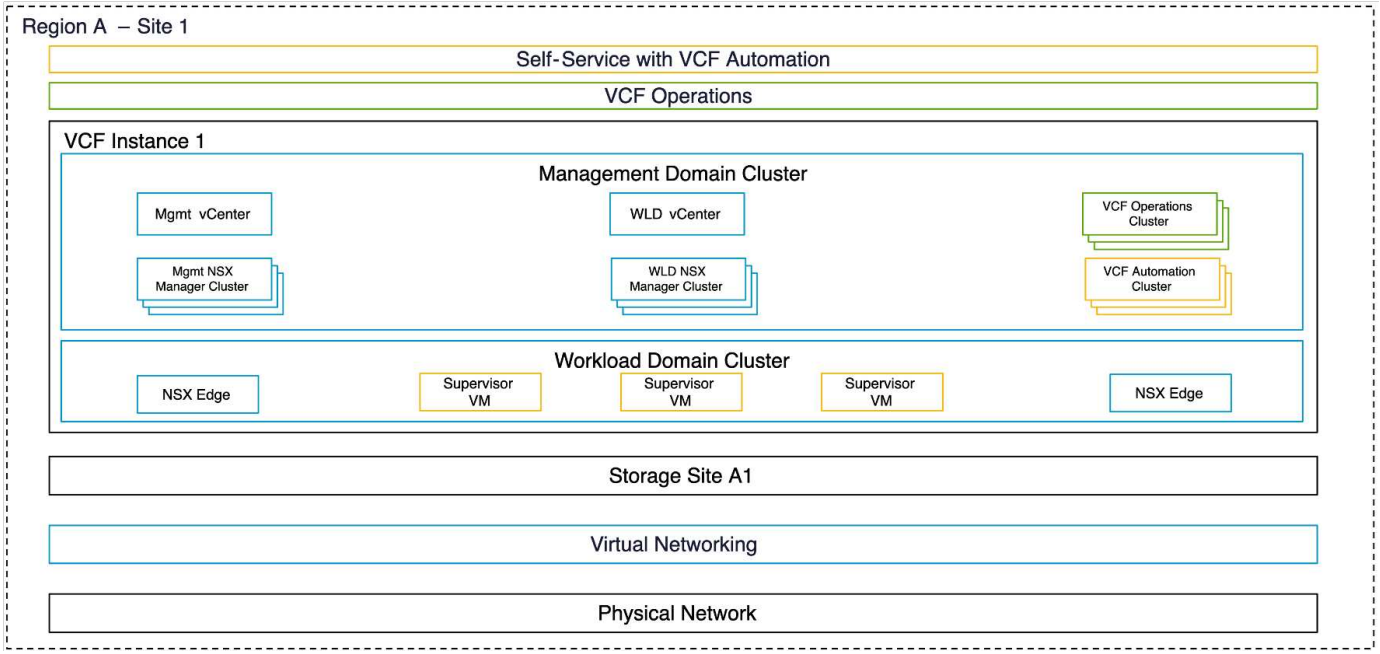
Weitere Einzelheiten zu diesem Design finden Sie im"Technische Dokumentation von Broadcom zur VCF-Flotte an einem einzigen Standort mit minimalem Platzbedarf" .

VCF-Flotte an einem einzigen Standort

Dieser Entwurf ist für Kunden mit einem einzigen primären Rechenzentrum gedacht, die auf die Hochverfügbarkeit von Anwendungen angewiesen sind. Normalerweise handelt es sich dabei um eine einzelne VCF-Umgebung. Sie können ASA für Block-Workloads und AFF für Datei-/Unified-Workloads verwenden.

Content Repository teilt VM-Vorlagen und Container-Registries über VCF-Domänen hinweg. Beim Hosten auf FlexGroup Volume ist die FlexCache -Funktion für den Abonnement-Datenspeicher verfügbar.

> Das Hosten von VMs auf FlexCache Datastore wird nicht unterstützt.



Eine einzelne Instanz von ONTAP Tools im HA-Modus kann alle vCenter in der VCF-Flotte verwalten. Weitere Informationen finden Sie im"Konfigurationsgrenzen von ONTAP -Tools" für weitere Informationen. ONTAP -Tools lassen sich in die intelligente Gruppierung von VCF SSO und VCF OPS integrieren, um den Zugriff auf mehrere vCenter in derselben Benutzeroberfläche zu ermöglichen.

Ergänzender VCF-Datenspeicher mit ONTAP -Tools

Sie müssen das SnapCenter Plug-in auf jeder vCenter-Instanz bereitstellen, um VM und Datastore zu schützen.

Die auf Speicherrichtlinien basierende Verwaltung wird mit vSphere Supervisor verwendet, um VMs von VKS zu hosten. Tags werden zentral bei VCF Ops verwaltet. NetApp Trident CSI wird mit VKS zum Schutz von Anwendungssicherungen mithilfe nativer Array-Funktionen verwendet. Wenn Sie vSphere CSI verwenden, werden persistente Volumedetails in der VCF-Automatisierung angezeigt.

Weitere Einzelheiten zu diesem Entwurf finden Sie im"Technische Dokumentation von Broadcom zur VCF-Flotte an einem einzigen Standort" .

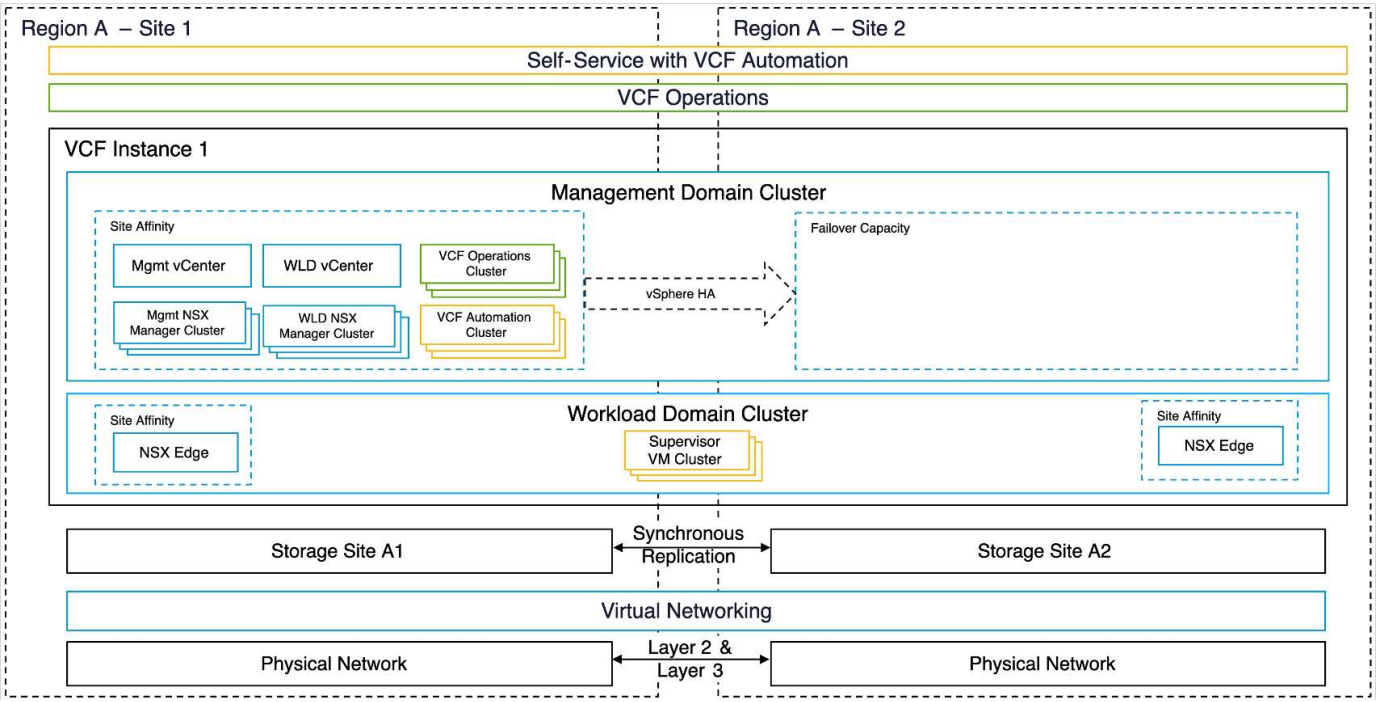
VCF-Flotte mit mehreren Standorten in einer einzigen Region

Dieses Design ist für Kunden gedacht, die Cloud-ähnliche Dienste mit höherer Verfügbarkeit bereitstellen, indem sie Arbeitslasten auf verschiedene Fehlerdomänen verteilen.

Für VMFS-Datenspeicher bietet SnapMirror Active Sync eine Active-Active-Speichereinheit zur Verwendung mit vSphere Metro Storage Cluster. Der einheitliche Zugriffsmodus bietet transparentes Speicher-Failover, während der nicht einheitliche Zugriffsmodus bei einem Fehlerdomänenfehler einen Neustart der VM erfordert.

Für NFS-Datenspeicher gewährleistet ONTAP MetroCluster mit vSphere Metro Storage Cluster eine hohe Verfügbarkeit. Ein Mediator vermeidet Split-Brain-Szenarien und kann jetzt auf BlueXP gehostet werden.

VM-Platzierungsregeln steuern VMs innerhalb derselben Fehlerdomäne für Managementdomänenkomponenten.



ONTAP -Tools bieten eine Benutzeroberfläche zum Einrichten aktiver SnapMirror -Synchronisierungsbeziehungen. Speichersysteme beider Fehlerdomänen müssen in ONTAP -Tools und im SnapCenter Plug-in for VMware vSphere registriert werden.

Sie können 3-2-1-Sicherungsrichtlinien mit BlueXP Backup and Recovery für VMs über SnapMirror und SnapMirror to Cloud implementieren. Sie können Wiederherstellungen von jedem der drei Standorte aus durchführen.

Trident Protect oder BlueXP Backup and Recovery für Kubernetes schützen VKS-Clusteranwendungen.

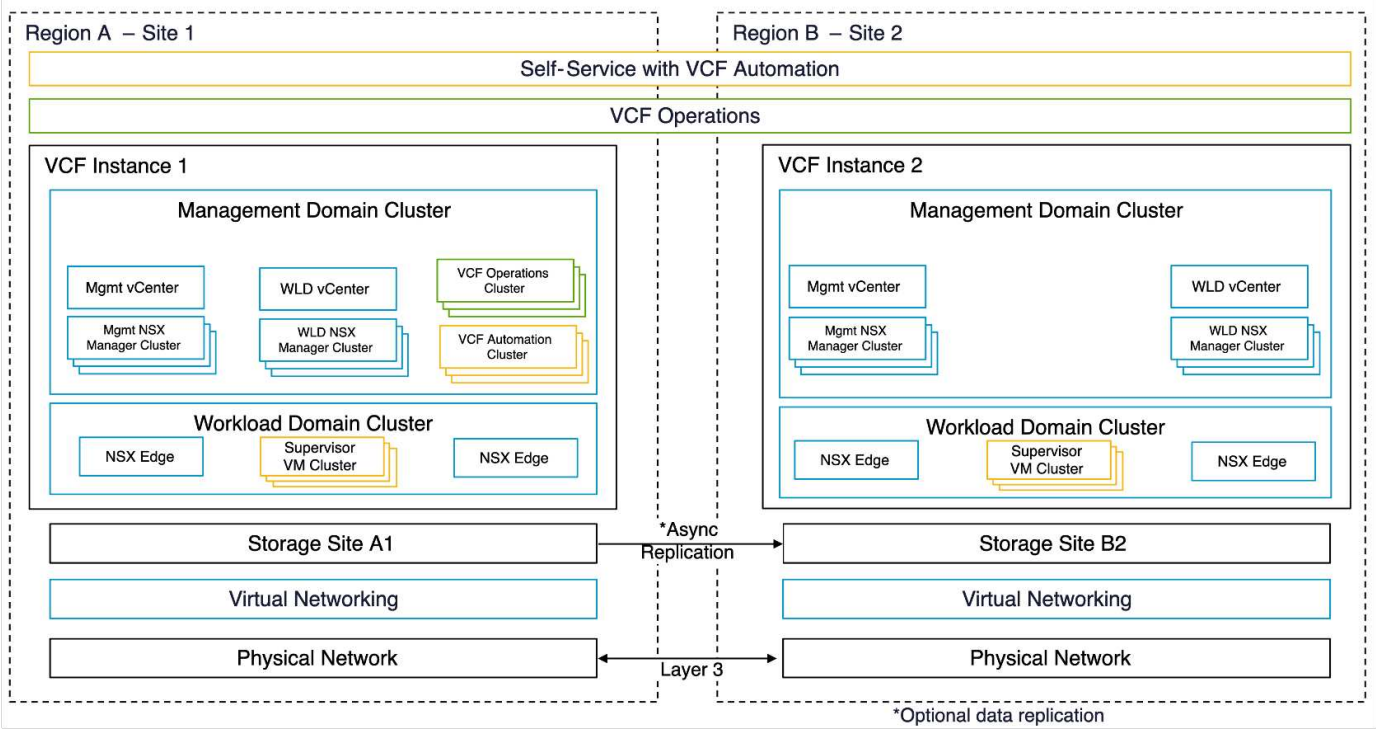
Weitere Informationen finden Sie im"Technische Dokumentation von Broadcom zur VCF-Flotte mit mehreren Standorten in einer einzigen Region" .

VCF-Flotte mit mehreren Standorten in mehreren Regionen

Dieses Design ist für weltweit verteilte Kunden gedacht und bietet Dienste in unmittelbarer Nähe sowie Lösungen zur Notfallwiederherstellung.

Sie können die Notfallwiederherstellung für VMs mit VMware Live Site Recovery oder BlueXP Disaster Recovery as a Service verwalten. ONTAP -Tools bieten den SRA (Storage Replication Adapter) zur Orchestrierung von Speichervorgängen mit ONTAP.

Produktfamilie	SnapMirror aktive Synchronisierung	MetroCluster
ASA A-Serie und C-Serie	Ja	Ja
AFF A-Serie und C-Serie	Ja	Ja
FAS	Nein	Ja



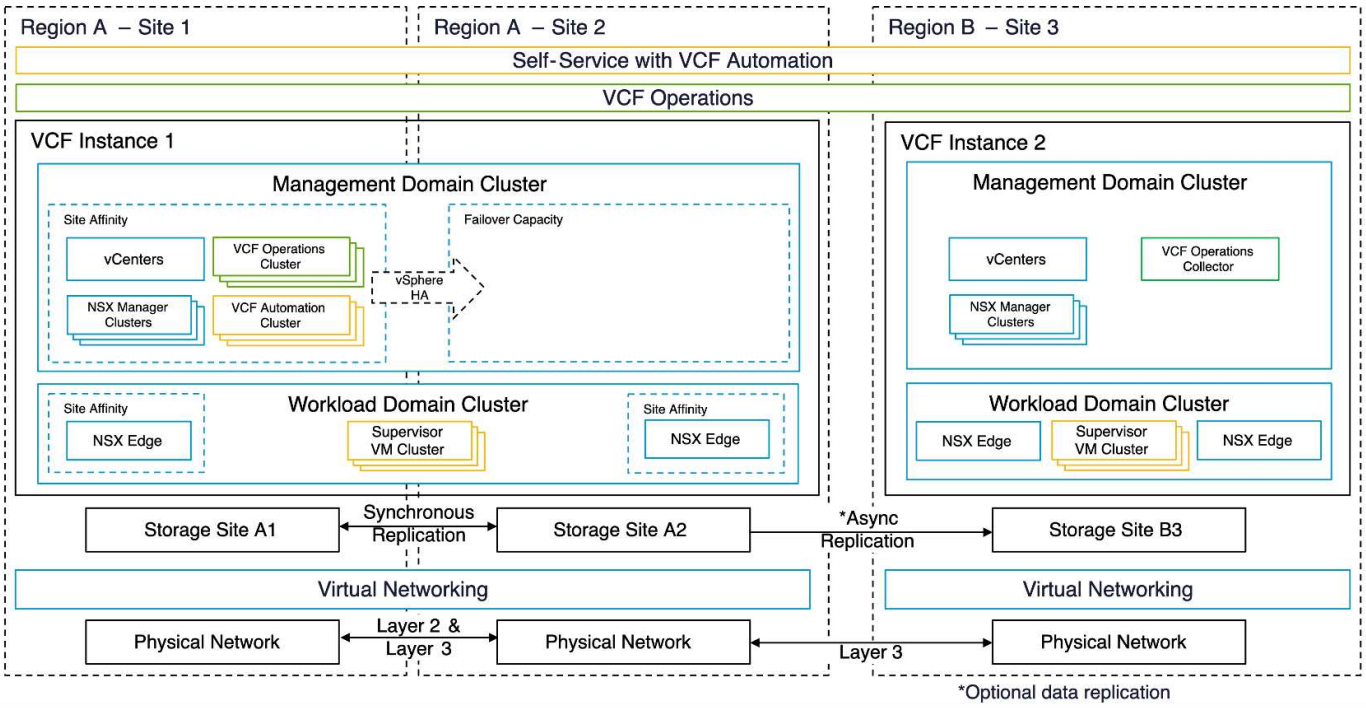
ONTAP -Tools bieten eine Benutzeroberfläche für die Einrichtung der Datenspeicherreplikation. BlueXP kann auch zur Replikation zwischen Speicher-Arrays verwendet werden. Das SnapCenter Plug-in for VMware vSphere nutzt vorhandene SnapMirror -Beziehungen für SnapShots.

Weitere Informationen finden Sie im"Technische Dokumentation von Broadcom zur VCF-Flotte mit mehreren Standorten in mehreren Regionen" .

VCF-Flotte mit mehreren Standorten in einer einzigen Region und zusätzlichen Regionen

Dieses Design berücksichtigt sowohl die Verfügbarkeit als auch die Notfallwiederherstellung von VMs und VKS-Anwendungen.

ASA, AFF und FAS unterstützen diese Designoption.



Sie können ONTAP Tools oder BlueXP verwenden, um die Replikationsbeziehung einzurichten.

Weitere Informationen finden Sie im "Technische Dokumentation von Broadcom zur VCF-Flotte mit mehreren Standorten in einer einzelnen Region und zusätzlichen Regionen" .

Einrichten privater Cloud-Umgebungen mit VMware Cloud Foundation und ONTAP

Stellen Sie VMware Cloud Foundation 9-Umgebungen mit ONTAP bereit, konvergieren Sie sie oder aktualisieren Sie sie. Erfahren Sie, wie Sie neue VCF 9.0-Umgebungen einrichten, vorhandene vCenter-Instanzen und ONTAP -Datenspeicher zusammenführen und frühere VCF-Bereitstellungen aktualisieren.

Bereitstellen einer neuen VCF 9-Instanz

Verwenden Sie diesen Workflow, um eine saubere VMware Cloud Foundation (VCF) 9.0-Umgebung bereitzustellen. Nach der Bereitstellung können Sie Workloads migrieren oder mit der Bereitstellung von Anwendungen und Infrastrukturdiensten beginnen.

Die wichtigsten Schritte finden Sie im"Build Journey – Installieren einer neuen VMware Cloud Foundation-Bereitstellung" .

Schritte

1. Folgen Sie den"Broadcom VCF 9-Bereitstellungsschritte" .
2. Führen Sie im Schritt „Bereitstellungsvorbereitung“ die Aufgaben für Ihre Hauptspeicheroption aus.

VMFS auf FC

1. Erfassen Sie die WWPNs für alle ESXi-Hosts. Du kannst laufen `esxcli storage san fc list`, verwenden Sie den ESXi Host Client oder PowerCLI.
2. Konfigurieren Sie die Zoneneinteilung. Sehen "Empfohlene FC-Zoning-Konfigurationen für ONTAP -Systeme" .

   Verwenden Sie die WWPNs der logischen SVM-Schnittstellen (LIFs), nicht die WWPNs des physischen Adapters.

3. Erstellen Sie eine LUN und ordnen Sie sie den Hosts per WWPN mithilfe von System Manager, der ONTAP CLI oder der API zu.
4. Scannen Sie den Speicheradapter auf ESXi erneut und erstellen Sie den VMFS-Datenspeicher.

NFSv3

1. Erstellen Sie eine VMkernel-Schnittstelle auf einem ESXi-Host.
2. Stellen Sie sicher, dass"SVM hat NFS aktiviert" Und"vStorage über NFS ist aktiviert" .
3. Erstellen Sie ein Volume und exportieren Sie es mit einer Richtlinie, die die ESXi-Hosts zulässt.
4. Passen Sie die Berechtigungen nach Bedarf an.
5. Stellen Sie das ONTAP NFS VAAI VIB bereit und fügen Sie es in das vLCM-Image ein. Zum Beispiel: `esxcli software vib install -d /NetAppNasPlugin2.0.1.zip`. (Laden Sie die ZIP-Datei von der NetApp Support-Site herunter.)
6. Mounten Sie das NFS-Volume auf dem Host, auf dem Sie die VMkernel-Schnittstelle erstellt haben. Zum Beispiel: `esxcli storage nfs add -c 4 -H 192.168.122.210 -s /use1_m01_nfs01 -v use1-m01-cl01-nfs01`.

   Der `nConnect` Die Sitzungsanzahl gilt pro Host. Aktualisieren Sie nach der Bereitstellung bei Bedarf andere Hosts.

1. Führen Sie am Ende von **Überprüfen Sie die Bereitstellungszusammenfassung und prüfen Sie die nächsten Schritte** in der Phase **VCF-Flotte bereitstellen** Folgendes aus:
   a. Bereitstellen von ONTAP -Tools
      - "ONTAP Tools 10.x herunterladen"von der NetApp Support-Site.
      - Erstellen Sie DNS-Einträge für den ONTAP Tools Manager, Knoten und die virtuelle IP, die für die interne Kommunikation verwendet wird.
      - Stellen Sie die OVA auf dem Verwaltungs-vCenter-Server bereit.
      - "Registrieren Sie das vCenter der Verwaltungsdomäne"mit ONTAP Tools Manager.
      - "Hinzufügen des Speicher-Backends"mithilfe der vSphere-Client-Benutzeroberfläche.
      - "Erstellen eines zusätzlichen Datenspeichers"(einschließlich eines für das Inhaltsregister).
      - Erstellen Sie die Inhaltsregistrierung, wenn Sie eine HA-Bereitstellung planen.
      - "Aktivieren von HA"im ONTAP Tools Manager.
   b. Bereitstellen des SnapCenter -Plug-Ins
      - "Bereitstellen des SnapCenter Plug-in for VMware vSphere" .

        - "Hinzufügen des Speicher-Backends" .
        - "Erstellen von Sicherungsrichtlinien" .
        - "Erstellen von Ressourcengruppen" .
    c. Stellen Sie den BlueXP Connector bereit
        - "Überprüfen Sie, was Sie ohne Connector tun können" .
        - "Bereitstellen des Connectors" .
    d. Verwenden Sie BlueXP für Backup und Wiederherstellung
        - "Schützen Sie VM -Workloads" .
        - "Schützen Sie VKS -Workloads" .
2. Nachdem Sie vCenter als Workload-Domäne in die VCF-Instanz importiert haben, führen Sie die folgenden Schritte aus:
    a. ONTAP -Tools registrieren
        - "Registrieren Sie das vCenter der Workloaddomäne"mit ONTAP Tools Manager.
        - "Hinzufügen des Speicher-Backends"mithilfe der vSphere-Client-Benutzeroberfläche.
        - "Erstellen eines zusätzlichen Datenspeichers" .
    b. Bereitstellen des SnapCenter Plug-in for VMware vSphere
        - "Bereitstellen des SnapCenter Plug-in for VMware vSphere" .
        - "Hinzufügen des Speicher-Backends" .
        - "Erstellen von Sicherungsrichtlinien" .
        - "Erstellen von Ressourcengruppen" .
    c. Verwenden Sie BlueXP für Backup und Wiederherstellung
        - "Schützen Sie VM -Workloads" .
        - "Schützen Sie VKS -Workloads" .

Sie können diese Schritte immer wieder verwenden, wenn Sie eine neue Workloaddomäne erstellen.

Konvergieren Sie vorhandene Komponenten in VCF 9

Möglicherweise verfügen Sie bereits über einige Komponenten der VCF-Flotte und möchten diese lieber wiederverwenden. Wenn Sie eine vCenter-Instanz wiederverwenden, werden Datenspeicher häufig mit ONTAP Tools bereitgestellt, die als Hauptspeicher für VCF dienen können.

Voraussetzungen

- Bestätigen Sie, dass vorhandene vCenter-Instanzen funktionsfähig sind.
- Überprüfen Sie, ob von ONTAP bereitgestellte Datenspeicher verfügbar sind.
- Gewährleisten Sie den Zugriff auf"Interoperabilitätsmatrix" .

Schritte

1. Überprüfen Sie die"unterstützte Szenarien zur Konvergenz zu VCF" .
2. Konvergieren Sie eine vCenter-Instanz mit von ONTAP bereitgestellten Datenspeichern als Hauptspeicher.
3. Überprüfen Sie die unterstützten Versionen mithilfe des"Interoperabilitätsmatrix" .

4. Upgrade"ONTAP -Tools" falls erforderlich.
5. Aktualisieren Sie die"SnapCenter -Plugin für VMware vSphere" falls erforderlich.

Aktualisieren Sie eine vorhandene VCF-Umgebung auf VCF 9

Aktualisieren Sie eine frühere VCF-Bereitstellung mithilfe des Standard-Upgradeprozesses auf Version 9.0. Das Ergebnis ist eine VCF-Umgebung mit Version 9.0 und aktualisierten Verwaltungs- und Workloaddomänen.

Voraussetzungen

- Sichern Sie die Verwaltungsdomäne und die Workloaddomänen.
- Überprüfen Sie die Kompatibilität von ONTAP Tools und SnapCenter -Plug-in mit VCF 9.0. Folgen Sie den"Interoperabilitätsmatrix" Zu"Upgrade der ONTAP -Tools" Und"SnapCenter -Plugin für VMware vSphere" die für VCF 9 unterstützt werden.

Schritte

1. Aktualisieren Sie die VCF-Verwaltungsdomäne. Sehen"Aktualisieren Sie die VCF-Verwaltungsdomäne auf VCF 9" Anweisungen hierzu finden Sie unter.
2. Aktualisieren Sie alle VCF 5.x-Workloaddomänen. Sehen"Upgrade der VCF 5.x-Workloaddomäne auf VCF 9" Anweisungen hierzu finden Sie unter.

Implementierung von Disaster Recovery mit NetApp SnapMirror und BlueXP DRaaS

VCF-Disaster-Recovery-Lösung für NFS-Datenspeicher mit NetApp SnapMirror und BlueXP DRaaS

Die Replikation auf Blockebene von einem Produktionsstandort zu einem Disaster Recovery-Standort (DR) bietet eine robuste und kostengünstige Strategie zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen, einschließlich Ransomware-Angriffen. Mithilfe der NetApp SnapMirror Replikation können VMware VCF 9-Workloaddomänen, die auf lokalen ONTAP Systemen ausgeführt werden (unter Verwendung von NFS- oder VMFS-Datenspeichern), auf ein sekundäres ONTAP -System repliziert werden, das sich in einem dafür vorgesehenen Wiederherstellungs-Rechenzentrum befindet, in dem auch VMware bereitgestellt wird.

In diesem Abschnitt wird die Konfiguration von BlueXP Disaster Recovery as a Service (DRaaS) zur Einrichtung von DR für lokale virtuelle VMware-Maschinen beschrieben.

Das Setup umfasst:

- Erstellen eines BlueXP -Kontos und Bereitstellen eines BlueXP Connectors.
- Hinzufügen von ONTAP Arrays zum BlueXP Canvas, um die Kommunikation zwischen VMware vCenter und ONTAP -Speicher zu erleichtern.
- Konfigurieren der Replikation zwischen Standorten mit SnapMirror.
- Einrichten und Testen eines Wiederherstellungsplans zur Validierung der Failover-Bereitschaft.

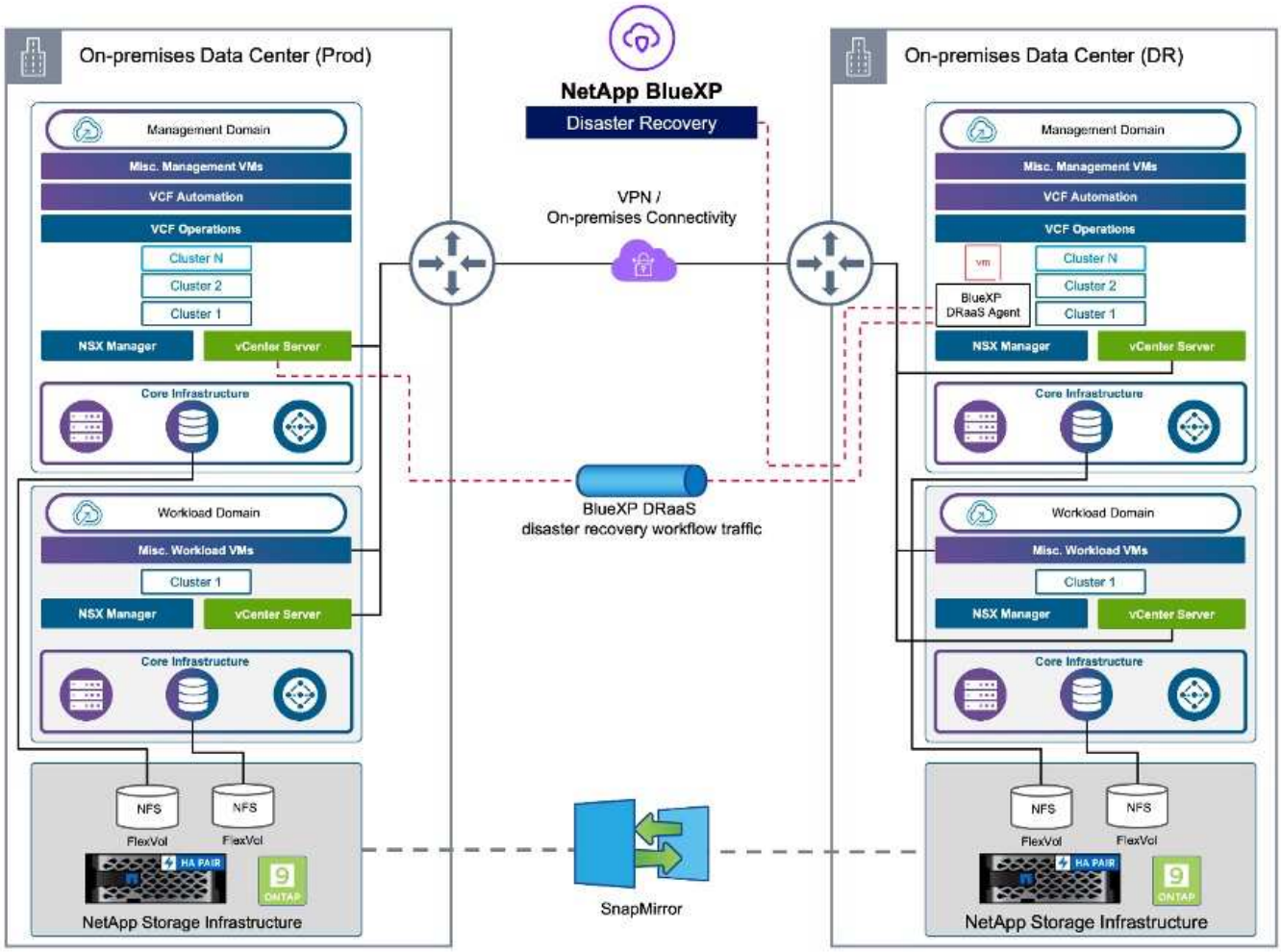
Der in die NetApp BlueXP Konsole integrierte BlueXP disaster recovery -Dienst ermöglicht Unternehmen die nahtlose Erkennung ihrer lokalen VMware vCenter- und ONTAP Speichersysteme. Nach der Erkennung können Administratoren Ressourcengruppierungen definieren, Notfallwiederherstellungspläne erstellen, diese mit den entsprechenden Ressourcen verknüpfen und Failover- und Failback-Vorgänge einleiten oder testen. NetApp SnapMirror bietet eine effiziente Replikation auf Blockebene und stellt sicher, dass der DR-Standort

durch inkrementelle Updates mit der Produktionsumgebung synchronisiert bleibt. Dies ermöglicht ein Recovery Point Objective (RPO) von nur fünf Minuten.

BlueXP DRaaS unterstützt auch unterbrechungsfreie Disaster-Recovery-Tests. Durch Nutzung der FlexClone -Technologie von ONTAP werden platzsparende, temporäre Kopien des NFS-Datenspeichers aus dem aktuellsten replizierten Snapshot erstellt – ohne Auswirkungen auf die Produktionsarbeitslast oder zusätzliche Speicherkosten. Nach dem Testen kann die Umgebung problemlos abgebaut werden, wobei die Integrität der replizierten Daten erhalten bleibt.

Im Falle eines tatsächlichen Failovers orchestriert BlueXP den Wiederherstellungsprozess und ruft geschützte virtuelle Maschinen am vorgesehenen DR-Standort automatisch und mit minimalem Benutzereingriff auf. Wenn die primäre Site wiederhergestellt ist, kehrt der Dienst die SnapMirror -Beziehung um und repliziert alle Änderungen zurück auf die ursprüngliche Site, wodurch ein reibungsloses und kontrolliertes Failback ermöglicht wird.

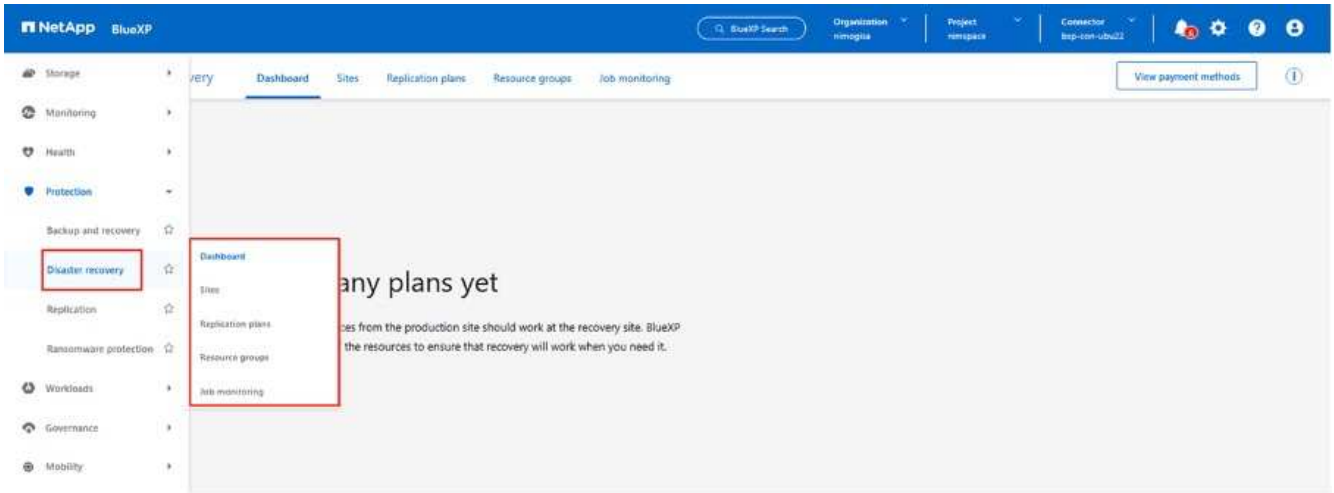
Alle diese Funktionen werden im Vergleich zu herkömmlichen Disaster-Recovery-Lösungen zu deutlich geringeren Kosten bereitgestellt.



Erste Schritte

Um mit der BlueXP disaster recovery zu beginnen, verwenden Sie die BlueXP -Konsole und greifen Sie dann auf den Dienst zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste von BlueXP „Schutz“ > „Notfallwiederherstellung“ aus.
3. Das BlueXP disaster recovery wird angezeigt.



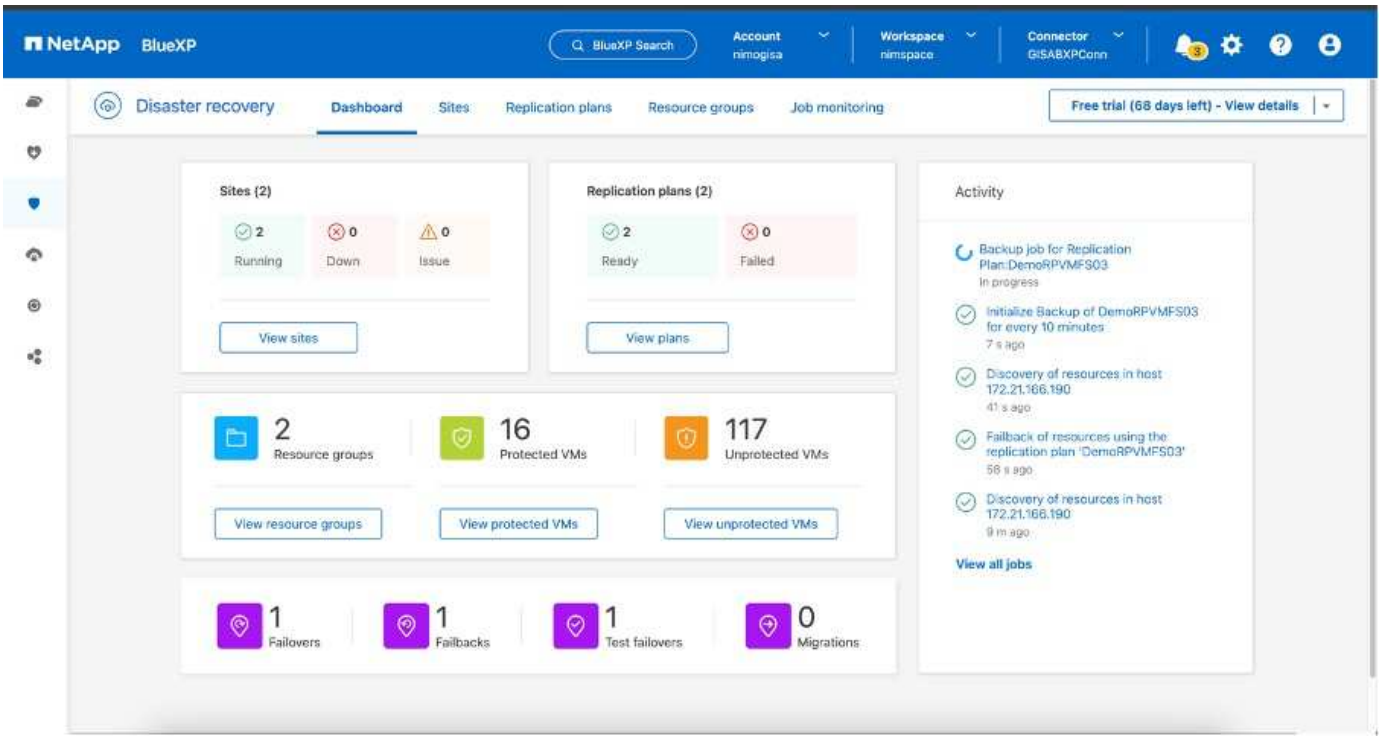
Stellen Sie vor der Konfiguration des Notfallwiederherstellungsplans Folgendes sicher"Voraussetzungen" erfüllt sind:

- BlueXP Connector wird in NetApp BlueXP eingerichtet.
- Die BlueXP Connector-Instanz verfügt über Konnektivität zum vCenter und den Speichersystemen der Quell- und Ziel-Workloaddomäne.
- NetApp Data ONTAP Cluster zur Bereitstellung von NFS- oder VMFS-Datenspeichern.
- In BlueXP werden lokale NetApp -Speichersysteme hinzugefügt, die NFS- oder VMFS-Datenspeicher für VMware hosten.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen NFS- oder VMFS-basierten Datenspeichervolumes konfiguriert.
- Stellen Sie sicher, dass die Umgebung über unterstützte Versionen von vCenter Server und ESXi-Servern verfügt.

Sobald die Verbindung zwischen Quell- und Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte einige Klicks dauern und etwa 3 bis 5 Minuten dauern.

Hinweis: NetApp empfiehlt, den BlueXP Connector am Zielstandort oder an einem dritten Standort bereitzustellen, damit der BlueXP Connector über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.

In dieser Demonstration werden die Workload-Domänen mit ONTAP NFS-Speicher konfiguriert. Die Schritte im Hinblick auf den Workflow bleiben für VMFS-basierte Datenspeicher gleich.



BlueXP disaster recovery

Der erste Schritt bei der Vorbereitung der Notfallwiederherstellung besteht darin, die Quell-vCenter- und Speicherressourcen zu ermitteln und zur BlueXP disaster recovery hinzuzufügen.

Öffnen Sie die BlueXP -Konsole und wählen Sie in der linken Navigation „Schutz“ > „Notfallwiederherstellung“. Wählen Sie „vCenter-Server ermitteln“ oder verwenden Sie das Hauptmenü. Wählen Sie „Sites > Hinzufügen > vCenter hinzufügen“.

Fügen Sie die folgenden Plattformen hinzu:

- Quell-Workloaddomäne vCenter
- Ziel-Workloaddomäne vCenter.

Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array

SnapMirror bietet Datenreplikation in einer NetApp Umgebung. Die SnapMirror -Replikation basiert auf der NetApp Snapshot®-Technologie und ist äußerst effizient, da sie nur die Blöcke repliziert, die seit dem letzten Update geändert oder hinzugefügt wurden. SnapMirror lässt sich einfach mithilfe von NetApp OnCommand® System Manager oder der ONTAP CLI konfigurieren. BlueXP DRaaS erstellt auch die SnapMirror -Beziehung, sofern Cluster- und SVM-Peering zuvor konfiguriert wurden.

In Fällen, in denen der primäre Speicher nicht vollständig verloren geht, bietet SnapMirror eine effiziente Möglichkeit zur Neusynchronisierung der primären und DR-Sites. SnapMirror kann die beiden Sites neu synchronisieren und nur geänderte oder neue Daten von der DR-Site zurück zur primären Site übertragen, indem einfach die SnapMirror Beziehungen umgekehrt werden. Dies bedeutet, dass Replikationspläne in BlueXP DRaaS nach einem Failover in beide Richtungen neu synchronisiert werden können, ohne das gesamte Volume erneut zu kopieren. Wenn eine Beziehung in umgekehrter Richtung erneut synchronisiert wird, werden nur neue Daten an das Ziel zurückgesendet, die seit der letzten erfolgreichen Synchronisierung

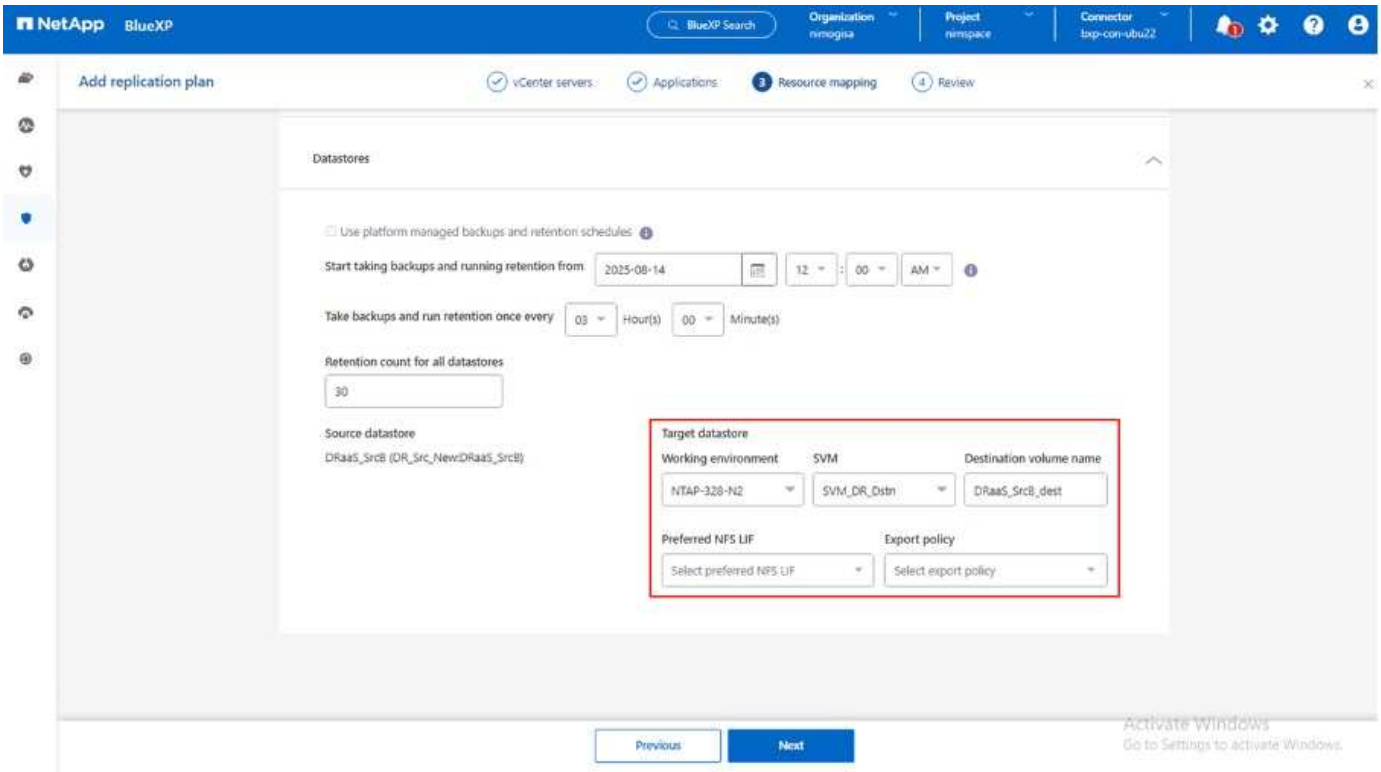
der Snapshot-Kopie geschrieben wurden.

> Wenn die SnapMirror -Beziehung für das Volume bereits über CLI oder System Manager konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.

So richten Sie es für VMware Disaster Recovery ein

Der Vorgang zum Erstellen der SnapMirror Replikation bleibt für jede Anwendung derselbe. Der Vorgang kann manuell oder automatisiert erfolgen. Am einfachsten ist es, BlueXP DRaaS zu nutzen, das dies automatisiert, sofern die folgenden beiden Kriterien erfüllt sind:

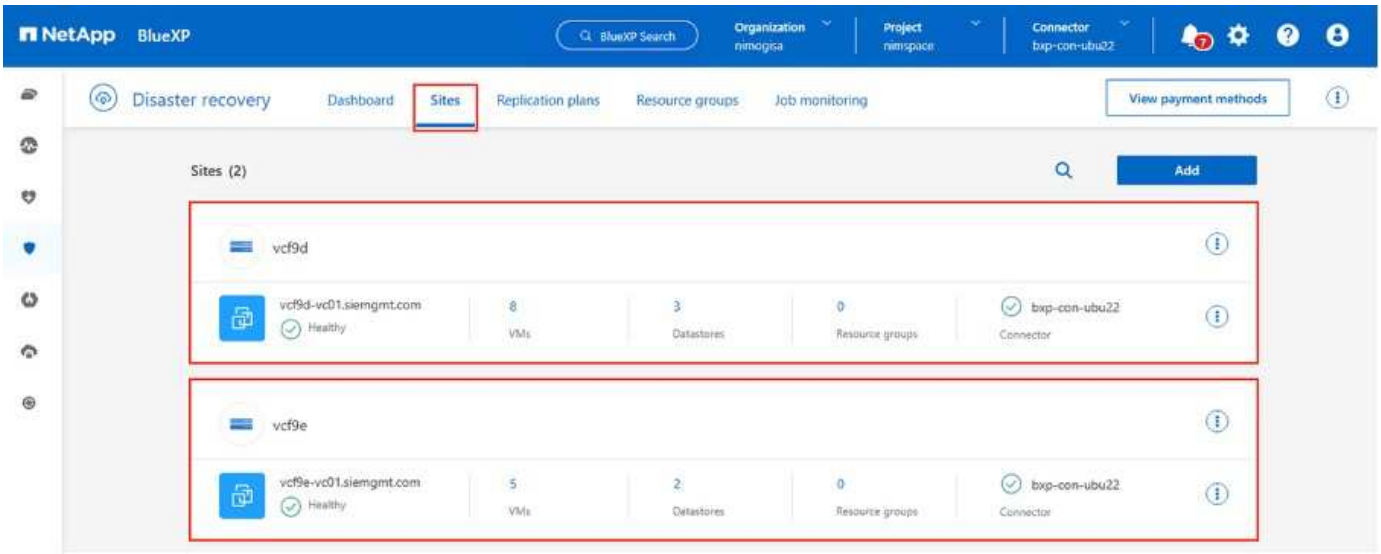
- Quell- und Zielcluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



BlueXP bietet auch eine alternative Option zum Konfigurieren der SnapMirror Replikation durch einfaches Ziehen und Ablegen des Quell- ONTAP -Systems in der Umgebung auf das Ziel, um den Assistenten auszulösen, der durch den Rest des Prozesses führt.

Was kann BlueXP disaster recovery für Sie tun?

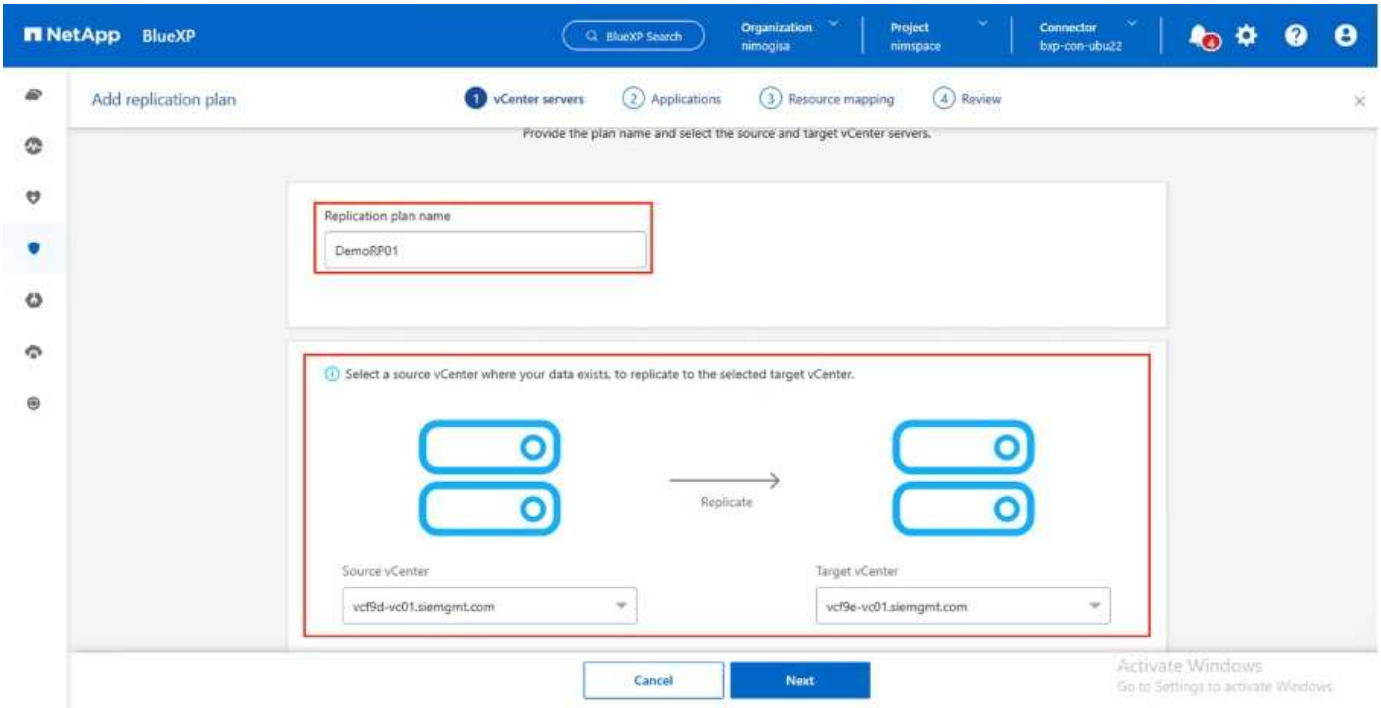
Nachdem die Quell- und Zielsites hinzugefügt wurden, führt die BlueXP disaster recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Die BlueXP disaster recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.



Nachdem die Sites hinzugefügt wurden, konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

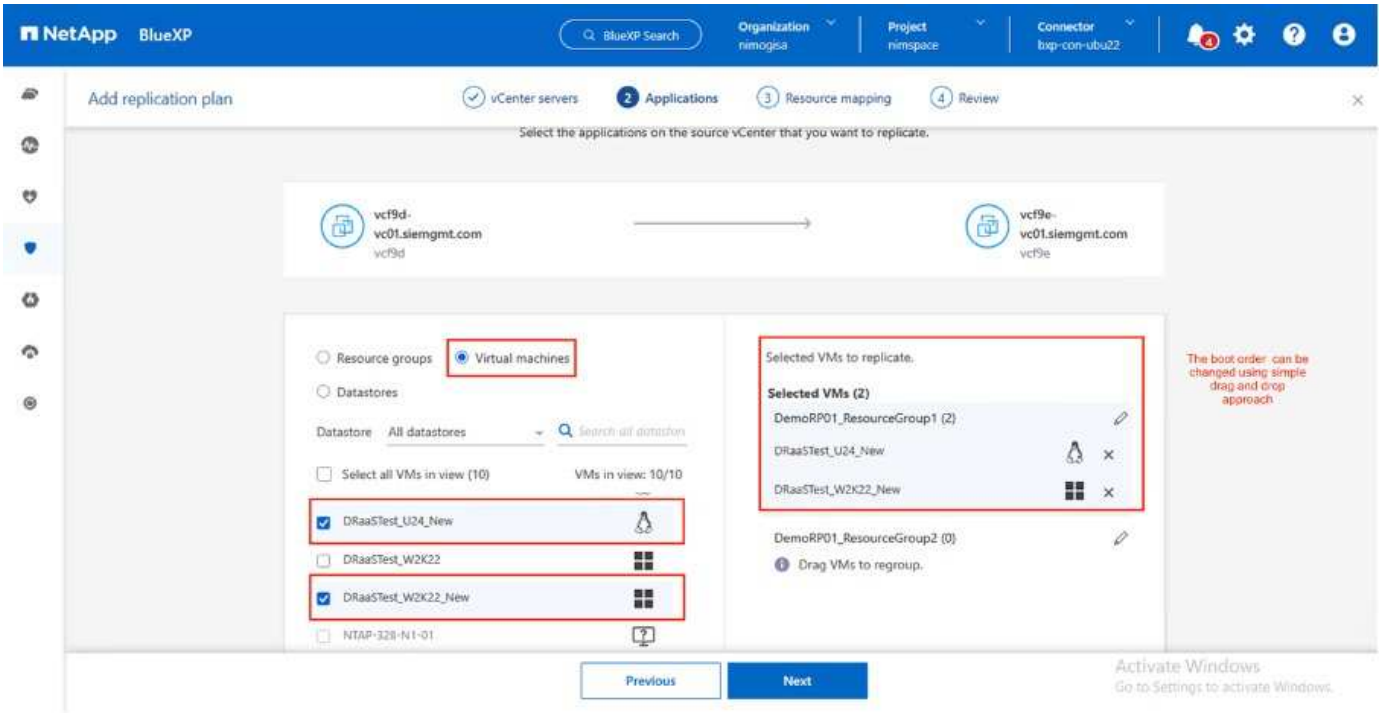
In diesem Schritt können die VMs in Ressourcengruppen gruppiert werden. Mit den BlueXP disaster recovery können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen und Startverzögerungen enthalten, die bei der Wiederherstellung ausgeführt werden können. Die Ressourcengruppe kann auch über die Registerkarte „Ressourcengruppe“ erstellt werden.

Wählen Sie zuerst das Quell-vCenter und dann das Ziel-vCenter aus.



Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend

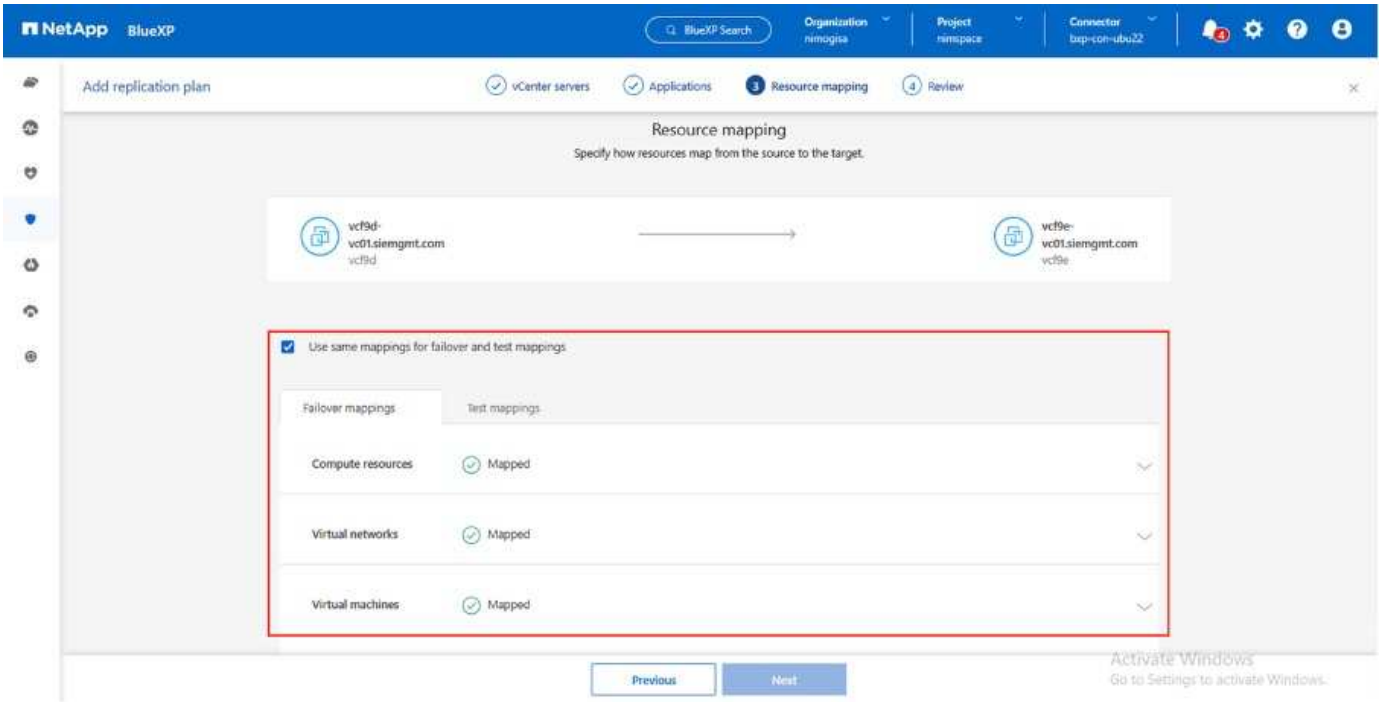
auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.



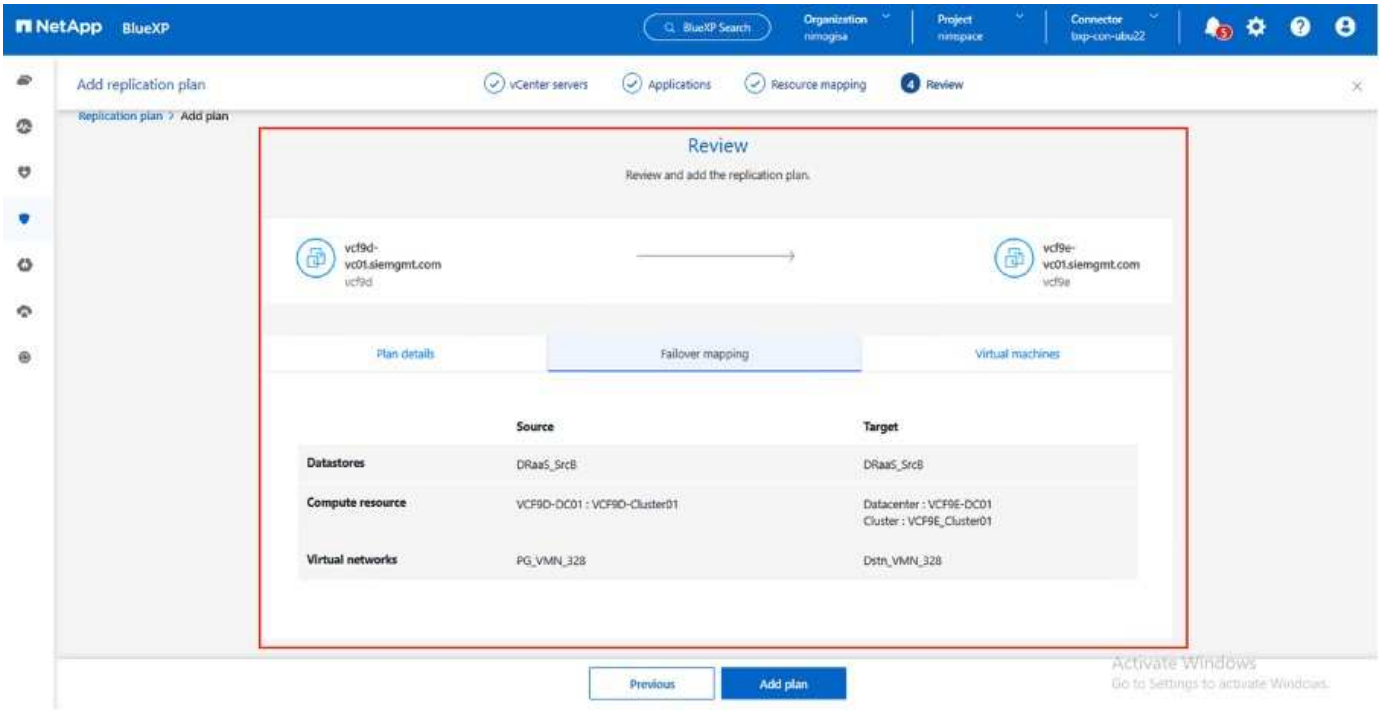
Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

Sobald die Ressourcengruppen über den Replikationsplan erstellt wurden, besteht der nächste Schritt darin, den Blueprint oder eine Zuordnung auszuwählen, um virtuelle Maschinen und Anwendungen im Katastrophenfall wiederherzustellen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen, virtuelle Netzwerke, IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Anwendungskonsistenz und so weiter. Ausführliche Informationen finden Sie unter"Erstellen eines Replikationsplans" . Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des Replikationsplans angegeben wurden.

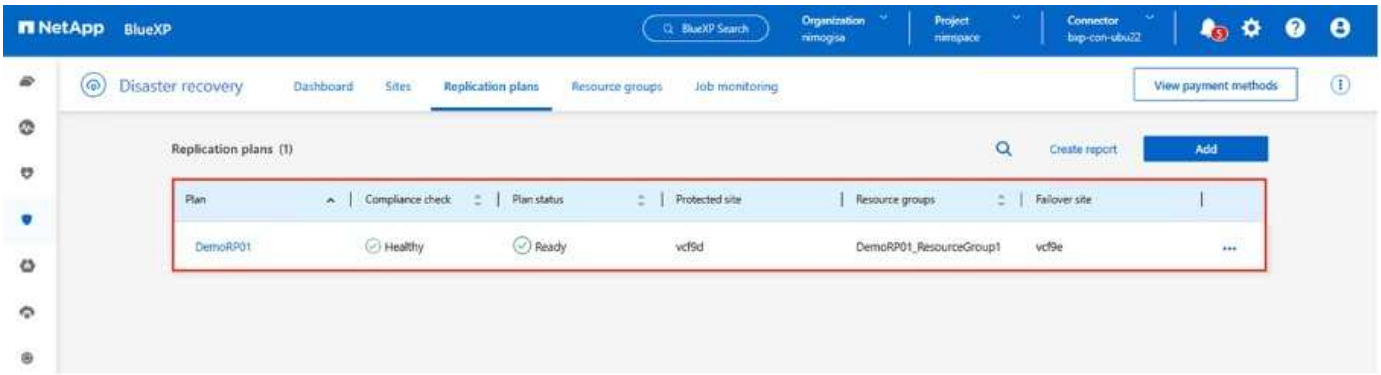
Hinweis: Standardmäßig werden für Test- und Failover-Vorgänge dieselben Zuordnungsparameter verwendet. Um unterschiedliche Zuordnungen für die Testumgebung festzulegen, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen „Gleiche Zuordnungen für Failover- und Testzuordnungen verwenden“ deaktiviert haben. Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.



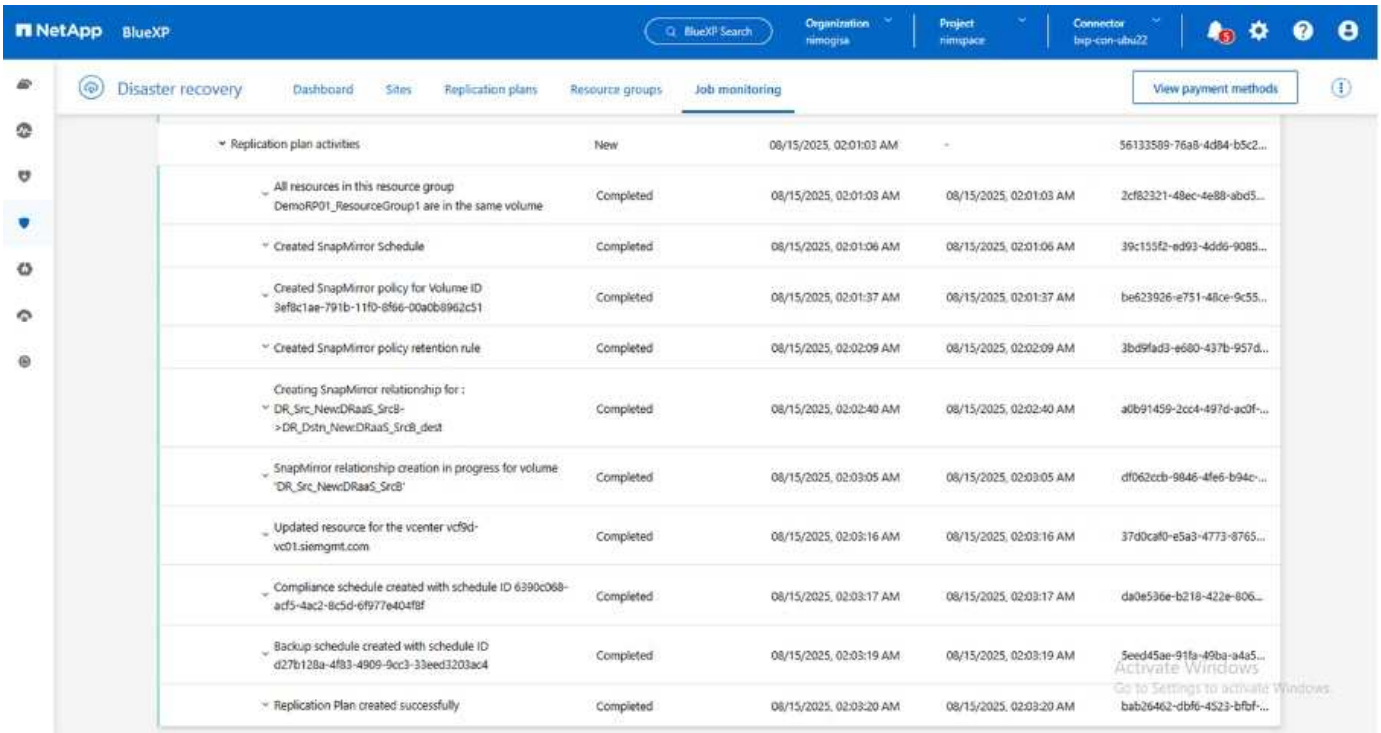
Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf „Plan hinzufügen“.



VMs aus verschiedenen Volumes und SVMs können in einen Replikationsplan aufgenommen werden. Abhängig von der VM-Platzierung (sei es auf demselben Volume oder einem separaten Volume innerhalb derselben SVM, separate Volumes auf verschiedenen SVMs) erstellt die BlueXP disaster recovery einen Consistency Group Snapshot.

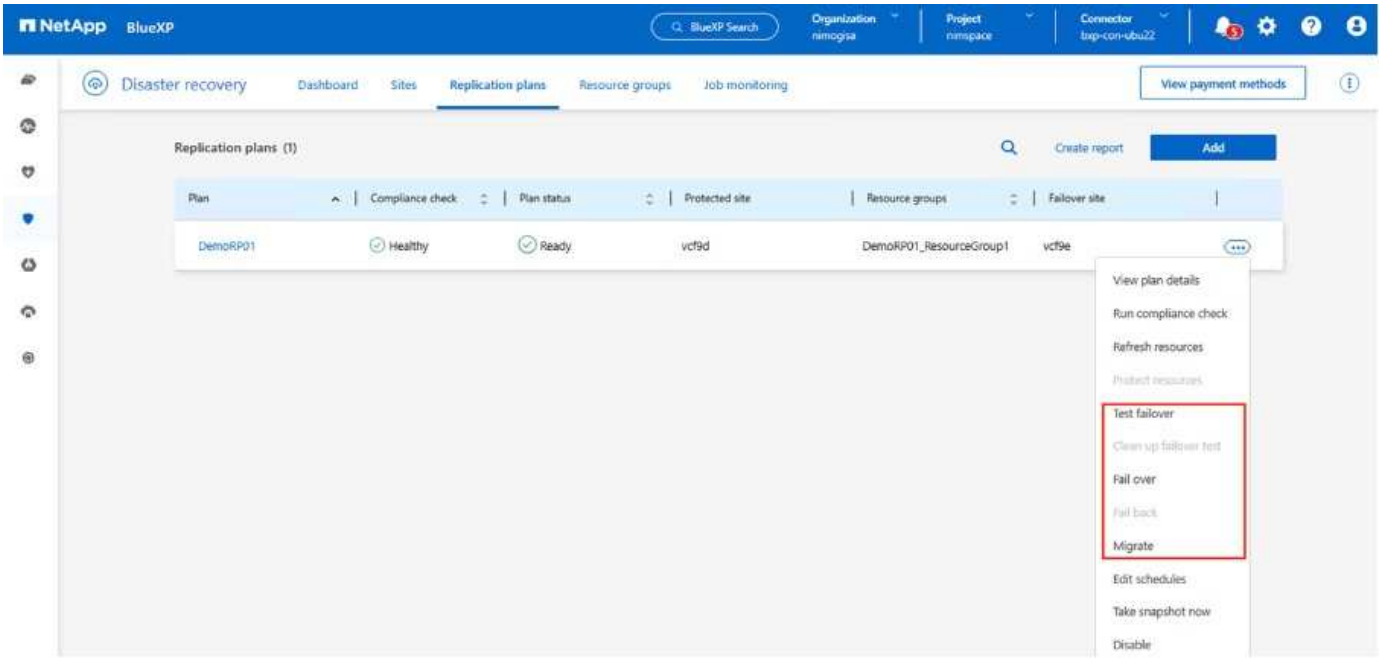


Sobald der Plan erstellt ist, werden eine Reihe von Validierungen ausgelöst und die SnapMirror Replikation und -Zeitpläne entsprechend der Auswahl konfiguriert.



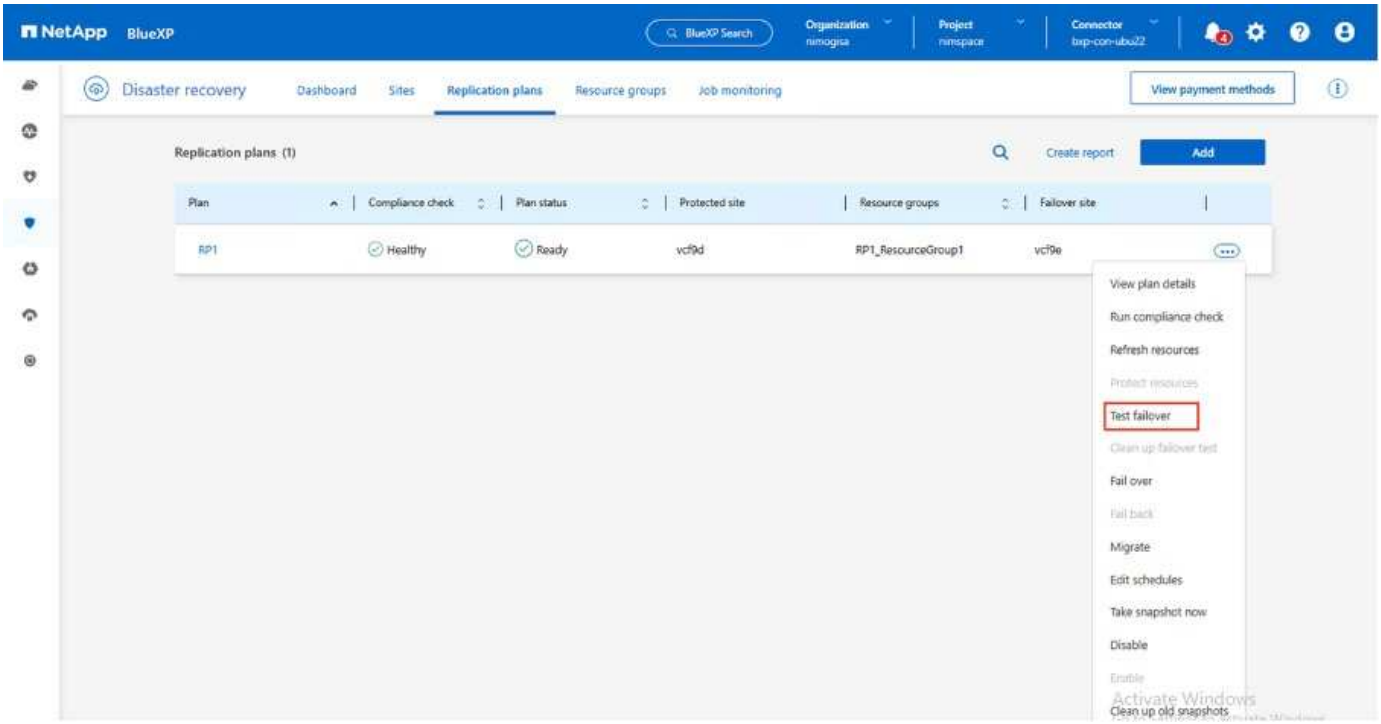
BlueXP DRaaS besteht aus den folgenden Workflows:

- Test-Failover (einschließlich regelmäßiger automatisierter Simulationen)
- Failovertest bereinigen
- Ausfallsicherung:
  - Geplante Migration (Erweiterung des Anwendungsfalls für einmaliges Failover)
  - Notfallwiederherstellung
- Failback

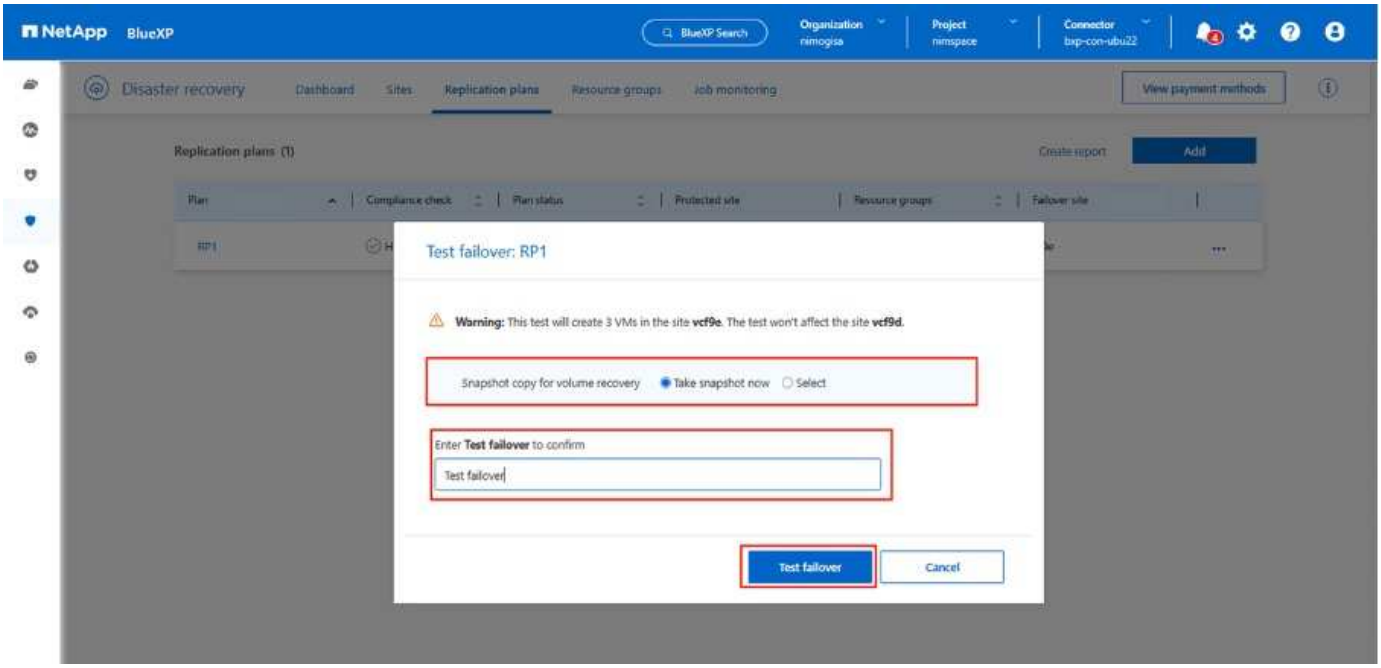


Testen des Failovers

Test-Failover in BlueXP DRaaS ist ein Betriebsverfahren, das es VMware-Administratoren ermöglicht, ihre Wiederherstellungspläne vollständig zu validieren, ohne ihre Produktionsumgebungen zu stören.

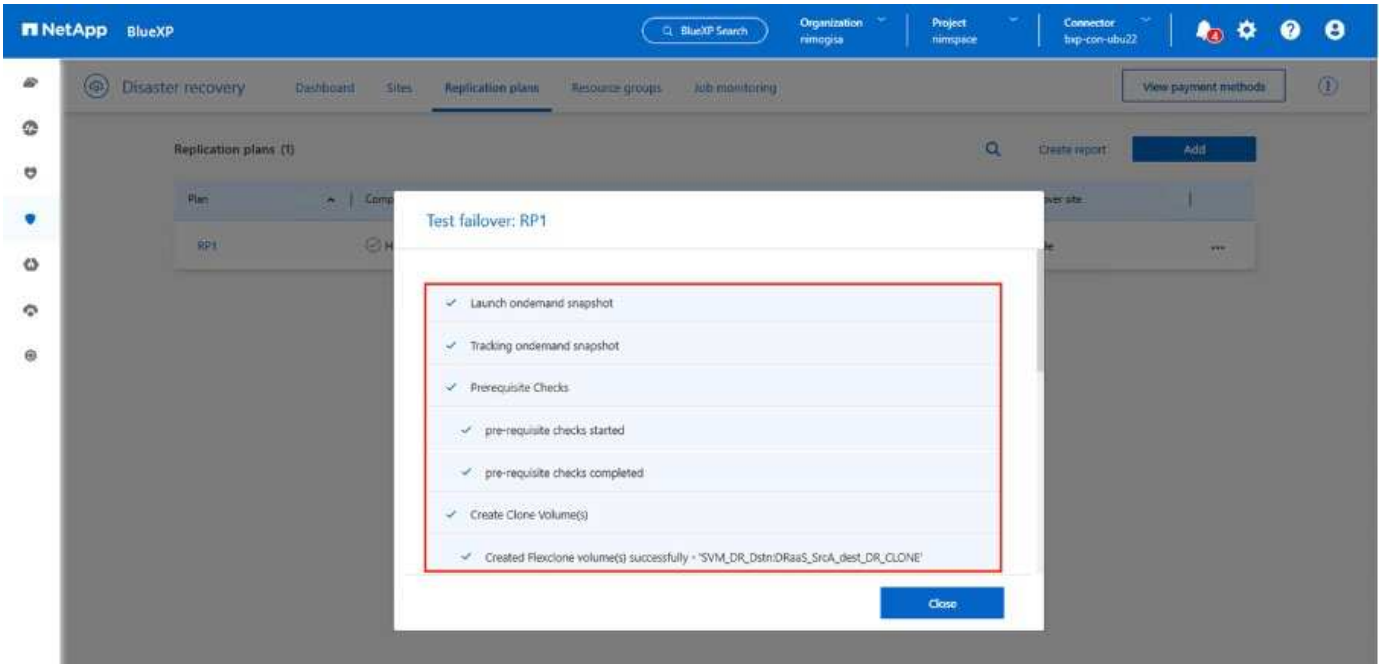


BlueXP DRaaS bietet die Möglichkeit, den Snapshot als optionale Funktion im Test-Failover-Vorgang auszuwählen. Mit dieser Funktion kann der VMware-Administrator überprüfen, ob alle kürzlich in der Umgebung vorgenommenen Änderungen auf die Zielsite repliziert werden und somit während des Tests vorhanden sind. Zu diesen Änderungen gehören Patches für das VM-Gastbetriebssystem.



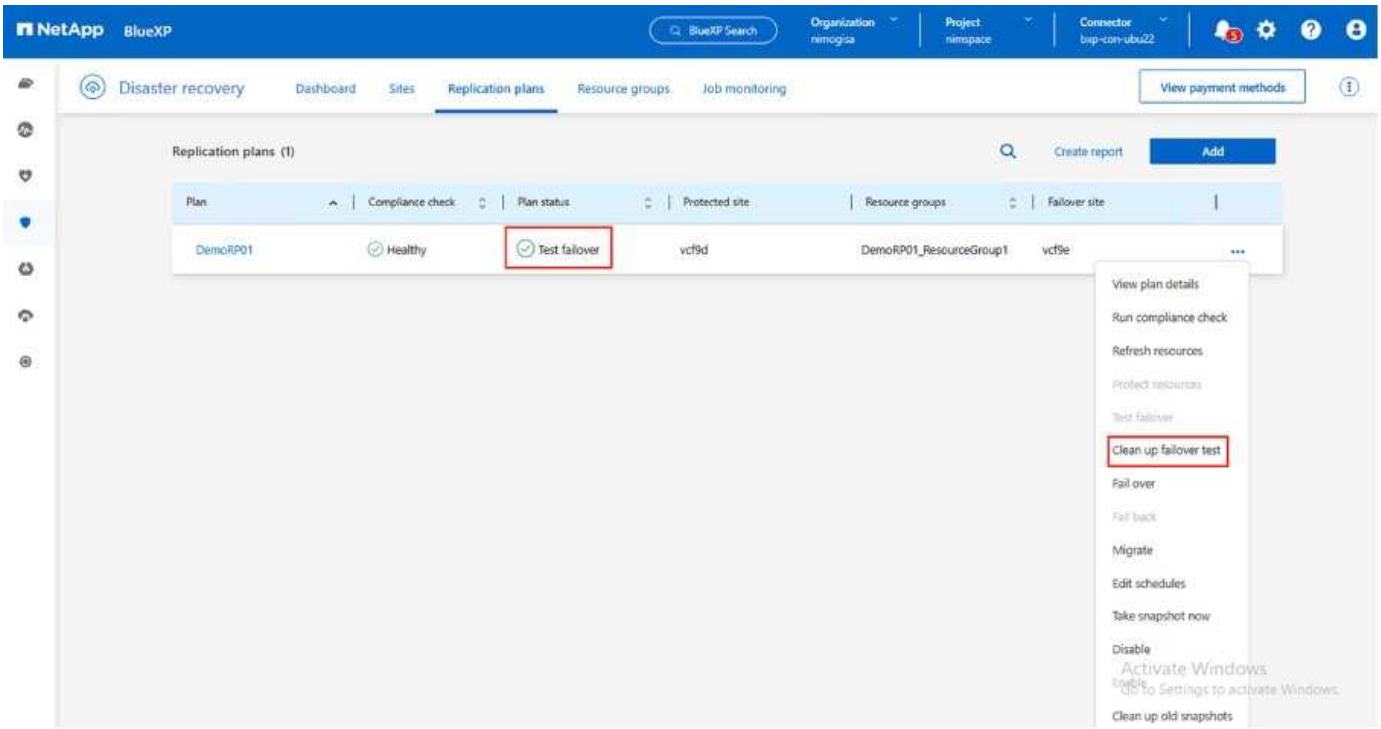
Wenn der VMware-Administrator einen Test-Failover-Vorgang ausführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

- Auslösen von SnapMirror -Beziehungen, um den Speicher am Zielstandort mit allen kürzlich am Produktionsstandort vorgenommenen Änderungen zu aktualisieren.
- Erstellen von NetApp FlexClone -Volumes der FlexVol -Volumes auf dem DR-Speicherarray.
- Verbinden der Datenspeicher in den FlexClone -Volumes mit den ESXi-Hosts am DR-Standort.
- Verbinden der VM-Netzwerkadapter mit dem während der Zuordnung angegebenen Testnetzwerk.
- Neukonfigurieren der Netzwerkeinstellungen des VM-Gastbetriebssystems wie für das Netzwerk am DR-Standort definiert.
- Ausführen aller benutzerdefinierten Befehle, die im Replikationsplan gespeichert wurden.
- Einschalten der VMs in der im Replikationsplan festgelegten Reihenfolge.



Bereinigungs-Failover-Testvorgang

Der Bereinigungs-Failover-Testvorgang wird ausgeführt, nachdem der Replikationsplantest abgeschlossen wurde und der VMware-Administrator auf die Bereinigungsaufforderung reagiert.

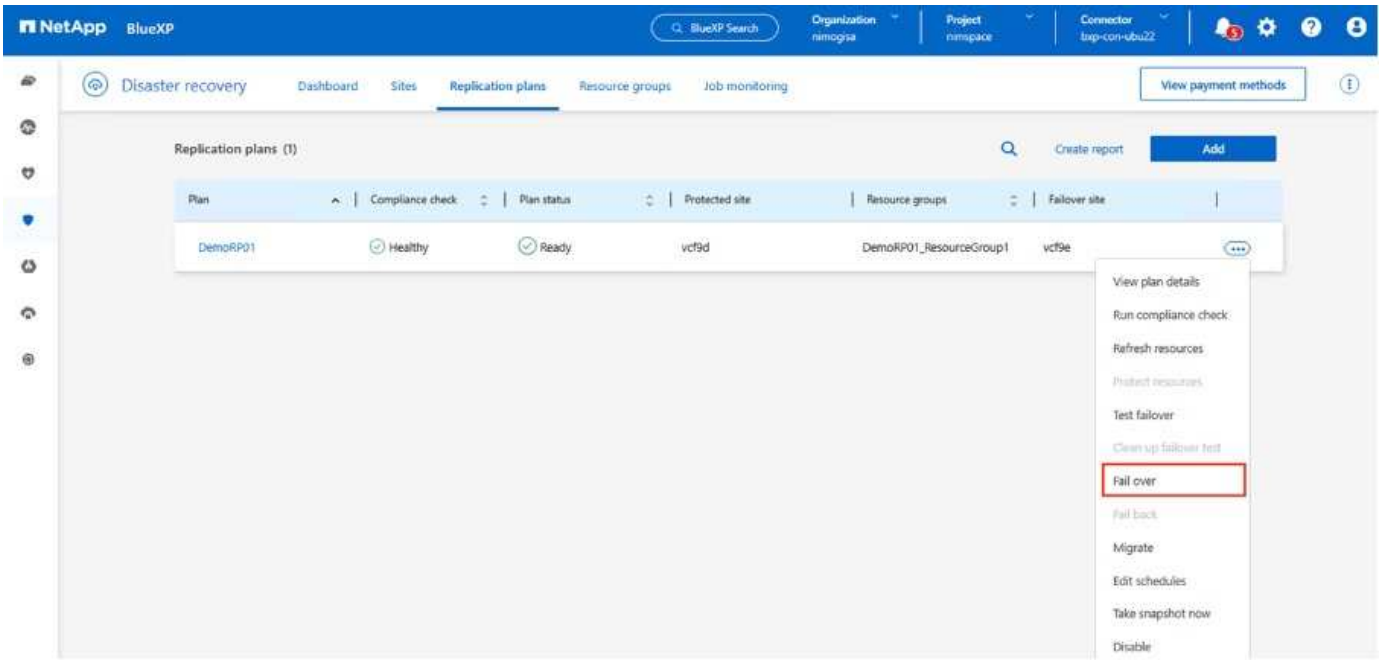


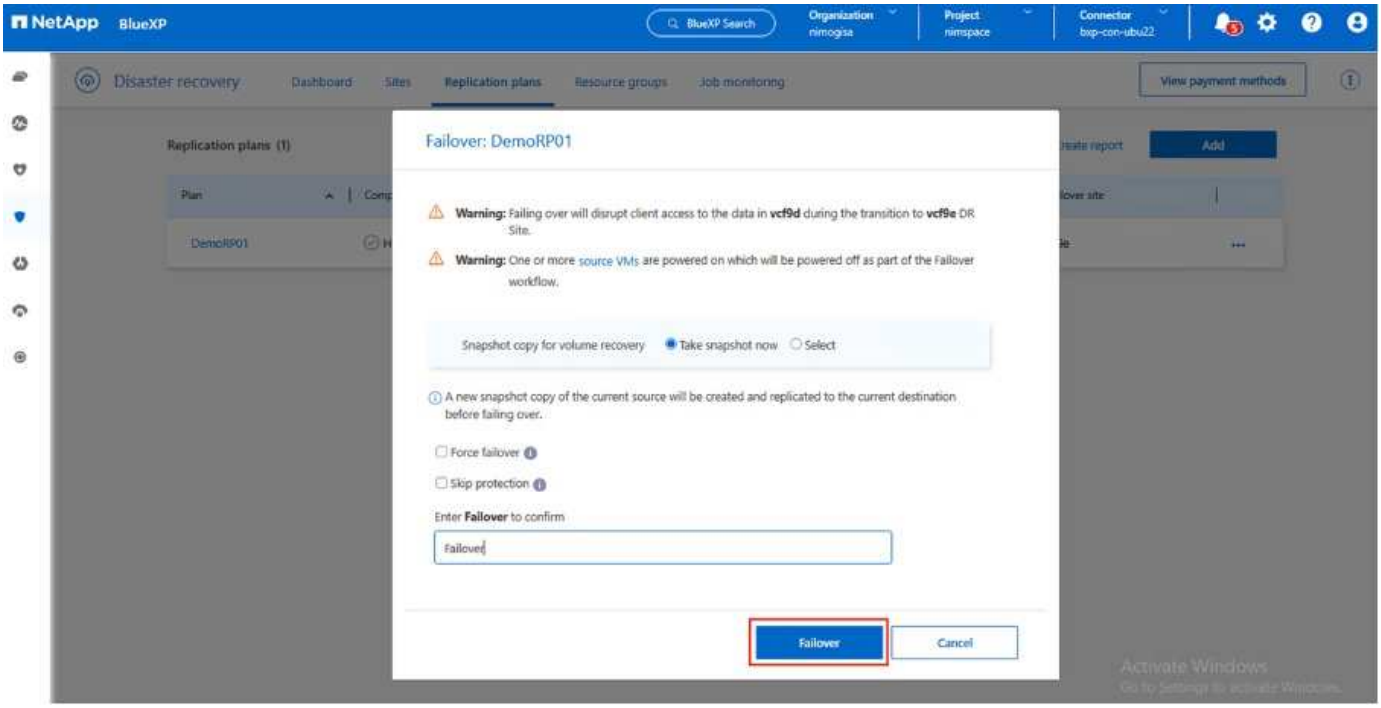
Durch diese Aktion werden die virtuellen Maschinen (VMs) und der Status des Replikationsplans auf den Bereitschaftszustand zurückgesetzt. Wenn der VMware-Administrator einen Wiederherstellungsvorgang durchführt, führt BlueXP DRaaS den folgenden Prozess durch:

1. Es schaltet jede wiederhergestellte VM in der FlexClone -Kopie aus, die zum Testen verwendet wurde.
2. Es löscht das FlexClone Volume, das während des Tests zum Präsentieren der wiederhergestellten VMs verwendet wurde.

Geplante Migration und Failover

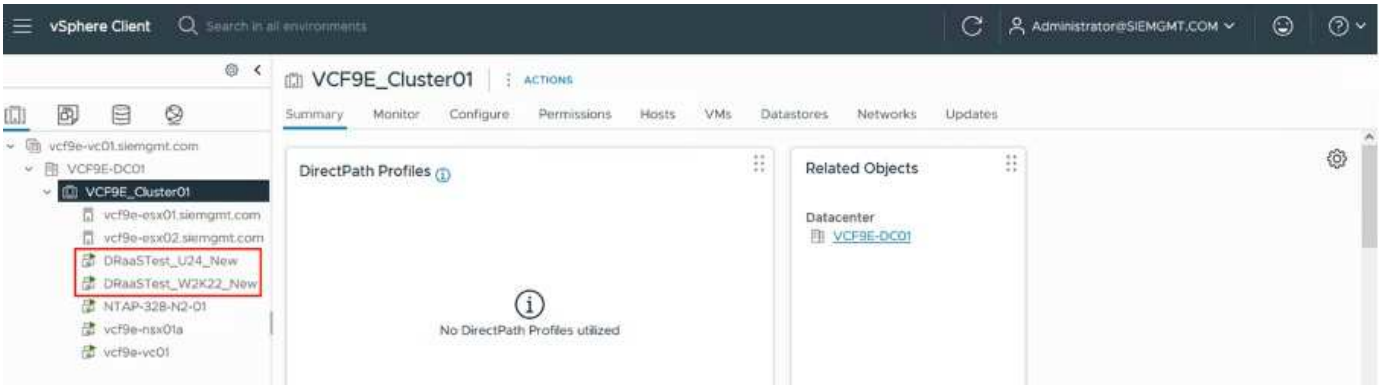
BlueXP DRaaS bietet zwei Methoden zur Durchführung eines echten Failovers: geplante Migration und Failover. Bei der ersten Methode, der geplanten Migration, werden das Herunterfahren der VM und die Synchronisierung der Speicherreplikation in den Prozess integriert, um die VMs wiederherzustellen oder effektiv an den Zielstandort zu verschieben. Für die geplante Migration ist Zugriff auf die Quellsite erforderlich. Die zweite Methode, Failover, ist ein geplantes/ungeplantes Failover, bei dem die VMs am Zielstandort aus dem letzten Speicherreplikationsintervall wiederhergestellt werden, das abgeschlossen werden konnte. Abhängig vom RPO, das in die Lösung integriert wurde, ist im DR-Szenario mit einem gewissen Datenverlust zu rechnen.





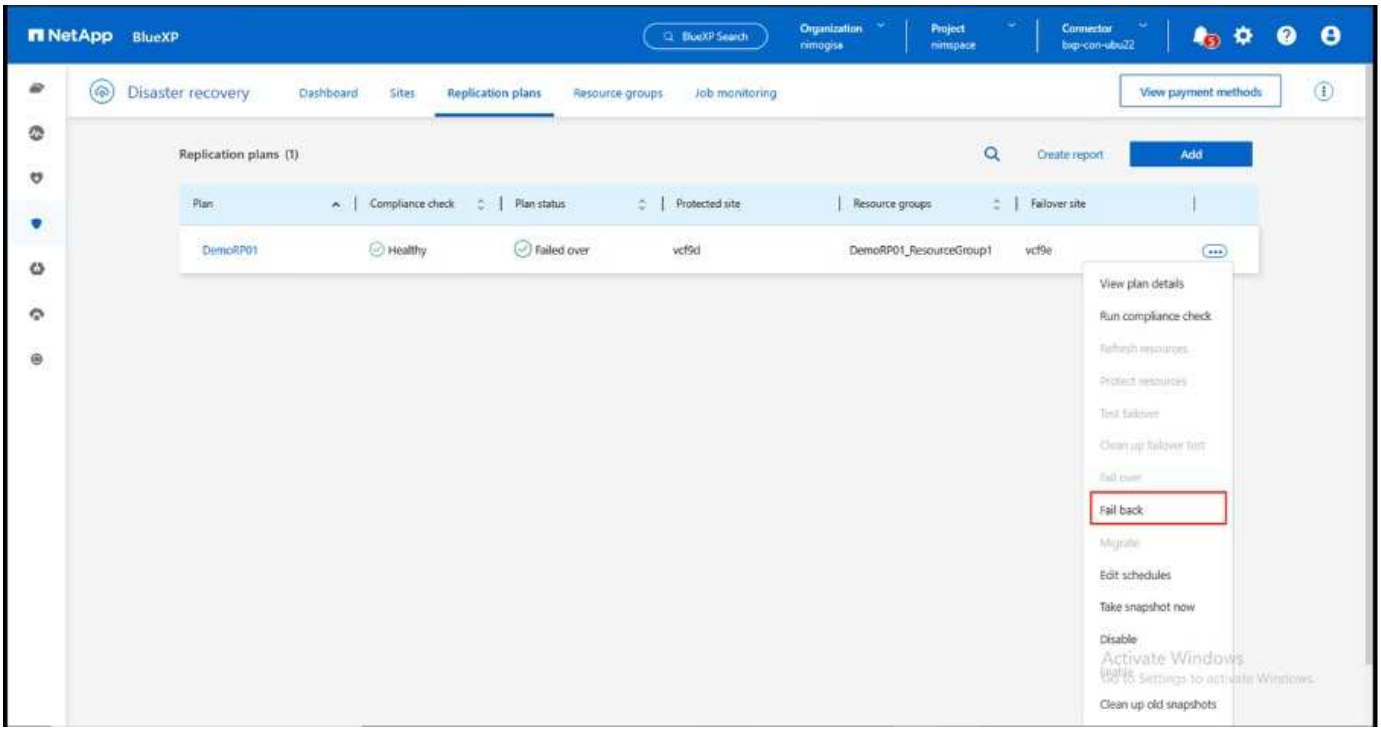
Wenn der VMware-Administrator einen Failover-Vorgang durchführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

- Unterbrechen und Failover der NetApp SnapMirror -Beziehungen.
- Verbinden Sie die replizierten Datenspeicher mit den ESXi-Hosts am DR-Standort.
- Verbinden Sie die VM-Netzwerkadapter mit dem entsprechenden Zielstandortnetzwerk.
- Konfigurieren Sie die Netzwerkeinstellungen des VM-Gastbetriebssystems neu, wie für das Netzwerk am Zielstandort definiert.
- Führen Sie alle benutzerdefinierten Befehle (sofern vorhanden) aus, die im Replikationsplan gespeichert wurden.
- Schalten Sie die VMs in der im Replikationsplan festgelegten Reihenfolge ein.



Failback

Ein Failback ist ein optionales Verfahren, das nach einer Wiederherstellung die ursprüngliche Konfiguration der Quell- und Zielsites wiederherstellt.

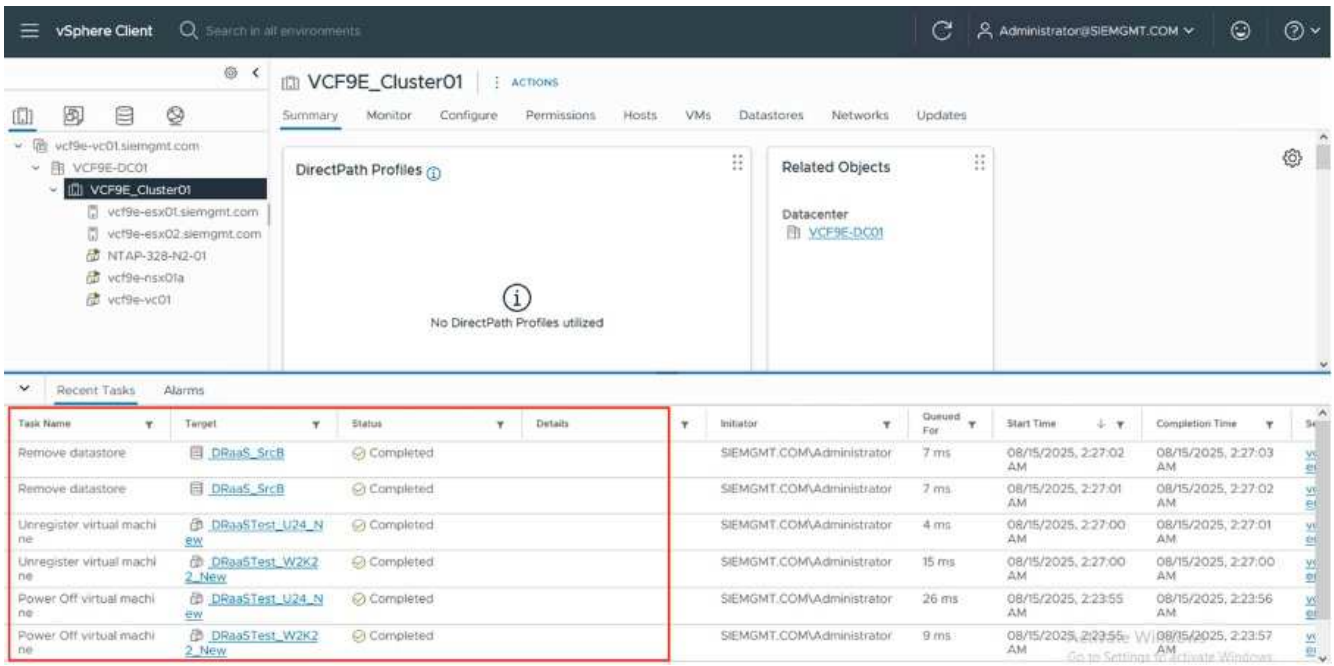


VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie bereit sind, die Dienste auf der ursprünglichen Quellsite wiederherzustellen.

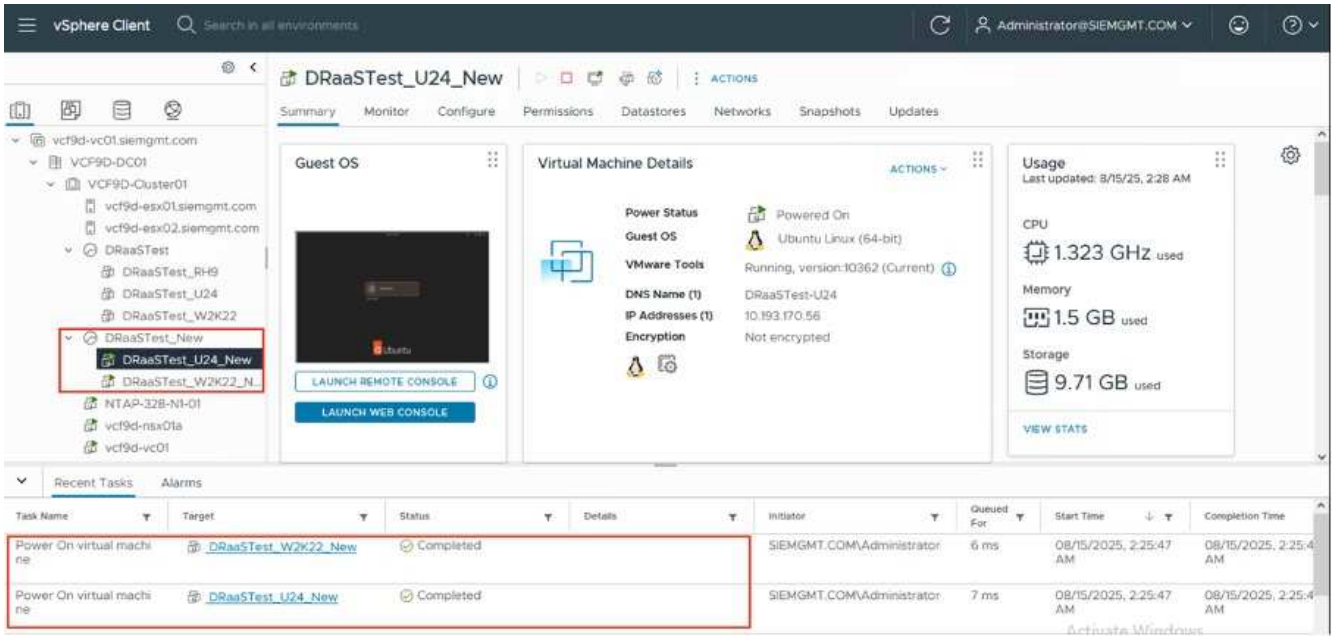
> BlueXP DRaaS repliziert (resynchronisiert) alle Änderungen zurück zur ursprünglichen virtuellen Quellmaschine, bevor die Replikationsrichtung umgekehrt wird.

Dieser Prozess beginnt mit einer Beziehung, deren Failover zu einem Ziel abgeschlossen ist, und umfasst die folgenden Schritte:

- Schalten Sie die virtuellen Maschinen aus und heben Sie die Registrierung auf. Die Volumes auf der Zielsite werden ausgehängt.



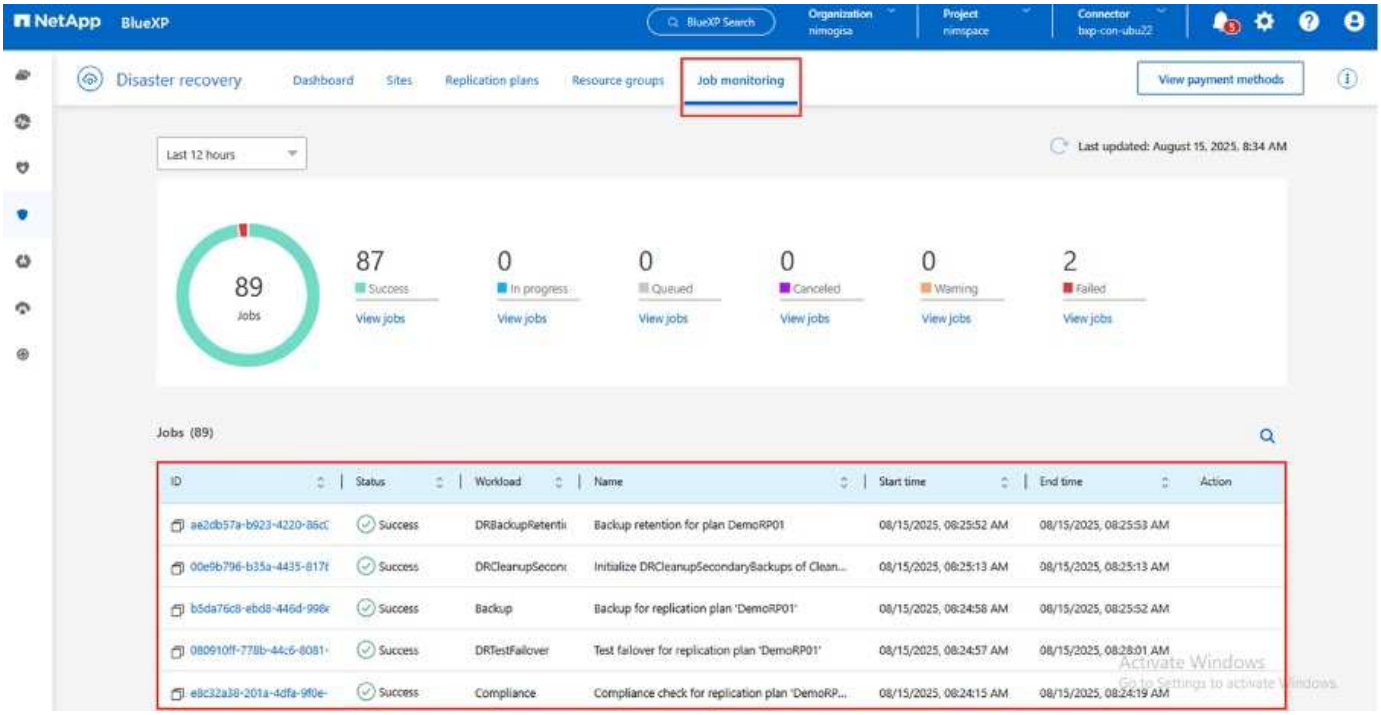
- Unterbrechen Sie die SnapMirror -Beziehung zur Originalquelle, um Lese-/Schreibzugriff zu ermöglichen.
- Synchronisieren Sie die SnapMirror -Beziehung erneut, um die Replikation umzukehren.
- Mounten Sie das Volume auf der Quelle, schalten Sie die virtuellen Quellmaschinen ein und registrieren Sie sie.



Weitere Informationen zum Zugriff auf und zur Konfiguration von BlueXP DRaaS finden Sie im"Erfahren Sie mehr über BlueXP Disaster Recovery für VMware" .

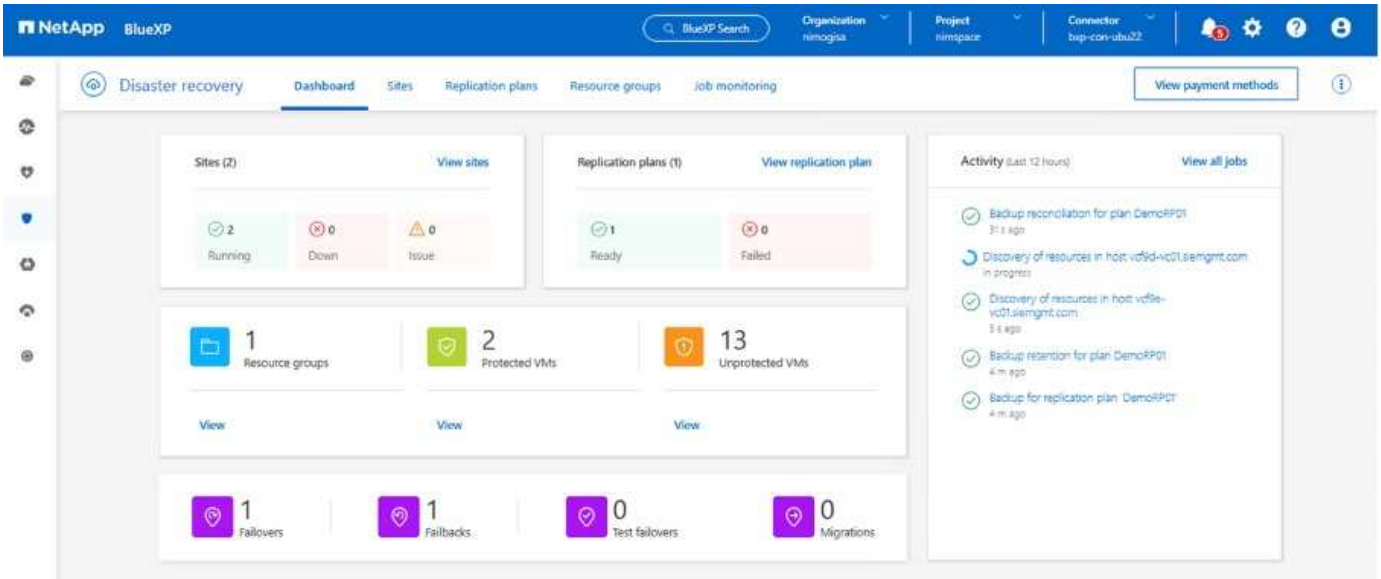
Überwachung und Dashboard

Von BlueXP oder der ONTAP CLI aus können Sie den Replikationszustand für die entsprechenden Datenspeichervolumes überwachen und den Status eines Failovers oder Testfailovers über die Jobüberwachung verfolgen.



Wenn ein Auftrag gerade ausgeführt wird oder sich in der Warteschlange befindet und Sie ihn stoppen möchten, können Sie ihn mit der Option „Abbrechen“ abbrechen.

Mit dem BlueXP disaster recovery können Sie den Status von Notfallwiederherstellungsstandorten und Replikationsplänen zuverlässig bewerten. Dadurch können Administratoren schnell fehlerfreie, nicht verbundene oder beeinträchtigte Sites und Pläne identifizieren.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Konvertieren Sie vorhandene vSphere-Cluster in VCF

Erfahren Sie mehr über die Konvertierung einer vSphere-Umgebung mit vorhandenen Datenspeichern in VCF

Die Konvertierung einer vSphere-Umgebung mit vorhandenen, auf ONTAP laufenden Datenspeichern in eine VMware Cloud Foundation (VCF)-Umgebung beinhaltet die Integration der aktuellen Infrastruktur in eine moderne Private-Cloud-Architektur.

Dieser Prozess nutzt die Flexibilität des ONTAP Speichers für nahtlosen Datenzugriff und -verwaltung. Sobald die VCF-Verwaltungsdomäne eingerichtet ist, können Administratoren zusätzliche vSphere-Umgebungen effizient in das VCF-Ökosystem importieren. Diese Integration verbessert die Ressourcennutzung, vereinfacht die Verwaltung privater Clouds und gewährleistet einen reibungslosen Übergang mit minimaler Unterbrechung bestehender Workloads.

Die technischen Details zur Konvertierung einer vCenter-Instanz finden Sie in den folgenden Lösungen.

- "Konvertieren einer vorhandenen vCenter-Instanz in eine VCF-Verwaltungsdomäne (NFS)"
- "Konvertieren Sie die vCenter-Instanz (FC-Datenspeicher) in eine VCF-Verwaltungsdomäne"

Konvertieren Sie die vCenter-Serverinstanz in eine VCF-Verwaltungsdomäne (NFS-Datenspeicher).

Konvertieren Sie einen vorhandenen vSphere 8-Cluster mit NetApp ONTAP NFS-Datenspeichern in eine VMware Cloud Foundation (VCF)-Verwaltungsdomäne. Dieses Verfahren umfasst die Bereitstellung von NFS-Speicher, die Implementierung von ONTAP Tools für VMware und die Verwendung des VCF-Importtools zum Konvertieren des Clusters für eine optimierte Verwaltung und Ressourcennutzung innerhalb von VCF.

Einführung

Die Konvertierung eines Clusters mit einem vorhandenen NFS-Datenspeicher, der auf ONTAP ausgeführt wird, umfasst die Integration der vorhandenen Infrastruktur in eine moderne private Cloud-Architektur. Dieser Prozess profitiert von der Flexibilität des NFS-Speichers, um einen nahtlosen Datenzugriff und eine nahtlose Datenverwaltung zu gewährleisten. Nachdem durch den Konvertierungsprozess eine VCF-Verwaltungsdomäne eingerichtet wurde, können Administratoren zusätzliche vSphere-Cluster, einschließlich solcher, die NFS-Datenspeicher verwenden, effizient in das VCF-Ökosystem importieren. Diese Integration verbessert nicht nur die Ressourcennutzung, sondern vereinfacht auch die Verwaltung der privaten Cloud-Infrastruktur und gewährleistet einen reibungslosen Übergang mit minimaler Unterbrechung der vorhandenen Arbeitslasten.

In dieser Lösung zeigen wir, wie ein NFS-Datenspeicher in vSphere 8 zum Hauptspeicher wird, wenn der Cluster in eine VCF-Verwaltungsdomäne konvertiert wird.

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Stellen Sie ONTAP tools for VMware vSphere 10 bereit.
- Stellen Sie einen NFS-Datenspeicher mit ONTAP -Tools bereit.
- Verwenden Sie das VCF-Importtool, um den vSphere-Cluster zu validieren.
- Stellen Sie den SDDC Manager im vSphere-Cluster bereit.
- Konfigurieren Sie eine JSON-Datei, um während der VCF-Konvertierung NSX zu erstellen.
- Verwenden Sie das VCF-Importtool, um den vSphere 8-Cluster in VCF 5.2 zu konvertieren.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- NetApp AFF -Speichersystem mit einer Storage Virtual Machine (SVM), die für die Zulassung von NFS-Verkehr konfiguriert ist.
- Im IP-Netzwerk wurde eine logische Schnittstelle (LIF) erstellt, die den NFS-Verkehr übertragen soll und mit der SVM verknüpft ist.
- Ein vSphere 8-Cluster mit 4 x ESXi-Hosts und einer auf dem Cluster co-lokalisierten vCenter-Appliance.
- Verteilte Portgruppe, die für vMotion- und NFS-Speicherverkehr auf den zu diesem Zweck eingerichteten VLANs oder Netzwerksegmenten konfiguriert ist.
- Laden Sie die für die VCF-Konvertierung erforderliche Software herunter.

ONTAP tools for VMware vSphere 10 können entweder in HA- oder Nicht-HA-Konfigurationen installiert werden. Ausführliche Informationen zu den Voraussetzungen für ONTAP -Tools finden Sie unter "Voraussetzungen für ONTAP tools for VMware vSphere" .

Informationen zum unterstützten Speicher und andere Überlegungen zum Konvertieren oder Importieren von vSphere in VCF 5.2 finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Die erforderliche Software finden Sie im "Broadcom Support-Portal" .

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Bereitstellungsschritte

Die Lösung umfasst die Verwendung von ONTAP tools for VMware vSphere zur Bereitstellung von NFS-Datenspeichern und den Prozess der Konvertierung eines vorhandenen vSphere 8-Clusters in eine VCF-Verwaltungsdomäne.

Führen Sie die folgenden Schritte aus:

- Stellen Sie ONTAP tools for VMware vSphere 10 bereit.
- Stellen Sie einen NFS-Datenspeicher mit ONTAP -Tools bereit.
- Kopieren Sie das VCF-Importtool auf die vCenter-Appliance.

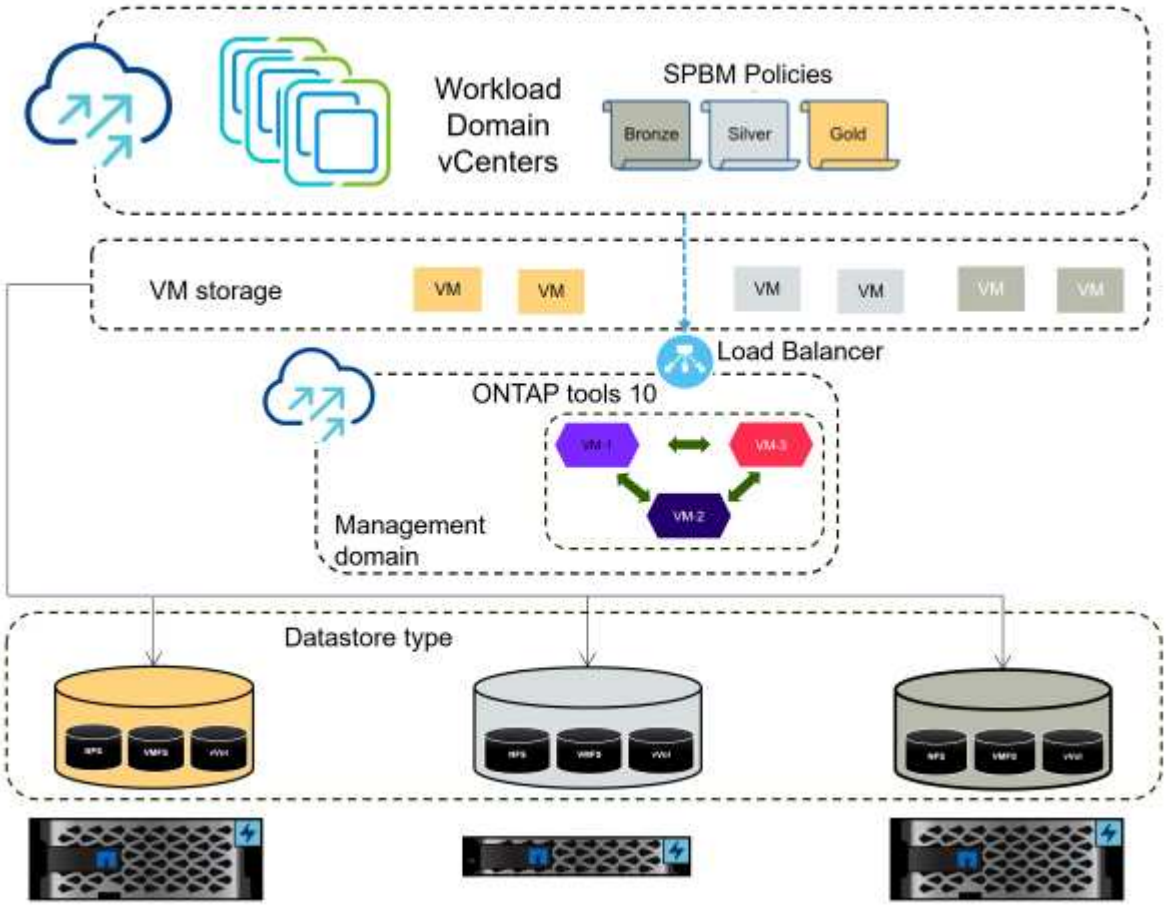
- Führen Sie mit dem VCF-Importtool eine Vorprüfung auf der vCenter-Appliance durch.
- Stellen Sie die SDDC-Manager-VM auf dem vCenter-Cluster bereit.
- Erstellen Sie eine JSON-Datei für einen NSX-Cluster, der während des Konvertierungsvorgangs bereitgestellt werden soll.
- Laden Sie die erforderliche Software in den SDDC-Manager hoch.
- Konvertieren Sie den vSphere-Cluster in das SDDC-Manager-Inventar.

Eine Übersicht über den Konvertierungsprozess finden Sie unter "Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workload-Domäne in VMware Cloud Foundation" .

Bereitstellen von ONTAP -Tools und Bereitstellen eines NFS-Datenspeichers

Die Architektur von ONTAP Tools 10 ist auf eine nahtlose Integration in VMware-Umgebungen ausgelegt und nutzt ein modulares und skalierbares Framework, das die ONTAP Tools-Dienste, das vSphere-Plug-in und REST-APIs umfasst, um eine effiziente Speicherverwaltung, Automatisierung und Datensicherung zu ermöglichen.

ONTAP tools for VMware vSphere 10 können entweder in HA- oder Nicht-HA-Konfigurationen installiert werden.

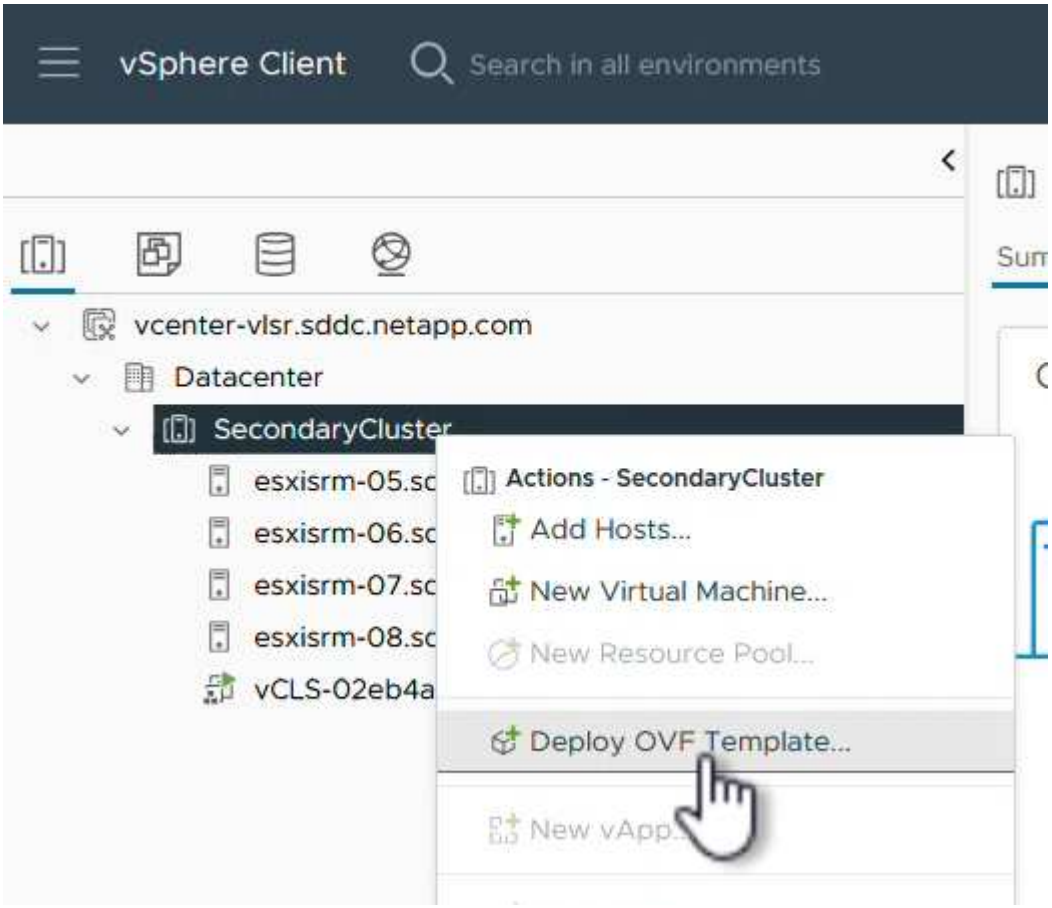


Bereitstellen von ONTAP tools for VMware vSphere 10

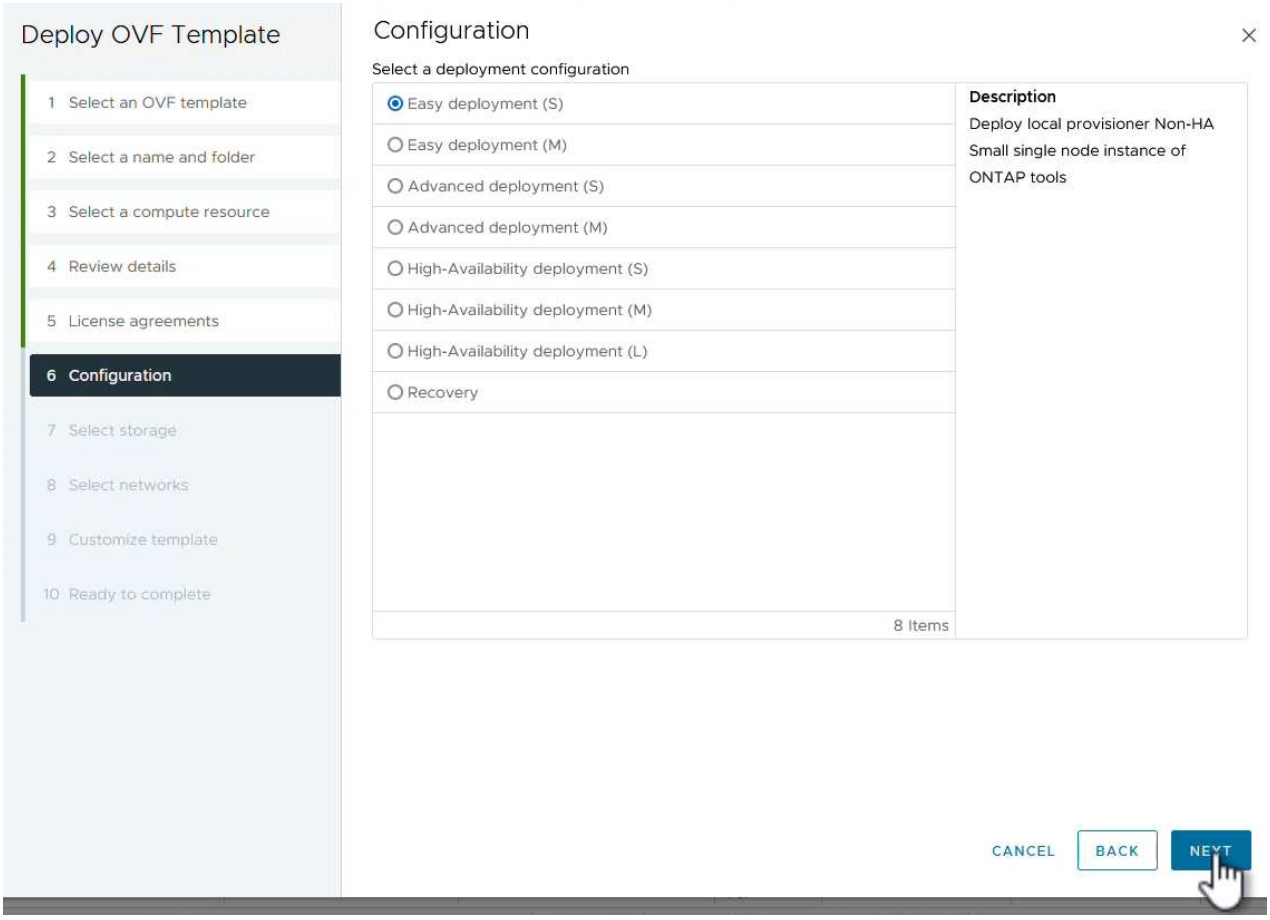
In diesem Schritt wird ONTAP Tools 10 mit einer Nicht-HA-Konfiguration bereitgestellt.

Weitere Informationen zur Bereitstellung von HA- und Nicht-HA-Konfigurationen finden Sie unter "Bereitstellen von ONTAP tools for VMware vSphere" .

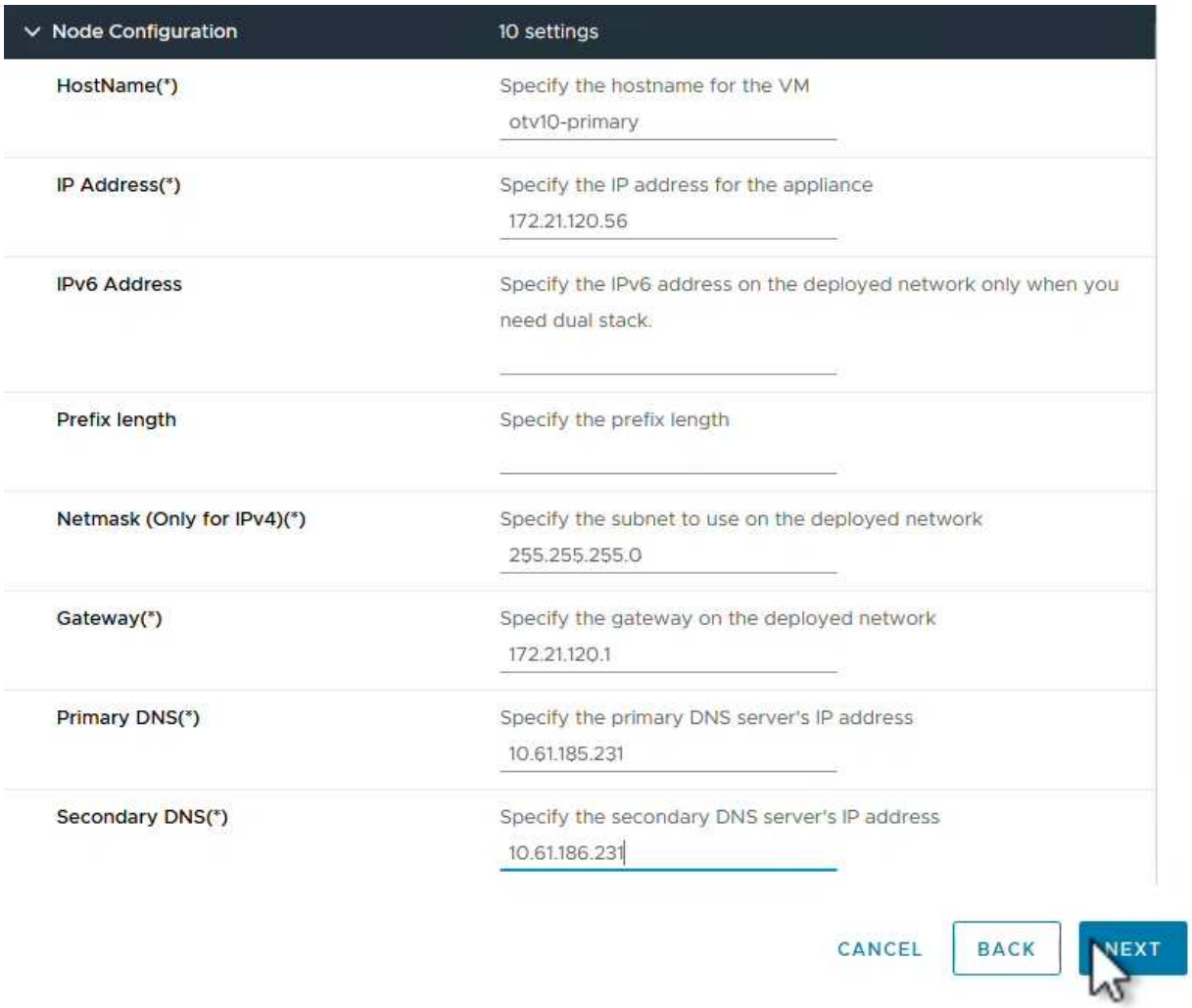
1. Laden Sie die ONTAP Tools 10 OVA-Vorlage von der "NetApp Support-Site" .
2. Klicken Sie im vSphere-Client mit der rechten Maustaste auf den Cluster und klicken Sie auf **OVF-Vorlage bereitstellen**



3. Führen Sie in der **OVF-Vorlage bereitstellen** die folgenden Schritte aus:
   - Wählen Sie eine OVF-Vorlage aus.
   - Wählen Sie einen Namen und einen Ordner aus.
   - Wählen Sie eine Rechenressource aus.
   - Details überprüfen.
   - Stimmen Sie der Lizenzvereinbarung zu.
4. Wählen Sie auf der Seite **Konfiguration** der Vorlage den Bereitstellungstyp aus und geben Sie an, ob ONTAP -Tools in einer HA-Konfiguration bereitgestellt werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.



5. Wählen Sie auf der Seite **Speicher auswählen** den Datenspeicher aus, auf dem die VM installiert werden soll, und klicken Sie auf **Weiter**.
6. Wählen Sie das Netzwerk aus, über das die ONTAP -Tools-VM kommunizieren wird. Klicken Sie auf **Weiter**, um fortzufahren.
7. Geben Sie im Fenster „Vorlage anpassen“ alle erforderlichen Informationen ein.
    - Benutzername und Passwort der Anwendung
    - Wählen Sie, ob ASUP (Auto Support) einschließlich einer Proxy-URL aktiviert werden soll.
    - Benutzername und Passwort des Administrators.
    - NTP-Server.
    - Benutzername und Passwort für die Wartung (Wartungskonto, das an der Konsole verwendet wird).
    - Geben Sie die erforderlichen IP-Adressen für die Bereitstellungskonfiguration an.
    - Geben Sie alle Netzwerkinformationen für die Knotenkonfiguration an.

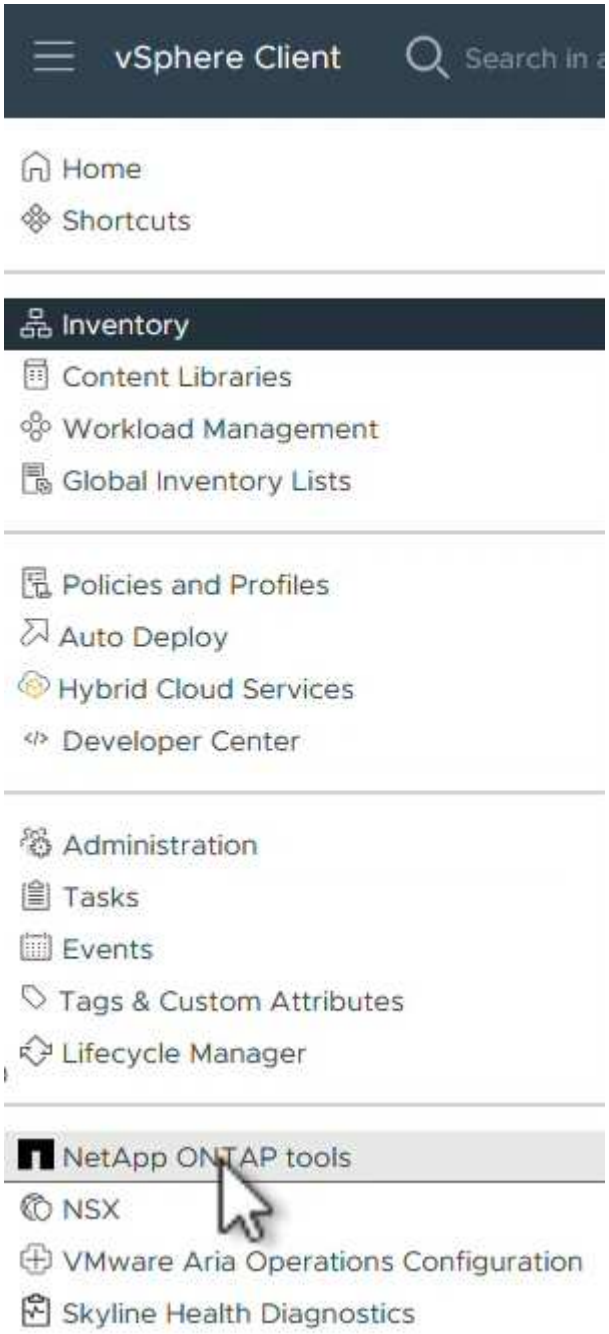


8. Klicken Sie abschließend auf **Weiter**, um fortzufahren, und dann auf **Fertig**, um mit der Bereitstellung zu beginnen.

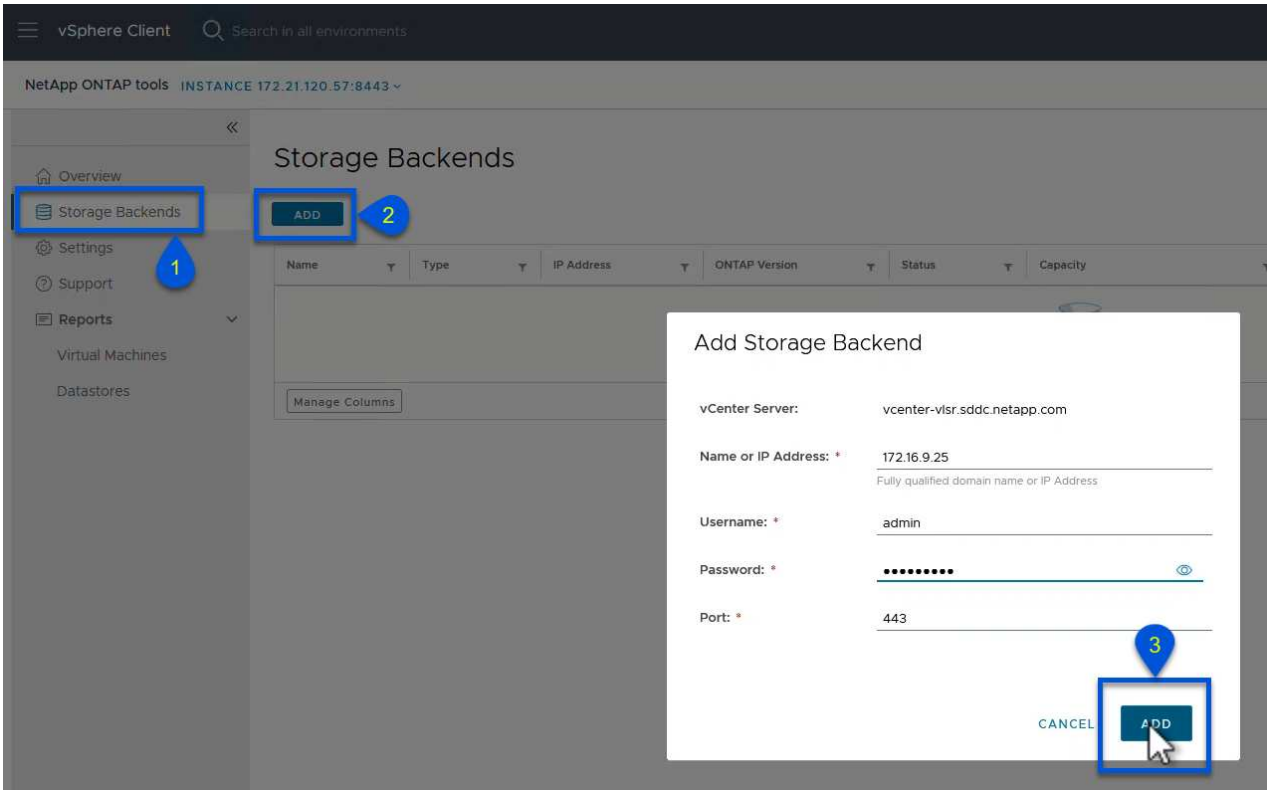
Konfigurieren Sie ONTAP -Tools

Sobald die ONTAP -Tools-VM installiert und eingeschaltet ist, sind einige grundlegende Konfigurationsschritte erforderlich, beispielsweise das Hinzufügen von vCenter-Servern und ONTAP Speichersystemen zur Verwaltung. Weitere Informationen finden Sie in der Dokumentation unter "ONTAP tools for VMware vSphere Dokumentation" für detaillierte Informationen.

1. Siehe "vCenter-Instanzen hinzufügen" um die vCenter-Instanzen für die Verwaltung mit ONTAP -Tools zu konfigurieren.
2. Um ein ONTAP Speichersystem hinzuzufügen, melden Sie sich beim vSphere-Client an und navigieren Sie zum Hauptmenü auf der linken Seite. Klicken Sie auf * NetApp ONTAP -Tools*, um die Benutzeroberfläche zu starten.



3. Navigieren Sie im linken Menü zu **Storage Backends** und klicken Sie auf **Hinzufügen**, um auf das Fenster **Storage Backend hinzufügen** zuzugreifen.
4. Geben Sie die IP-Adresse und Anmeldeinformationen für das zu verwaltende ONTAP Speichersystem ein. Klicken Sie zum Abschluss auf **Hinzufügen**.

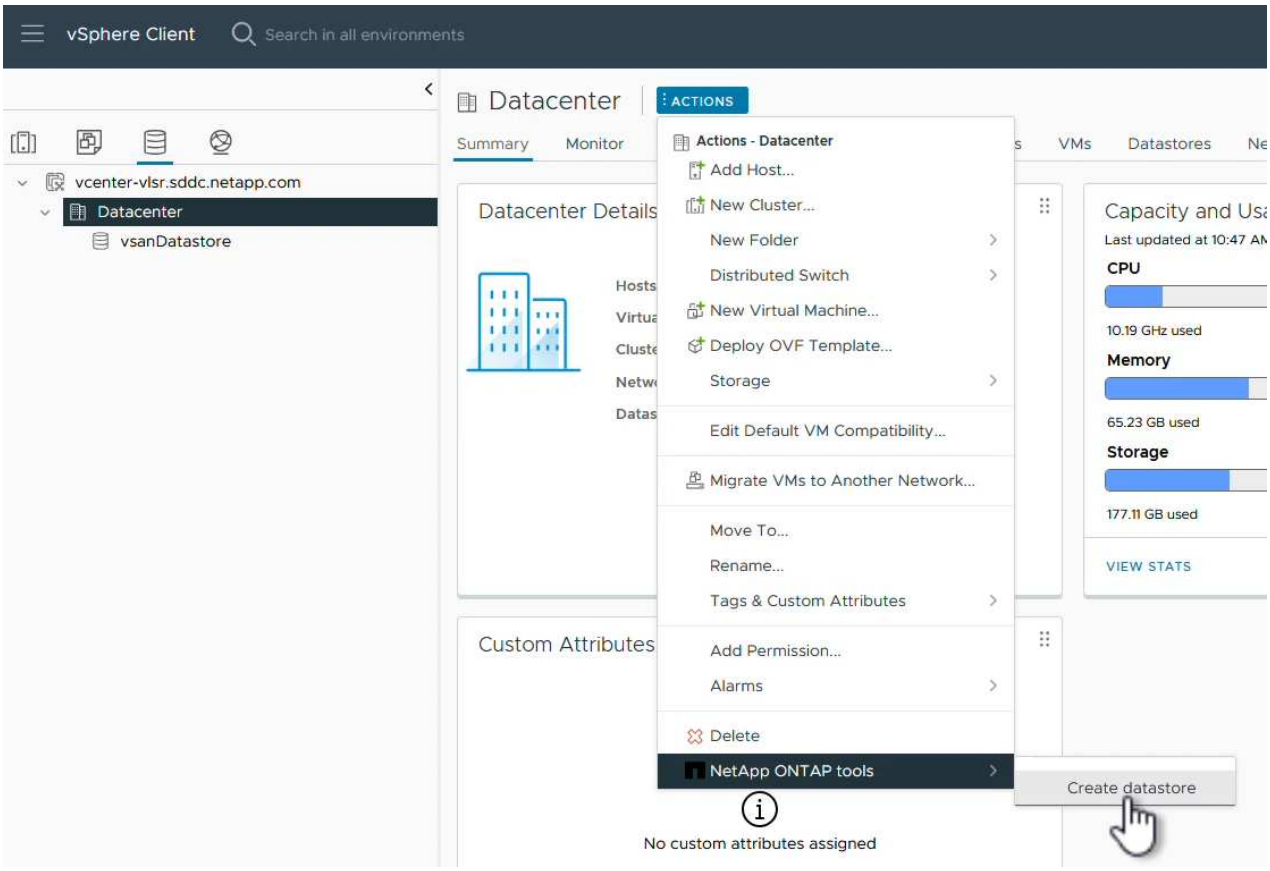


Hier wird das Speicher-Backend mithilfe der Cluster-IP-Adresse in der vSphere-Client-Benutzeroberfläche hinzugefügt. Dies ermöglicht die vollständige Verwaltung aller SVMs im Speichersystem. Alternativ kann das Storage-Backend hinzugefügt und mit einer vCenter-Instanz verknüpft werden, indem man den ONTAP Tools Manager verwendet. `https://loadBalanceIP:8443/virtualization/ui/` . Mit dieser Methode können in der Benutzeroberfläche des vSphere-Clients nur SVM-Anmeldeinformationen hinzugefügt werden, was eine genauere Kontrolle über den Speicherzugriff ermöglicht.

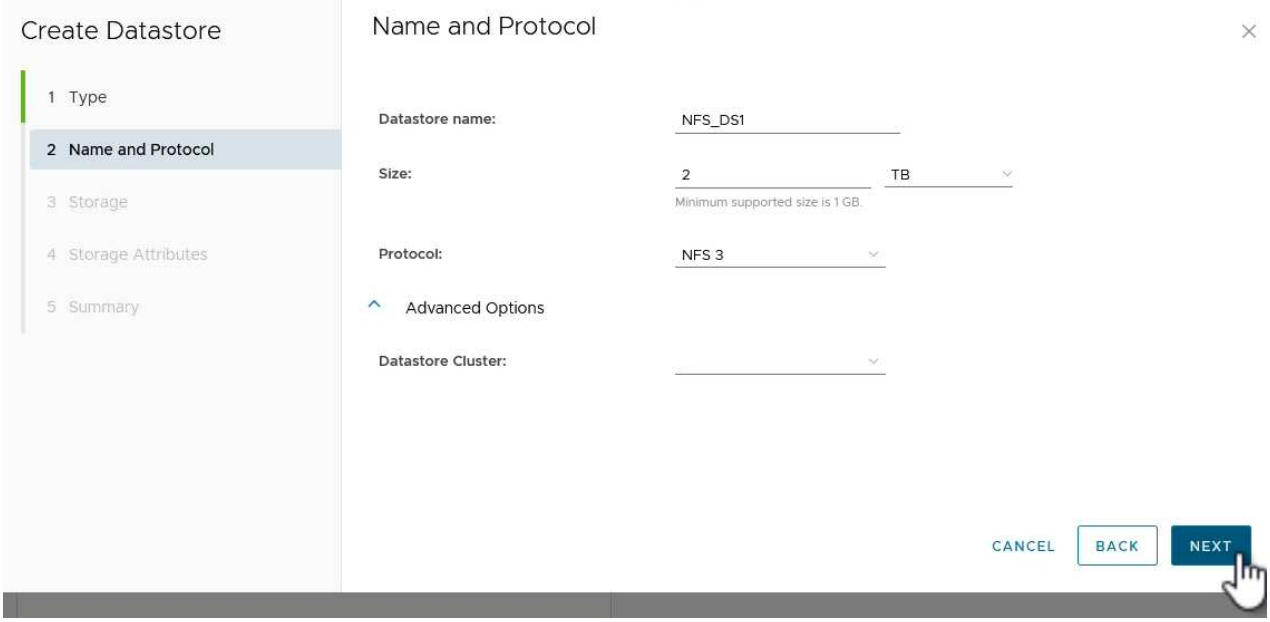
Bereitstellen eines NFS-Datenspeichers mit ONTAP -Tools

ONTAP -Tools integrieren Funktionen in die gesamte vSphere-Client-Benutzeroberfläche. In diesem Schritt wird ein NFS-Datenspeicher von der Speicherinventarseite bereitgestellt.

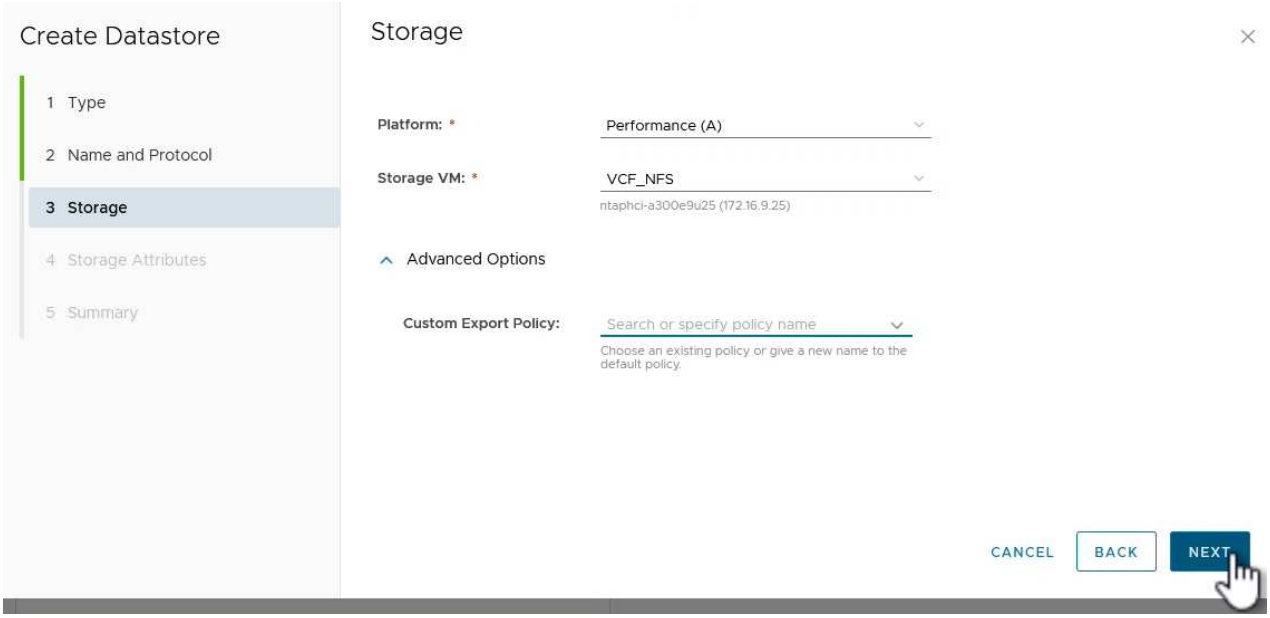
1. Navigieren Sie im vSphere-Client zum Speicherinventar.
2. Navigieren Sie zu **AKTIONEN > NetApp ONTAP -Tools > Datenspeicher erstellen**.



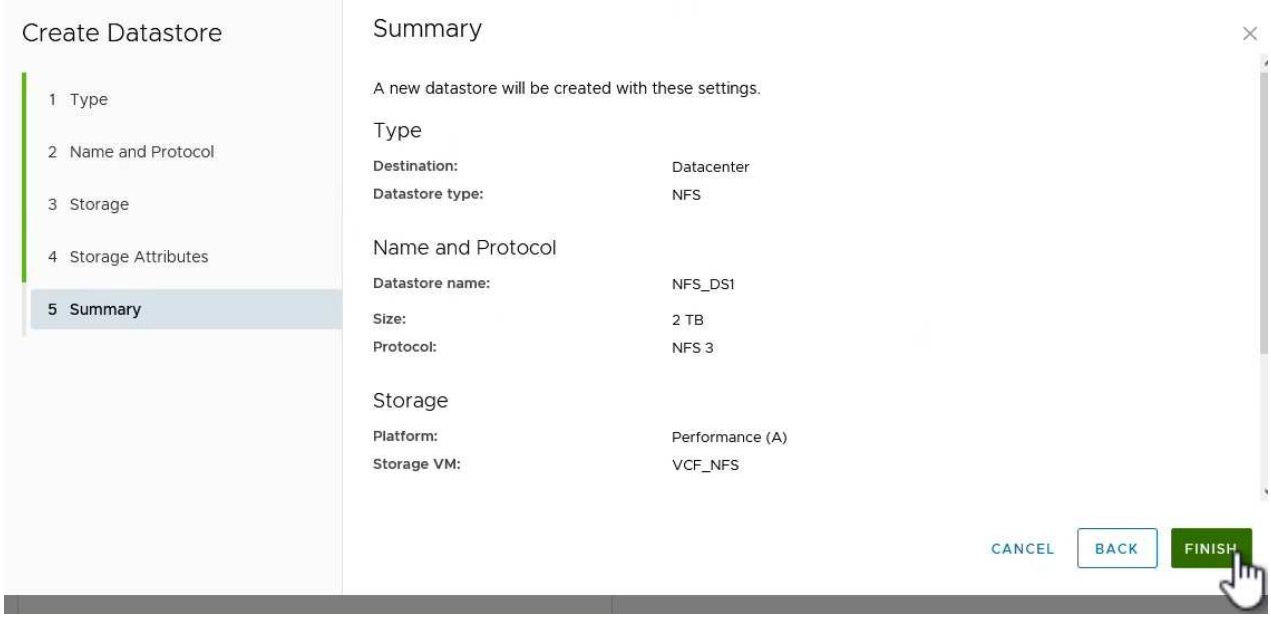
3. Wählen Sie im Assistenten **Datenspeicher erstellen** den Typ des zu erstellenden Datenspeichers aus. Optionen sind NFS oder VMFS.
4. Geben Sie auf der Seite **Name und Protokoll** einen Namen für den Datenspeicher, die Größe und das zu verwendende NFS-Protokoll ein.



5. Wählen Sie auf der Seite **Speicher** die ONTAP -Speicherplattform und die Storage Virtual Machine (SVM) aus. Sie können hier auch alle verfügbaren benutzerdefinierten Exportrichtlinien auswählen. Klicken Sie auf **Weiter**, um fortzufahren.



6. Wählen Sie auf der Seite **Speicherattribute** das zu verwendende Speicheraggregat aus. Klicken Sie auf **Weiter**, um fortzufahren.
7. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie auf **Fertig**, um den Bereitstellungsprozess zu starten. ONTAP -Tools erstellen ein Volume auf dem ONTAP Speichersystem und mounten es als NFS-Datenspeicher auf allen ESXi-Hosts im Cluster.



Konvertieren Sie den vSphere-Cluster in VCF 5.2

Der folgende Abschnitt behandelt die Schritte zum Bereitstellen des SDDC-Managers und zum Konvertieren des vSphere 8-Clusters in eine VCF 5.2-Verwaltungsdomäne. Gegebenenfalls wird für weitere Einzelheiten auf die VMware-Dokumentation verwiesen.

Das VCF-Importtool von VMware by Broadcom ist ein Dienstprogramm, das sowohl auf der vCenter-Appliance als auch auf dem SDDC-Manager verwendet wird, um Konfigurationen zu validieren und Konvertierungs- und Importdienste für vSphere- und VCF-Umgebungen bereitzustellen.

Weitere Informationen finden Sie unter "Optionen und Parameter des VCF-Importtools" .

VCF-Importtool kopieren und extrahieren

Die VCF-Importtools werden auf der vCenter-Appliance verwendet, um zu überprüfen, ob sich der vSphere-Cluster für den VCF-Konvertierungs- oder Importvorgang in einem fehlerfreien Zustand befindet.

Führen Sie die folgenden Schritte aus:

1. Folgen Sie den Schritten unter "Kopieren Sie das VCF-Importtool auf die Ziel-vCenter-Appliance" bei VMware Docs, um das VCF-Importtool an den richtigen Speicherort zu kopieren.
2. Extrahieren Sie das Paket mit dem folgenden Befehl:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validieren der vCenter-Appliance

Verwenden Sie das VCF-Importtool, um die vCenter-Appliance vor der Konvertierung zu validieren.

1. Folgen Sie den Schritten unter "Führen Sie vor der Konvertierung eine Vorprüfung des Ziel-vCenters durch" um die Validierung auszuführen.
2. Die folgende Ausgabe zeigt, dass die vCenter-Appliance die Vorprüfung bestanden hat.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Bereitstellen des SDDC Managers

Der SDDC-Manager muss sich am selben Standort wie der vSphere-Cluster befinden, der in eine VCF-Verwaltungsdomäne umgewandelt wird.

Befolgen Sie die Bereitstellungsanweisungen in den VMware-Dokumenten, um die Bereitstellung abzuschließen.

Siehe "Stellen Sie die SDDC Manager Appliance auf dem Ziel-vCenter bereit" .

Weitere Informationen finden Sie unter"Kommissionsgastgeber" im VCF-Administrationshandbuch.

Erstellen einer JSON-Datei für die NSX-Bereitstellung

Um NSX Manager bereitzustellen, während Sie eine vSphere-Umgebung in VMware Cloud Foundation importieren oder konvertieren, erstellen Sie eine NSX-Bereitstellungsspezifikation. Für die NSX-Bereitstellung sind mindestens 3 Hosts erforderlich.

> Beim Bereitstellen eines NSX Manager-Clusters in einem Konvertierungs- oder Importvorgang wird das NSX-VLAN-Netzwerk verwendet. Einzelheiten zu den Einschränkungen der NSX-VLAN-Vernetzung finden Sie im Abschnitt „Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation“. Informationen zu NSX-VLAN-Netzwerkbeschränkungen finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Nachfolgend sehen Sie ein Beispiel einer JSON-Datei für die NSX-Bereitstellung:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "NetApp!23456789",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Kopieren Sie die JSON-Datei in ein Verzeichnis im SDDC Manager.

Laden Sie Software in den SDDC Manager hoch

Kopieren Sie das VCF-Importtool und das NSX-Bereitstellungspaket in das Verzeichnis /home/vcf/vcfimport im SDDC Manager.

Sehen "Laden Sie die erforderliche Software auf die SDDC Manager Appliance hoch" für detaillierte Anweisungen.

Konvertieren Sie den vSphere-Cluster in eine VCF-Verwaltungsdomäne

Zur Durchführung des Konvertierungsprozesses wird das VCF-Importtool verwendet. Führen Sie den folgenden Befehl aus dem Verzeichnis /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset aus, um einen Ausdruck der Funktionen des VCF-Importtools anzuzeigen:

```
python3 vcf_brownfield.py --help
```

Der folgende Befehl wird ausgeführt, um den vSphere-Cluster in eine VCF-Verwaltungsdomäne zu konvertieren und den NSX-Cluster bereitzustellen:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Vollständige Anweisungen finden Sie unter "Konvertieren oder importieren Sie die vSphere-Umgebung in das SDDC Manager-Inventar" .

Lizenzierung zu VCF hinzufügen

Nach Abschluss der Konvertierung muss der Umgebung eine Lizenzierung hinzugefügt werden.

1. Melden Sie sich bei der SDDC Manager-Benutzeroberfläche an.
2. Navigieren Sie im Navigationsbereich zu **Administration > Lizenzierung**.
3. Klicken Sie auf **+ Lizenzschlüssel**.
4. Wählen Sie ein Produkt aus dem Dropdown-Menü.
5. Geben Sie den Lizenzschlüssel ein.
6. Geben Sie eine Beschreibung für die Lizenz ein.
7. Klicken Sie auf **Hinzufügen**.
8. Wiederholen Sie diese Schritte für jede Lizenz.

Videodemo für ONTAP tools for VMware vSphere 10

NFS-Datenspeicher mit ONTAP tools for VMware vSphere 10

Konvertieren Sie die vCenter-Serverinstanz in eine VCF-Verwaltungsdomäne (FC-Datenspeicher).

Konvertieren Sie einen vSphere 8-Cluster mit ONTAP Fibre Channel-Datenspeichern in eine VMware Cloud Foundation-Verwaltungsdomäne. Dieses Verfahren umfasst die Bereitstellung von FC-Speicher, die Bereitstellung von ONTAP Tools für VMware und die Verwendung des VCF-Importtools zum Migrieren und Verwalten des Clusters innerhalb der VCF-Umgebung.

Einführung

Die Konvertierung einer vSphere-Umgebung mit einem vorhandenen Fibre Channel (FC)-Datenspeicher, der auf ONTAP ausgeführt wird, umfasst die Integration der vorhandenen Infrastruktur in eine moderne private Cloud-Architektur. Dieser Prozess profitiert von der Robustheit des FC-Speichers, um einen nahtlosen Datenzugriff und eine nahtlose Datenverwaltung zu gewährleisten. Nachdem durch den Konvertierungsprozess eine VCF-Verwaltungsdomäne eingerichtet wurde, können Administratoren zusätzliche vSphere-Umgebungen, einschließlich solcher, die FC-Datenspeicher verwenden, effizient in das VCF-Ökosystem importieren. Diese Integration verbessert nicht nur die Ressourcennutzung, sondern vereinfacht auch die Verwaltung der privaten Cloud-Infrastruktur und gewährleistet einen reibungslosen Übergang mit minimaler Unterbrechung der vorhandenen Arbeitslasten.

In dieser Lösung zeigen wir, wie ein FC-Datenspeicher in vSphere 8 zum Hauptspeicher wird, wenn der Cluster in eine VCF-Verwaltungsdomäne konvertiert wird.

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Stellen Sie ONTAP tools for VMware vSphere 10 bereit.
- Stellen Sie einen FC-Datenspeicher mit ONTAP -Tools bereit.
- Verwenden Sie das VCF-Importtool, um den vSphere-Cluster zu validieren.
- Stellen Sie den SDDC Manager im vSphere-Cluster bereit.
- Konfigurieren Sie eine JSON-Datei, um während der VCF-Konvertierung NSX zu erstellen.
- Verwenden Sie das VCF-Importtool, um den vSphere 8-Cluster in VCF 5.2.1 zu konvertieren

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- NetApp ASA R2/ ASA/ AFF -Speichersystem mit einer Storage Virtual Machine (SVM), die für die Zulassung von Fibre Channel (FC)-Verkehr konfiguriert ist.
- Die logische Schnittstelle (LIF) wurde zur Übertragung des FC-Verkehrs erstellt und ist mit der SVM verknüpft.
- Auf den Switches, die für die Übertragung von FC-Verkehr vorgesehen sind, wurde FC-Zoning konfiguriert.
- Ein vSphere 8-Cluster mit 4 x ESXi-Hosts und einer auf dem Cluster co-lokalisierten vCenter-Appliance.
- Für vMotion konfigurierte verteilte Portgruppe auf den zu diesem Zweck eingerichteten VLANs oder Netzwerksegmenten.
- Laden Sie die für die VCF-Konvertierung erforderliche Software herunter.

ONTAP tools for VMware vSphere 10 können entweder in HA- oder Nicht-HA-Konfigurationen installiert werden. Ausführliche Informationen zu den Voraussetzungen für ONTAP -Tools finden Sie unter "Voraussetzungen für ONTAP tools for VMware vSphere" .

Informationen zum unterstützten Speicher und andere Überlegungen zum Konvertieren oder Importieren von vSphere in VCF 5.2 finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Die erforderliche Software finden Sie unter "Laden Sie Software zum Konvertieren oder Importieren vorhandener vSphere-Umgebungen herunter" .

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"Dokumentation zu VMware Cloud Foundation 5.2" .

Bereitstellungsschritte

Die Lösung umfasst die Verwendung von ONTAP tools for VMware vSphere zur Bereitstellung von FC-Datenspeichern und den Prozess der Konvertierung eines vorhandenen vSphere 8-Clusters in eine VCF-Verwaltungsdomäne.

Führen Sie die folgenden Schritte aus:

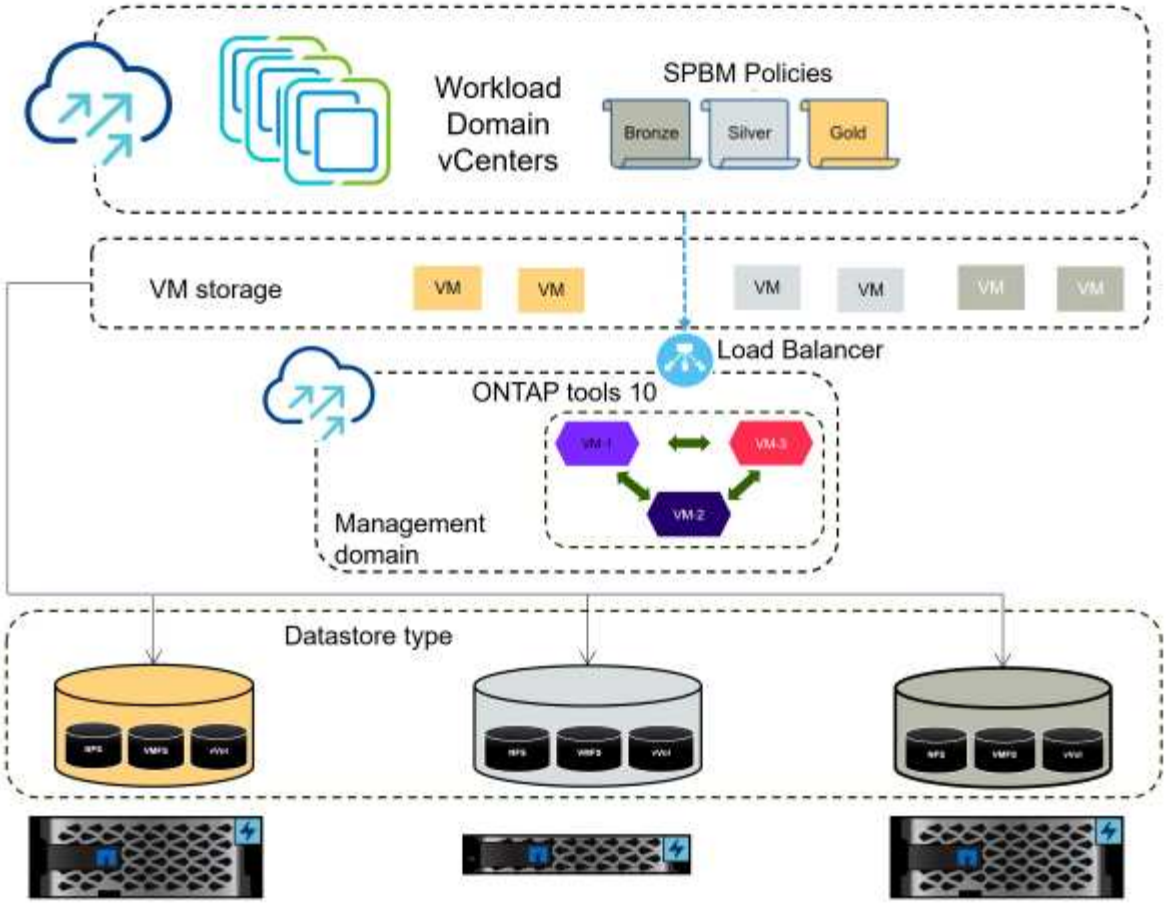
- Stellen Sie ONTAP tools for VMware vSphere 10 bereit.
- Stellen Sie einen FC-Datenspeicher mit ONTAP -Tools bereit.
- Kopieren Sie das VCF-Importtool auf die vCenter-Appliance.
- Führen Sie mit dem VCF-Importtool eine Vorprüfung auf der vCenter-Appliance durch.
- Stellen Sie die SDDC-Manager-VM auf dem vCenter-Cluster bereit.
- Erstellen Sie eine JSON-Datei für einen NSX-Cluster, der während des Konvertierungsvorgangs bereitgestellt werden soll.
- Laden Sie die erforderliche Software in den SDDC-Manager hoch.
- Konvertieren Sie den vSphere-Cluster in das SDDC-Manager-Inventar.

Eine Übersicht über den Konvertierungsprozess finden Sie unter "Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workload-Domäne in VMware Cloud Foundation" .

Bereitstellen von ONTAP -Tools und Bereitstellen eines FC-Datenspeichers

Die Architektur von ONTAP Tools 10 ist auf eine nahtlose Integration in VMware-Umgebungen ausgelegt und nutzt ein modulares und skalierbares Framework, das die ONTAP Tools-Dienste, das vSphere-Plug-in und REST-APIs umfasst, um eine effiziente Speicherverwaltung, Automatisierung und Datensicherung zu ermöglichen.

ONTAP tools for VMware vSphere 10 können entweder in HA- oder Nicht-HA-Konfigurationen installiert werden.

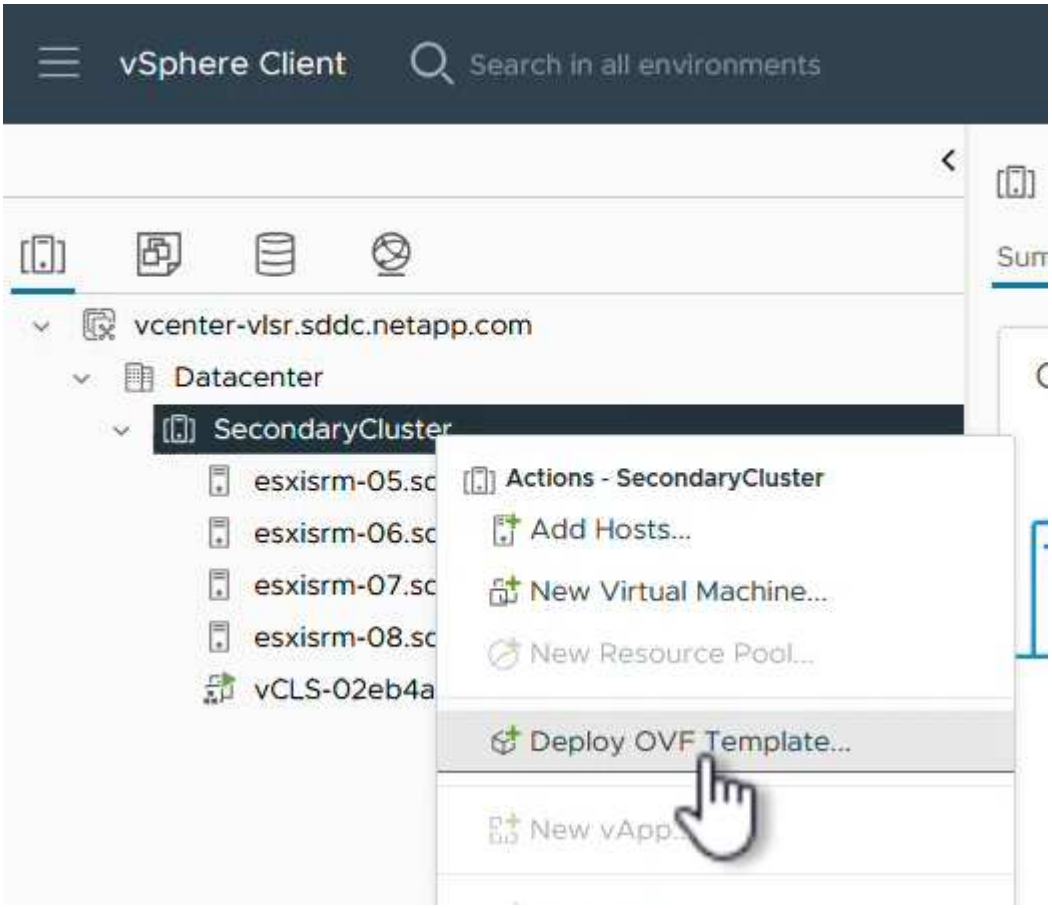

Workload
Domain
vCenters
SPBM Policies
Bronze
Silver
Gold
VM storage
VM
VM
VM
VM
VM
VM
Load Balancer
ONTAP tools 10
VM-1
VM-3
VM-2
Management
domain
Datastore type

Bereitstellen von ONTAP tools for VMware vSphere 10

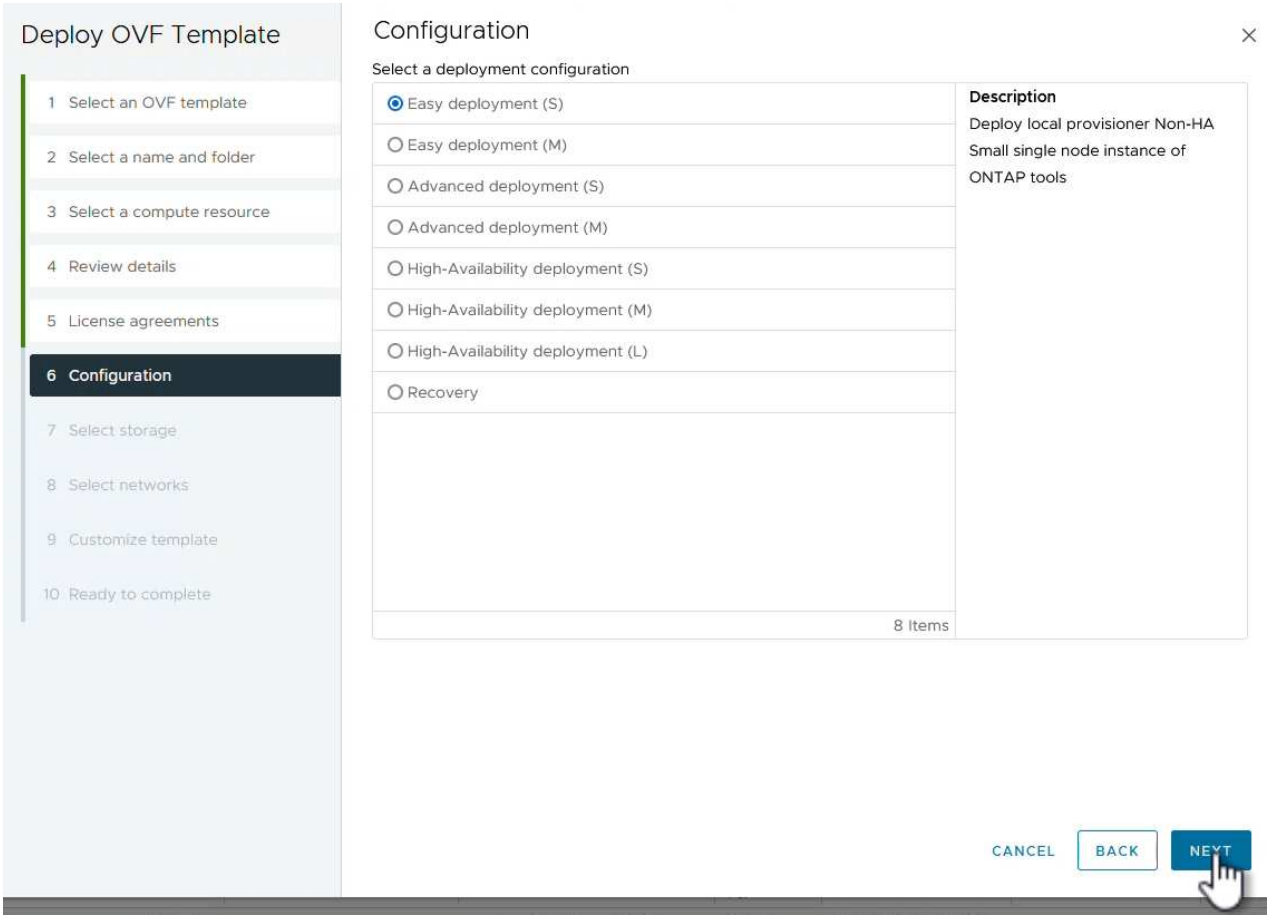
In diesem Schritt wird ONTAP Tools 10 mit einer Nicht-HA-Konfiguration bereitgestellt.

Weitere Informationen zur Bereitstellung von HA- und Nicht-HA-Konfigurationen finden Sie unter "Bereitstellen von ONTAP tools for VMware vSphere" .

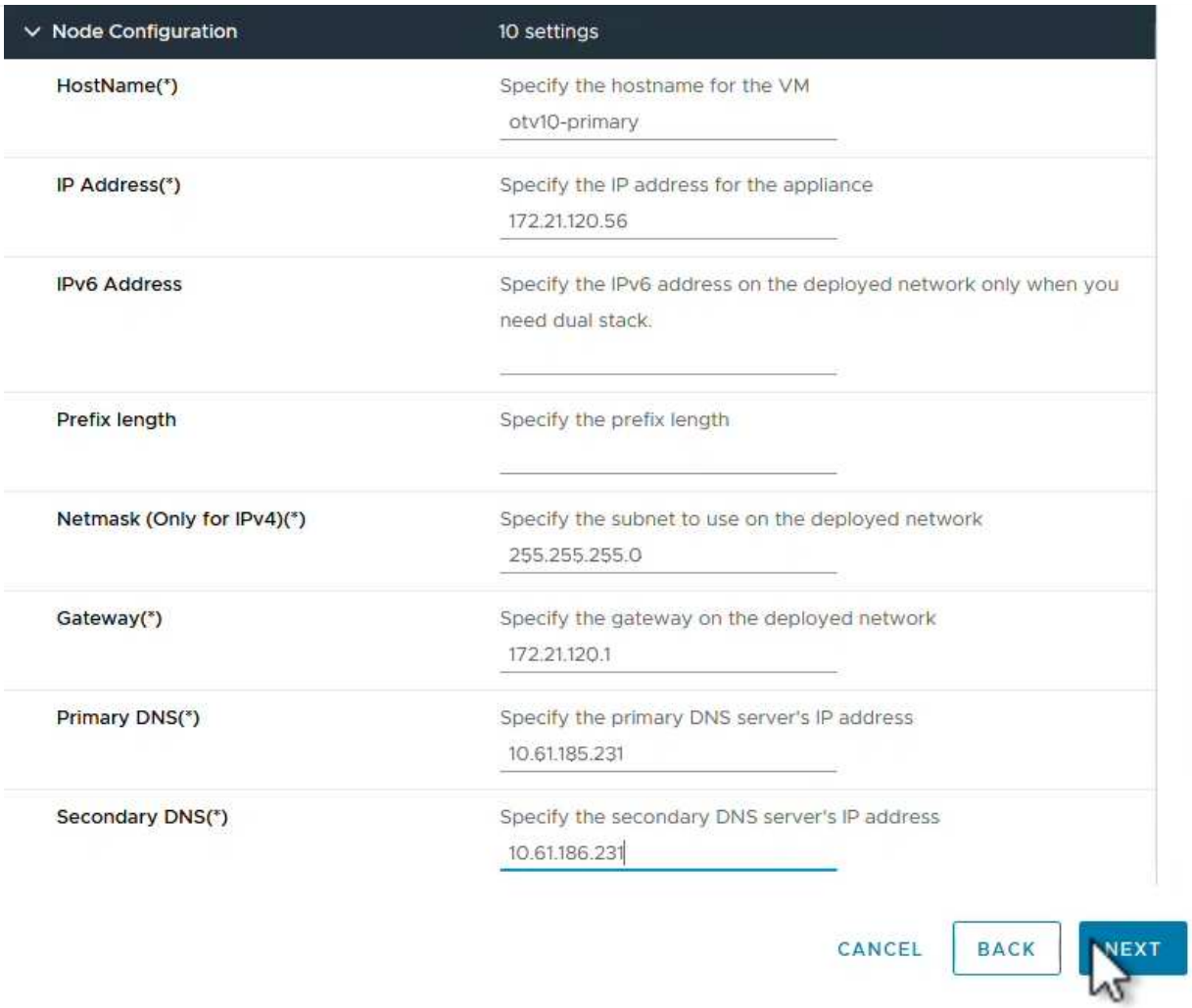
1. Laden Sie die ONTAP Tools 10 OVA-Vorlage von der "NetApp Support-Site" .
2. Klicken Sie im vSphere-Client mit der rechten Maustaste auf den Cluster und klicken Sie auf **OVF-Vorlage bereitstellen**



3. Führen Sie in der **OVF-Vorlage bereitstellen** die folgenden Schritte aus:
   - Wählen Sie eine OVF-Vorlage aus.
   - Wählen Sie einen Namen und einen Ordner aus.
   - Wählen Sie eine Rechenressource aus.
   - Details überprüfen.
   - Stimmen Sie der Lizenzvereinbarung zu.
4. Wählen Sie auf der Seite **Konfiguration** der Vorlage den Bereitstellungstyp aus und geben Sie an, ob ONTAP -Tools in einer HA-Konfiguration bereitgestellt werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.



5. Wählen Sie auf der Seite **Speicher auswählen** den Datenspeicher aus, auf dem die VM installiert werden soll, und klicken Sie auf **Weiter**.
6. Wählen Sie das Netzwerk aus, über das die ONTAP -Tools-VM kommunizieren wird. Klicken Sie auf **Weiter**, um fortzufahren.
7. Geben Sie im Fenster „Vorlage anpassen“ alle erforderlichen Informationen ein.
    - Benutzername und Passwort der Anwendung
    - Wählen Sie, ob ASUP (Auto Support) einschließlich einer Proxy-URL aktiviert werden soll.
    - Benutzername und Passwort des Administrators.
    - NTP-Server.
    - Benutzername und Passwort für die Wartung (Wartungskonto, das an der Konsole verwendet wird).
    - Geben Sie die erforderlichen IP-Adressen für die Bereitstellungskonfiguration an.
    - Geben Sie alle Netzwerkinformationen für die Knotenkonfiguration an.

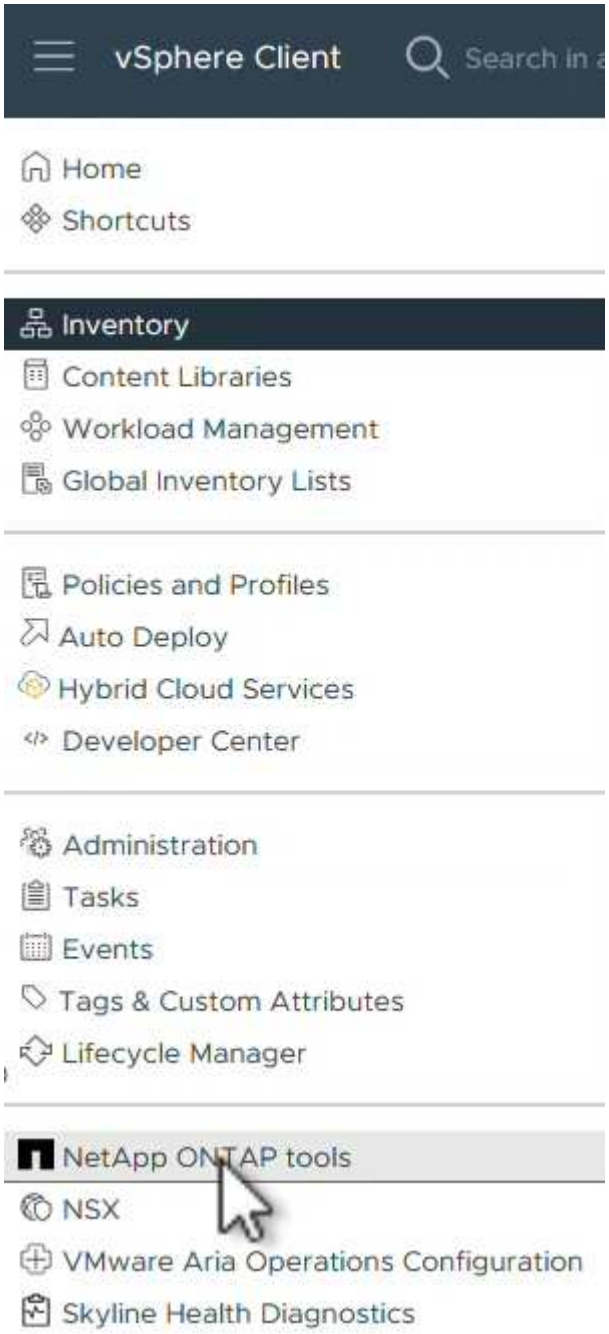


8. Klicken Sie abschließend auf **Weiter**, um fortzufahren, und dann auf **Fertig**, um mit der Bereitstellung zu beginnen.

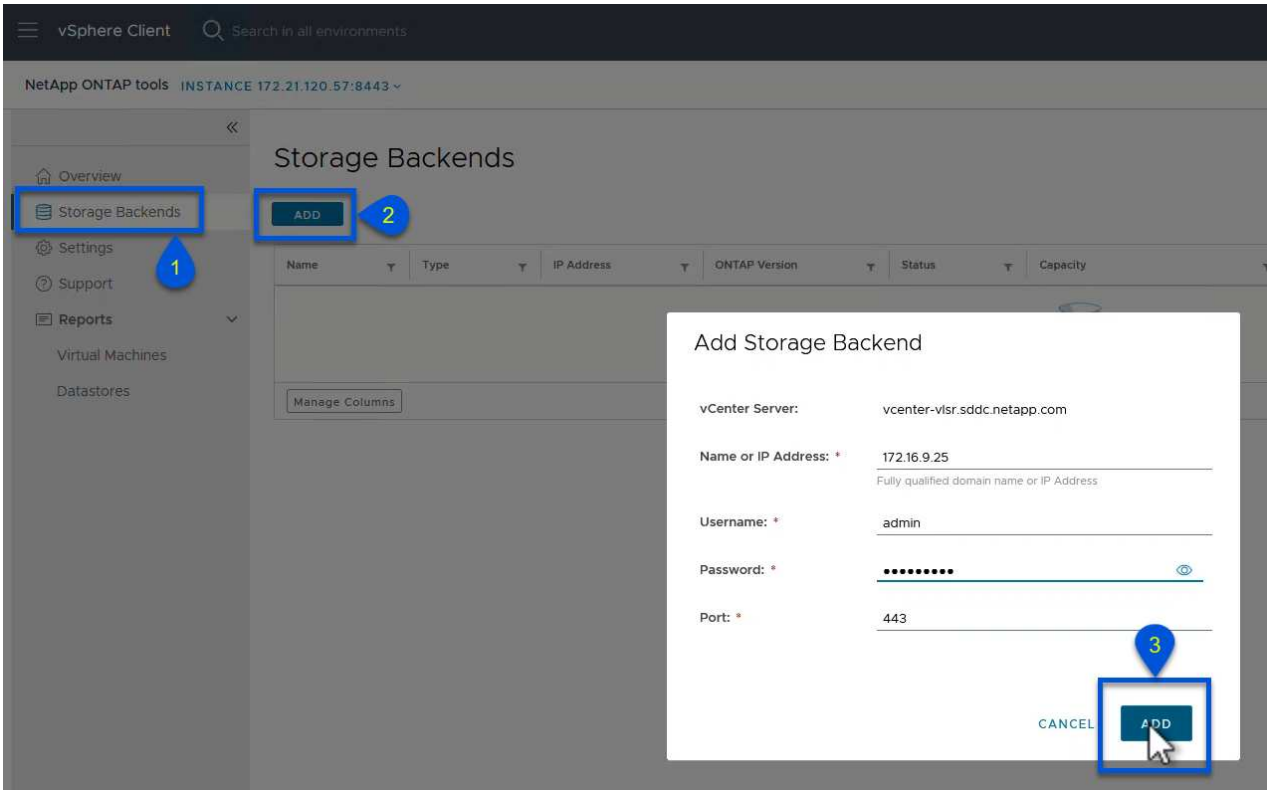
Konfigurieren Sie ONTAP -Tools

Sobald die ONTAP -Tools-VM installiert und eingeschaltet ist, sind einige grundlegende Konfigurationsschritte erforderlich, beispielsweise das Hinzufügen von vCenter-Servern und ONTAP Speichersystemen zur Verwaltung. Weitere Informationen finden Sie in der Dokumentation unter "ONTAP tools for VMware vSphere Dokumentation" für detaillierte Informationen.

1. Siehe "vCenter-Instanzen hinzufügen" um die vCenter-Instanzen für die Verwaltung mit ONTAP -Tools zu konfigurieren.
2. Um ein ONTAP Speichersystem hinzuzufügen, melden Sie sich beim vSphere-Client an und navigieren Sie zum Hauptmenü auf der linken Seite. Klicken Sie auf * NetApp ONTAP -Tools*, um die Benutzeroberfläche zu starten.



3. Navigieren Sie im linken Menü zu **Storage Backends** und klicken Sie auf **Hinzufügen**, um auf das Fenster **Storage Backend hinzufügen** zuzugreifen.
4. Geben Sie die IP-Adresse und Anmeldeinformationen für das zu verwaltende ONTAP Speichersystem ein. Klicken Sie zum Abschluss auf **Hinzufügen**.

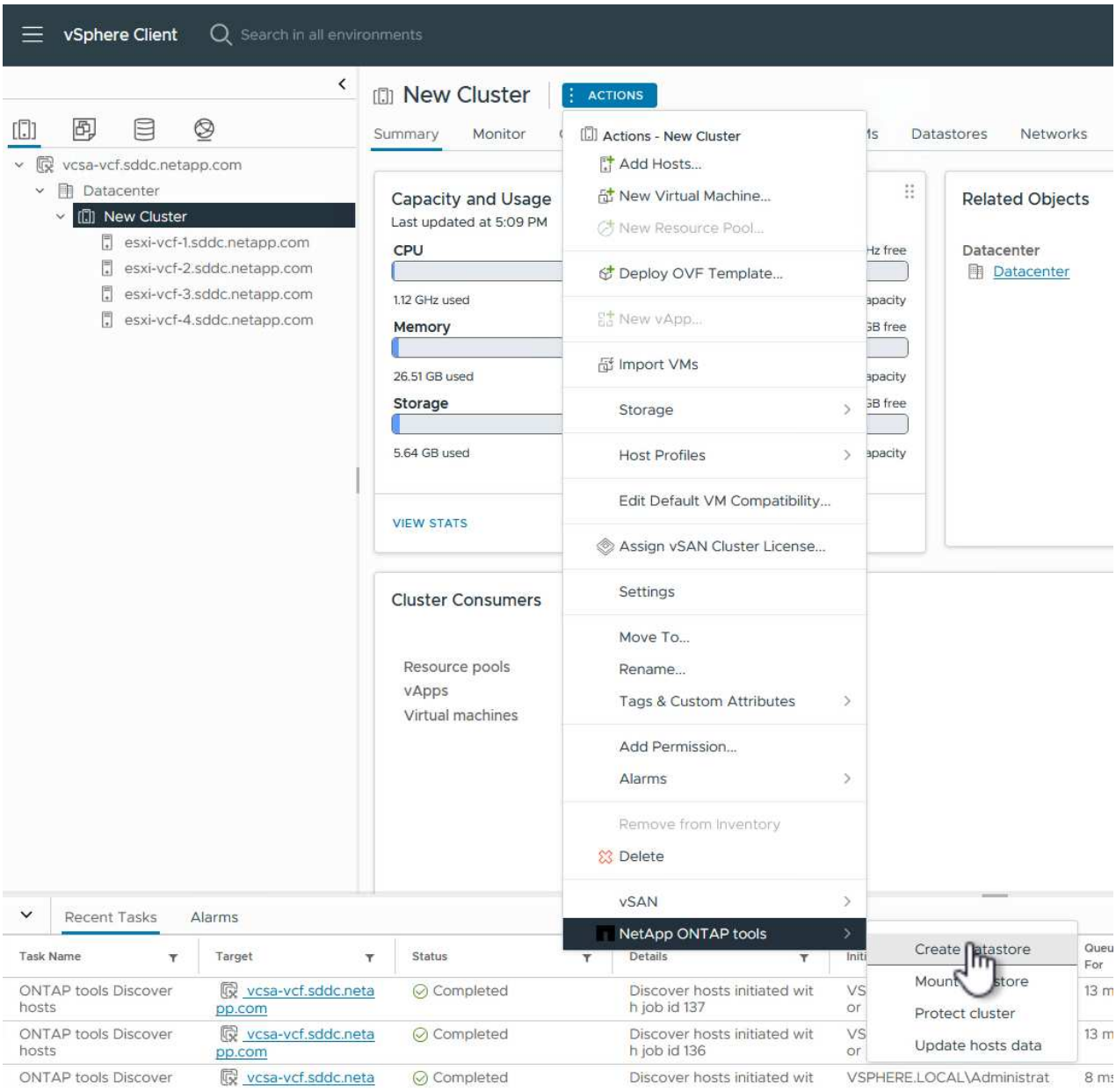


Hier wird das Speicher-Backend mithilfe der Cluster-IP-Adresse in der vSphere-Client-Benutzeroberfläche hinzugefügt. Dies ermöglicht die vollständige Verwaltung aller SVMs im Speichersystem. Alternativ kann das Storage-Backend hinzugefügt und mit einer vCenter-Instanz verknüpft werden, indem man den ONTAP Tools Manager verwendet. `https://loadBalanceIP:8443/virtualization/ui/` . Mit dieser Methode können in der Benutzeroberfläche des vSphere-Clients nur SVM-Anmeldeinformationen hinzugefügt werden, was eine genauere Kontrolle über den Speicherzugriff ermöglicht.

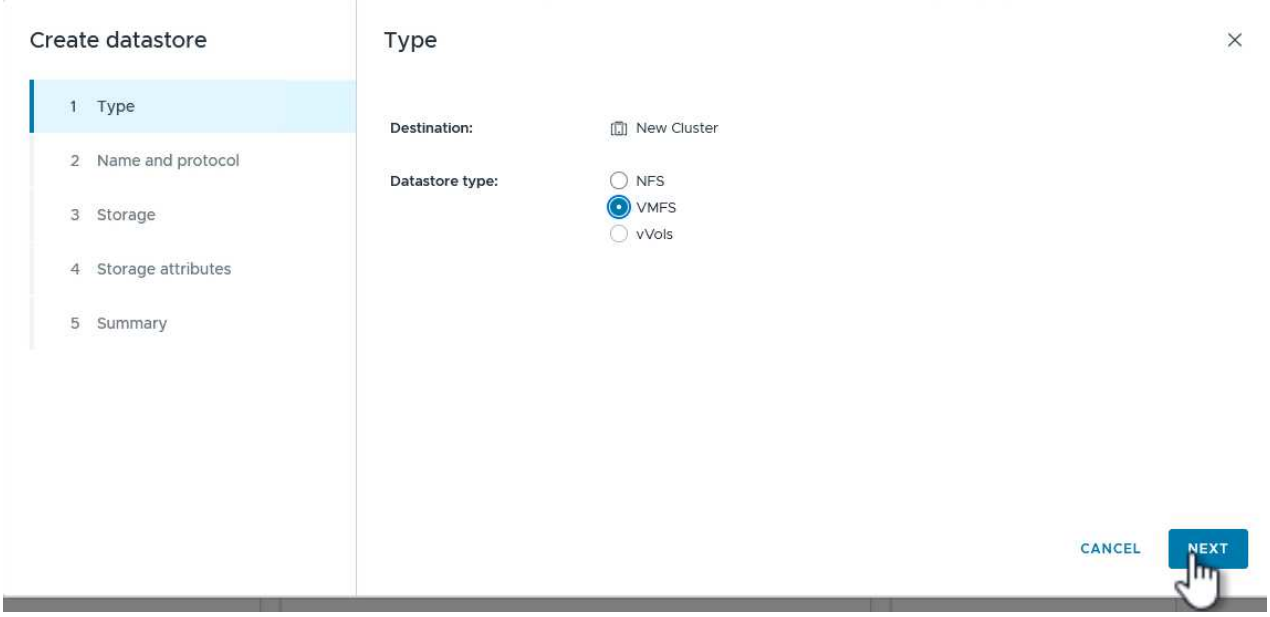
Bereitstellen eines FC-Datenspeichers mit ONTAP -Tools

ONTAP -Tools integrieren Funktionen in die gesamte vSphere-Client-Benutzeroberfläche. In diesem Schritt wird ein FC-Datenspeicher von der Inventarseite des Hosts bereitgestellt.

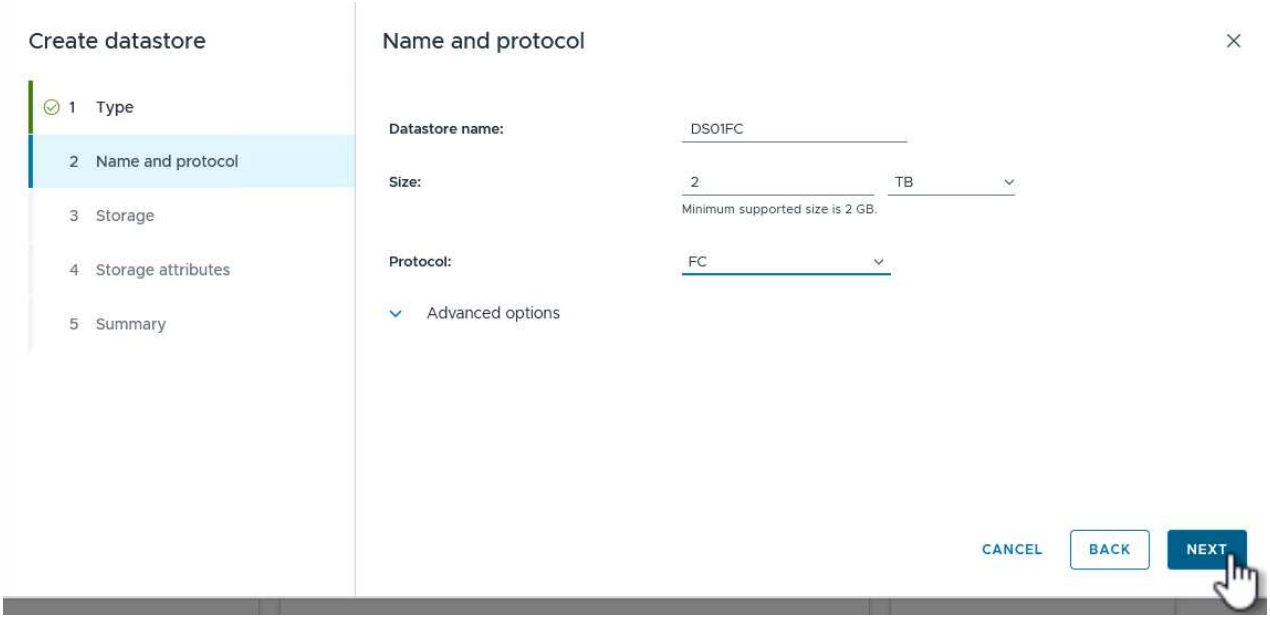
1. Navigieren Sie im vSphere-Client zum Inventar der Hosts (oder Speicher).
2. Navigieren Sie zu **AKTIONEN > NetApp ONTAP -Tools > Datenspeicher erstellen**.



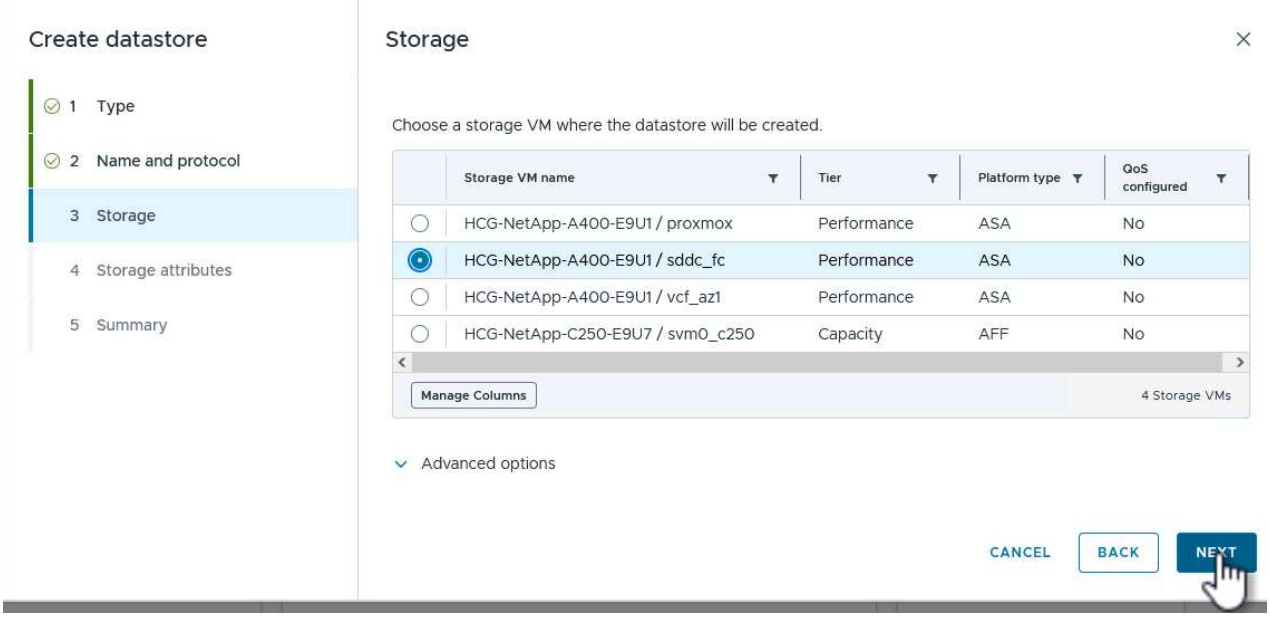
3. Wählen Sie im Assistenten **Datenspeicher erstellen** VMFS als Typ des zu erstellenden Datenspeichers aus.



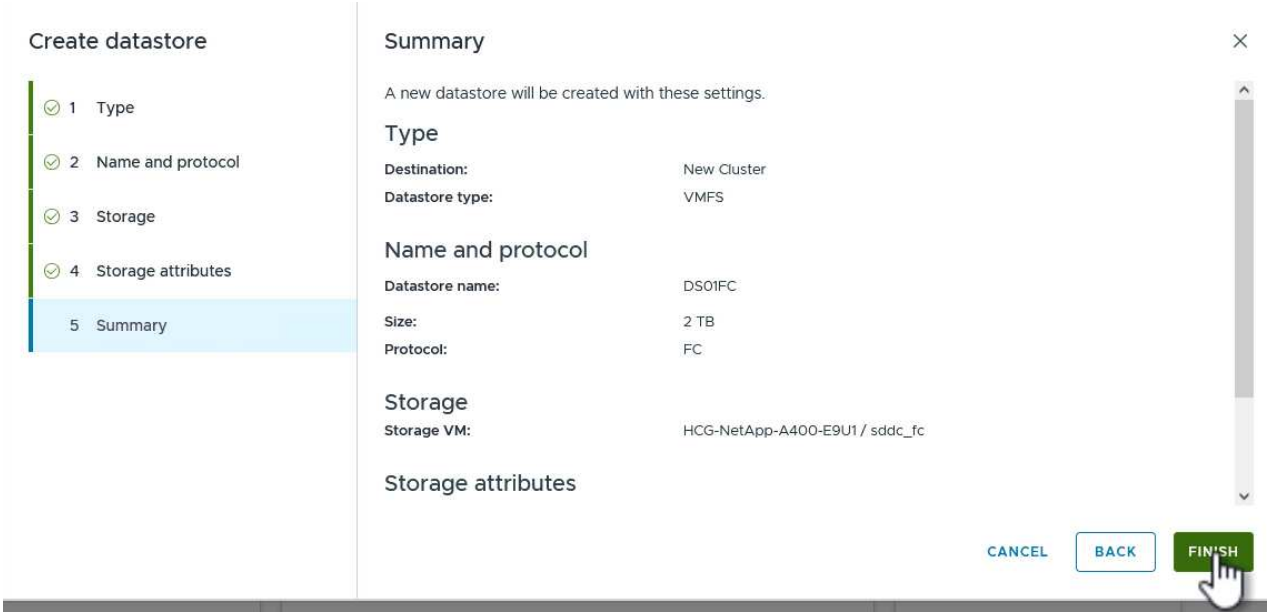
4. Geben Sie auf der Seite **Name und Protokoll** einen Namen für den Datenspeicher, die Größe und das zu verwendende FC-Protokoll ein.



5. Wählen Sie auf der Seite **Speicher** die ONTAP -Speicherplattform und die Storage Virtual Machine (SVM) aus. Sie können hier auch alle verfügbaren benutzerdefinierten Exportrichtlinien auswählen. Klicken Sie auf **Weiter**, um fortzufahren.



6. Wählen Sie auf der Seite **Speicherattribute** das zu verwendende Speicheraggregat aus. Klicken Sie auf **Weiter**, um fortzufahren.
7. Überprüfen Sie die Informationen auf der Seite **Zusammenfassung** und klicken Sie auf **Fertig**, um den Bereitstellungsprozess zu starten. ONTAP -Tools erstellen ein Volume auf dem ONTAP Speichersystem und mounten es als FC-Datenspeicher auf allen ESXi-Hosts im Cluster.



Konvertieren Sie die vSphere-Umgebung in VCF 5.2

Der folgende Abschnitt behandelt die Schritte zum Bereitstellen des SDDC-Managers und zum Konvertieren des vSphere 8-Clusters in eine VCF 5.2-Verwaltungsdomäne. Gegebenenfalls wird für weitere Einzelheiten auf die VMware-Dokumentation verwiesen.

Das VCF-Importtool von VMware by Broadcom ist ein Dienstprogramm, das sowohl auf der vCenter-Appliance

als auch auf dem SDDC-Manager verwendet wird, um Konfigurationen zu validieren und Konvertierungs- und Importdienste für vSphere- und VCF-Umgebungen bereitzustellen.

Weitere Informationen finden Sie unter "Optionen und Parameter des VCF-Importtools" .

VCF-Importtool kopieren und extrahieren

Die VCF-Importtools werden auf der vCenter-Appliance verwendet, um zu überprüfen, ob sich der vSphere-Cluster für den VCF-Konvertierungs- oder Importvorgang in einem fehlerfreien Zustand befindet.

Führen Sie die folgenden Schritte aus:

1. Folgen Sie den Schritten unter "Kopieren Sie das VCF-Importtool auf die Ziel-vCenter-Appliance" bei VMware Docs, um das VCF-Importtool an den richtigen Speicherort zu kopieren.
2. Extrahieren Sie das Paket mit dem folgenden Befehl:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validieren der vCenter-Appliance

Verwenden Sie das VCF-Importtool, um die vCenter-Appliance vor der Konvertierung zu validieren.

1. Folgen Sie den Schritten unter "Führen Sie vor der Konvertierung eine Vorprüfung des Ziel-vCenters durch" um die Validierung auszuführen.
2. Die folgende Ausgabe zeigt, dass die vCenter-Appliance die Vorprüfung bestanden hat.

```
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter 172.21.166.57 --sso-user administrator@vsphere.local
[2024-10-23 19:03:23,609] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.0-24307788
Enter vCenter SSO password:
[2024-10-23 19:03:28,825] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2024-10-23 19:03:28,938] [INFO] vc_precheck: Connected to vCenter 172.21.166.57 in 0.11 seconds
[2024-10-23 19:03:28,939] [INFO] vc_precheck: Running pre-checks for vCenter 172.21.166.57...
[2024-10-23 19:03:28,939] [INFO] vc_precheck: [1/10] VC BOM version check...                                PASS
[2024-10-23 19:03:28,975] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...                        PASS
[2024-10-23 19:03:28,999] [INFO] vc_precheck: [3/10] Supported storage available check...                   PASS
[2024-10-23 19:03:29,020] [INFO] vc_precheck: [4/10] vCenter VM location check...                           PASS
[2024-10-23 19:03:29,233] [INFO] vc_precheck: [5/10] VxRail registration check...                           PASS
[2024-10-23 19:03:29,414] [INFO] vc_precheck: [6/10] NSX-T registration check...                            PASS
[2024-10-23 19:03:29,437] [INFO] vc_precheck: [7/10] Standalone host check...                               PASS
[2024-10-23 19:03:31,870] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...            PASS
[2024-10-23 19:03:32,962] [INFO] vc_precheck: [9/10] ELM ring topology check...                             PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: [10/10] WCP import check...                                   PASS
[2024-10-23 19:03:33,383] [INFO] vc_precheck: All pre-checks passed!
[2024-10-23 19:03:33,383] [INFO] vc_precheck: Pre-checks for vCenter 172.21.166.57 completed in 4.44 seconds
root@localhost [ /tmp/vcfimport/vcf-brownfield-toolset ]#
```

Bereitstellen des SDDC Managers

Der SDDC-Manager muss sich am selben Standort wie der vSphere-Cluster befinden, der in eine VCF-Verwaltungsdomäne umgewandelt wird.

Befolgen Sie die Bereitstellungsanweisungen in den VMware-Dokumenten, um die Bereitstellung abzuschließen.

Siehe "Stellen Sie die SDDC Manager Appliance auf dem Ziel-vCenter bereit" .

Weitere Informationen finden Sie unter"Kommissionsgastgeber" im VCF-Administrationshandbuch.

Erstellen einer JSON-Datei für die NSX-Bereitstellung

Um NSX Manager bereitzustellen, während Sie eine vSphere-Umgebung in VMware Cloud Foundation importieren oder konvertieren, erstellen Sie eine NSX-Bereitstellungsspezifikation. Für die NSX-Bereitstellung sind mindestens 3 Hosts erforderlich.

Ausführliche Informationen finden Sie unter "Generieren einer NSX-Bereitstellungsspezifikation zum Konvertieren oder Importieren vorhandener vSphere-Umgebungen" .

> Beim Bereitstellen eines NSX Manager-Clusters in einem Konvertierungs- oder Importvorgang wird das NSX-VLAN-Netzwerk verwendet. Einzelheiten zu den Einschränkungen der NSX-VLAN-Vernetzung finden Sie im Abschnitt „Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation“. Informationen zu NSX-VLAN-Netzwerkbeschränkungen finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Nachfolgend sehen Sie ein Beispiel einer JSON-Datei für die NSX-Bereitstellung:

```
{
  "license_key": "xxxxx-xxxxx-xxxxx-xxxxx-xxxxx",
  "form_factor": "medium",
  "admin_password": "************************",
  "install_bundle_path": "/tmp/vcfimport/bundle-133764.zip",
  "cluster_ip": "172.21.166.72",
  "cluster_fqdn": "vcf-m02-nsx01.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "vcf-m02-nsx01a.sddc.netapp.com",
    "name": "vcf-m02-nsx01a",
    "ip_address": "172.21.166.73",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01b.sddc.netapp.com",
    "name": "vcf-m02-nsx01b",
    "ip_address": "172.21.166.74",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "vcf-m02-nsx01c.sddc.netapp.com",
    "name": "vcf-m02-nsx01c",
    "ip_address": "172.21.166.75",
    "gateway": "172.21.166.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Kopieren Sie die JSON-Datei in ein Verzeichnis im SDDC Manager.

Laden Sie Software in den SDDC Manager hoch

Kopieren Sie das VCF-Importtool und das NSX-Bereitstellungspaket in das Verzeichnis /home/vcf/vcfimport im SDDC Manager.

Sehen "Laden Sie die erforderliche Software auf die SDDC Manager Appliance hoch" für detaillierte Anweisungen.

Konvertieren Sie den vSphere-Cluster in eine VCF-Verwaltungsdomäne

Zur Durchführung des Konvertierungsprozesses wird das VCF-Importtool verwendet. Führen Sie den folgenden Befehl aus dem Verzeichnis /home/vcf/vcf-import-package/vcf-brownfield-import-<version>/vcf-brownfield-toolset aus, um einen Ausdruck der Funktionen des VCF-Importtools anzuzeigen:

```
python3 vcf_brownfield.py --help
```

Der folgende Befehl wird ausgeführt, um den vSphere-Cluster in eine VCF-Verwaltungsdomäne zu konvertieren und den NSX-Cluster bereitzustellen:

```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --domain-name '<wld-domain-name>' --nsx-deployment-spec
-path '<nsx-deployment-json-spec-path>'
```

Vollständige Anweisungen finden Sie unter "Konvertieren oder importieren Sie die vSphere-Umgebung in das SDDC Manager-Inventar" .

Lizenzierung zu VCF hinzufügen

Nach Abschluss der Konvertierung muss der Umgebung eine Lizenzierung hinzugefügt werden.

1. Melden Sie sich bei der SDDC Manager-Benutzeroberfläche an.
2. Navigieren Sie im Navigationsbereich zu **Administration > Lizenzierung**.
3. Klicken Sie auf **+ Lizenzschlüssel**.
4. Wählen Sie ein Produkt aus dem Dropdown-Menü.
5. Geben Sie den Lizenzschlüssel ein.
6. Geben Sie eine Beschreibung für die Lizenz ein.
7. Klicken Sie auf **Hinzufügen**.
8. Wiederholen Sie diese Schritte für jede Lizenz.

Videodemo für ONTAP tools for VMware vSphere 10

NFS-Datenspeicher mit ONTAP tools for VMware vSphere 10

Bereitstellen von VCF mit Hauptspeicher

Stellen Sie eine VCF-Umgebung mit ONTAP als primäre Speicherlösung bereit

NetApp ONTAP -Speicher ist eine ideale primäre Speicherlösung für VMware Cloud Foundation (VCF)-Management und Virtual Infrastructure (VI)-Workloaddomänen. ONTAP bietet hohe Leistung, Skalierbarkeit, erweitertes Datenmanagement und nahtlose Integration zur Verbesserung der Betriebseffizienz und des Datenschutzes.

Die technischen Details zur Bereitstellung einer VCF-Umgebung in der entsprechenden Domäne und mit dem entsprechenden Protokoll finden Sie in den folgenden Lösungen.

- "Managementdomäne mit FC"
- "Verwaltungsdomäne mit NFS"
- "Virtuelle Infrastruktur-Workloaddomäne mit FC"
- "Virtuelle Infrastruktur-Workloaddomäne mit NFS"

Verwenden Sie einen FC-basierten VMFS-Datenspeicher auf ONTAP als Hauptspeicher für die VCF-Verwaltungsdomäne

In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung eines vorhandenen FC-basierten VMFS-Datenspeichers auf ONTAP als primären Speicher für VMware Cloud Foundation (VCF)-Verwaltungsdomänen. Dieses Verfahren fasst die erforderlichen Komponenten, Konfigurationen und Bereitstellungsschritte zusammen.

Einführung

Gegebenenfalls verweisen wir auf externe Dokumentationen zu den Schritten, die im SDDC Manager von VCF ausgeführt werden müssen, und verweisen auf die Schritte, die sich speziell auf den Teil zur Speicherkonfiguration beziehen.

Informationen zum Konvertieren einer vorhandenen FC-basierten vSphere-Umgebung mit ONTAP finden Sie unter"Konvertieren Sie die vSphere-Umgebung (FC-Datenspeicher) in eine VCF-Verwaltungsdomäne" .

> Mit VCF Release 5.2 wurde die Möglichkeit eingeführt, eine vorhandene vSphere 8-Umgebung in eine VCF-Verwaltungsdomäne zu konvertieren oder als VCF VI-Workloaddomänen zu importieren. Vor dieser Version war VMware vSAN die einzige Option für den Hauptspeicher für die VCF-Verwaltungsdomäne.

> Diese Lösung ist für ONTAP -Plattformen anwendbar, die FC-Speicher unterstützen, einschließlich NetApp ASA, AFF und FAS.

Voraussetzungen

In diesem Szenario werden die folgenden Komponenten und Konfigurationen verwendet:

- NetApp -Speichersystem mit einer Storage Virtual Machine (SVM), die für die Zulassung von FC-Verkehr konfiguriert ist.
- Auf dem FC-Fabric wurden logische Schnittstellen (LIF) erstellt, die den FC-Verkehr übertragen sollen und mit der SVM verknüpft sind.
- Zoning wurde so konfiguriert, dass auf FC-Switches für Host-HBAs und Speicherziele ein einzelnes Initiator-Ziel-Zoning verwendet wird.

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Bereitstellungsschritte

Verwaltungsdomäne – Standardcluster

Der FC-Principal-Speicher auf dem ursprünglichen Cluster wird nur mit dem VCF-Brownfield-Importtool unterstützt. Wenn VCF mit dem Cloud Builder-Tool (vor Release-Version 5.2.x) bereitgestellt wird, wird nur vSAN unterstützt.

Weitere Informationen zur Verwendung einer vorhandenen vSphere-Umgebung finden Sie unter "Konvertieren der vorhandenen vSphere-Umgebung in eine Verwaltungsdomäne" für weitere Informationen.

Verwaltungsdomäne – Zusätzlicher Cluster

Der zusätzliche vSphere-Cluster in der Verwaltungsdomäne kann mit den folgenden Optionen bereitgestellt werden:

- Besitzen Sie einen zusätzlichen Cluster in der vSphere-Umgebung und verwenden Sie das VCF-Brownfield-Importtool, um die vSphere-Umgebung in eine Verwaltungsdomäne zu konvertieren. "ONTAP tools for VMware vSphere" "System Manager oder ONTAP API" kann verwendet werden, um den VMFS-Datenspeicher im vSphere-Cluster bereitzustellen.
- Verwenden Sie die SDDC-API, um zusätzliche Cluster bereitzustellen. Auf den vSphere-Hosts sollte der VMFS-Datenspeicher konfiguriert sein. Verwenden "System Manager oder ONTAP API" um LUN auf vSphere-Hosts bereitzustellen.
- Verwenden Sie die SDDC Manager-Benutzeroberfläche, um zusätzliche Cluster bereitzustellen. Diese Option erstellt jedoch nur VSAN-Datenspeicher bis Version 5.2.x.

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Verwenden Sie einen NFS-Datenspeicher auf ONTAP als Hauptspeicher für die VCF-Verwaltungsdomäne

In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung eines vorhandenen NFS-Datenspeichers auf ONTAP als primären Speicher für VMware Cloud Foundation (VCF)-Verwaltungsdomänen. Dieses Verfahren fasst die erforderlichen Komponenten, Konfigurationsschritte und den Bereitstellungsprozess zusammen.

Einführung

Gegebenenfalls verweisen wir auf externe Dokumentationen zu den Schritten, die im SDDC Manager von VCF ausgeführt werden müssen, und verweisen auf die Schritte, die sich speziell auf den Teil zur Speicherkonfiguration beziehen.

Informationen zum Konvertieren einer vorhandenen NFS-basierten vSphere-Umgebung mit ONTAP finden Sie unter"Konvertieren Sie die vSphere-Umgebung (NFS-Datenspeicher) in eine VCF-Verwaltungsdomäne" .

Mit VCF Release 5.2 wurde die Möglichkeit eingeführt, eine vorhandene vSphere 8-Umgebung in eine VCF-Verwaltungsdomäne zu konvertieren oder als VCF VI-Workloaddomänen zu importieren. Vor dieser Version war VMware vSAN die einzige Option für den Hauptspeicher für die VCF-Verwaltungsdomäne.

Diese Lösung ist für ONTAP -Plattformen anwendbar, die NFS-Speicher unterstützen, einschließlich NetApp AFF und FAS.

Voraussetzungen

In diesem Szenario werden die folgenden Komponenten und Konfigurationen verwendet:

- NetApp -Speichersystem mit einer Storage Virtual Machine (SVM), die für die Zulassung von NFS-Verkehr konfiguriert ist.
- Im IP-Netzwerk wurde eine logische Schnittstelle (LIF) erstellt, die den NFS-Verkehr übertragen soll und mit der SVM verknüpft ist.
- Ein vSphere 8-Cluster mit 4 x ESXi-Hosts und einer auf dem Cluster co-lokalisierten vCenter-Appliance.
- Verteilte Portgruppe, die für vMotion- und NFS-Speicherverkehr auf den zu diesem Zweck eingerichteten VLANs oder Netzwerksegmenten konfiguriert ist.
- Laden Sie die für die VCF-Konvertierung erforderliche Software herunter.

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Bereitstellungsschritte

Verwaltungsdomäne – Standardcluster

NFS-Prinzipalspeicher auf dem ursprünglichen Cluster wird nur mit dem VCF-Brownfield-Importtool unterstützt. Wenn VCF mit dem Cloud Builder-Tool (bis Version 5.2.x) bereitgestellt wird, wird nur VSAN unterstützt.

Weitere Informationen zur Verwendung einer vorhandenen vSphere-Umgebung finden Sie unter "Konvertieren der vorhandenen vSphere-Umgebung in eine Verwaltungsdomäne" für weitere Informationen.

Verwaltungsdomäne – Zusätzlicher Cluster

Der zusätzliche vSphere-Cluster in der Verwaltungsdomäne kann mit den folgenden Optionen bereitgestellt werden:

- Besitzen Sie einen zusätzlichen Cluster in der vSphere-Umgebung und verwenden Sie das VCF-Brownfield-Importtool, um die vSphere-Umgebung in eine Verwaltungsdomäne zu konvertieren. "ONTAP tools for VMware vSphere" "System Manager oder ONTAP API" kann verwendet werden, um den NFS-Datenspeicher im vSphere-Cluster bereitzustellen.
- Verwenden Sie die SDDC-API, um zusätzliche Cluster bereitzustellen. Für die vSphere-Hosts sollte der NFS-Datenspeicher konfiguriert sein. Verwenden "System Manager oder ONTAP API" um LUN auf vSphere-Hosts bereitzustellen.
- Verwenden Sie die SDDC Manager-Benutzeroberfläche, um zusätzliche Cluster bereitzustellen. Diese Option erstellt jedoch nur vSAN-Datenspeicher mit Versionen vor 5.2.x.

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Verwenden Sie einen FC-basierten VMFS-Datenspeicher auf ONTAP als Hauptspeicher für eine VI-Workload-Domäne

In diesem Anwendungsfall beschreiben wir das Verfahren zum Einrichten eines Fibre Channel (FC) VMFS-Datenspeichers auf ONTAP als primäre Speicherlösung für eine VMware Cloud Foundation (VCF) Virtual Infrastructure (VI)-Workloaddomäne. Dieses Verfahren fasst die erforderlichen Komponenten, Konfigurationsschritte und den Bereitstellungsprozess zusammen.

Vorteile von Fibre Channel

Hohe Leistung: FC bietet Hochgeschwindigkeitsdatenübertragungsraten und ist daher ideal für Anwendungen, die einen schnellen und zuverlässigen Zugriff auf große Datenmengen erfordern.

Geringe Latenz: Sehr geringe Latenz, die für leistungssensible Anwendungen wie Datenbanken und virtualisierte Umgebungen entscheidend ist.

Zuverlässigkeit: FC-Netzwerke sind für ihre Robustheit und Zuverlässigkeit bekannt und verfügen über Funktionen wie integrierte Redundanz und Fehlerkorrektur.

Dedizierte Bandbreite: FC bietet dedizierte Bandbreite für Speicherverkehr und reduziert so das Risiko einer Netzwerküberlastung.

Weitere Informationen zur Verwendung von Fibre Channel mit NetApp -Speichersystemen finden Sie unter "SAN-Bereitstellung mit FC" .

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Erstellen Sie eine Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für FC-Verkehr.
- Sammeln Sie WWPN-Informationen der bereitzustellenden Hosts und erstellen Sie entsprechende Initiatorgruppen auf dem ONTAP Speichersystem.
- Erstellen Sie ein FC-Volume auf dem ONTAP -Speichersystem.
- Ordnen Sie Initiatorgruppen zu, um ein FC-Volume zu erstellen
- Nutzen Sie Single-Initiator-Target-Zoning auf FC-Switches. Erstellen Sie für jeden Initiator eine Zone (Einzelinitiatorzone).
  - Fügen Sie für jede Zone ein Ziel ein, das die logische ONTAP FC-Schnittstelle (WWPN) für die SVMs ist. Es sollten mindestens zwei logische Schnittstellen pro Knoten und SVM vorhanden sein. Verwenden Sie nicht die WWPN der physischen Ports.
- Erstellen Sie im SDDC Manager einen Netzwerkpool für vMotion-Datenverkehr.
- Beauftragen Sie Hosts in VCF zur Verwendung in einer VI-Workload-Domäne.
- Stellen Sie eine VI-Workload-Domäne in VCF bereit, indem Sie einen FC-Datenspeicher als Hauptspeicher

verwenden.

> Diese Lösung ist für ONTAP -Plattformen anwendbar, die NFS-Speicher unterstützen, einschließlich NetApp AFF und FAS.

Voraussetzungen

In diesem Szenario werden die folgenden Komponenten und Konfigurationen verwendet:

- Ein ONTAP AFF oder ASA Speichersystem mit FC-Ports, die mit FC-Switches verbunden sind.
- SVM mit FC-Lifs erstellt.
- vSphere mit FC-HBAs, die mit FC-Switches verbunden sind.
- Auf FC-Switches ist eine einzelne Initiator-Ziel-Zonierung konfiguriert.

> NetApp empfiehlt Multipath für FC-LUNs.

Bereitstellungsschritte

Verwaltungsdomäne – Standardcluster

FC-Principal-Speicher auf dem ersten Cluster wird nur mit dem VCF-Brownfield-Importtool unterstützt. Wenn VCF mit dem Cloudbuilder-Tool (bis Version 5.2.x) bereitgestellt wird, wird nur VSAN unterstützt. Verweisen "Konvertieren der vorhandenen vSphere-Umgebung in eine Verwaltungsdomäne" für weitere Informationen.

Verwaltungsdomäne – Zusätzlicher Cluster

Der zusätzliche vSphere-Cluster in der Verwaltungsdomäne kann mit den folgenden Optionen bereitgestellt werden: * Sorgen Sie für einen zusätzlichen Cluster in der vSphere-Umgebung und verwenden Sie das VCF-Brownfield-Importtool, um die vSphere-Umgebung in eine Verwaltungsdomäne zu konvertieren. "ONTAP tools for VMware vSphere" , "System Manager oder ONTAP API" kann verwendet werden, um den VMFS-Datenspeicher im vSphere-Cluster bereitzustellen. * Verwenden Sie die SDDC-API, um zusätzliche Cluster bereitzustellen. Auf den vSphere-Hosts sollte der VMFS-Datenspeicher konfiguriert sein. Verwenden "System Manager oder ONTAP API" um LUN auf vSphere-Hosts bereitzustellen. * Verwenden Sie die SDDC Manager-Benutzeroberfläche, um zusätzliche Cluster bereitzustellen. Diese Option erstellt jedoch nur VSAN-Datenspeicher bis Version 5.2.x.

VI-Workloaddomäne – Standardcluster

Nachdem die Verwaltungsdomäne eingerichtet und ausgeführt wird, kann die VI-Workloaddomäne erstellt werden:

- Verwenden der SDDC Manager-Benutzeroberfläche. Auf den vSphere-Hosts sollte der VMFS-Datenspeicher konfiguriert sein. Verwenden Sie System Manager oder ONTAP API, um LUN auf vSphere-Hosts bereitzustellen.
- Importieren Sie eine vorhandene vSphere-Umgebung als neue VI-Workload-Domäne. ONTAP tools for VMware vSphere, System Manager oder ONTAP API können verwendet werden, um den VMFS-Datenspeicher im vSphere-Cluster bereitzustellen.

VI-Workloaddomäne – Zusätzlicher Cluster

Sobald die VI-Arbeitslast läuft, können mithilfe der folgenden Optionen zusätzliche Cluster mit VMFS auf FC LUN bereitgestellt werden.

- Zusätzliche Cluster in der vSphere-Umgebung wurden mit dem VCF-Brownfield-Importtool importiert. ONTAP tools for VMware vSphere, System Manager oder ONTAP API können verwendet werden, um den VMFS-Datenspeicher im vSphere-Cluster bereitzustellen.
- Verwenden Sie die SDDC Manager-Benutzeroberfläche oder API, um zusätzliche Cluster bereitzustellen. Auf den vSphere-Hosts sollte der VMFS-Datenspeicher konfiguriert sein. Verwenden Sie System Manager oder ONTAP API, um LUN auf vSphere-Hosts bereitzustellen.

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Verwenden Sie einen NFS-Datenspeicher auf ONTAP als Hauptspeicher für eine VI-Workloaddomäne

In diesem Anwendungsfall beschreiben wir das Verfahren zum Konfigurieren eines NFS-Datenspeichers auf ONTAP als primäre Speicherlösung für eine VMware Cloud Foundation (VCF) Virtual Infrastructure (VI)-Workloaddomäne. Dieses Verfahren fasst die erforderlichen Komponenten, Konfigurationsschritte und den Bereitstellungsprozess zusammen.

Vorteile von NFS

Einfachheit und Benutzerfreundlichkeit: NFS lässt sich unkompliziert einrichten und verwalten und ist daher eine ausgezeichnete Wahl für Umgebungen, in denen eine schnelle und einfache Dateifreigabe erforderlich ist.

Skalierbarkeit: Die Architektur von ONTAP ermöglicht eine effiziente Skalierung von NFS und unterstützt wachsende Datenanforderungen ohne wesentliche Änderungen an der Infrastruktur.

Flexibilität: NFS unterstützt eine breite Palette von Anwendungen und Workloads und ist daher vielseitig für verschiedene Anwendungsfälle geeignet, einschließlich virtualisierter Umgebungen.

Weitere Informationen finden Sie im NFS v3-Referenzhandbuch für vSphere 8.

Weitere Informationen zur Verwendung von Fibre Channel mit NetApp -Speichersystemen finden Sie unter"NFS v3-Referenzhandbuch für vSphere 8" .

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Erstellen Sie eine Storage Virtual Machine (SVM) mit logischer Schnittstelle (LIFs) für NFS-Straftic
- Überprüfen Sie die Vernetzung für die ONTAP Storage Virtual Machine (SVM) und stellen Sie sicher, dass eine logische Schnittstelle (LIF) zur Übertragung des NFS-Verkehrs vorhanden ist.
- Erstellen Sie eine Exportrichtlinie, um den ESXi-Hosts Zugriff auf das NFS-Volume zu gewähren.
- Erstellen Sie ein NFS-Volume auf dem ONTAP Speichersystem.
- Erstellen Sie im SDDC Manager einen Netzwerkpool für NFS- und vMotion-Datenverkehr.
- Beauftragen Sie Hosts in VCF zur Verwendung in einer VI-Workload-Domäne.

- Stellen Sie eine VI-Workload-Domäne in VCF bereit, indem Sie einen NFS-Datenspeicher als Hauptspeicher verwenden.
- Installieren Sie das NetApp NFS-Plug-in für VMware VAAI

> Diese Lösung ist für ONTAP -Plattformen anwendbar, die NFS-Speicher unterstützen, einschließlich NetApp AFF und FAS.

Voraussetzungen

In diesem Szenario werden die folgenden Komponenten und Konfigurationen verwendet:

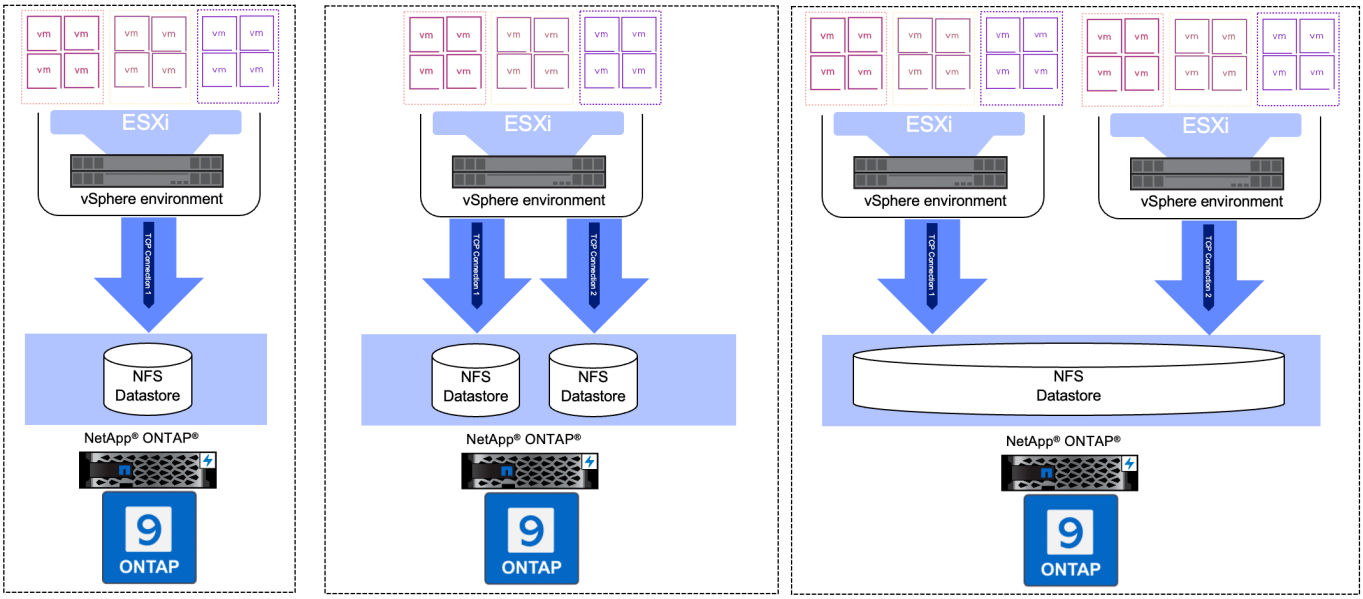
- NetApp AFF -Speichersystem mit einer Storage Virtual Machine (SVM), die für die Zulassung von NFS-Verkehr konfiguriert ist.
- Im IP-Netzwerk wurde eine logische Schnittstelle (LIF) erstellt, die den NFS-Verkehr übertragen soll und mit der SVM verknüpft ist.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf die SDDC Manager-Schnittstelle kann zugegriffen werden.
- 4 x ESXi-Hosts, die für die Kommunikation im VCF-Verwaltungsnetzwerk konfiguriert sind.
- Für vMotion- und NFS-Speicherverkehr reservierte IP-Adressen im zu diesem Zweck eingerichteten VLAN oder Netzwerksegment.

> Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass entweder 1) das Verwaltungsnetzwerk zum NFS-Server geroutet werden kann oder 2) dem SVM, auf dem das NFS-Datenspeichervolume gehostet wird, ein LIF für das Verwaltungsnetzwerk hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Weitere Informationen zur Verwendung von NFS mit vSphere-Clustern finden Sie im"NFS v3-Referenzhandbuch für vSphere 8" .



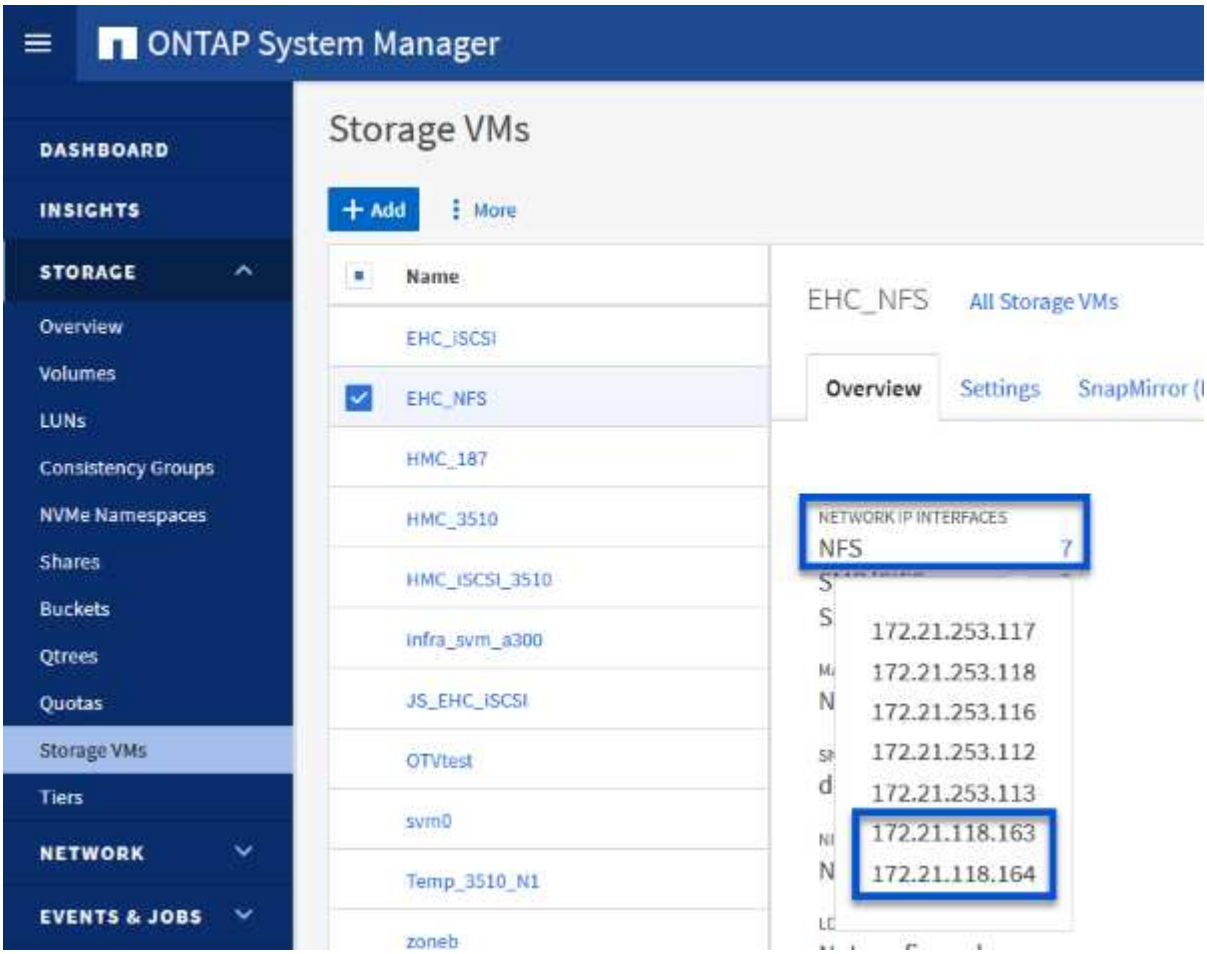
Bereitstellungsschritte

Führen Sie die folgenden Schritte aus, um eine VI-Workload-Domäne mit einem NFS-Datenspeicher als Hauptspeicher bereitzustellen:

Überprüfen des Netzwerks für ONTAP SVM

Stellen Sie sicher, dass die erforderlichen logischen Schnittstellen für das Netzwerk eingerichtet wurden, das den NFS-Verkehr zwischen dem ONTAP -Speichercluster und der VI-Workload-Domäne überträgt.

1. Navigieren Sie im ONTAP System Manager im linken Menü zu **Storage VMs** und klicken Sie auf die SVM, die für den NFS-Verkehr verwendet werden soll. Klicken Sie auf der Registerkarte **Übersicht** unter **NETZWERK-IP-SCHNITTSTELLEN** auf die Zahl rechts neben **NFS**. Überprüfen Sie in der Liste, ob die erforderlichen LIF-IP-Adressen aufgeführt sind.



Alternativ können Sie die mit einem SVM verknüpften LIFs über die ONTAP -CLI mit dem folgenden Befehl überprüfen:

```
network interface show -vserver <SVM_NAME>
```

1. Überprüfen Sie, ob die ESXi-Hosts mit dem ONTAP NFS-Server kommunizieren können. Melden Sie sich per SSH beim ESXi-Host an und pingen Sie das SVM-LIF an:

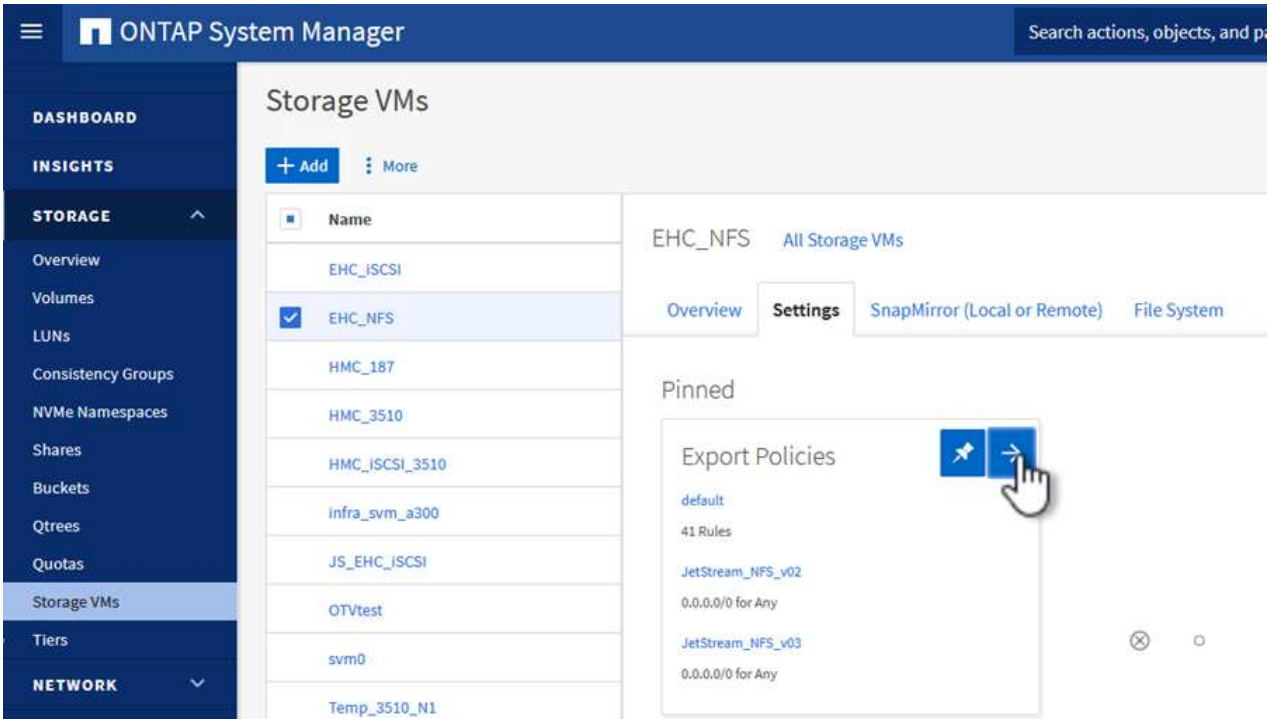
```
vmkping <IP Address>
```

Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass entweder 1) das Verwaltungsnetzwerk zum NFS-Server geroutet werden kann oder 2) dem SVM, auf dem das NFS-Datenspeichervolume gehostet wird, ein LIF für das Verwaltungsnetzwerk hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

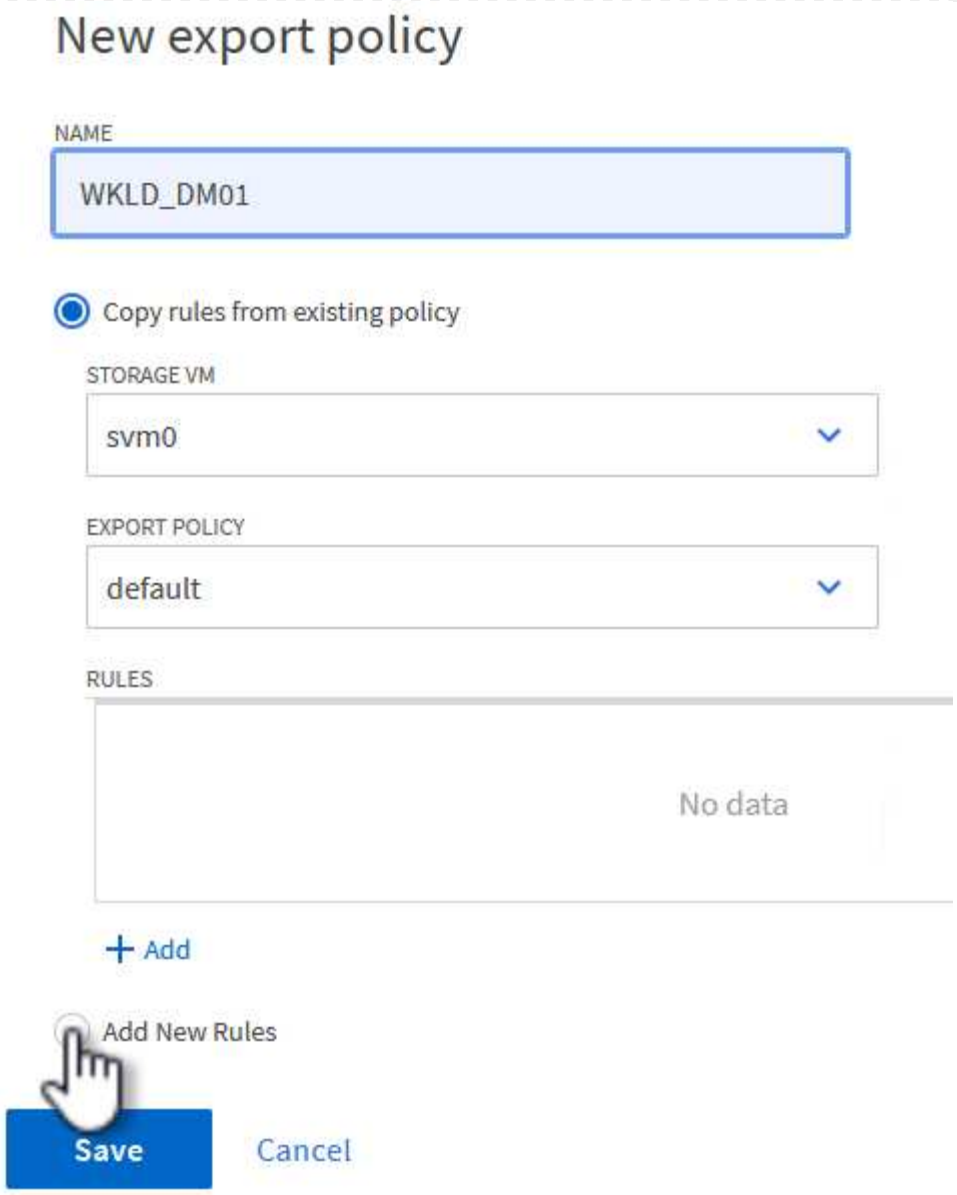
Erstellen Sie eine Exportrichtlinie zum Freigeben des NFS-Volumes

Erstellen Sie eine Exportrichtlinie im ONTAP System Manager, um die Zugriffskontrolle für NFS-Volumes zu definieren.

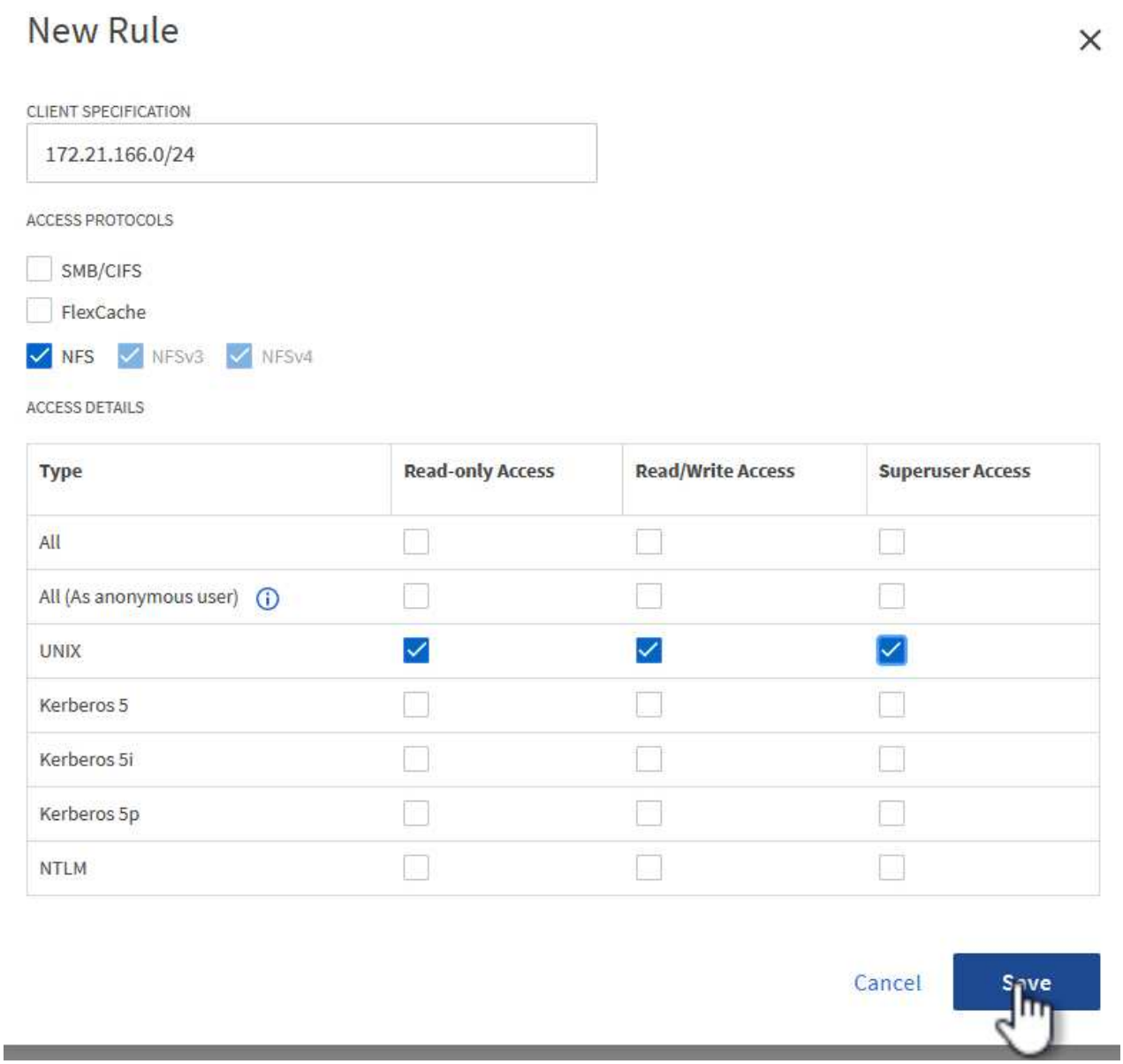
1. Klicken Sie im ONTAP System Manager im linken Menü auf **Storage VMs** und wählen Sie eine SVM aus der Liste aus.
2. Suchen Sie auf der Registerkarte **Einstellungen** nach **Exportrichtlinien** und klicken Sie auf den Pfeil, um darauf zuzugreifen.



3. Geben Sie im Fenster **Neue Exportrichtlinie** einen Namen für die Richtlinie ein, klicken Sie auf die Schaltfläche **Neue Regeln hinzufügen** und dann auf die Schaltfläche **+Hinzufügen**, um mit dem Hinzufügen einer neuen Regel zu beginnen.



4. Geben Sie die IP-Adressen, den IP-Adressbereich oder das Netzwerk ein, das Sie in die Regel einschließen möchten. Deaktivieren Sie die Kontrollkästchen **SMB/Cifs** und * FlexCache* und treffen Sie unten eine Auswahl für die Zugriffsdetails. Für den Zugriff auf den ESXi-Host ist die Auswahl der UNIX-Boxen ausreichend.



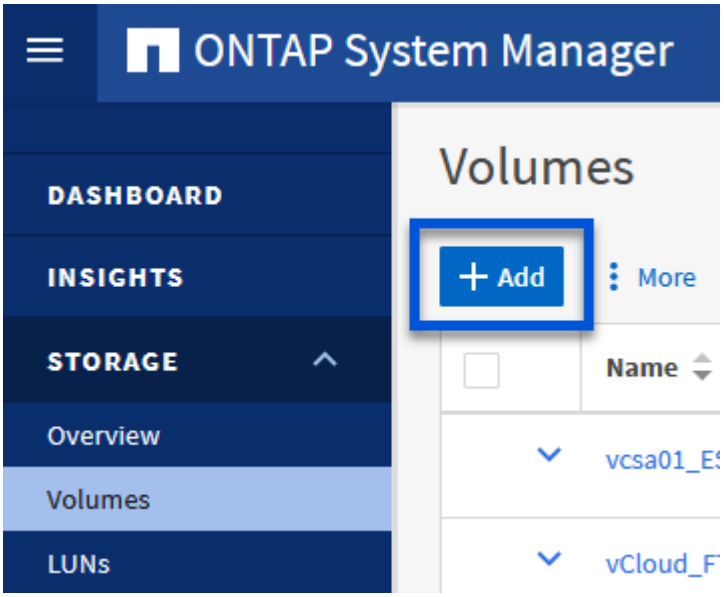
> Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass die Exportrichtlinie das VCF-Verwaltungsnetzwerk umfasst, damit die Validierung fortgesetzt werden kann.

5. Nachdem alle Regeln eingegeben wurden, klicken Sie auf die Schaltfläche **Speichern**, um die neue Exportrichtlinie zu speichern.
6. Alternativ können Sie Exportrichtlinien und -regeln in der ONTAP CLI erstellen. Die Schritte zum Erstellen einer Exportrichtlinie und Hinzufügen von Regeln finden Sie in der ONTAP Dokumentation.
   - Verwenden Sie die ONTAP CLI, um"Erstellen einer Exportrichtlinie" .
   - Verwenden Sie die ONTAP CLI, um"Hinzufügen einer Regel zu einer Exportrichtlinie" .

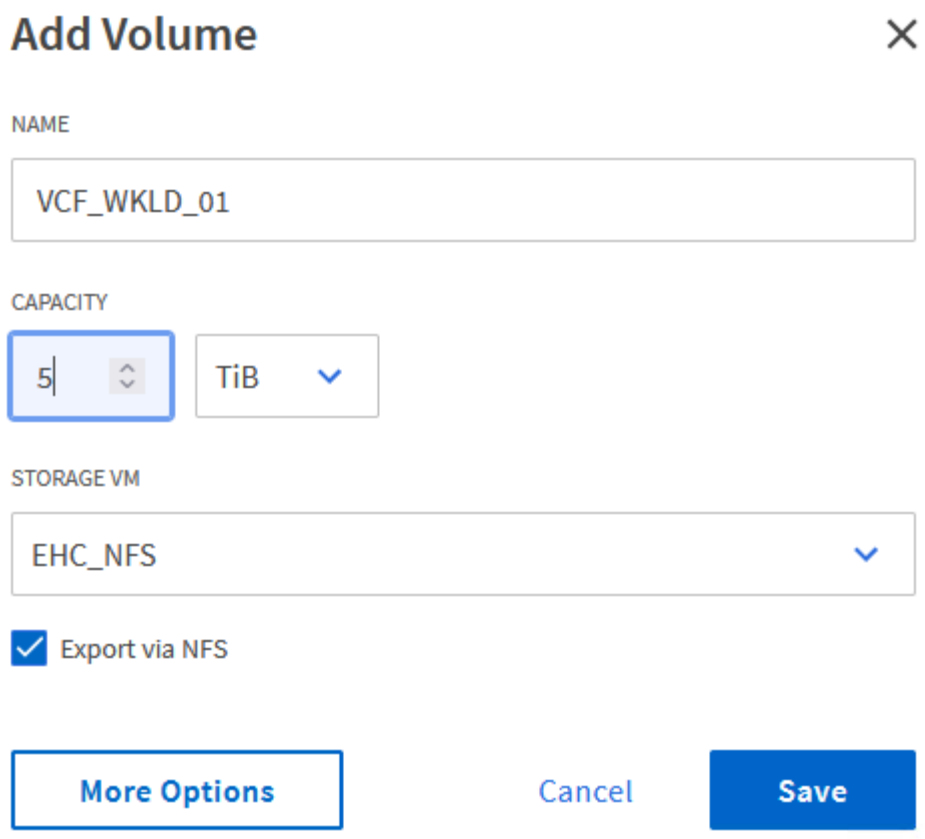
NFS-Volume erstellen

Erstellen Sie ein NFS-Volume auf dem ONTAP -Speichersystem, das als Datenspeicher in der Workload Domain-Bereitstellung verwendet werden soll.

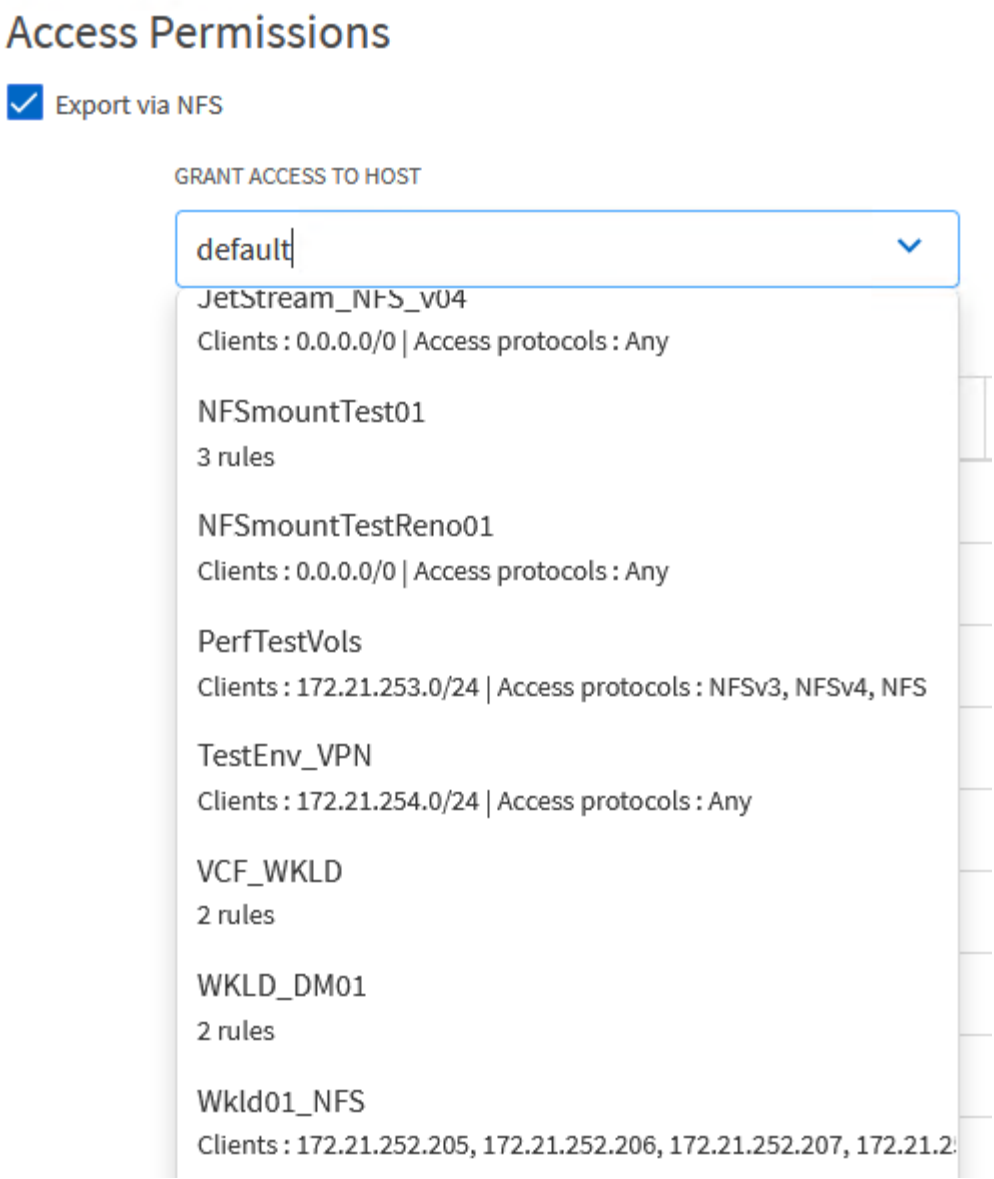
1. Navigieren Sie im ONTAP System Manager im linken Menü zu **Speicher > Volumes** und klicken Sie auf **+Hinzufügen**, um ein neues Volume zu erstellen.



2. Geben Sie einen Namen für das Volume ein, geben Sie die gewünschte Kapazität ein und wählen Sie die Speicher-VM aus, die das Volume hosten soll. Klicken Sie auf **Weitere Optionen**, um fortzufahren.



3. Wählen Sie unter „Zugriffsberechtigungen“ die Exportrichtlinie aus, die das VCF-Verwaltungsnetzwerk oder die IP-Adresse und die NFS-Netzwerk-IP-Adressen enthält, die sowohl für die Validierung des NFS-Servers als auch des NFS-Verkehrs verwendet werden.



+

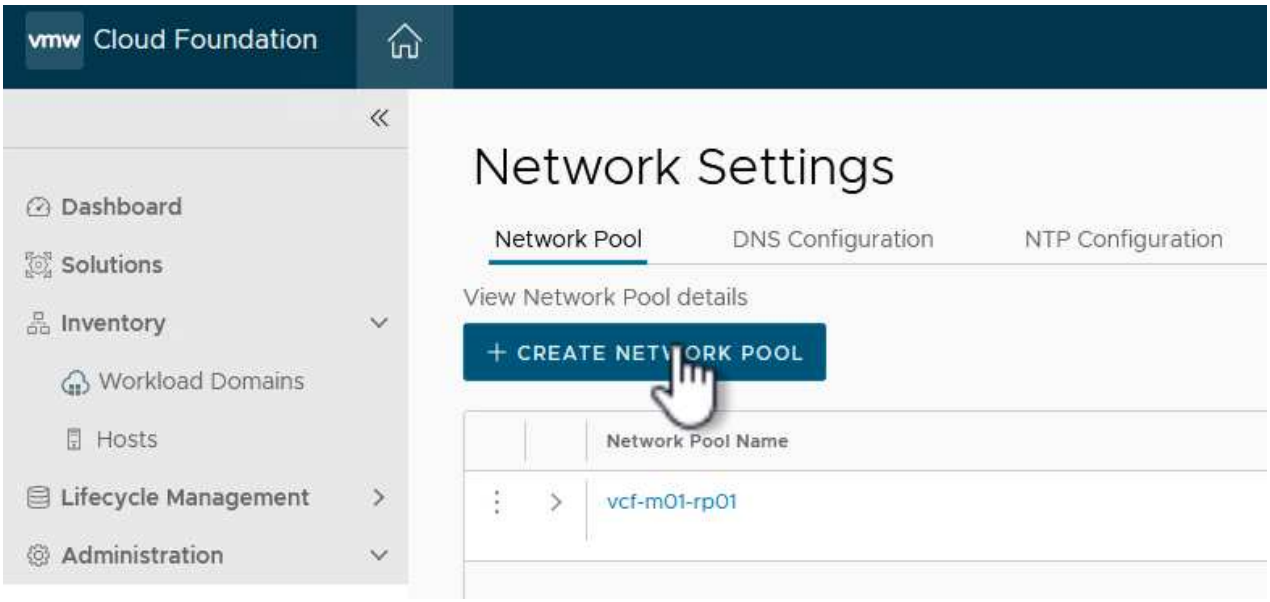
> Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass entweder 1) das Verwaltungsnetzwerk zum NFS-Server geroutet werden kann oder 2) dem SVM, auf dem das NFS-Datenspeichervolume gehostet wird, ein LIF für das Verwaltungsnetzwerk hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

4. Alternativ können ONTAP Volumes in der ONTAP CLI erstellt werden. Weitere Informationen finden Sie im"LUN erstellen" Befehl in der ONTAP -Befehlsdokumentation.

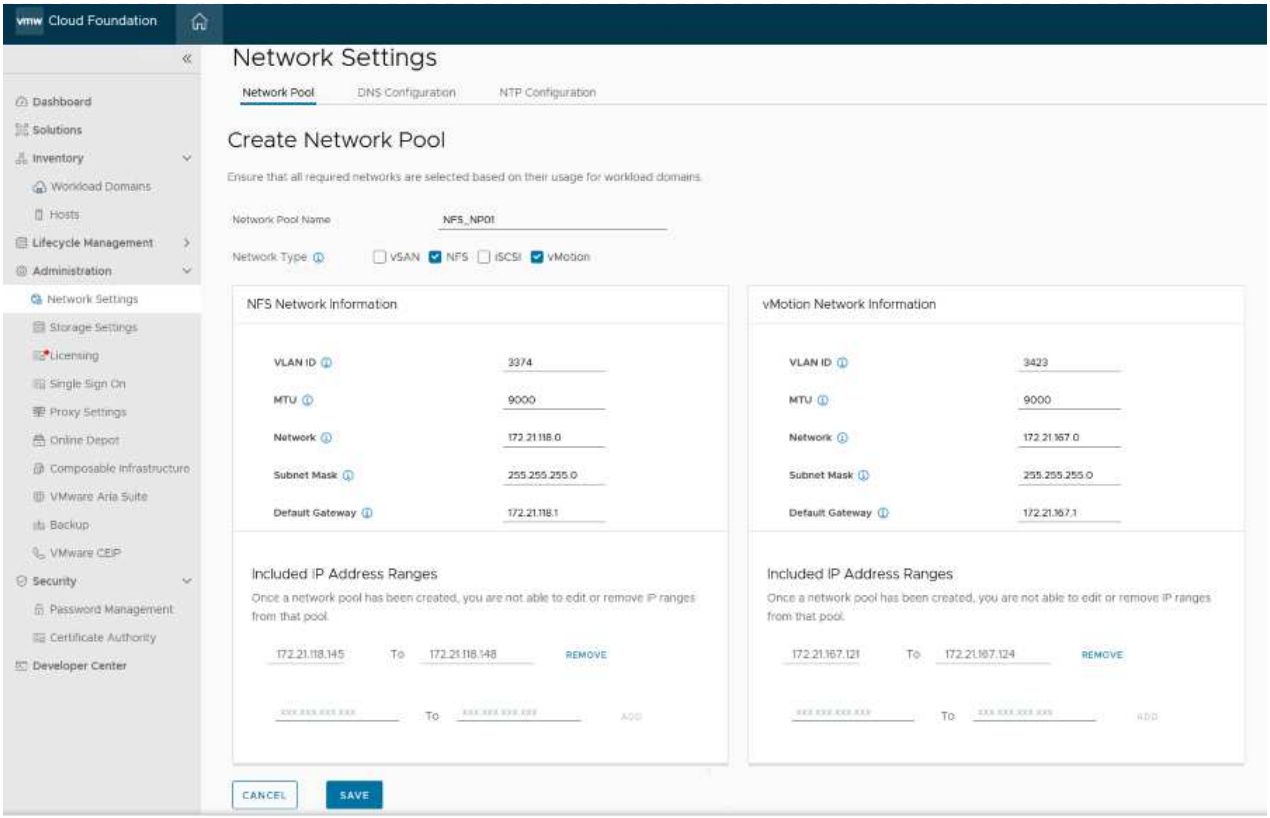
Erstellen eines Netzwerkpools im SDDC Manager

Vor der Inbetriebnahme der ESXi-Hosts muss im SDDC Manager ein Netzwerkpool erstellt werden, um sie für die Bereitstellung in einer VI-Workload-Domäne vorzubereiten. Der Netzwerkpool muss die Netzwerkinformationen und IP-Adressbereiche für VMkernel-Adapter enthalten, die für die Kommunikation mit dem NFS-Server verwendet werden sollen.

1. Navigieren Sie in der SDDC Manager-Weboberfläche im linken Menü zu **Netzwerkeinstellungen** und klicken Sie auf die Schaltfläche **+ Netzwerkpool erstellen**.



2. Geben Sie einen Namen für den Netzwerkpool ein, aktivieren Sie das Kontrollkästchen für NFS und geben Sie alle Netzwerkdetails ein. Wiederholen Sie dies für die vMotion-Netzwerkinformationen.



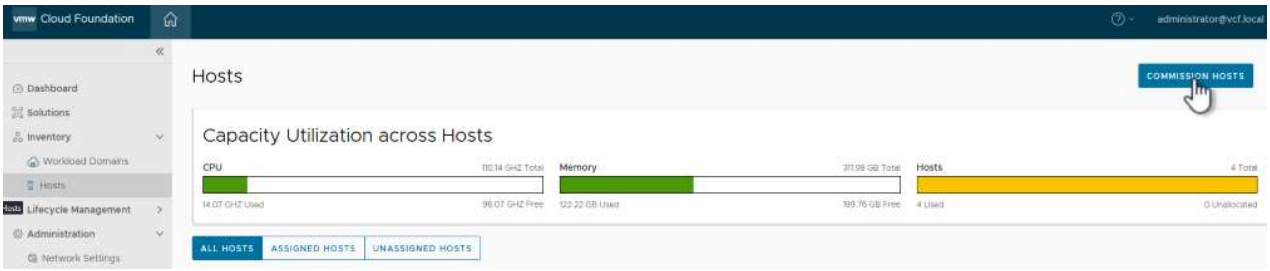
3. Klicken Sie auf die Schaltfläche **Speichern**, um die Erstellung des Netzwerkpools abzuschließen.

Kommissionsgastgeber

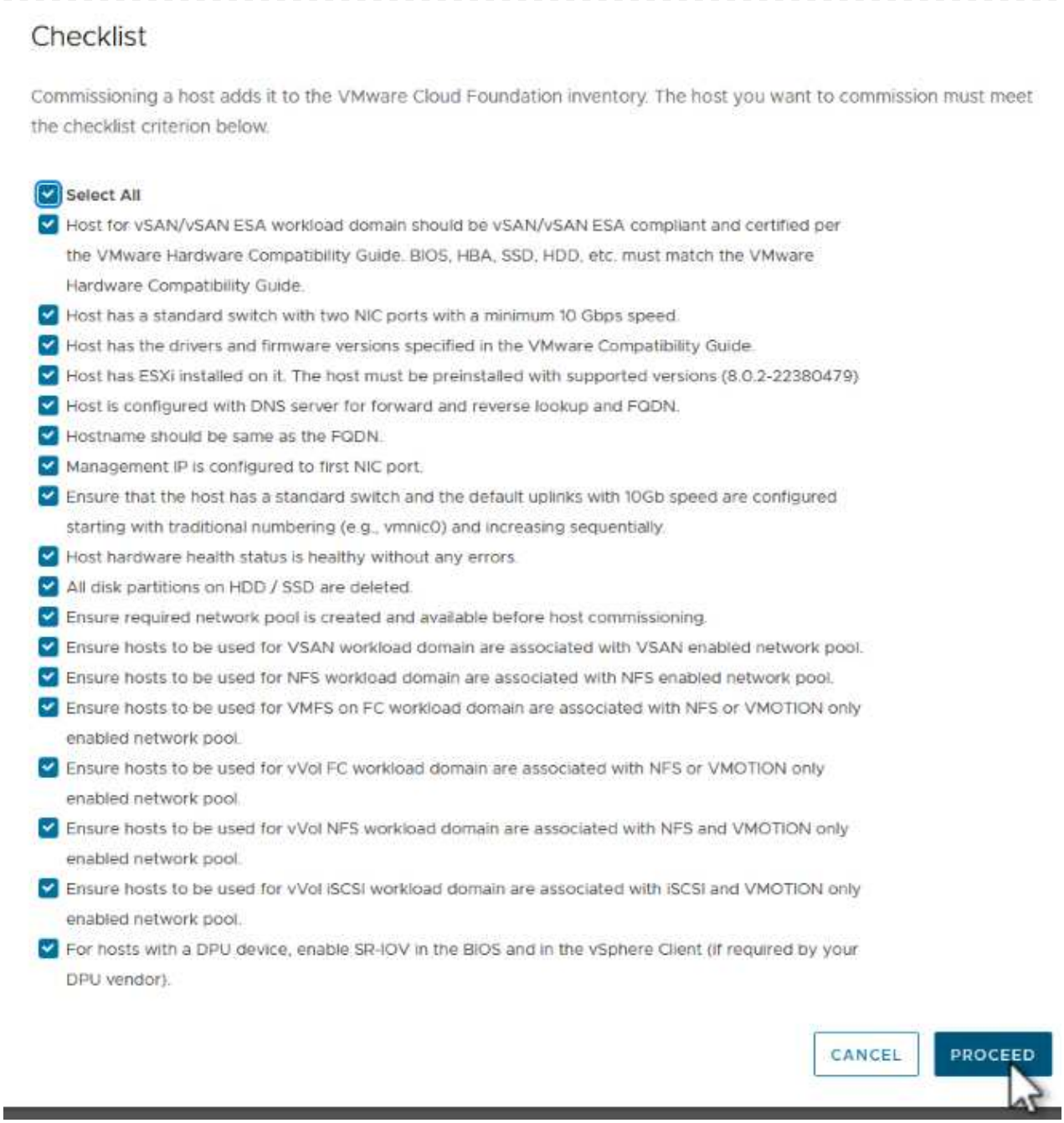
Bevor ESXi-Hosts als Workload-Domäne bereitgestellt werden können, müssen sie zum SDDC Manager-Inventar hinzugefügt werden. Dazu gehört die Bereitstellung der erforderlichen Informationen, die Durchführung der Validierung und der Start des Inbetriebnahmeprozesses.

Weitere Informationen finden Sie unter"Kommissionsgastgeber" im VCF-Administrationshandbuch.

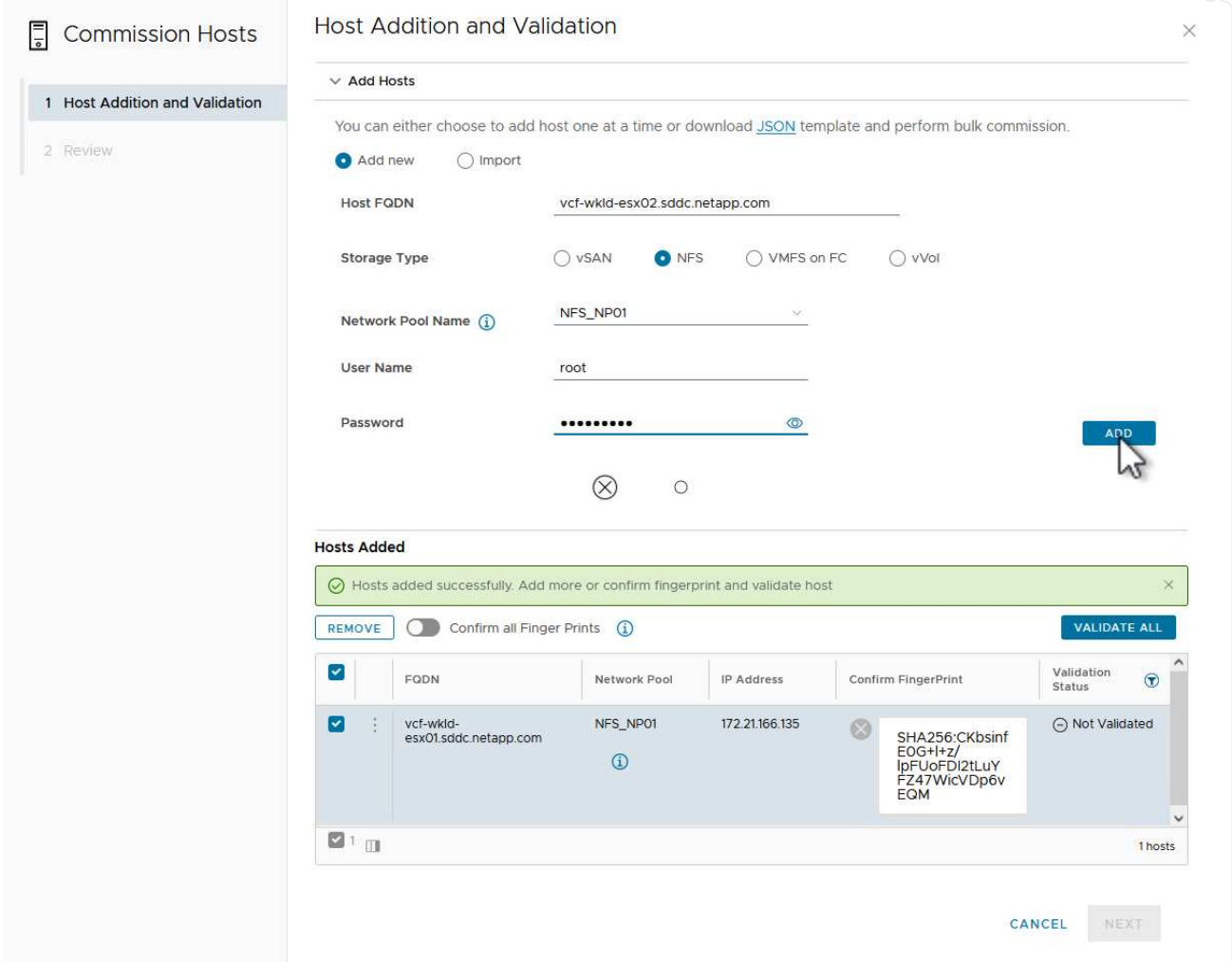
1. Navigieren Sie in der SDDC Manager-Oberfläche im linken Menü zu **Hosts** und klicken Sie auf die Schaltfläche **Hosts beauftragen**.



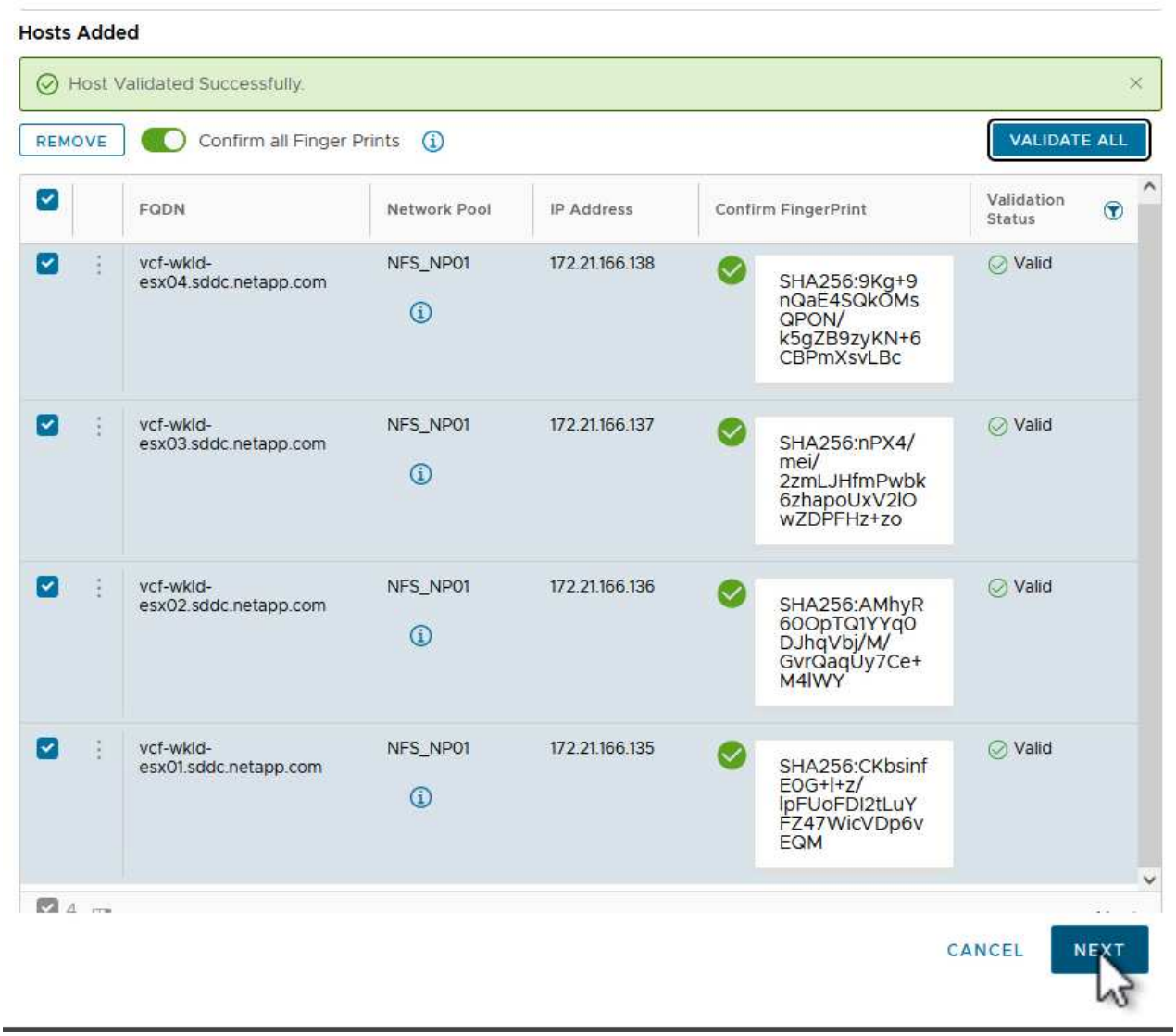
2. Die erste Seite ist eine Checkliste mit den Voraussetzungen. Überprüfen Sie alle Voraussetzungen und aktivieren Sie alle Kontrollkästchen, um fortzufahren.



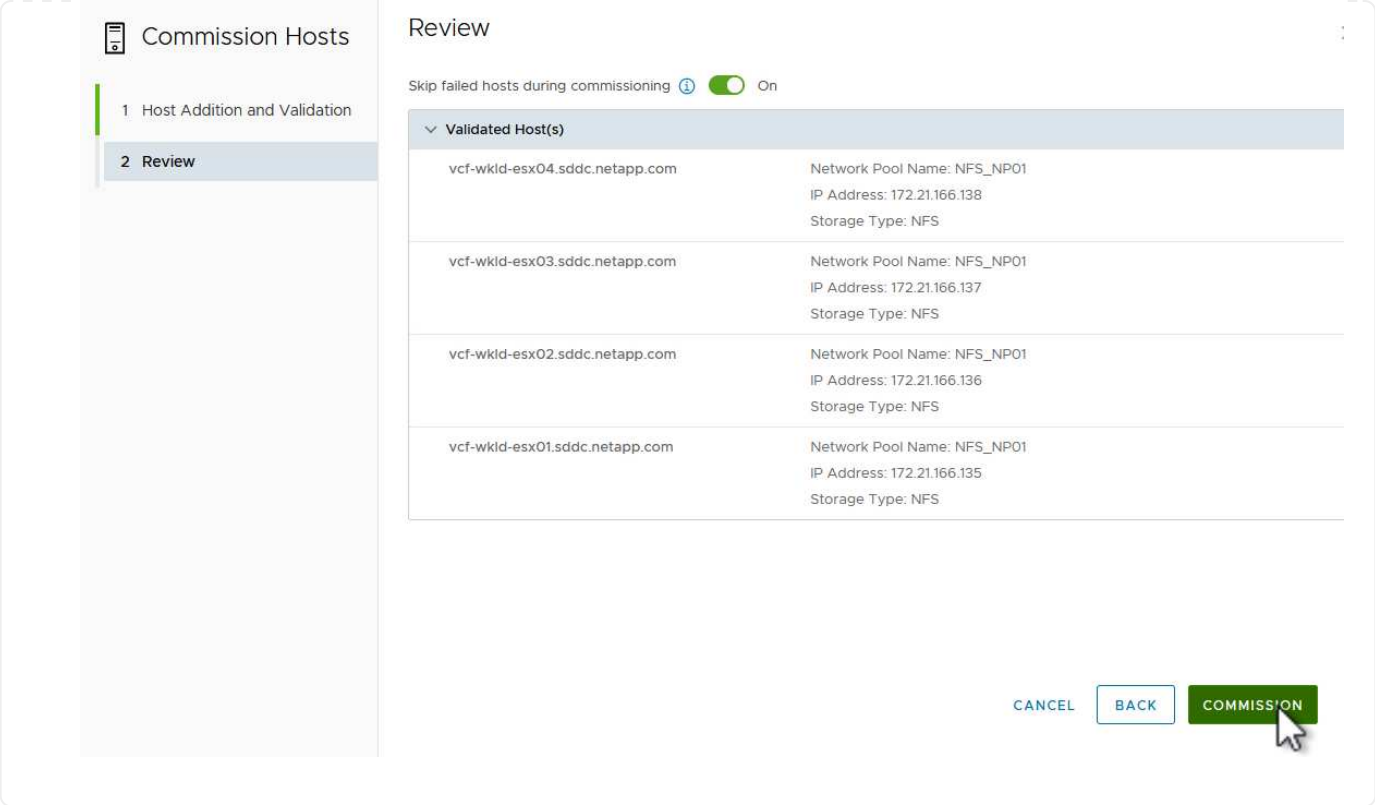
3. Geben Sie im Fenster „Host hinzufügen und validieren“ den **Host-FQDN**, den **Speichertyp**, den Namen des **Netzwerkpools** (einschließlich der für die Workloaddomäne zu verwendenden vMotion- und NFS-Speicher-IP-Adressen) und die Anmeldeinformationen für den Zugriff auf den ESXi-Host ein. Klicken Sie auf **Hinzufügen**, um den Host zur Gruppe der zu validierenden Hosts hinzuzufügen.



4. Nachdem alle zu validierenden Hosts hinzugefügt wurden, klicken Sie auf die Schaltfläche **Alle validieren**, um fortzufahren.
5. Vorausgesetzt, alle Hosts sind validiert, klicken Sie auf **Weiter**, um fortzufahren.



6. Überprüfen Sie die Liste der zu beauftragenden Hosts und klicken Sie auf die Schaltfläche **Beauftragen**, um den Vorgang zu starten. Überwachen Sie den Inbetriebnahmeprozess über den Aufgabenbereich im SDDC-Manager.

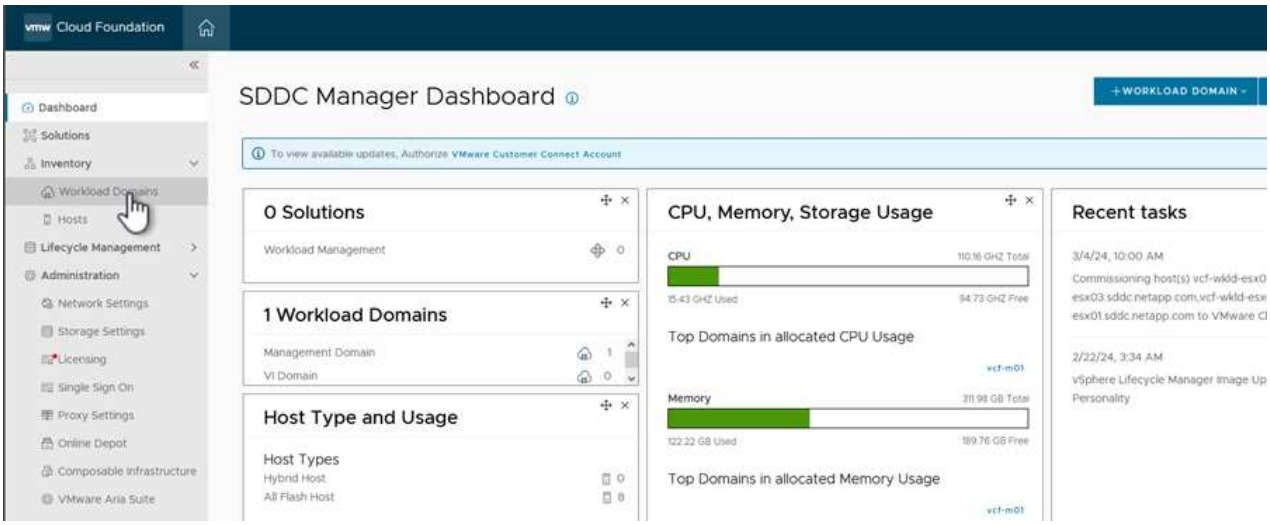

Commission Hosts
1 Host Addition and Validation
2 Review
Review
Skip failed hosts during commissioning
On
Validated Host(s)
vcf-wkld-esx04.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.138
Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.137
Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.136
Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com
Network Pool Name: NFS_NP01
IP Address: 172.21.166.135
Storage Type: NFS
CANCEL
BACK
COMMISSION

Bereitstellen der VI-Workloaddomäne

Die Bereitstellung von VI-Workloaddomänen erfolgt über die VCF Cloud Manager-Schnittstelle. Hier werden nur die Schritte zur Speicherkonfiguration vorgestellt.

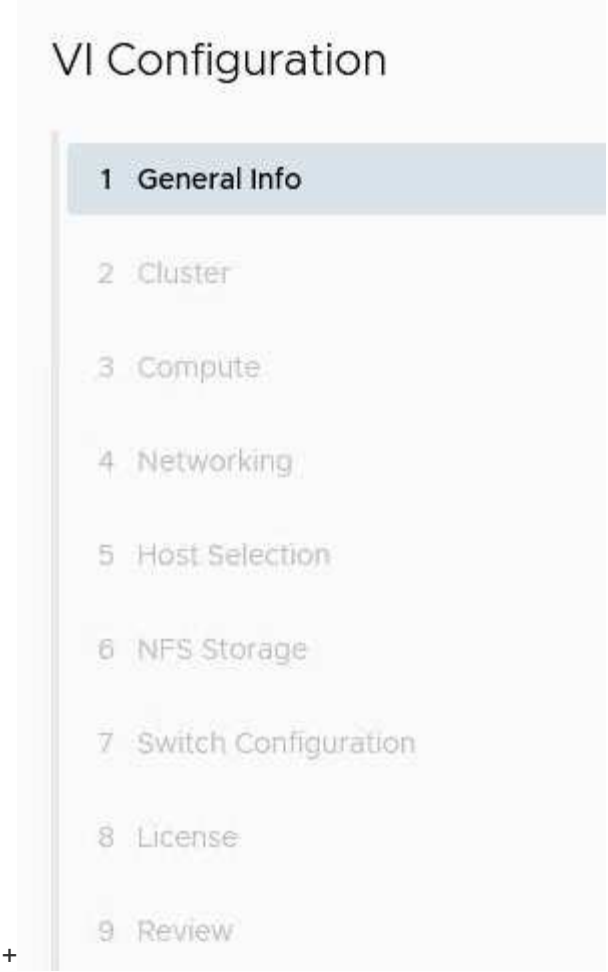
Eine Schritt-für-Schritt-Anleitung zur Bereitstellung einer VI-Workloaddomäne finden Sie unter"Bereitstellen einer VI-Workloaddomäne mithilfe der SDDC Manager-Benutzeroberfläche" .

1. Klicken Sie im SDDC Manager-Dashboard oben rechts auf **+ Workload-Domäne**, um eine neue Workload-Domäne zu erstellen.



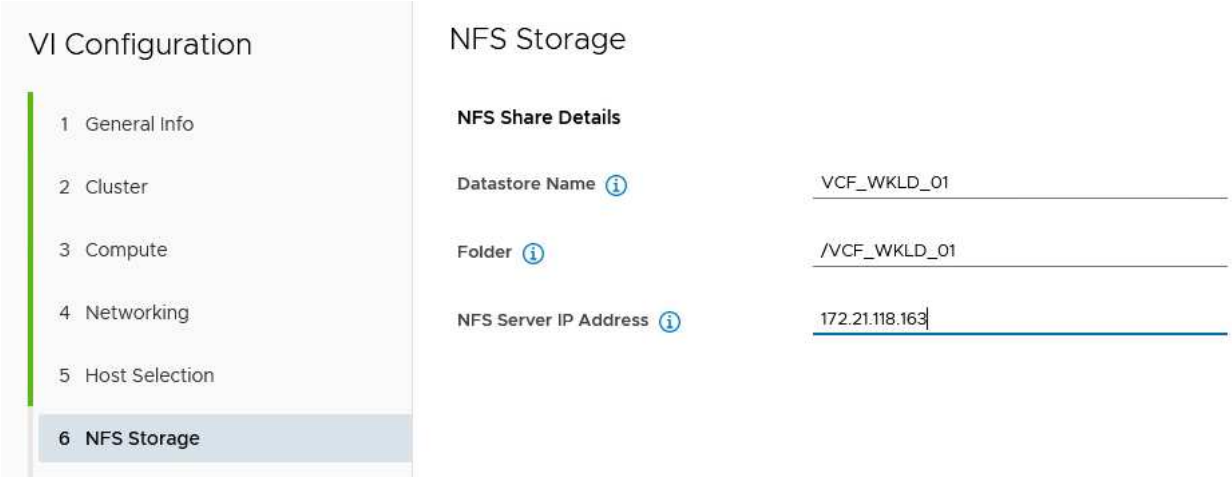
2. Füllen Sie im VI-Konfigurationsassistenten die Abschnitte für **Allgemeine Informationen, Cluster, Compute, Netzwerk** und **Hostauswahl** nach Bedarf aus.

Informationen zum Ausfüllen der im VI-Konfigurationsassistenten erforderlichen Informationen finden Sie unter"Bereitstellen einer VI-Workloaddomäne mithilfe der SDDC Manager-Benutzeroberfläche" .

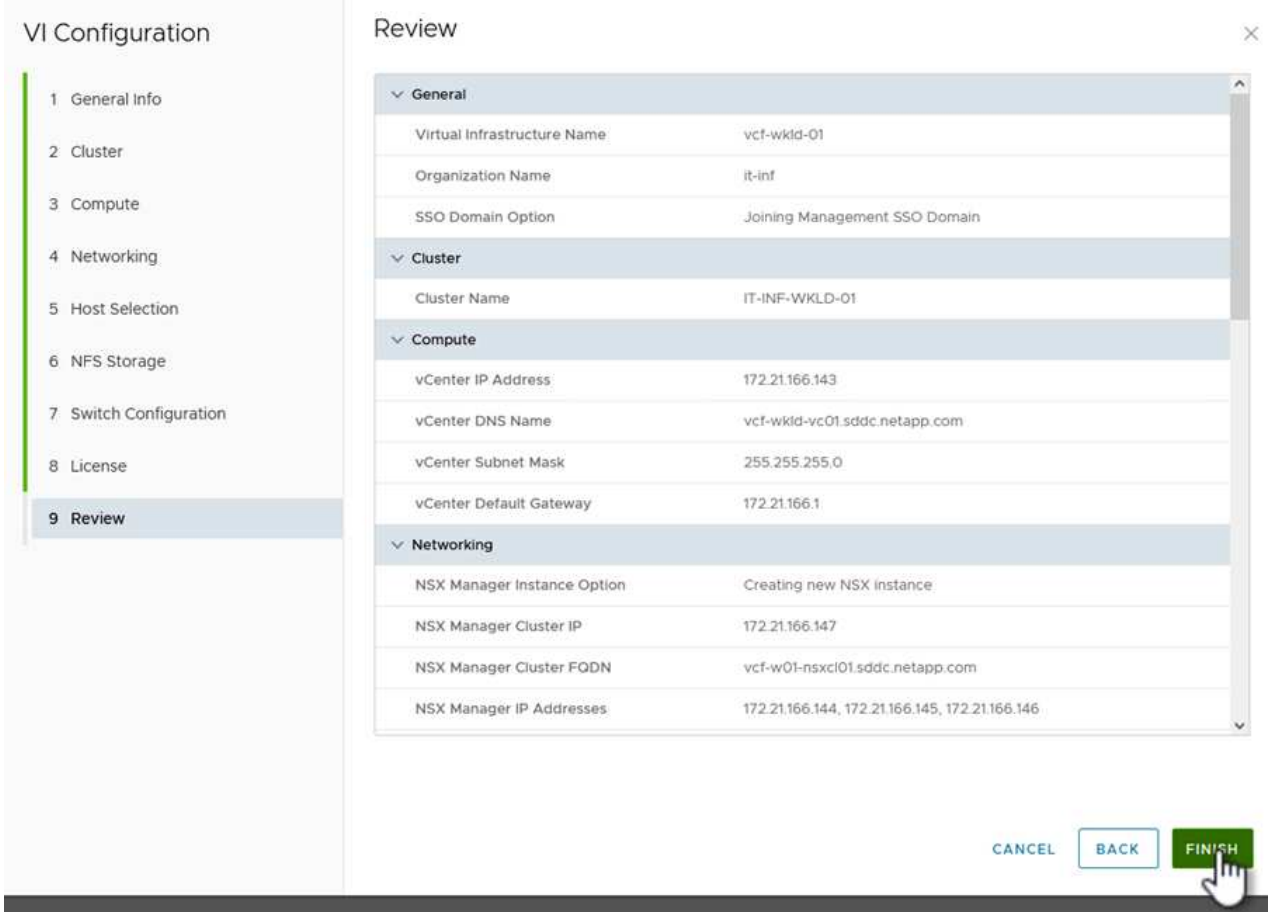


+

1. Geben Sie im Abschnitt „NFS-Speicher“ den Datastore-Namen, den Ordner-Mount-Punkt des NFS-Volumes und die IP-Adresse des ONTAP NFS-Speicher-VM-LIF ein.



2. Führen Sie im VI-Konfigurationsassistenten die Schritte zur Switch-Konfiguration und Lizenzierung aus und klicken Sie dann auf **Fertig**, um den Prozess zur Erstellung der Workload-Domäne zu starten.



3. Überwachen Sie den Prozess und lösen Sie alle Validierungsprobleme, die während des Prozesses auftreten.

Installieren Sie das NetApp NFS-Plug-in für VMware VAAI

Das NetApp NFS-Plug-in für VMware VAAI integriert die auf dem ESXi-Host installierten VMware Virtual Disk Libraries und ermöglicht leistungsstärkere und schneller abgeschlossene Klonvorgänge. Dies ist ein empfohlenes Verfahren bei der Verwendung von ONTAP Speichersystemen mit VMware vSphere.

Eine Schritt-für-Schritt-Anleitung zur Bereitstellung des NetApp NFS Plug-ins für VMware VAAI finden Sie unter"Installieren Sie das NetApp NFS-Plug-in für VMware VAAI" .

Videodemo für diese Lösung

NFS-Datenspeicher als Hauptspeicher für VCF-Workload-Domänen

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Erweitern Sie VCF mit zusätzlichem Speicher

Erfahren Sie mehr über die Speichererweiterung für eine VCF-Umgebung mithilfe von zusätzlichem Speicher

VMware Cloud Foundation (VCF) unterstützt eine breite Palette zusätzlicher Speicheroptionen zur Erweiterung des Speichers in VCF-Verwaltungsdomänen und Workloaddomänen der virtuellen Infrastruktur (VI).

Die ONTAP Tools von NetApp für VMware vSphere bieten eine effiziente Lösung für diese Erweiterung, indem sie NetApp -Speicher nahtlos in die VCF-Umgebung integrieren. ONTAP Tools vereinfachen die Einrichtung und Verwaltung von Datenspeichern und ermöglichen Administratoren die Bereitstellung und Verwaltung von Speicher direkt vom vSphere Client aus. Die erweiterten Funktionen von ONTAP wie Snapshots, Klonen und Datenschutz verbessern die Speicherleistung, Effizienz und Skalierbarkeit innerhalb der VCF-Umgebung.

Die technischen Details zur Erweiterung der VCF-Umgebung finden Sie in den folgenden Lösungen.

- "Verwaltungsdomäne mit iSCSI"
- "Managementdomäne mit FC"
- "Virtuelle Infrastruktur-Workload-Domäne mit vVols (iSCSI)"
- "Virtuelle Infrastruktur-Workload-Domäne mit vVols (NFS)"
- "Virtuelle Infrastruktur-Workloaddomäne mit NVMe/TCP"
- "Virtuelle Infrastruktur-Workloaddomäne mit FC"

Fügen Sie mithilfe von ONTAP tools for VMware vSphere einen iSCSI-Datenspeicher als zusätzlichen Speicher für eine Verwaltungsdomäne hinzu

In diesem Anwendungsfall beschreiben wir das Verfahren zum Hinzufügen eines iSCSI-Datenspeichers als zusätzlichen Speicher für eine VMware Cloud Foundation (VCF)-Verwaltungsdomäne. Dieses Verfahren fasst das Einrichten einer Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI, das Konfigurieren von iSCSI-Netzwerken auf ESXi-Hosts, das Bereitstellen von ONTAP Tools für VMware vSphere und das Erstellen eines VMFS-Datenspeichers zusammen.

Vorteile von iSCSI

Hohe Leistung: Bietet hohe Leistung für schnelle, effiziente Datenübertragungsraten und geringe Latenz. Ideal für anspruchsvolle Unternehmensanwendungen und virtualisierte Umgebungen.

Einfache Verwaltung: Vereinfacht die Speicherverwaltung durch die Verwendung vertrauter IP-basierter Tools und Protokolle.

Kostengünstig: Nutzt die vorhandene Ethernet-Infrastruktur, reduziert den Bedarf an Spezialhardware und ermöglicht Unternehmen die Erzielung zuverlässiger und skalierbarer Speicherlösungen.

Weitere Informationen zur Verwendung von iSCSI mit NetApp -Speichersystemen finden Sie unter "SAN-Bereitstellung mit iSCSI" .

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

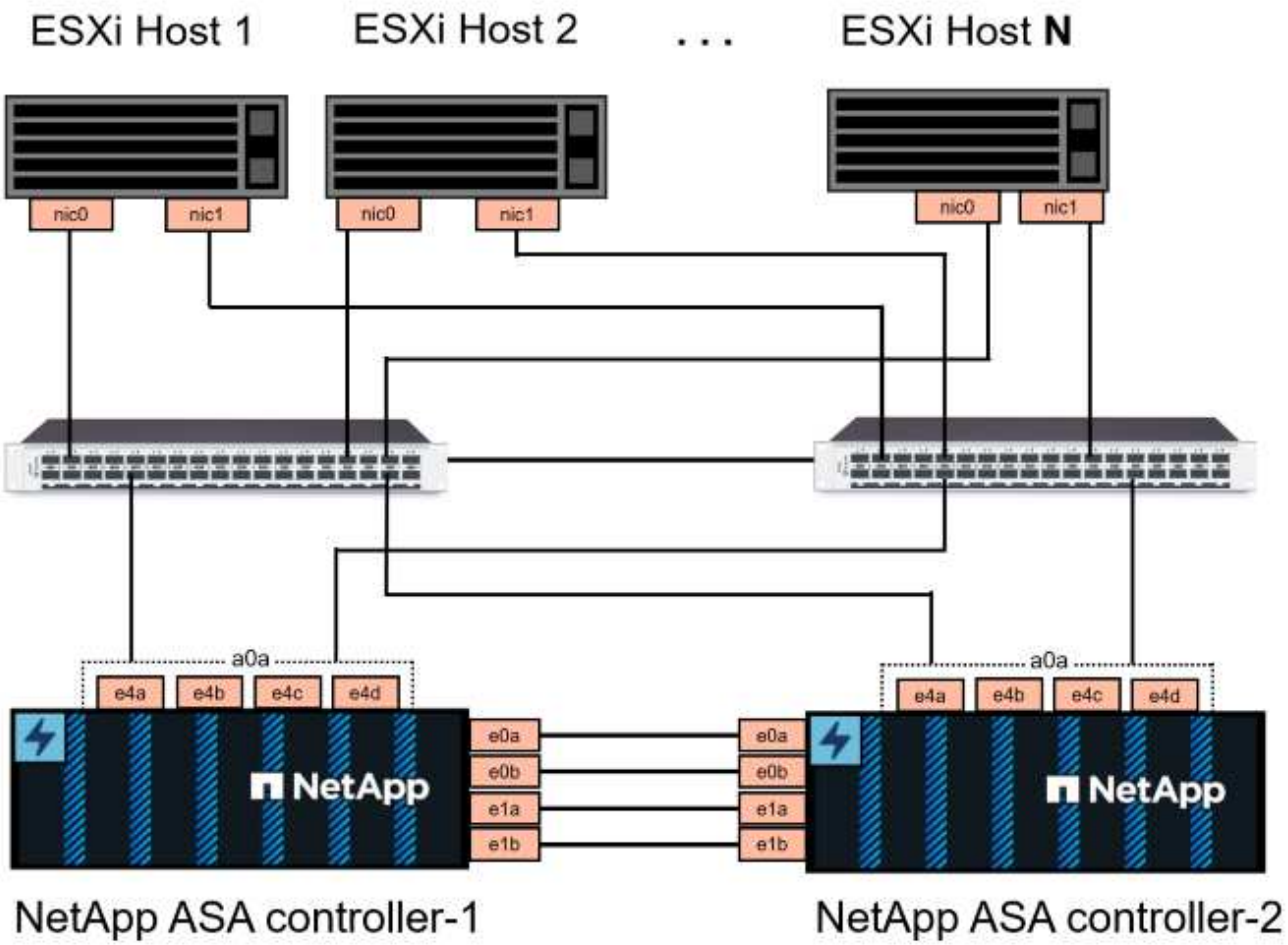
- Erstellen Sie eine Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Verkehr.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VCF-Verwaltungsdomäne.
- Erstellen Sie VMkernel-Adapter für iSCSI auf den ESXi-Hosts für die VCF-Verwaltungsdomäne.
- Stellen Sie ONTAP Tools in der VCF-Verwaltungsdomäne bereit.
- Erstellen Sie einen neuen VMFS-Datenspeicher in der VCF-Verwaltungsdomäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF oder ASA Speichersystem mit physischen Datenports auf Ethernet-Switches, die für den Speicherverkehr vorgesehen sind.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf den vSphere-Client kann zugegriffen werden.

NetApp empfiehlt vollständig redundante Netzwerkdesigns für iSCSI. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration, die Fehlertoleranz für Speichersysteme, Switches, Netzwerkadapter und Hostsysteme bietet. Weitere Informationen finden Sie in der NetApp"SAN-Konfigurationsreferenz" für weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp , für alle SVMs in iSCSI-Konfigurationen mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken zu haben.

Diese Dokumentation veranschaulicht den Vorgang zum Erstellen einer neuen SVM und zum Angeben der IP-Adressinformationen zum Erstellen mehrerer LIFs für iSCSI-Verkehr. Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie unter"Erstellen Sie eine LIF (Netzwerkschnittstelle)" .

Weitere Informationen zur Verwendung von VMFS iSCSI-Datenspeichern mit VMware finden Sie unter"vSphere VMFS-Datenspeicher – iSCSI-Speicher-Backend mit ONTAP" .

> In Situationen, in denen mehrere VMkernel-Adapter im selben IP-Netzwerk konfiguriert sind, wird empfohlen, die Software-iSCSI-Portbindung auf den ESXi-Hosts zu verwenden, um sicherzustellen, dass ein Lastenausgleich zwischen den Adaptern erfolgt. Siehe KB-Artikel"Überlegungen zur Verwendung der Software-iSCSI-Portbindung in ESX/ESXi (2038869)" .

Bereitstellungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und damit einen VMFS-Datenspeicher in der VCF-Verwaltungsdomäne zu erstellen:

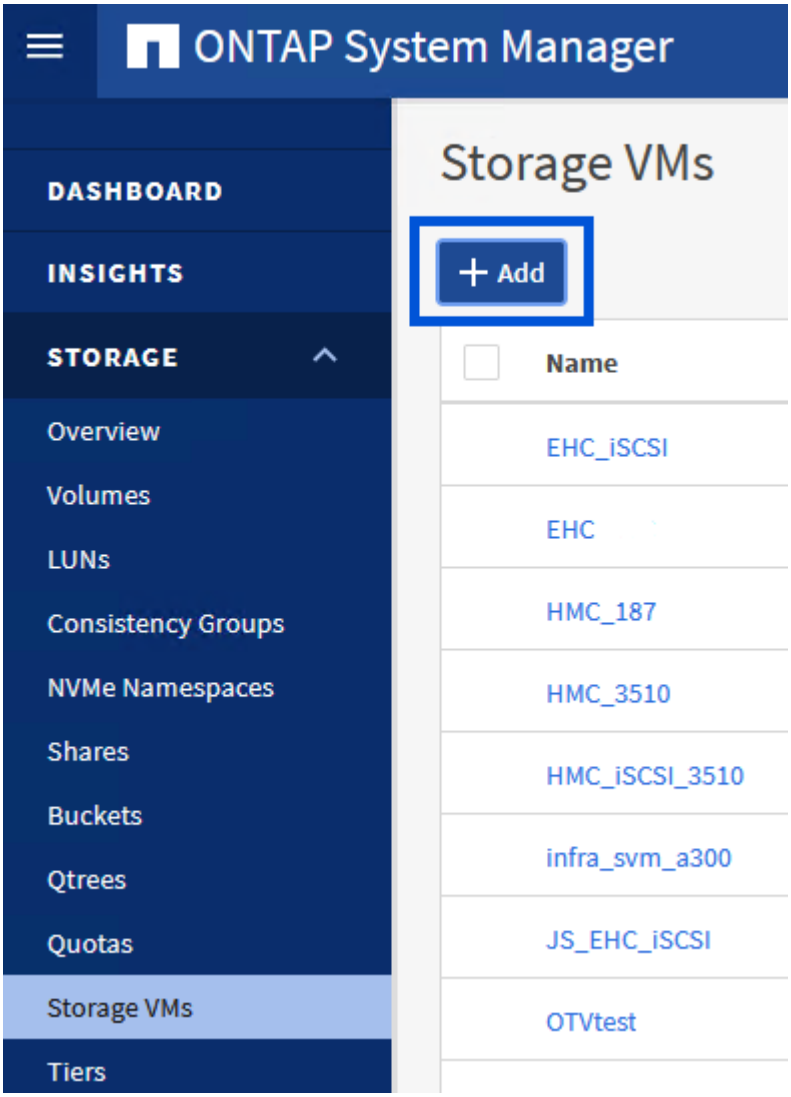
Erstellen Sie SVM und LIFs auf dem ONTAP Speichersystem

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

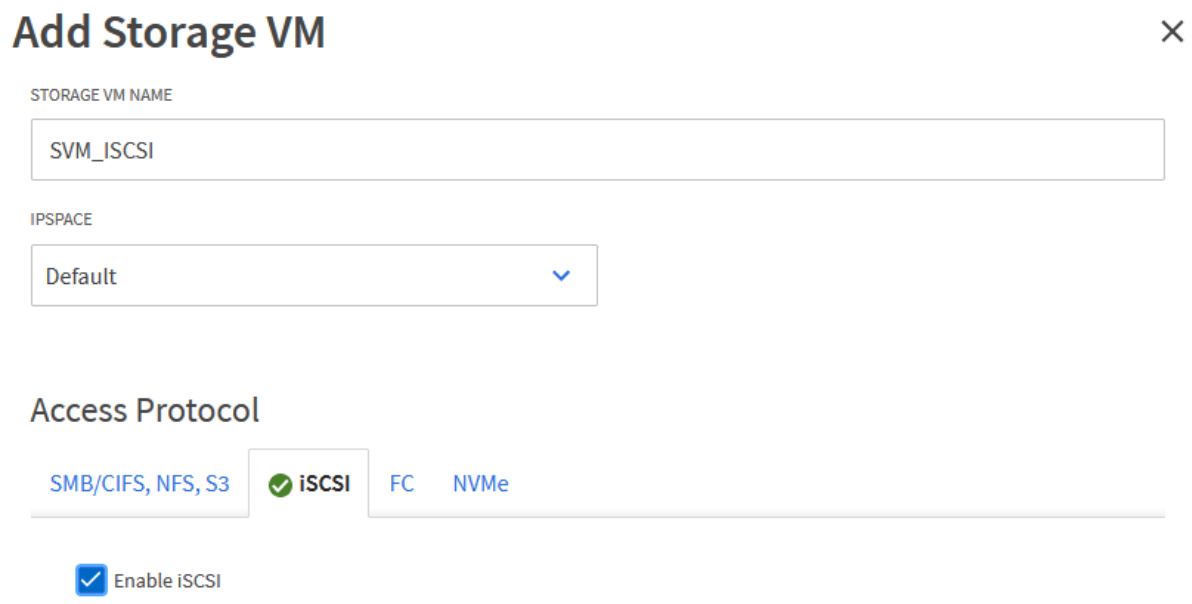
Erstellen der Speicher-VM und LIFs

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für iSCSI-Verkehr zu erstellen.

1. Navigieren Sie im ONTAP System Manager im linken Menü zu **Storage VMs** und klicken Sie zum Starten auf **+ Hinzufügen**.

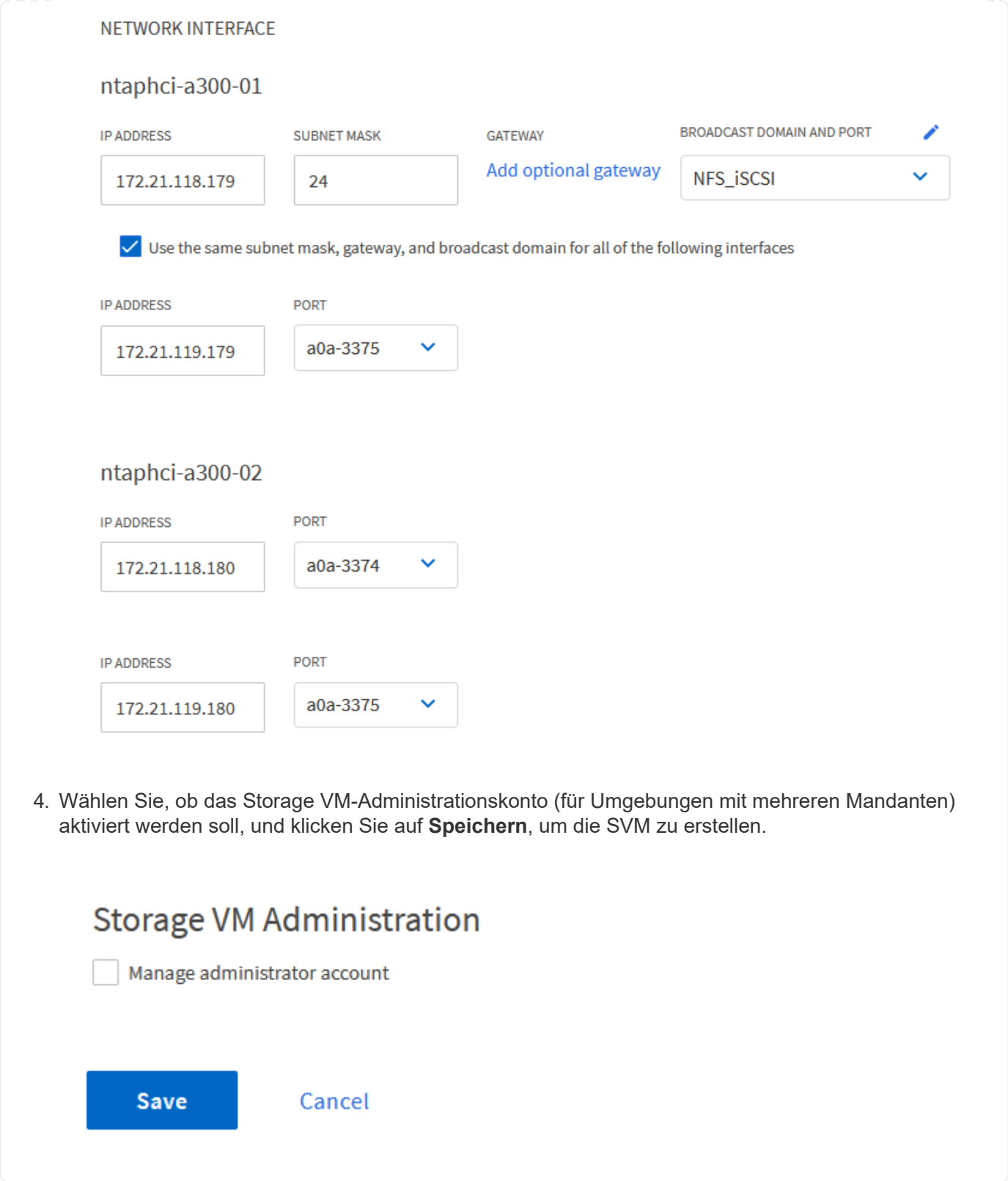


2. Geben Sie im Assistenten **Speicher-VM hinzufügen** einen **Namen** für die SVM ein, wählen Sie den **IP-Bereich** aus und klicken Sie dann unter **Zugriffsprotokoll auf die Registerkarte *iSCSI** und aktivieren Sie das Kontrollkästchen **iSCSI aktivieren**.



3. Geben Sie im Abschnitt **Netzwerkschnittstelle** die **IP-Adresse**, **Subnetzmaske** und **Broadcast-Domäne und -Port** für das erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert werden, um gemeinsame Einstellungen für alle verbleibenden LIFs oder separate Einstellungen zu verwenden.

> Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp , für alle SVMs in iSCSI-Konfigurationen mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken zu haben.



4. Wählen Sie, ob das Storage VM-Administrationskonto (für Umgebungen mit mehreren Mandanten) aktiviert werden soll, und klicken Sie auf **Speichern**, um die SVM zu erstellen.

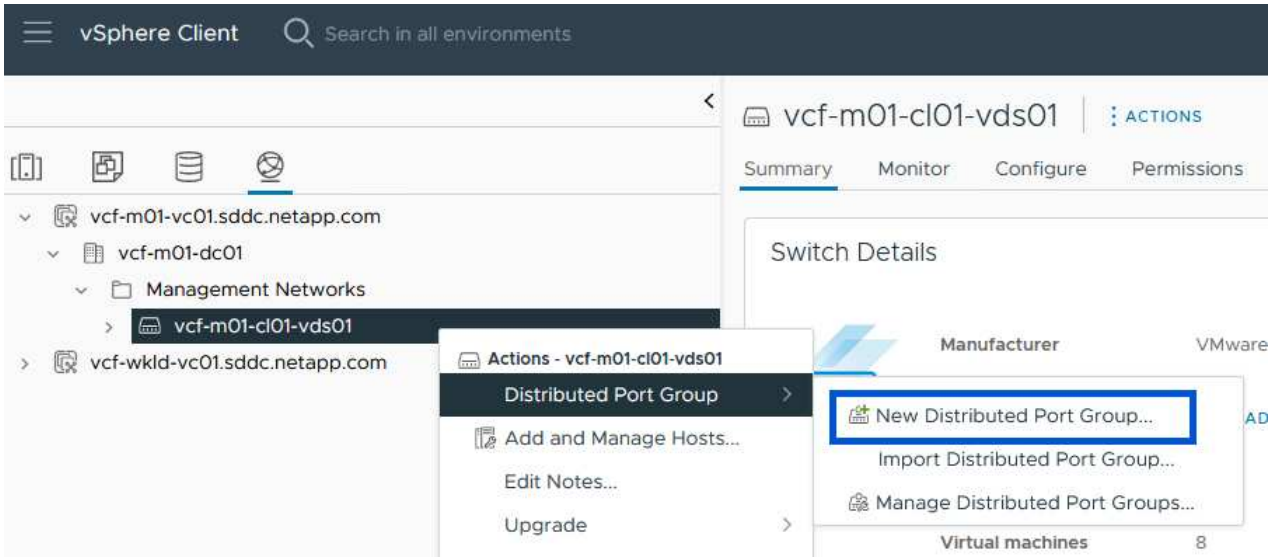
Einrichten des Netzwerks für iSCSI auf ESXi-Hosts

Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VCF-Verwaltungsdomänencluster ausgeführt.

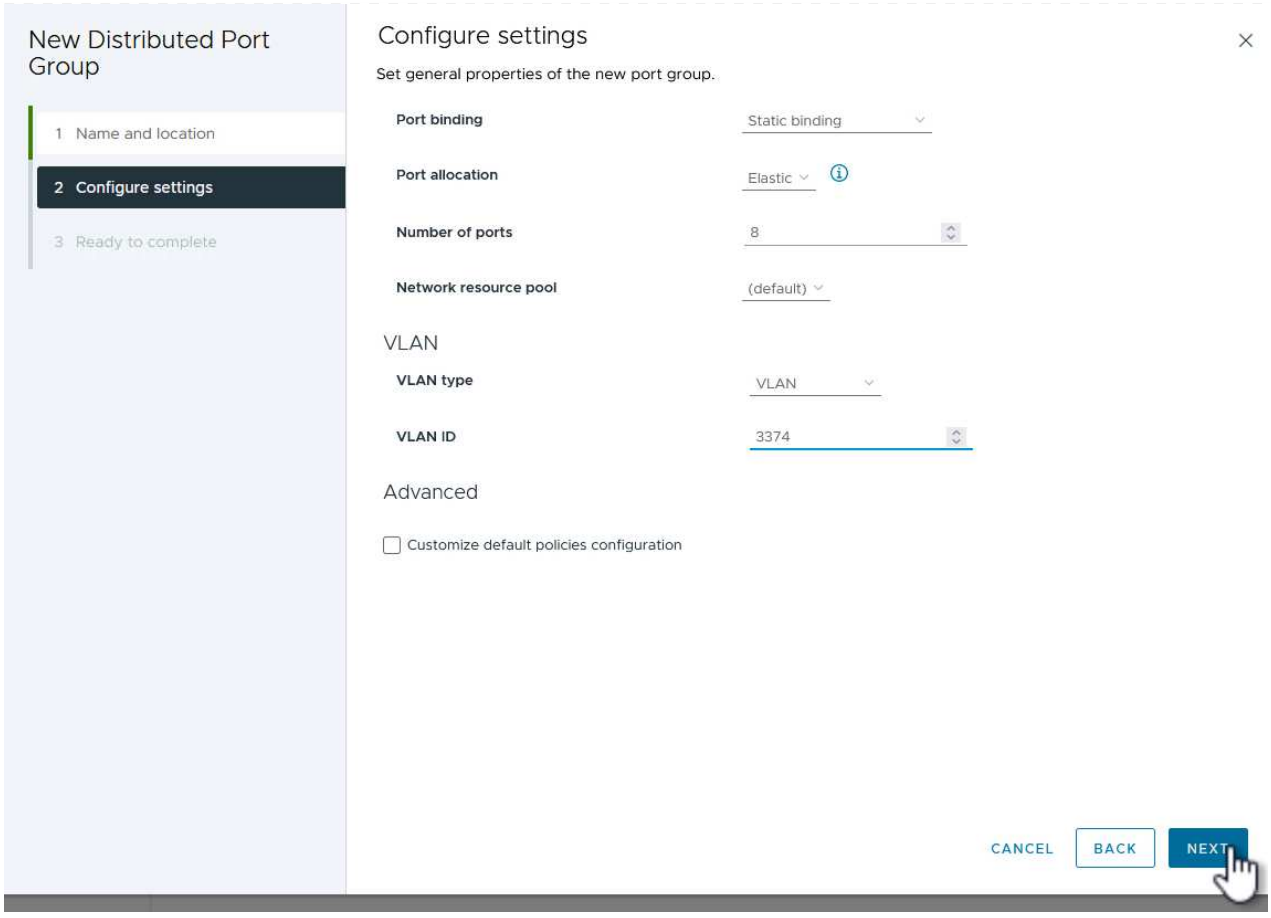
Erstellen Sie verteilte Portgruppen für iSCSI-Verkehr

Führen Sie die folgenden Schritte aus, um für jedes iSCSI-Netzwerk eine neue verteilte Portgruppe zu erstellen:

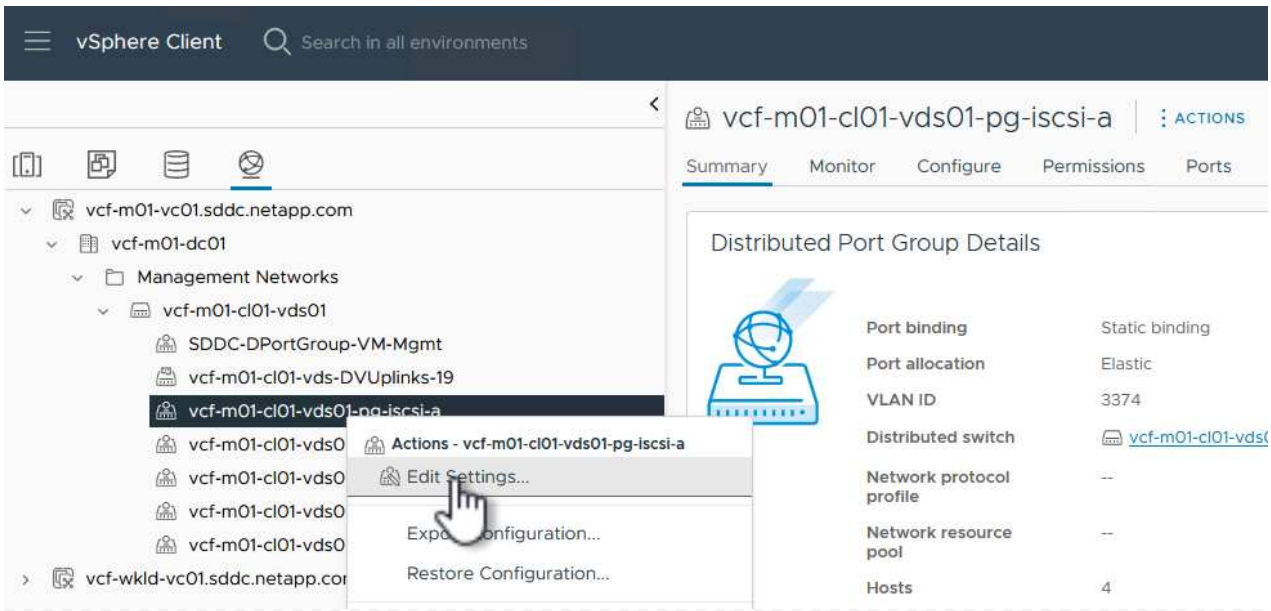
1. Navigieren Sie vom vSphere-Client für den Managementdomänencluster zu **Inventar > Netzwerk**. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen einer **Neuen verteilten Portgruppe…**.



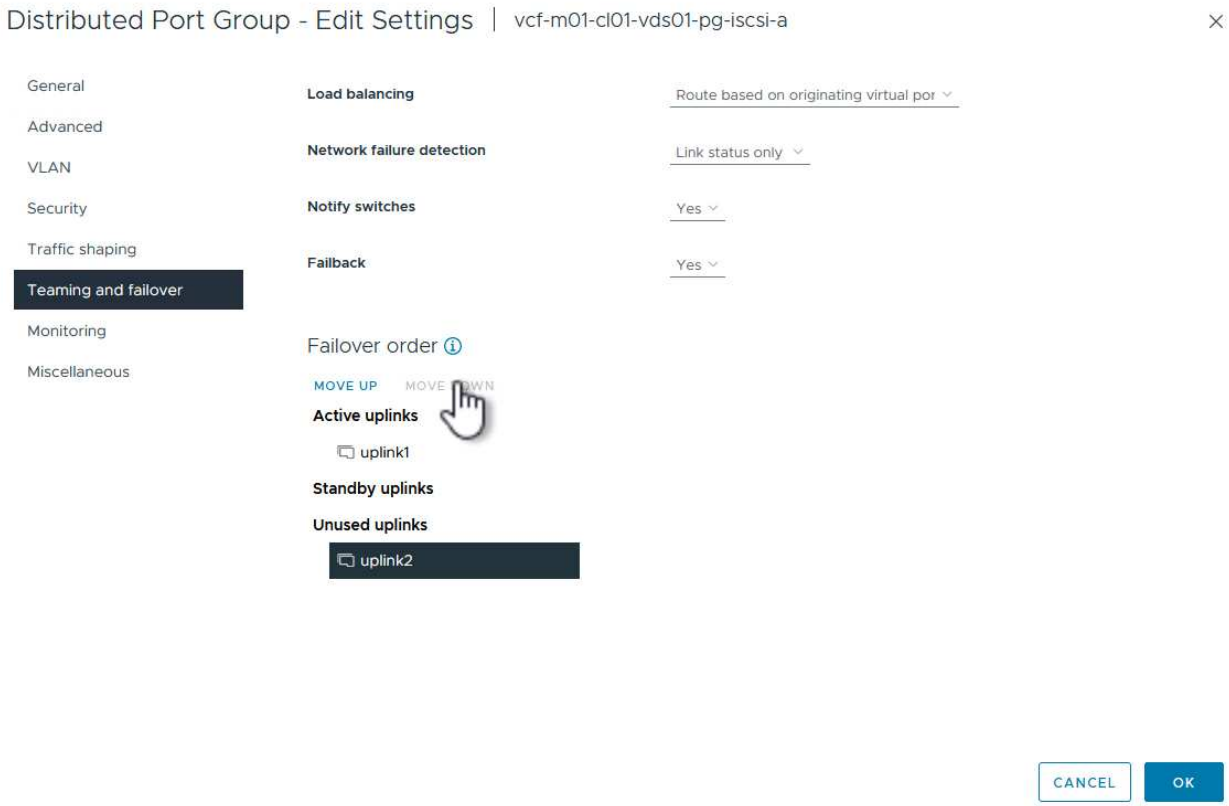
2. Geben Sie im Assistenten **Neue verteilte Portgruppe** einen Namen für die neue Portgruppe ein und klicken Sie auf **Weiter**, um fortzufahren.
3. Füllen Sie auf der Seite **Einstellungen konfigurieren** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige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



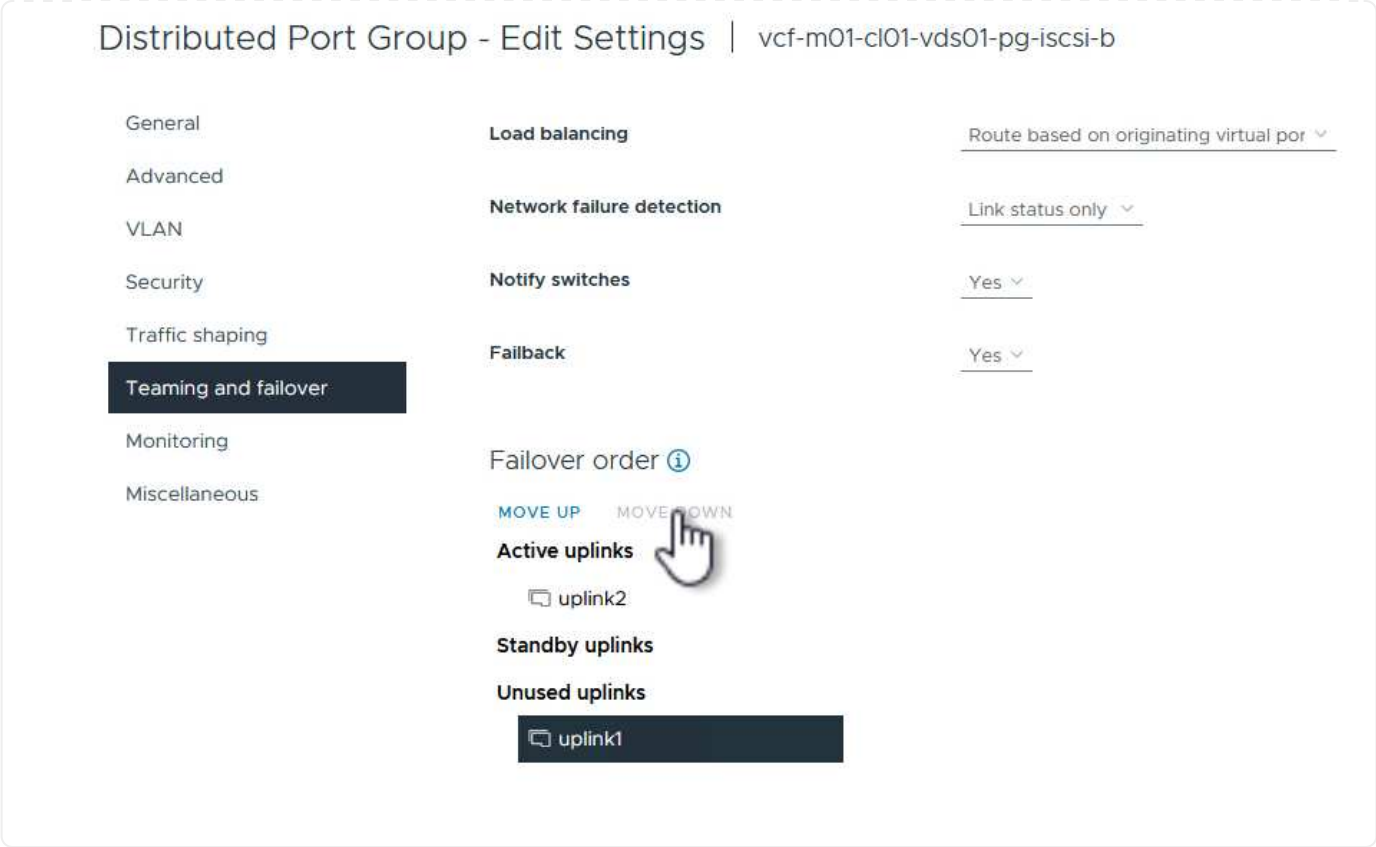
4. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Änderungen und klicken Sie auf **Fertig**, um die neue verteilte Portgruppe zu erstellen.
5. Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen, und stellen Sie sicher, dass Sie die richtige **VLAN-ID** eingegeben haben.
6. Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion „Einstellungen bearbeiten…“ aus.



7. Navigieren Sie auf der Seite **Verteilte Portgruppe – Einstellungen bearbeiten** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **Nicht verwendete Uplinks** zu verschieben.



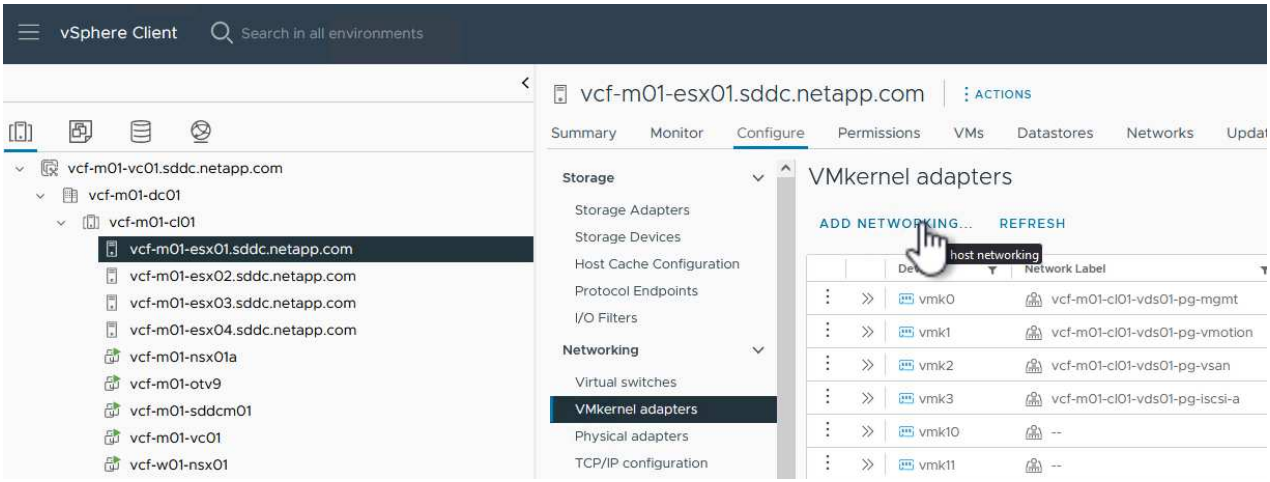
8. Wiederholen Sie diesen Schritt für die zweite iSCSI-Portgruppe. Verschieben Sie dieses Mal jedoch **Uplink1** nach unten zu **Ungenutzte Uplinks**.


Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b
General
Advanced
VLAN
Security
Traffic shaping
Teaming and failover
Monitoring
Miscellaneous
Load balancing
Route based on originating virtual por
Network failure detection
Link status only
Notify switches
Yes
Failback
Yes
Failover order
MOVE UP
MOVE DOWN
Active uplinks
uplink2
Standby uplinks
Unused uplinks
uplink1

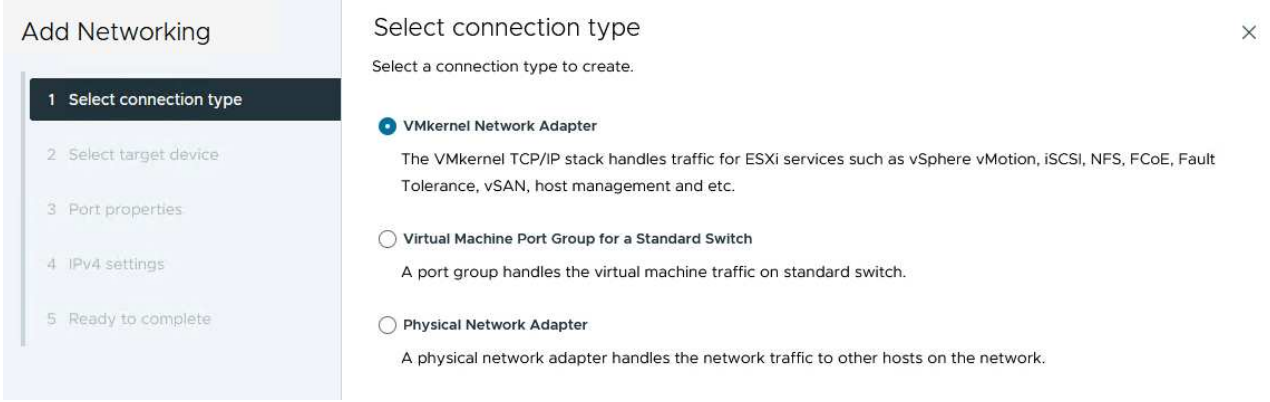
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

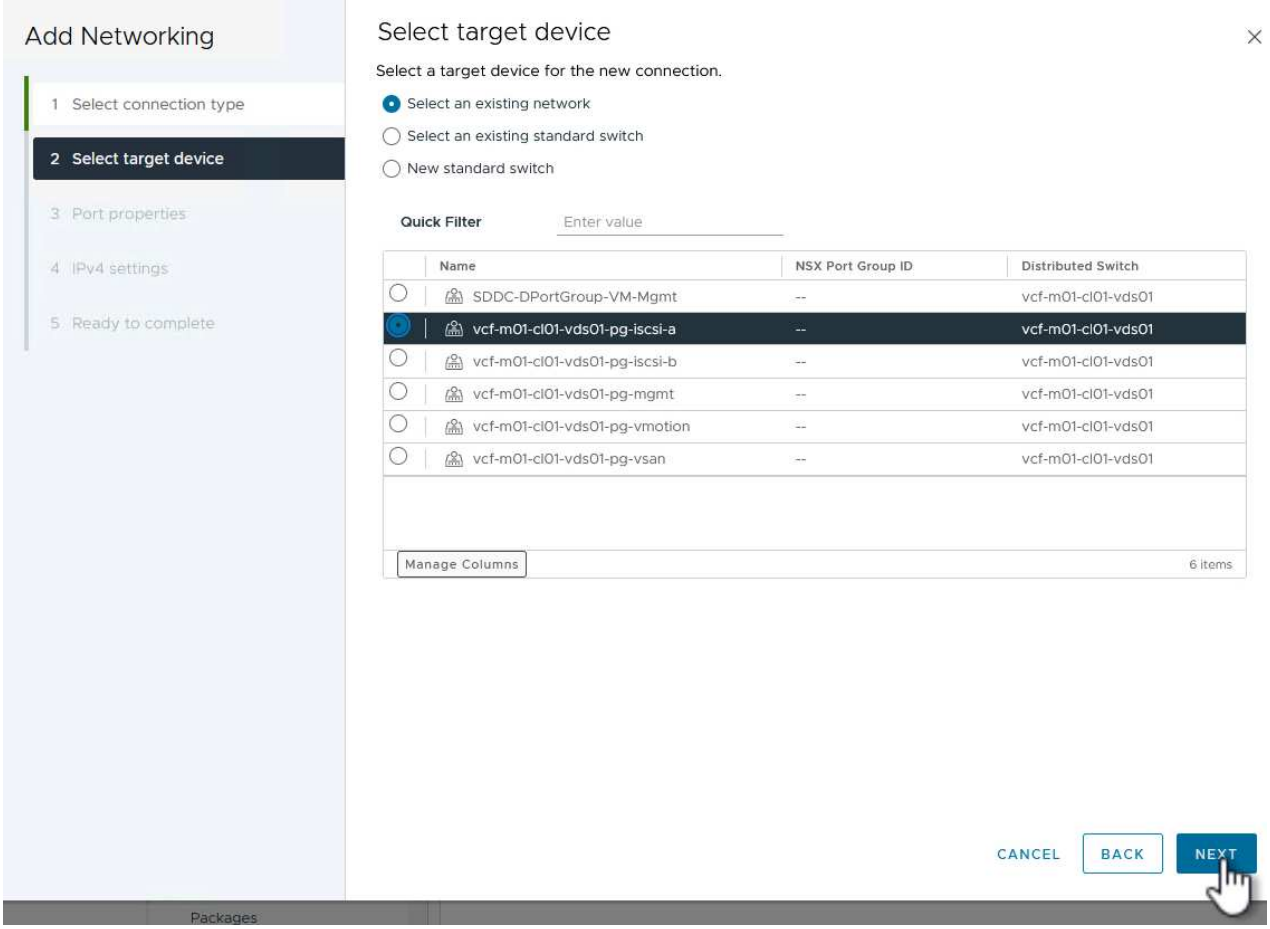
1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts im Inventar der Verwaltungsdomäne. Wählen Sie auf der Registerkarte **Konfigurieren VMkernel-Adapter** aus und klicken Sie zum Starten auf **Netzwerk hinzufügen…**.



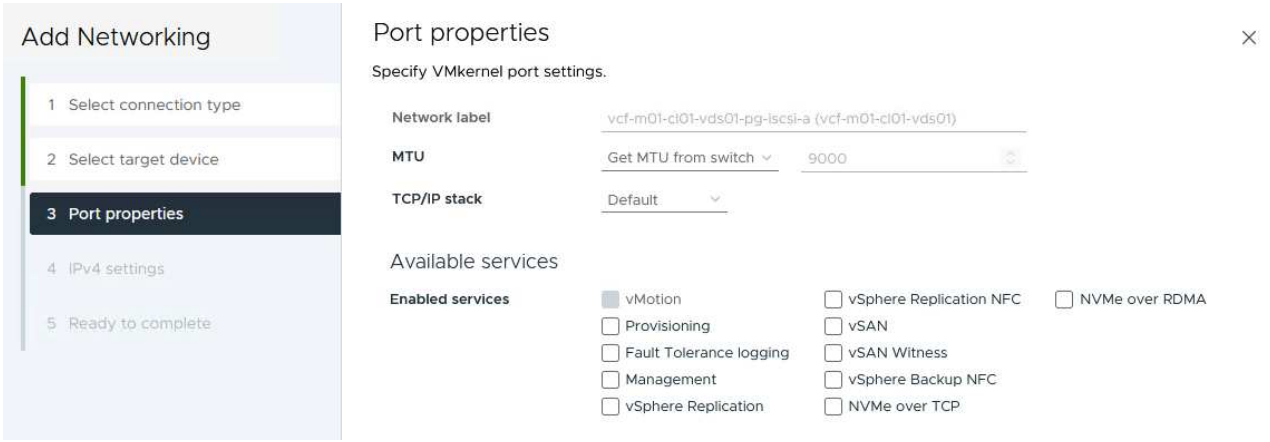
2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel-Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



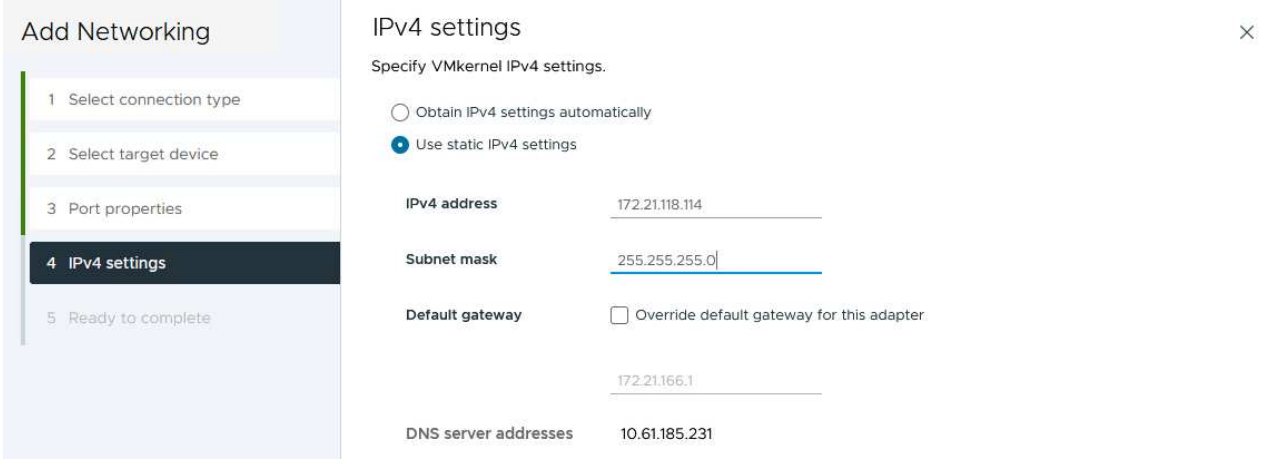
3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für iSCSI aus.



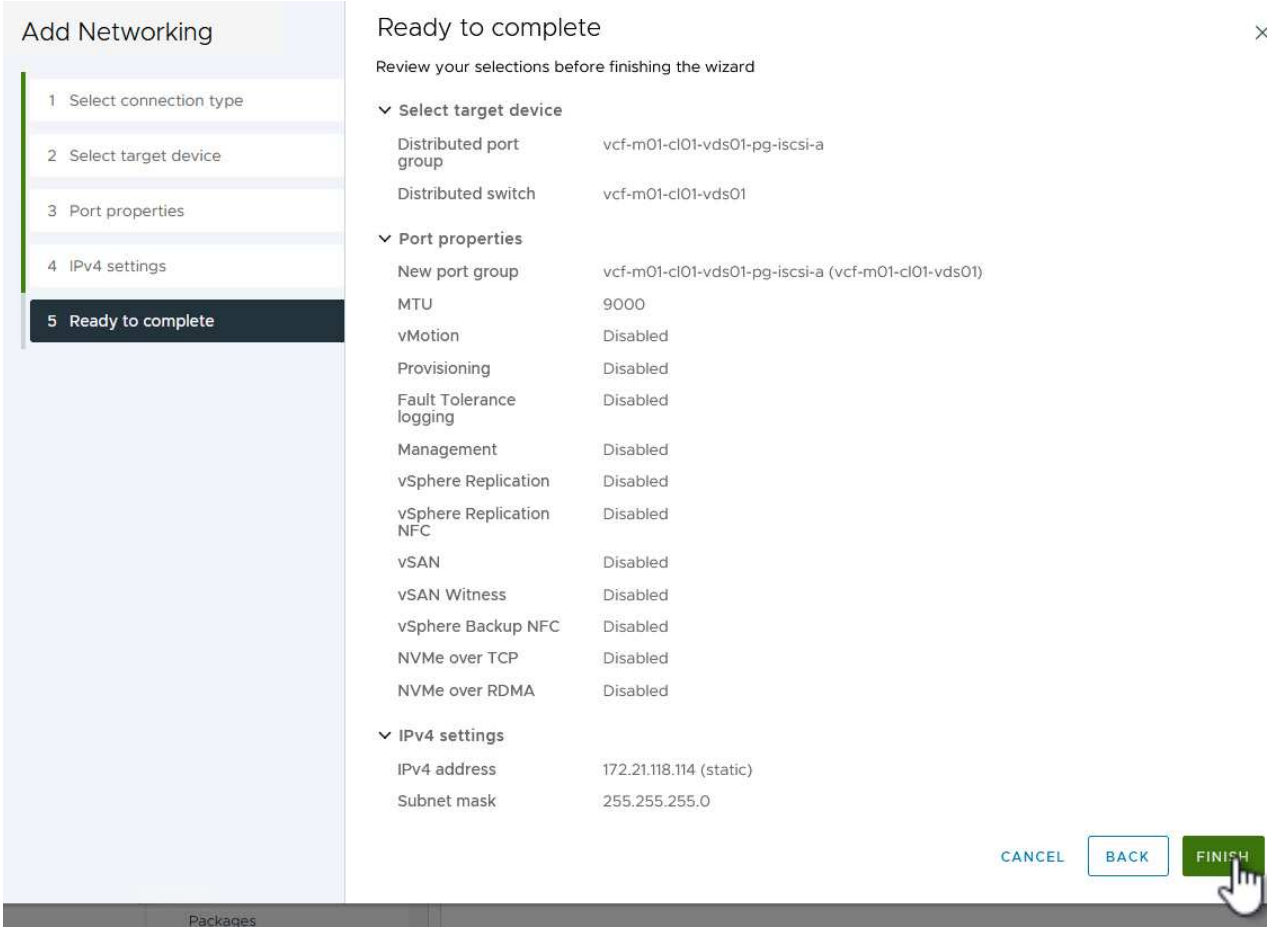
4. Behalten Sie auf der Seite **Porteigenschaften** die Standardeinstellungen bei und klicken Sie auf **Weiter**, um fortzufahren.



5. Geben Sie auf der Seite **IPv4-Einstellungen** die **IP-Adresse** und **Subnetzmaske** ein und geben Sie eine neue Gateway-IP-Adresse an (nur falls erforderlich). Klicken Sie auf **Weiter**, um fortzufahren.



6. Überprüfen Sie Ihre Auswahl auf der Seite **Bereit zum Abschließen** und klicken Sie auf **Fertig**, um den VMkernel-Adapter zu erstellen.



7. Wiederholen Sie diesen Vorgang, um einen VMkernel-Adapter für das zweite iSCSI-Netzwerk zu erstellen.

Bereitstellen und Verwenden von ONTAP Tools zum Konfigurieren von Speicher

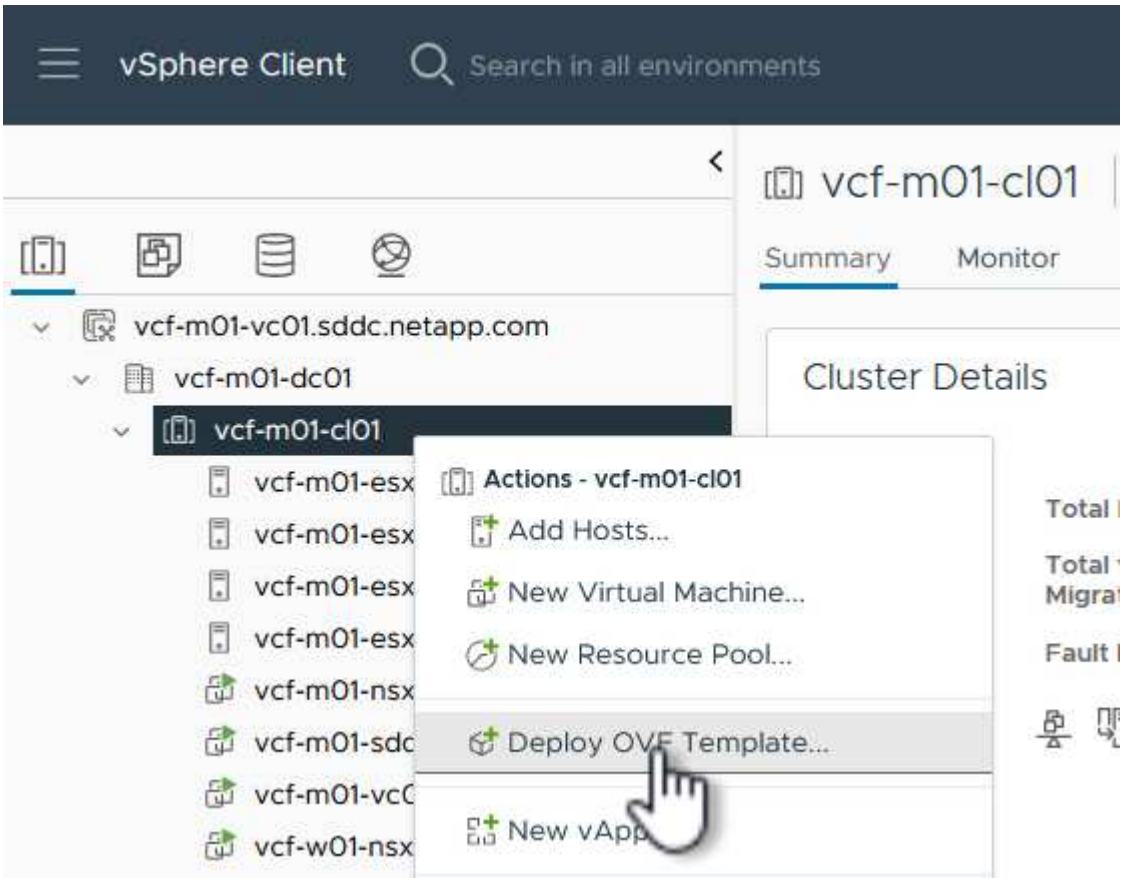
Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VCF-Verwaltungsdomänencluster ausgeführt und umfassen die Bereitstellung von OTV, die Erstellung eines VMFS-iSCSI-Datenspeichers und die Migration von Verwaltungs-VMs in den neuen Datenspeicher.

Bereitstellen von ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere (OTV) werden als VM-Appliance bereitgestellt und bieten eine integrierte vCenter-Benutzeroberfläche zur Verwaltung des ONTAP Speichers.

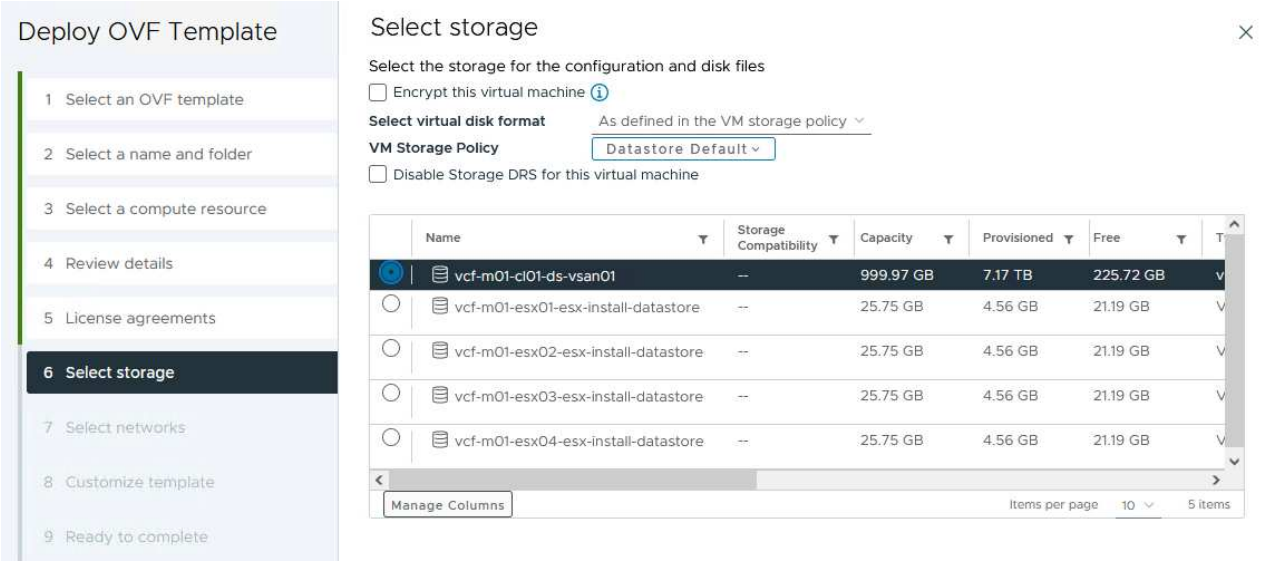
Führen Sie die folgenden Schritte aus, um ONTAP tools for VMware vSphere bereitzustellen:

1. Besorgen Sie sich das OVA-Image der ONTAP -Tools von der"NetApp Support-Site" und in einen lokalen Ordner herunterladen.
2. Melden Sie sich bei der vCenter-Appliance für die VCF-Verwaltungsdomäne an.
3. Klicken Sie in der vCenter-Appliance-Schnittstelle mit der rechten Maustaste auf den Verwaltungscluster und wählen Sie **OVF-Vorlage bereitstellen…**

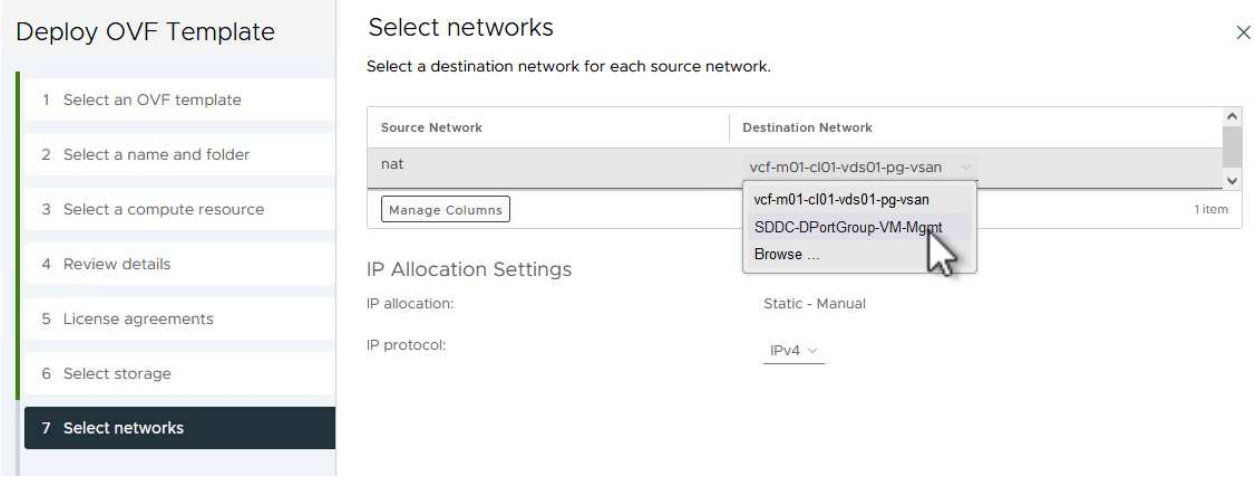


4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei der ONTAP -Tools aus.

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und einen Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie als Speicherort der Konfigurations- und Datenträgerdateien den vSAN-Datenspeicher des VCF-Managementdomänenclusters aus.

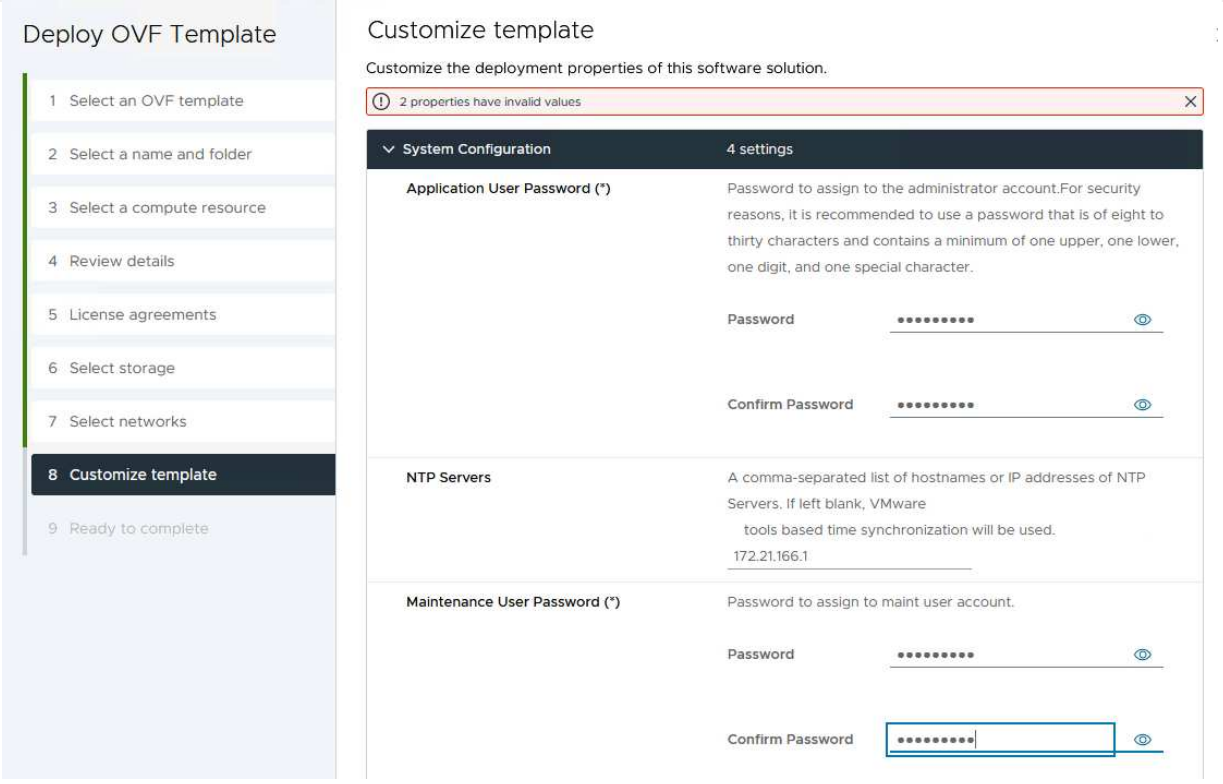


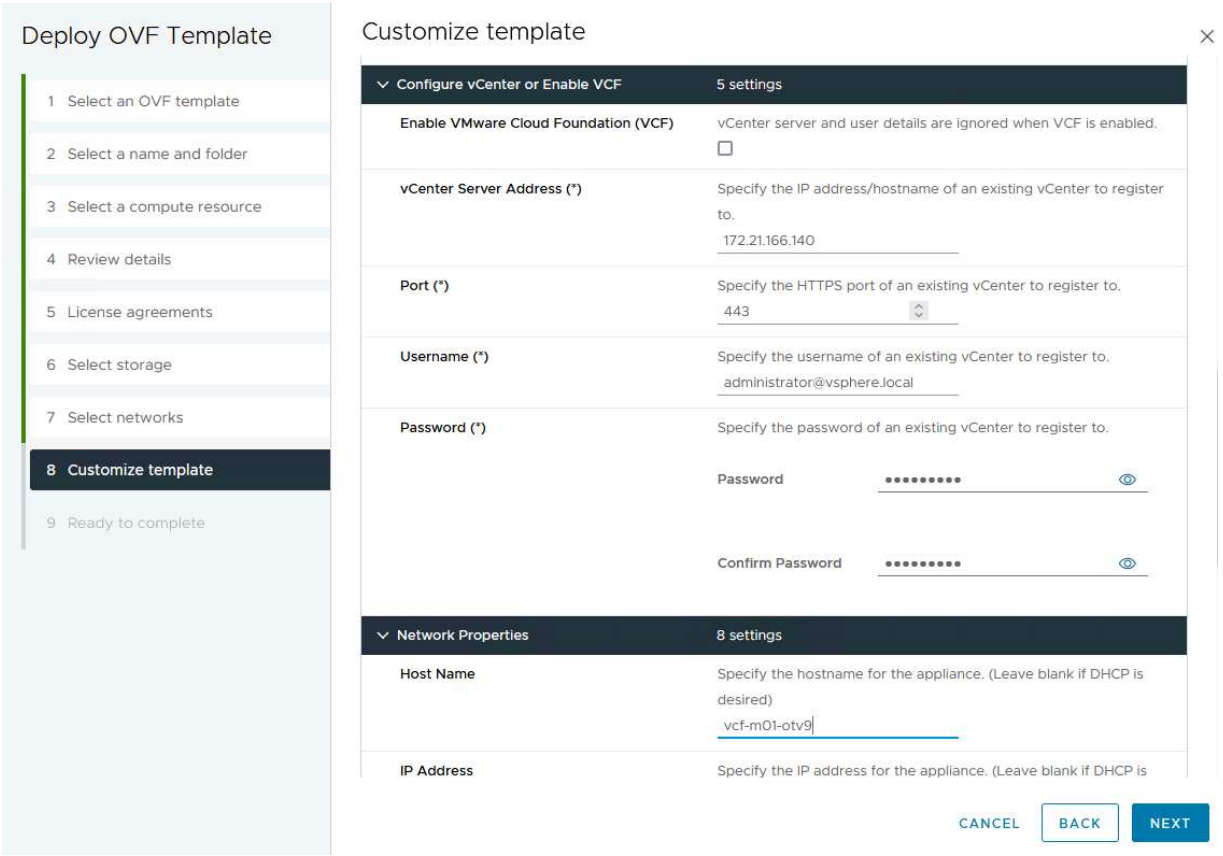
7. Wählen Sie auf der Seite „Netzwerk auswählen“ das für den Verwaltungsverkehr verwendete Netzwerk aus.



8. Geben Sie auf der Seite „Vorlage anpassen“ alle erforderlichen Informationen ein:
   - Für den administrativen Zugriff auf OTV zu verwendendes Passwort.
   - IP-Adresse des NTP-Servers.
   - Passwort für das OTV-Wartungskonto.
   - OTV Derby DB-Passwort.
   - Aktivieren Sie das Kontrollkästchen **VMware Cloud Foundation (VCF) aktivieren** nicht. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
   - FQDN oder IP-Adresse des vCenter-Geräts und geben Sie Anmeldeinformationen für vCenter an.
   - Geben Sie die erforderlichen Felder für die Netzwerkeigenschaften an.

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



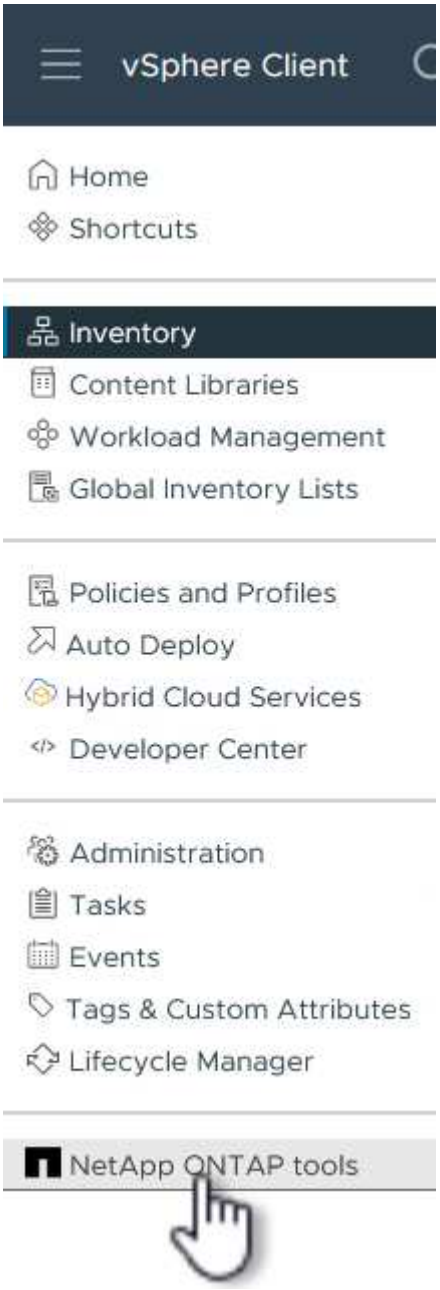


9. Überprüfen Sie alle Informationen auf der Seite „Bereit zum Abschließen“ und klicken Sie auf „Fertig stellen“, um mit der Bereitstellung des OTV-Geräts zu beginnen.

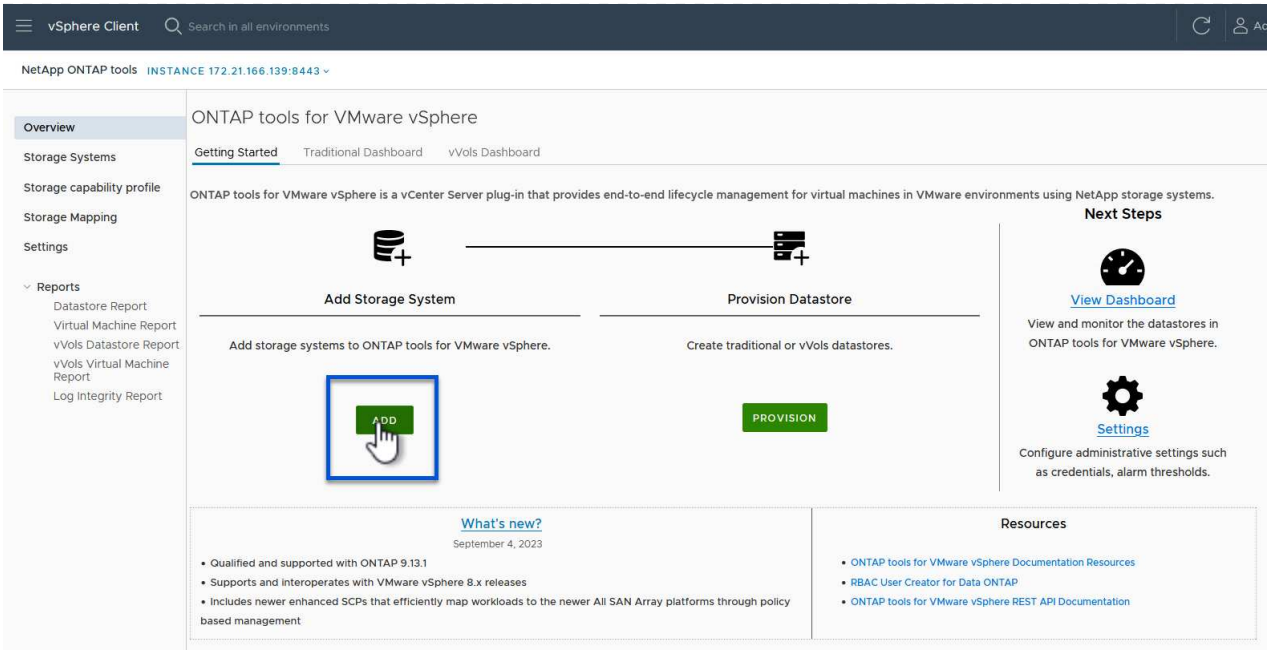
Konfigurieren Sie einen VMFS-iSCSI-Datenspeicher in der Verwaltungsdomäne mithilfe von OTV

Führen Sie die folgenden Schritte aus, um mithilfe von OTV einen VMFS-iSCSI-Datenspeicher als zusätzlichen Speicher in der Verwaltungsdomäne zu konfigurieren:

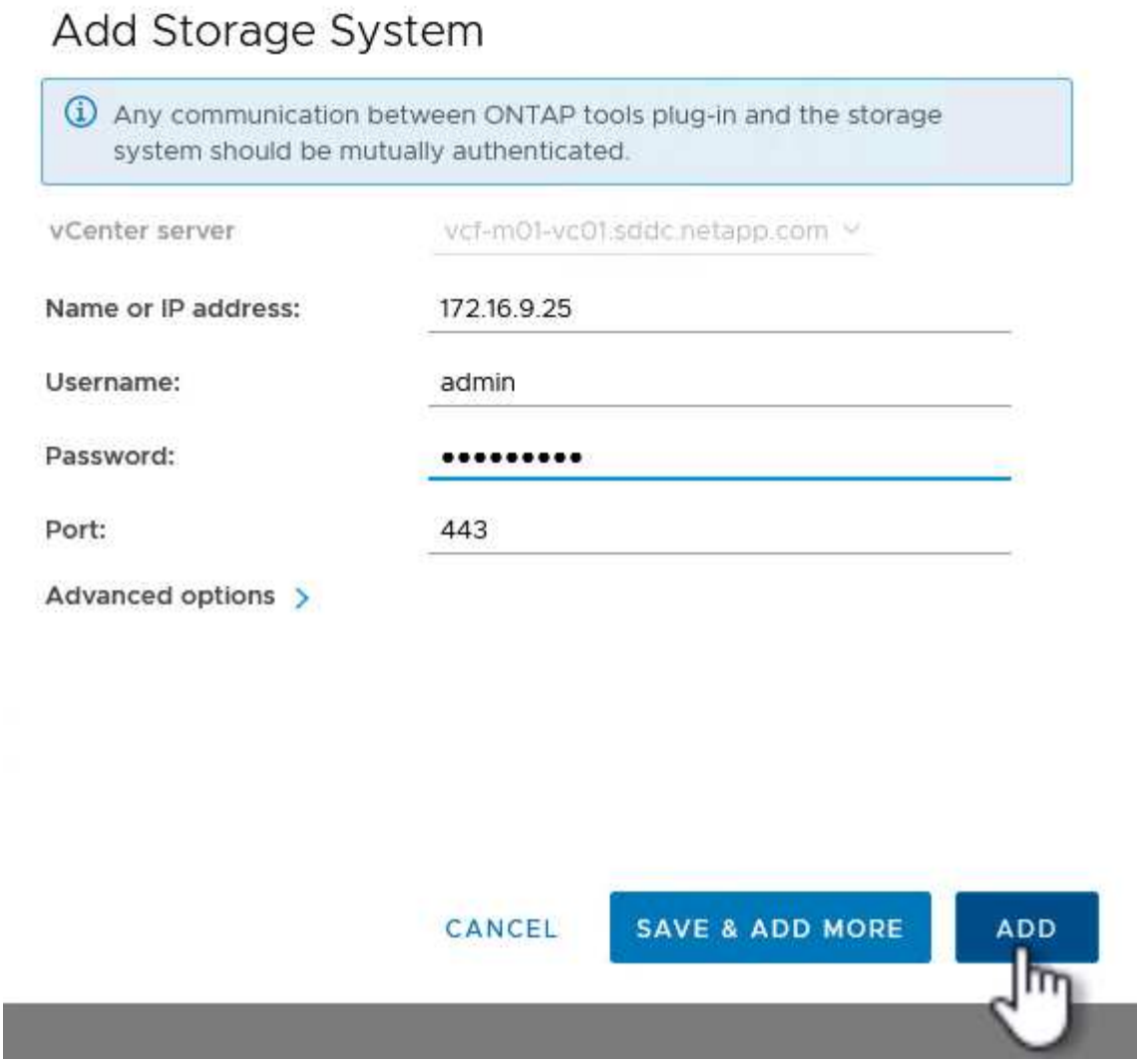
1. Navigieren Sie im vSphere-Client zum Hauptmenü und wählen Sie * NetApp ONTAP Tools*.



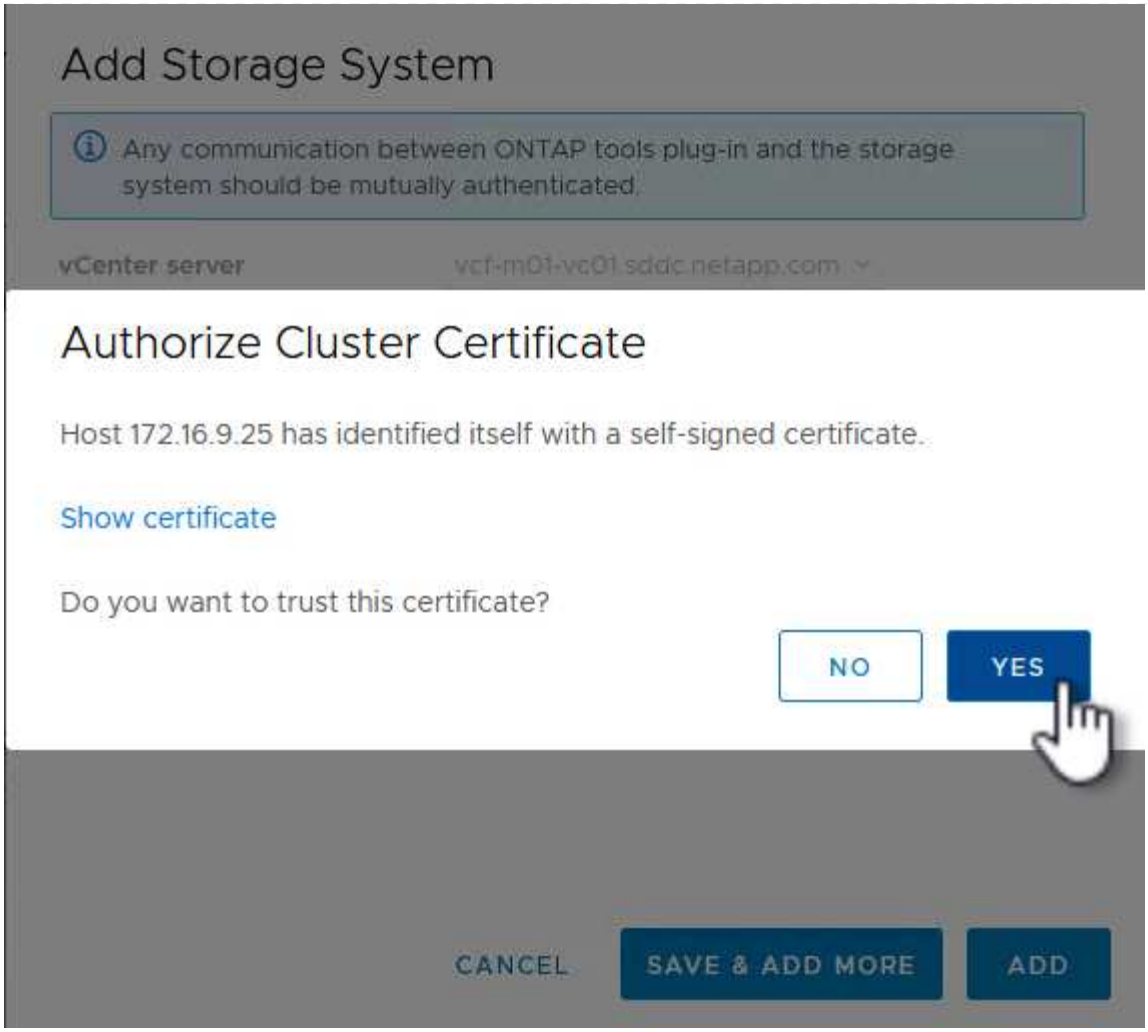
2. Klicken Sie in * ONTAP Tools* auf der Seite „Erste Schritte“ (oder unter „Speichersysteme“**) auf *Hinzufügen**, um ein neues Speichersystem hinzuzufügen.



3. Geben Sie die IP-Adresse und Anmeldeinformationen des ONTAP Speichersystems ein und klicken Sie auf **Hinzufügen**.



4. Klicken Sie auf **Ja**, um das Cluster-Zertifikat zu autorisieren und das Speichersystem hinzuzufügen.

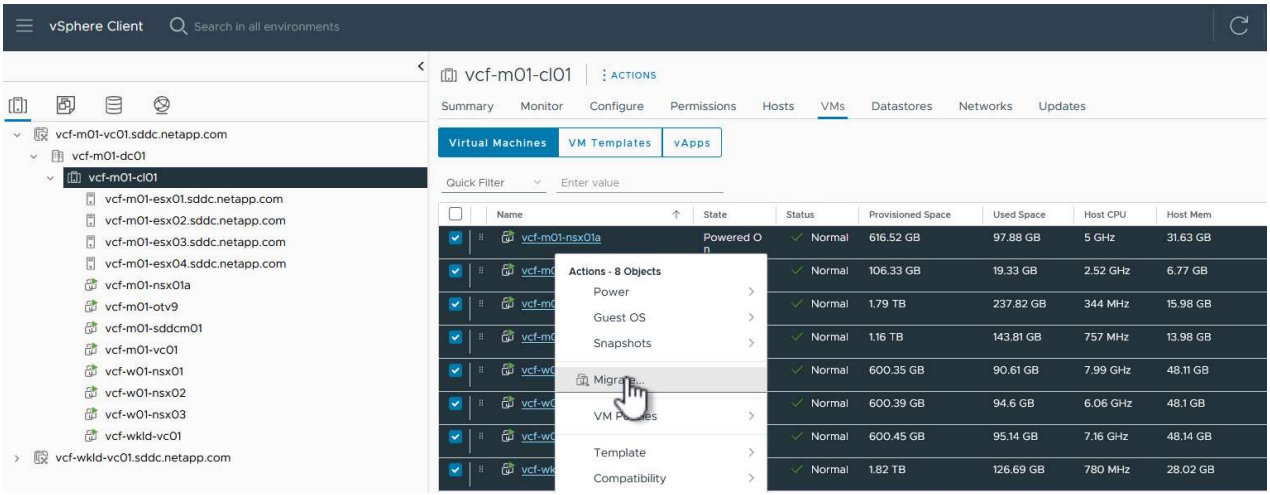

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Authorize Cluster Certificate
Host 172.16.9.25 has identified itself with a self-signed certificate.
Show certificate
Do you want to trust this certificate?
NO
YES
CANCEL
SAVE & ADD MORE
ADD

Migrieren Sie Management-VMs zum iSCSI-Datenspeicher

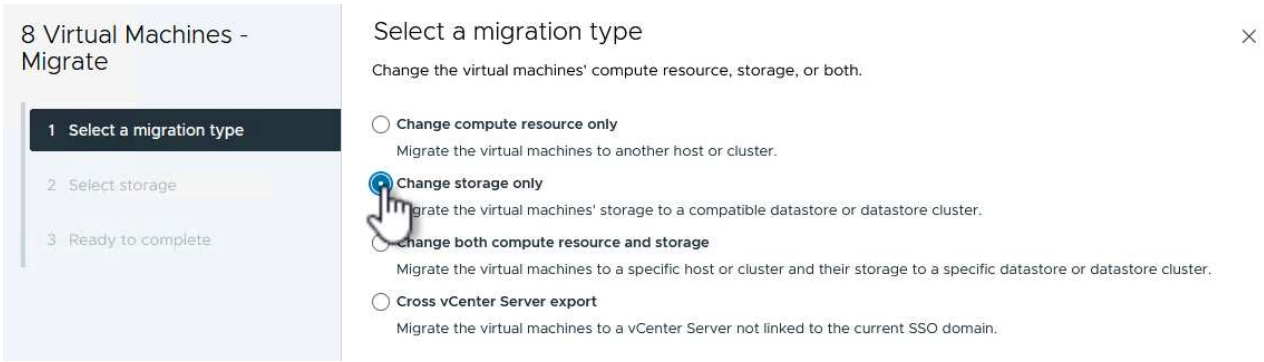
In Fällen, in denen die Verwendung von ONTAP -Speicher zum Schutz der VCF-Verwaltungs-VMs bevorzugt wird, kann vMotion zum Migrieren der VMs in den neu erstellten iSCSI-Datenspeicher verwendet werden.

Führen Sie die folgenden Schritte aus, um die VCF-Verwaltungs-VMs zum iSCSI-Datenspeicher zu migrieren.

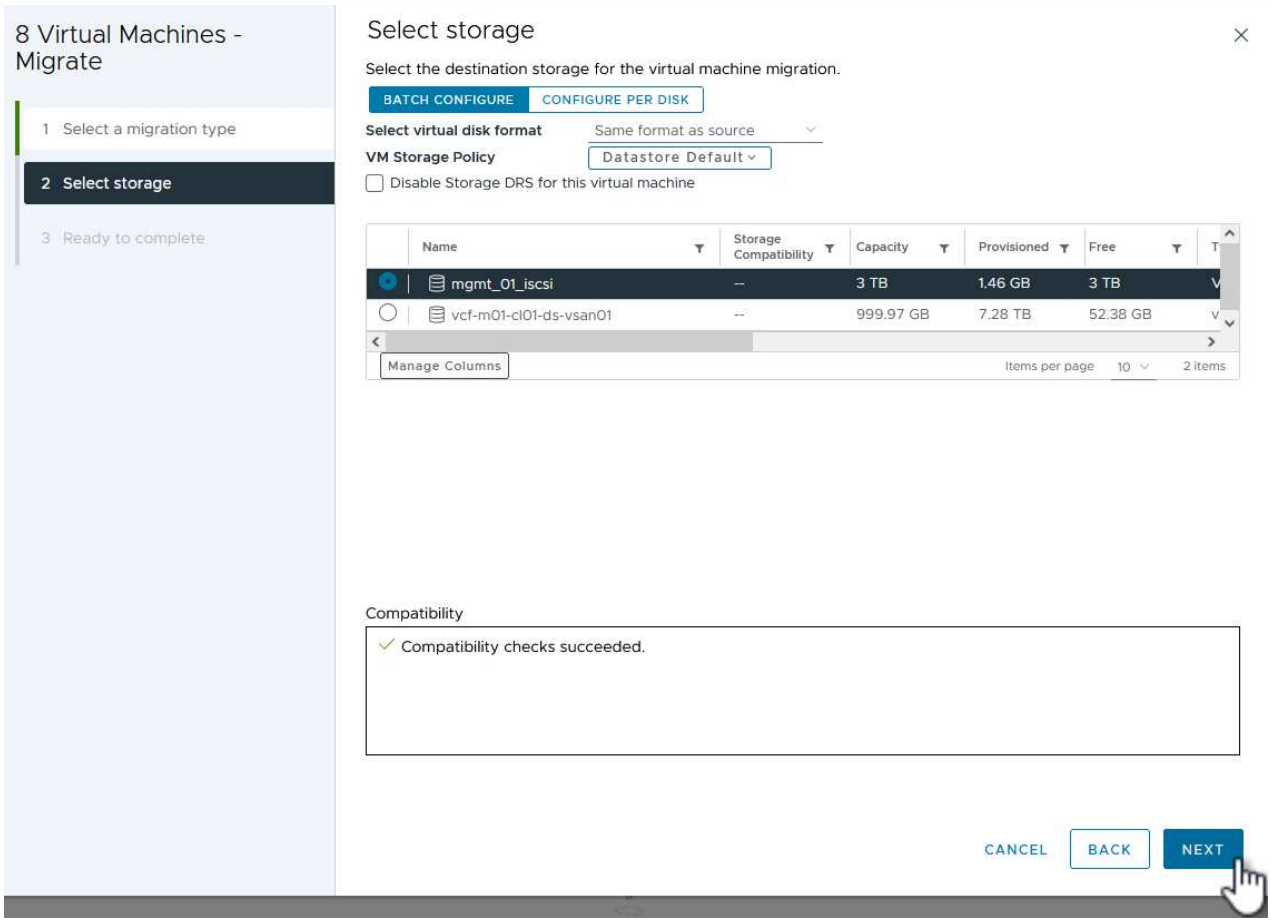
1. Navigieren Sie vom vSphere-Client zum Managementdomänencluster und klicken Sie auf die Registerkarte **VMs**.
2. Wählen Sie die VMs aus, die zum iSCSI-Datenspeicher migriert werden sollen, klicken Sie mit der rechten Maustaste und wählen Sie **Migrieren...**.



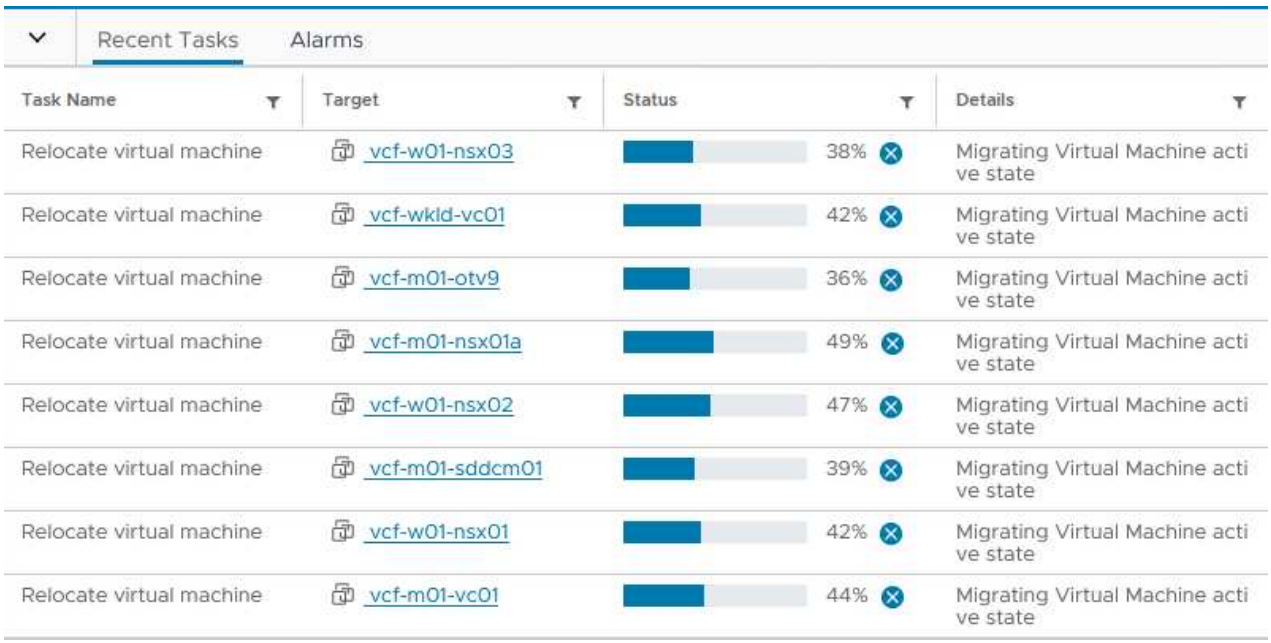
3. Wählen Sie im Assistenten **Virtuelle Maschinen – Migrieren** als Migrationstyp **Nur Speicher ändern** aus und klicken Sie auf **Weiter**, um fortzufahren.



4. Wählen Sie auf der Seite **Speicher auswählen** den iSCSi-Datenspeicher aus und klicken Sie auf **Weiter**, um fortzufahren.



5. Überprüfen Sie die Auswahl und klicken Sie auf **Fertig**, um die Migration zu starten.
6. Der Umzugsstatus kann im Bereich **Letzte Aufgaben** angezeigt werden.



Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Videodemo für diese Lösung

iSCSI-Datenspeicher als zusätzlicher Speicher für VCF-Verwaltungsdomänen

Fügen Sie mithilfe von ONTAP tools for VMware vSphere einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher für eine Verwaltungsdomäne hinzu

In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung von ONTAP Tools für VMware zum Konfigurieren eines VMFS-Datenspeichers über Fiber Channel (FC) als zusätzlichen Speicher für die Verwaltungsdomäne von VMware Cloud Foundation (VCF). Dieses Verfahren fasst die Bereitstellung von ONTAP Tools für VMware vSphere, die Registrierung von vCenter-Servern, die Definition des Speicher-Backends und die Bereitstellung des FC-Datenspeichers zusammen.

Vorteile von Fibre Channel

Hohe Leistung: FC bietet Hochgeschwindigkeitsdatenübertragungsraten und ist daher ideal für Anwendungen, die einen schnellen und zuverlässigen Zugriff auf große Datenmengen erfordern.

Geringe Latenz: Sehr geringe Latenz, die für leistungssensible Anwendungen wie Datenbanken und virtualisierte Umgebungen entscheidend ist.

Zuverlässigkeit: FC-Netzwerke sind für ihre Robustheit und Zuverlässigkeit bekannt und verfügen über Funktionen wie integrierte Redundanz und Fehlerkorrektur.

Dedizierte Bandbreite: FC bietet dedizierte Bandbreite für Speicherverkehr und reduziert so das Risiko einer Netzwerküberlastung.

Weitere Informationen zur Verwendung von Fibre Channel mit NetApp -Speichersystemen finden Sie unter "SAN-Bereitstellung mit FC" .

Szenarioübersicht

Der VCF-Zusatzdatenspeicher wird im Rahmen der Day-2-Operationen mithilfe von vCenter bereitgestellt. Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Bereitstellung von ONTAP -Tools in der Verwaltungsdomäne
- Registrieren Sie VI-Workload-vCenter-Server bei ONTAP -Tools
- Definieren Sie das Storage-Backend im ONTAP -Tools-Plugin für VMware vSphere
- Bereitstellen von VMFS auf FC-Transport

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP Speichersystem mit FC-Ports, die mit FC-Switches verbunden sind.
- SVM mit FC-Lifs erstellt.
- vSphere mit FC-HBAs, die mit FC-Switches verbunden sind.
- Auf FC-Switches ist eine einzelne Initiator-Ziel-Zonierung konfiguriert.

> Verwenden Sie in der Zonenkonfiguration die logische SVM FC-Schnittstelle anstelle physischer FC-Ports auf ONTAP -Systemen.

NetApp empfiehlt Multipath für FC-LUNs.

Ausführliche Informationen zur Konfiguration von Fibre Channel auf ONTAP Speichersystemen finden Sie unter "SAN-Speicherverwaltung" in der ONTAP 9-Dokumentation.

Weitere Informationen zur Verwendung von VMFS mit ONTAP Speichersystemen finden Sie im"Bereitstellungshandbuch für VMFS" .

Bereitstellungsschritte für die Verwaltungsdomäne

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und damit einen VMFS-Datenspeicher in der VCF-Verwaltungsdomäne zu erstellen:

- "Stellen Sie ONTAP -Tools in der Verwaltungsdomäne bereit"
- "Definieren Sie das Speicher-Backend mithilfe der vSphere-Clientschnittstelle"
- "Bereitstellen von VMFS auf FC"

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Videodemo für diese Lösung

VMFS(FC)-Datenspeicher als zusätzlicher Speicher für die VCF-Verwaltungsdomäne

Fügen Sie vVols als zusätzlichen Speicher zu VI-Workload-Domänen hinzu, indem Sie ONTAP tools for VMware vSphere verwenden

In diesem Anwendungsfall beschreiben wir das Verfahren zum Konfigurieren eines vVols -Datenspeichers mit iSCSI für zusätzlichen Speicher in einer VMware Cloud Foundation (VCF) Virtual Infrastructure (VI)-Workloaddomäne. Dieses Verfahren fasst die Einrichtung des iSCSI-Netzwerks, die Bereitstellung von ONTAP Tools für VMware vSphere und die Bereitstellung des vVols Datenspeichers zusammen.

iSCSI wird als Speicherprotokoll für den vVols Datenspeicher verwendet.

Vorteile von iSCSI

Hohe Leistung: Bietet hohe Leistung für schnelle, effiziente Datenübertragungsraten und geringe Latenz. Ideal für anspruchsvolle Unternehmensanwendungen und virtualisierte Umgebungen.

Einfache Verwaltung: Vereinfacht die Speicherverwaltung durch die Verwendung vertrauter IP-basierter Tools und Protokolle.

Kostengünstig: Nutzt die vorhandene Ethernet-Infrastruktur, reduziert den Bedarf an Spezialhardware und ermöglicht Unternehmen die Erzielung zuverlässiger und skalierbarer Speicherlösungen.

Weitere Informationen zur Verwendung von iSCSI mit NetApp -Speichersystemen finden Sie unter "SAN-Bereitstellung mit iSCSI" .

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

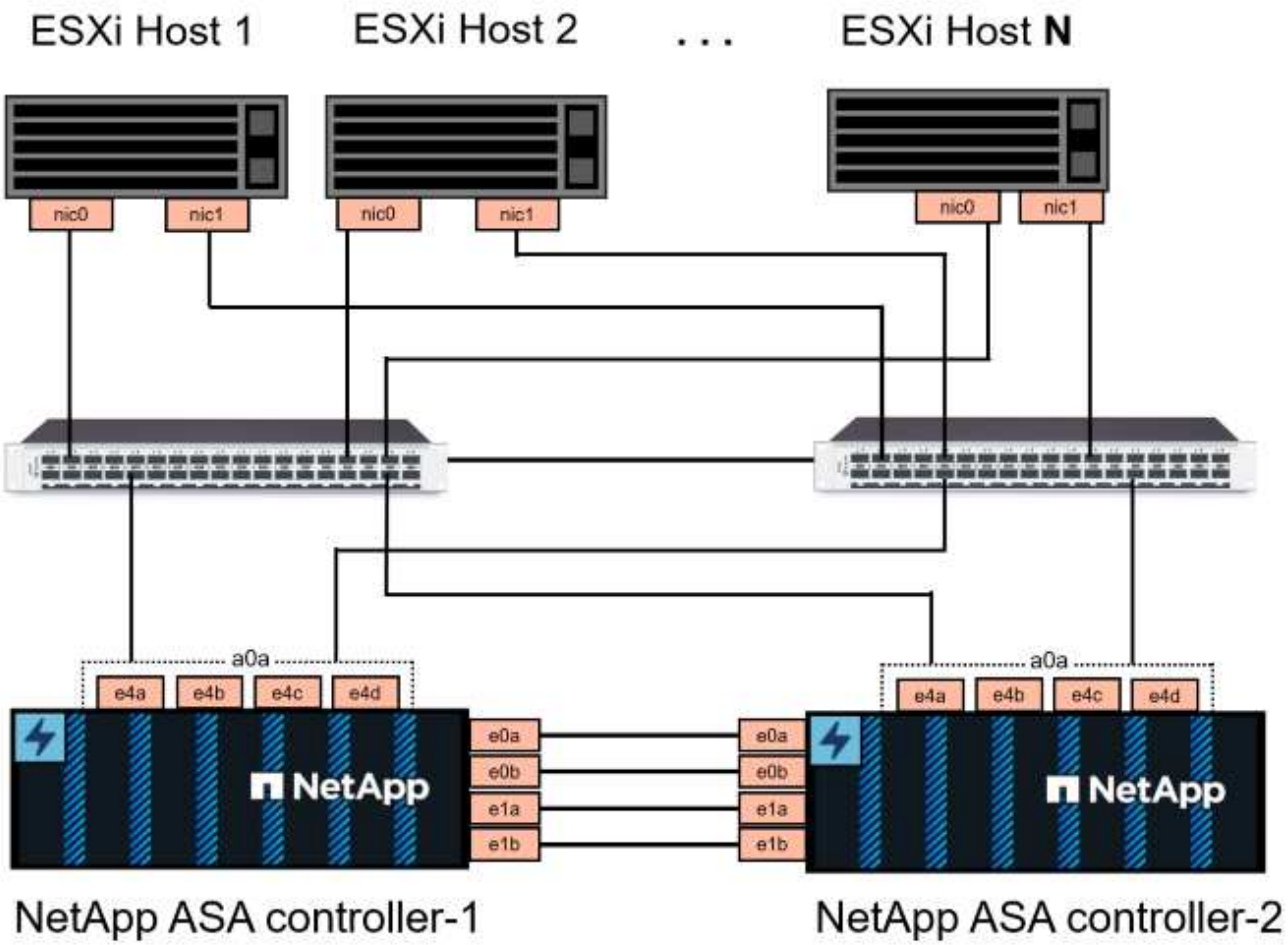
- Erstellen Sie eine Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Verkehr.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workloaddomäne.
- Erstellen Sie VMkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workloaddomäne.
- Stellen Sie ONTAP Tools in der VI-Workloaddomäne bereit.
- Erstellen Sie einen neuen vVols Datenspeicher in der VI-Workloaddomäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF oder ASA Speichersystem mit physischen Datenports auf Ethernet-Switches, die für den Speicherverkehr vorgesehen sind.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf den vSphere-Client kann zugegriffen werden.
- Zuvor wurde eine VI-Workloaddomäne bereitgestellt.

NetApp empfiehlt vollständig redundante Netzwerkdesigns für iSCSI. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration, die Fehlertoleranz für Speichersysteme, Switches, Netzwerkadapter und Hostsysteme bietet. Weitere Informationen finden Sie in der NetApp"SAN-Konfigurationsreferenz" für weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp , für alle SVMs in iSCSI-Konfigurationen mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken zu haben.

Diese Dokumentation veranschaulicht den Vorgang zum Erstellen einer neuen SVM und zum Angeben der IP-Adressinformationen zum Erstellen mehrerer LIFs für iSCSI-Verkehr. Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie unter"Erstellen Sie eine LIF (Netzwerkschnittstelle)" .

> In Situationen, in denen mehrere VMkernel-Adapter im selben IP-Netzwerk konfiguriert sind, wird empfohlen, die Software-iSCSI-Portbindung auf den ESXi-Hosts zu verwenden, um sicherzustellen, dass ein Lastenausgleich zwischen den Adaptern erfolgt. Siehe KB-Artikel"Überlegungen zur Verwendung der Software-iSCSI-Portbindung in ESX/ESXi (2038869)" .

Weitere Informationen zur Verwendung von VMFS iSCSI-Datenspeichern mit VMware finden Sie unter"vSphere VMFS-Datenspeicher – iSCSI-Speicher-Backend mit ONTAP" .

Bereitstellungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und damit einen vVols Datenspeicher in der VCF-Verwaltungsdomäne zu erstellen:

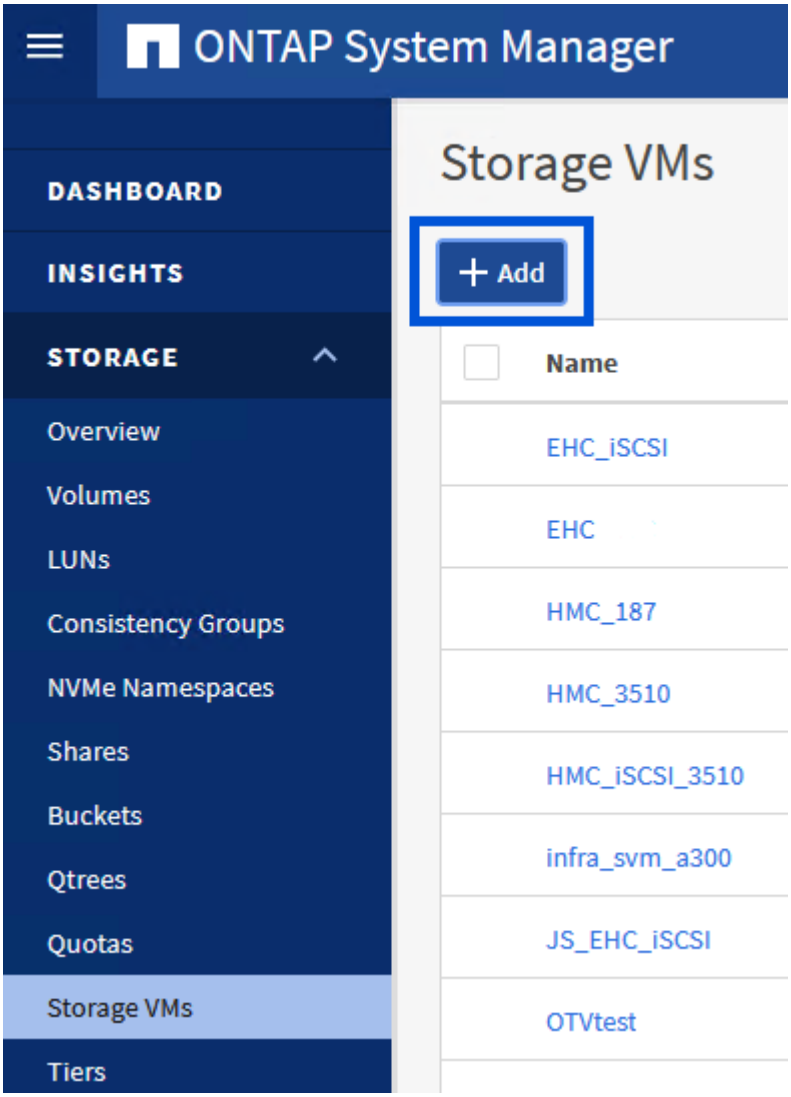
Erstellen Sie SVM und LIFs auf dem ONTAP Speichersystem

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

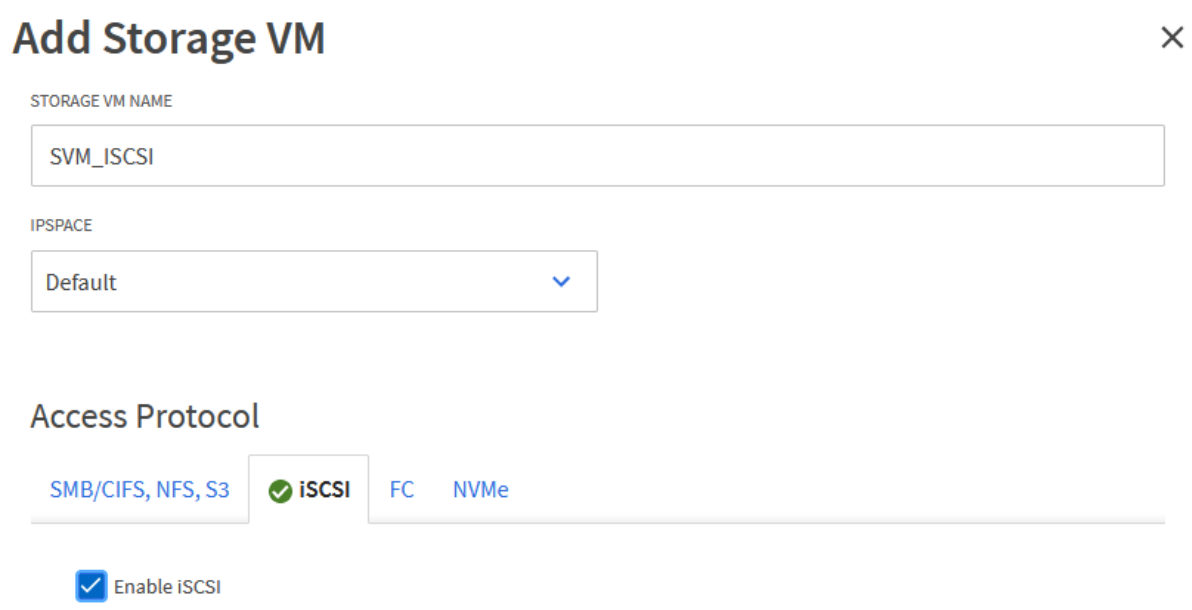
Erstellen der Speicher-VM und LIFs

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für iSCSI-Verkehr zu erstellen.

1. Navigieren Sie im ONTAP System Manager im linken Menü zu **Storage VMs** und klicken Sie zum Starten auf **+ Hinzufügen**.

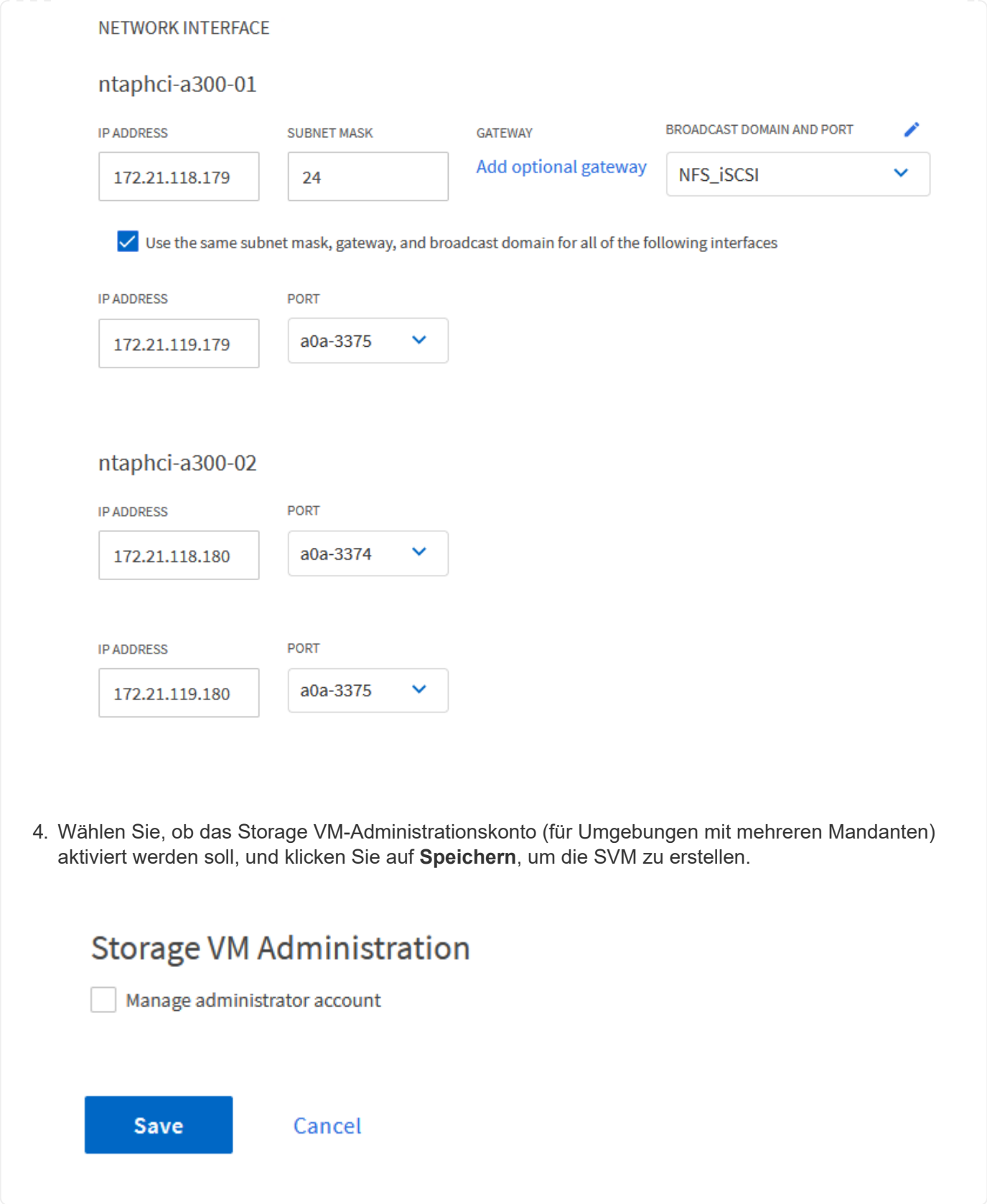


2. Geben Sie im Assistenten **Speicher-VM hinzufügen** einen **Namen** für die SVM ein, wählen Sie den **IP-Bereich** aus und klicken Sie dann unter **Zugriffsprotokoll** auf die Registerkarte **iSCSI** und aktivieren Sie das Kontrollkästchen **iSCSI aktivieren**.



3. Geben Sie im Abschnitt **Netzwerkschnittstelle** die **IP-Adresse**, **Subnetzmaske** und **Broadcast-Domäne und -Port** für das erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert werden, um gemeinsame Einstellungen für alle verbleibenden LIFs oder separate Einstellungen zu verwenden.

> Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp , für alle SVMs in iSCSI-Konfigurationen mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken zu haben.



4. Wählen Sie, ob das Storage VM-Administrationskonto (für Umgebungen mit mehreren Mandanten) aktiviert werden soll, und klicken Sie auf **Speichern**, um die SVM zu erstellen.

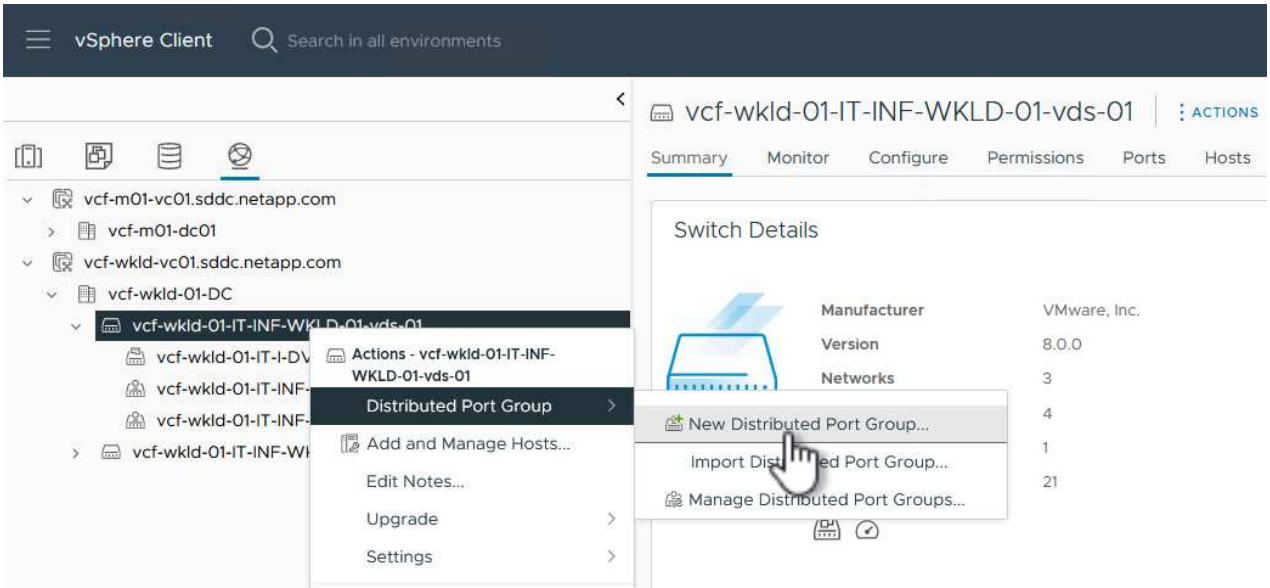
Einrichten des Netzwerks für iSCSI auf ESXi-Hosts

Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VI Workload Domain-Cluster ausgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client in allen Verwaltungs- und Workloaddomänen gleich ist.

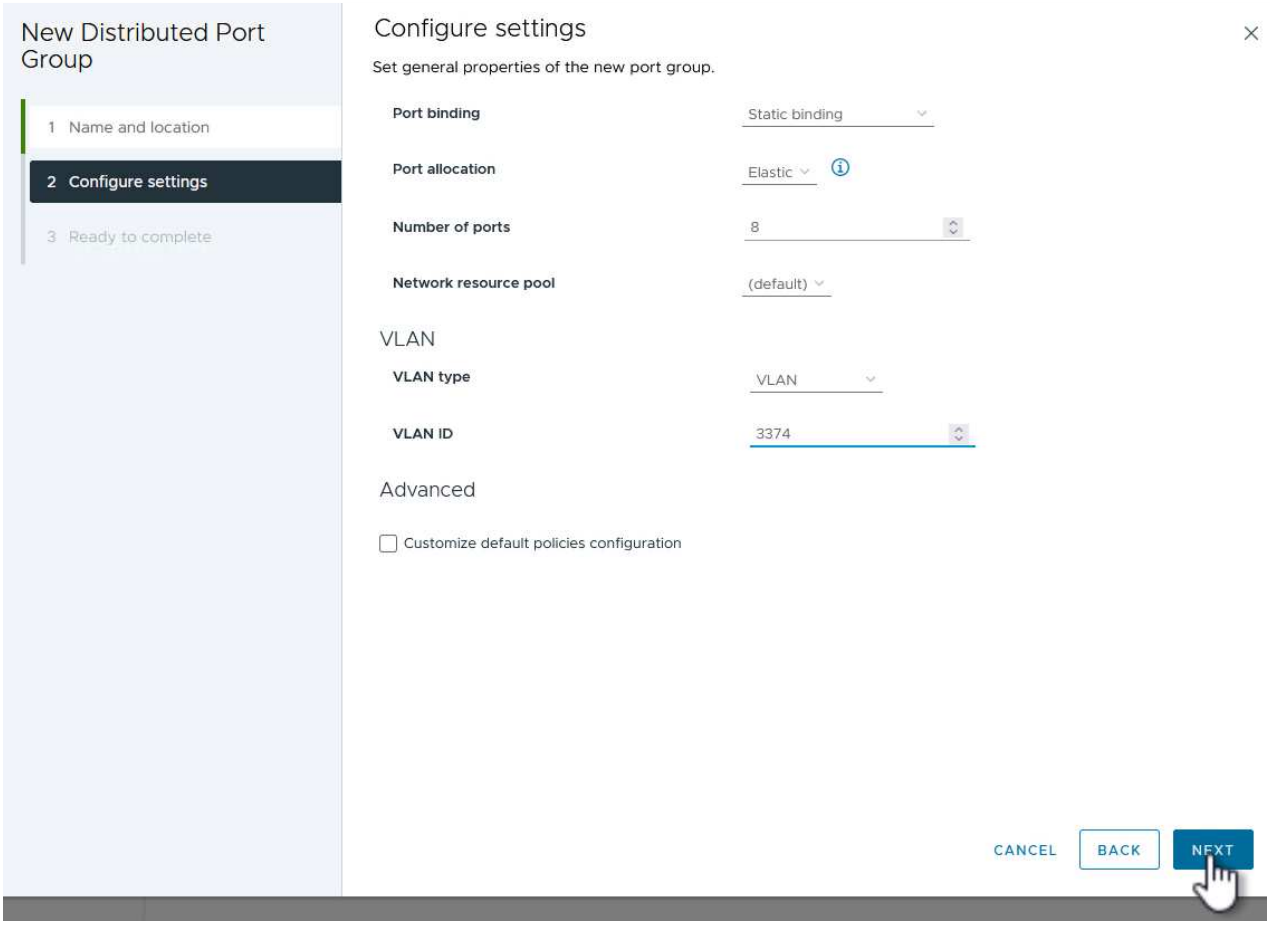
Erstellen Sie verteilte Portgruppen für iSCSI-Verkehr

Führen Sie die folgenden Schritte aus, um für jedes iSCSI-Netzwerk eine neue verteilte Portgruppe zu erstellen:

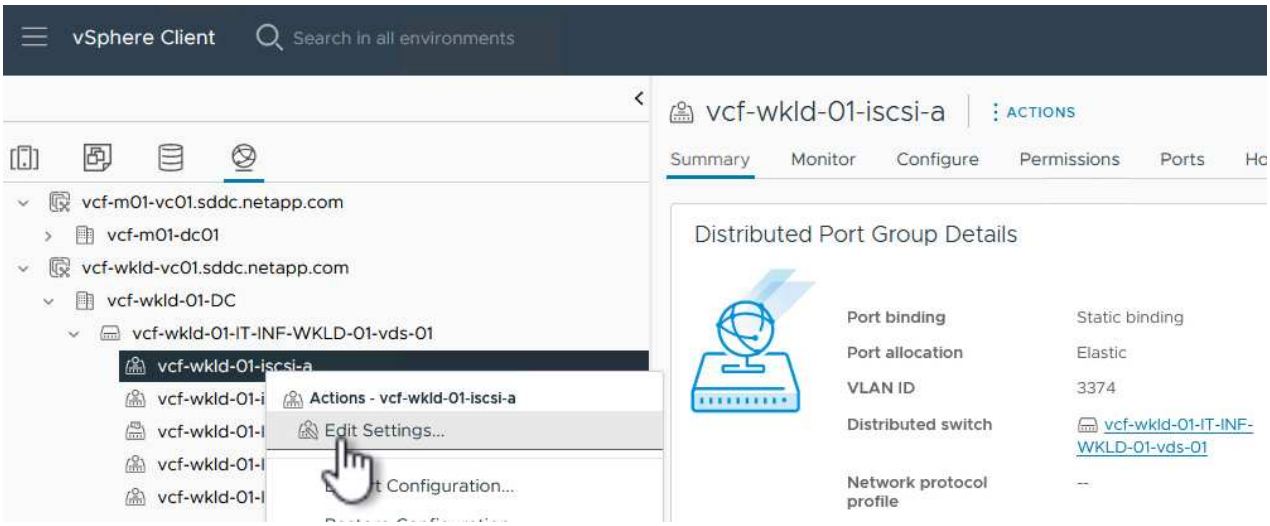
1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workloaddomäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen einer **Neuen verteilten Portgruppe…**.



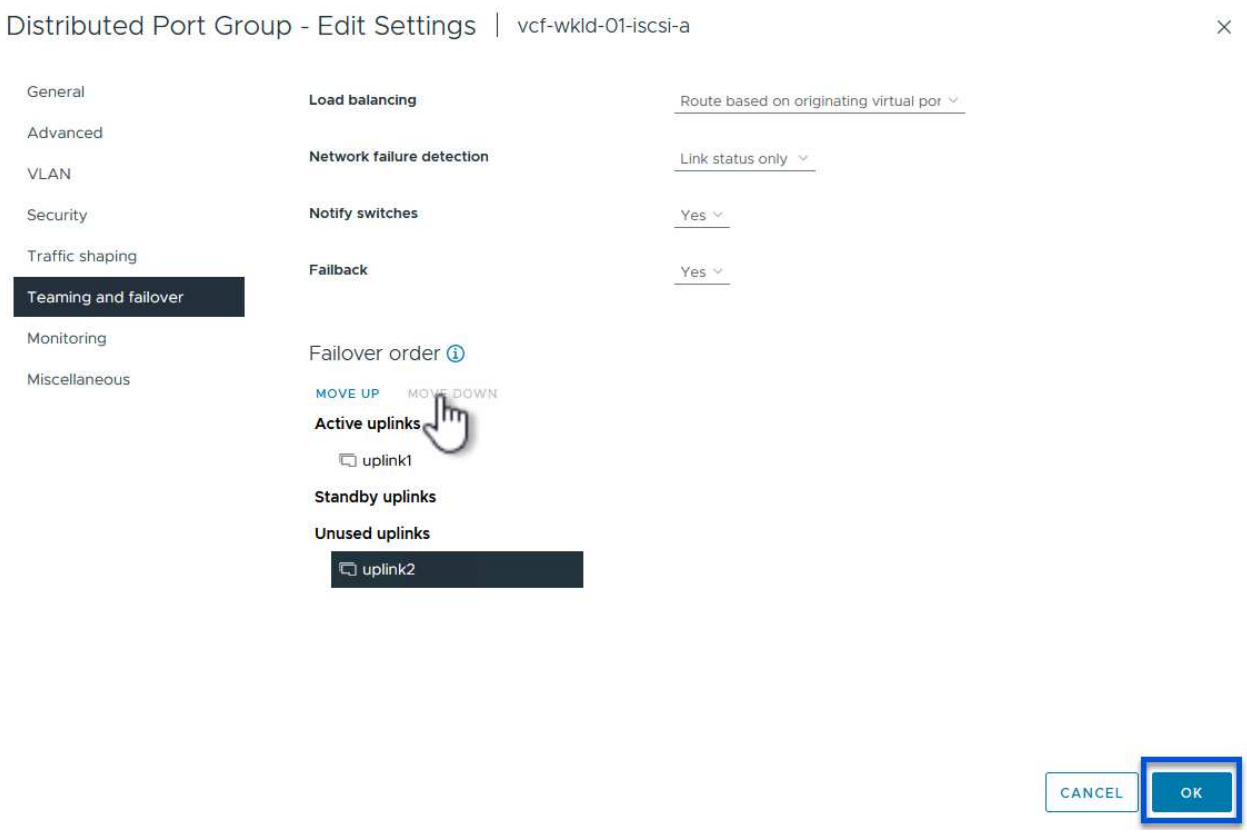
2. Geben Sie im Assistenten **Neue verteilte Portgruppe** einen Namen für die neue Portgruppe ein und klicken Sie auf **Weiter**, um fortzufahren.
3. Füllen Sie auf der Seite **Einstellungen konfigurieren** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige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



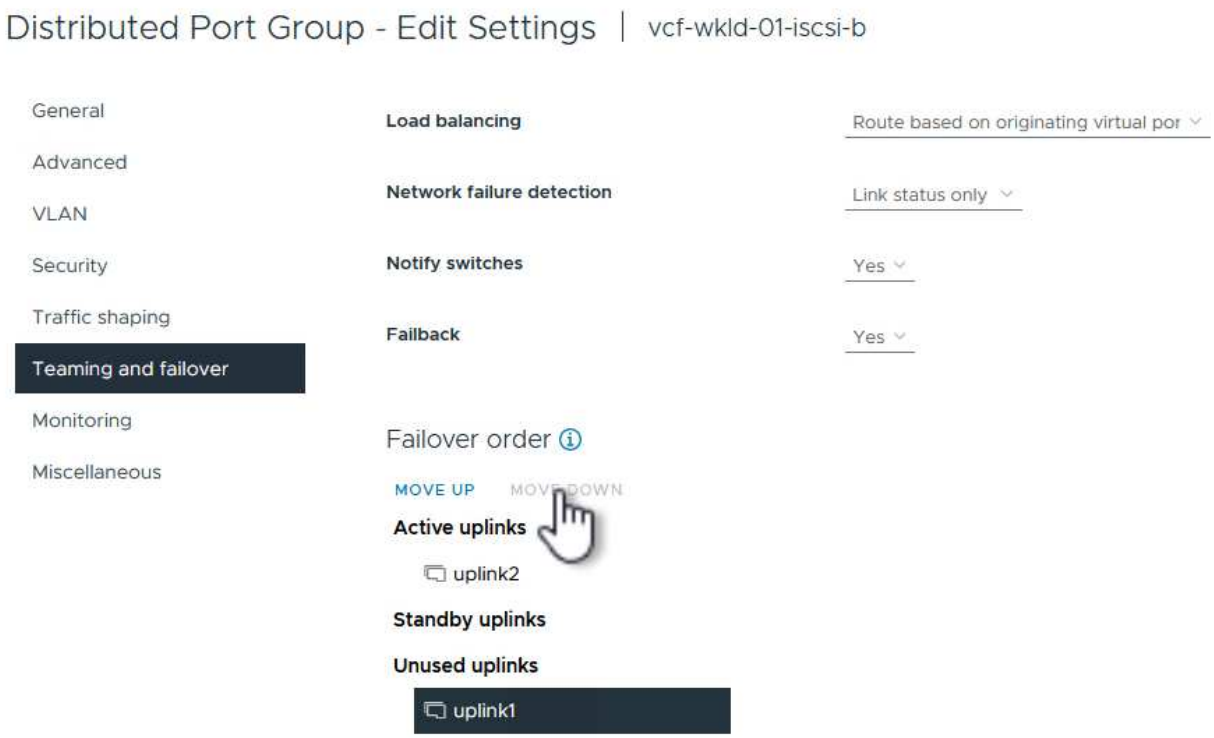
4. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Änderungen und klicken Sie auf **Fertig**, um die neue verteilte Portgruppe zu erstellen.
5. Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen, und stellen Sie sicher, dass Sie die richtige **VLAN-ID** eingegeben haben.
6. Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion „Einstellungen bearbeiten…“ aus.



7. Navigieren Sie auf der Seite **Verteilte Portgruppe – Einstellungen bearbeiten** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **Nicht verwendete Uplinks** zu verschieben.



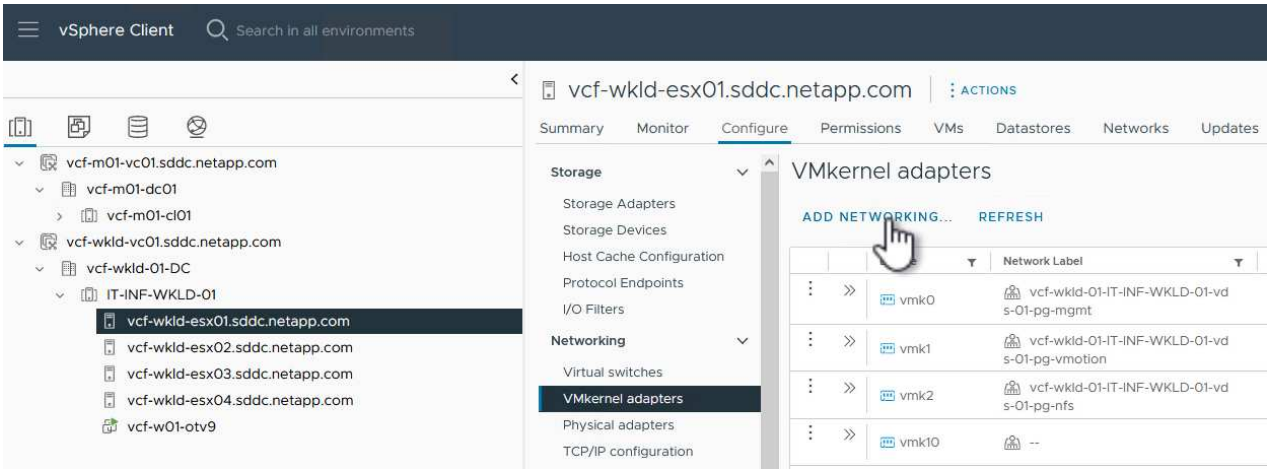
8. Wiederholen Sie diesen Schritt für die zweite iSCSI-Portgruppe. Verschieben Sie dieses Mal jedoch **Uplink1** nach unten zu **Ungenutzte Uplinks**.



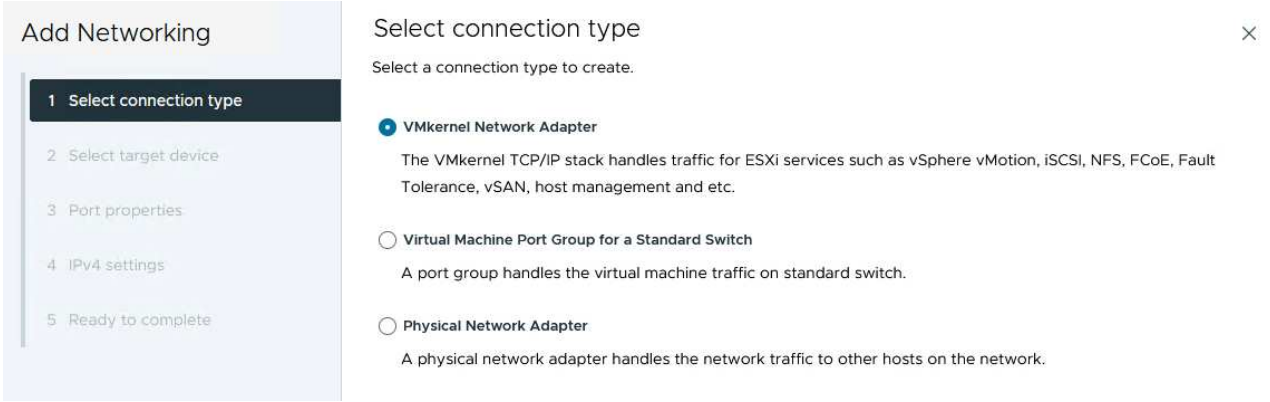
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

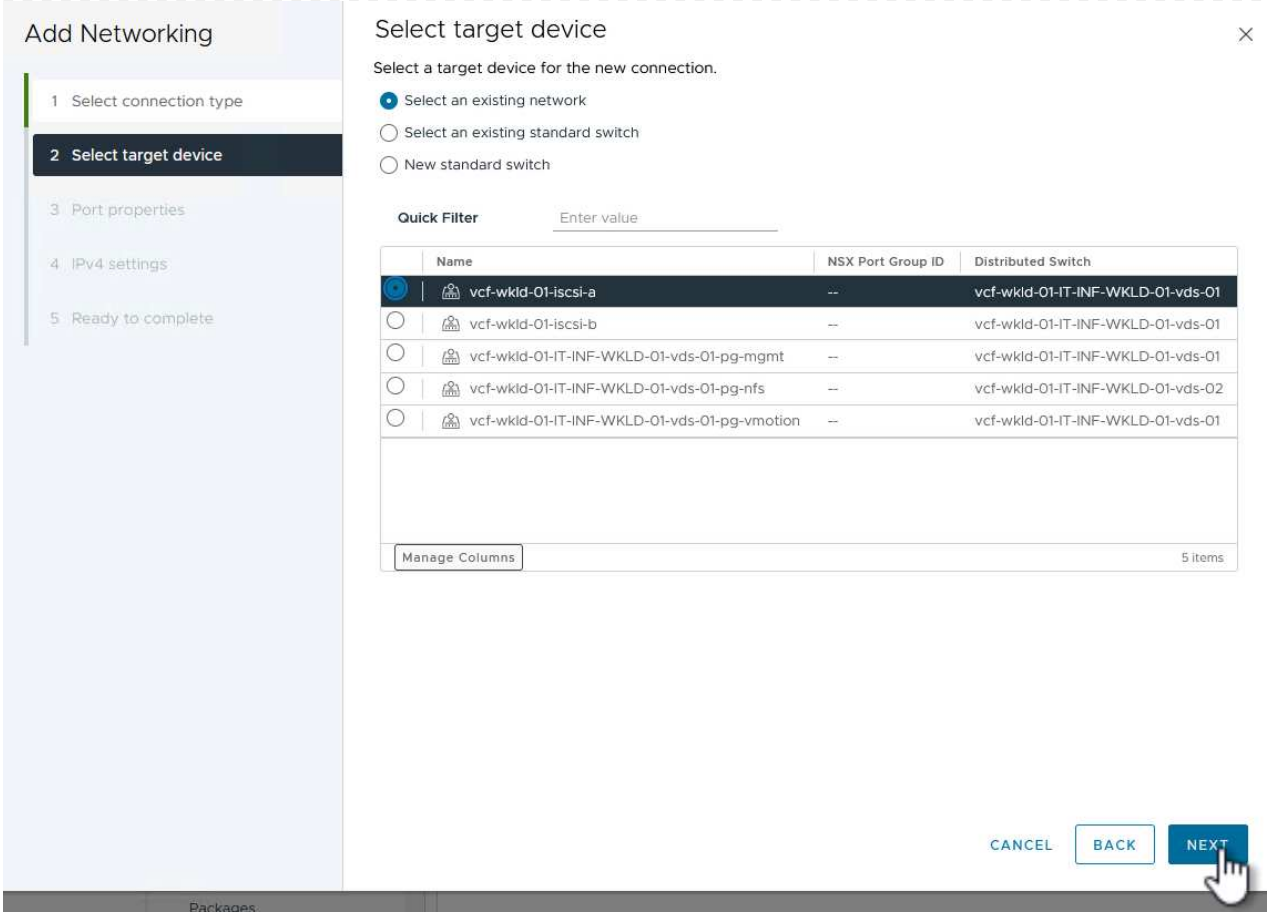
1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts im Workload-Domäneninventar. Wählen Sie auf der Registerkarte **Konfigurieren VMkernel-Adapter** aus und klicken Sie zum Starten auf **Netzwerk hinzufügen…**.



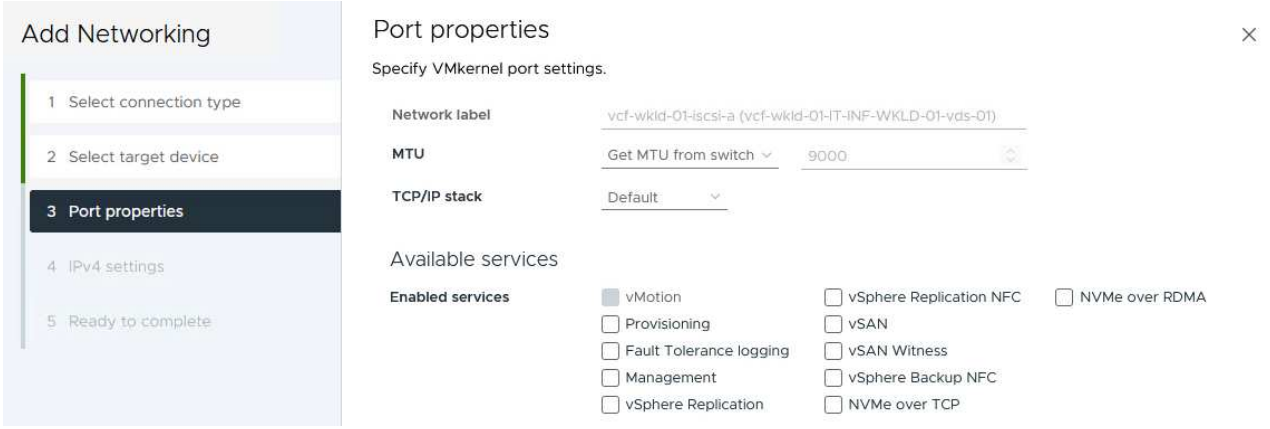
2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel-Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



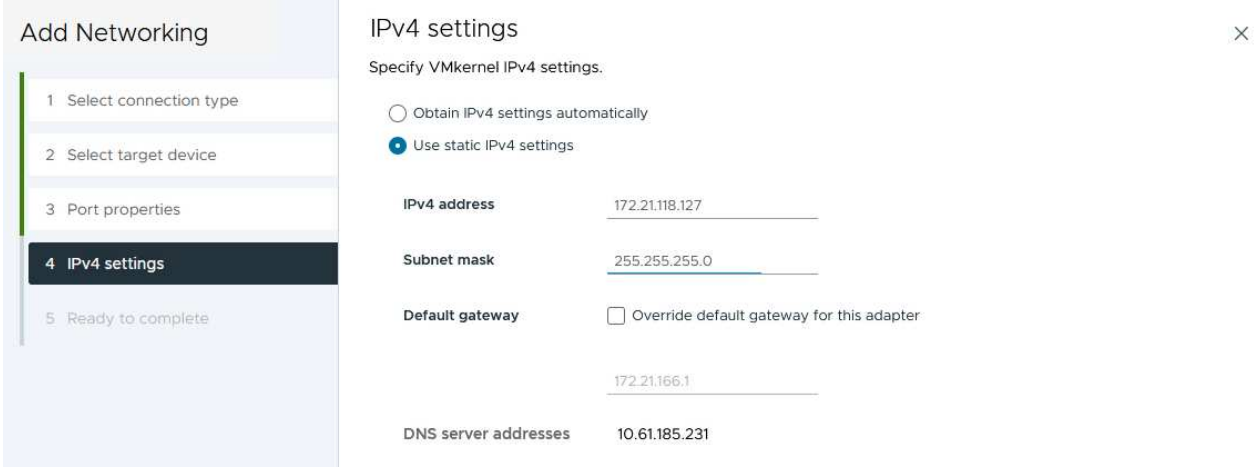
3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für iSCSI aus.



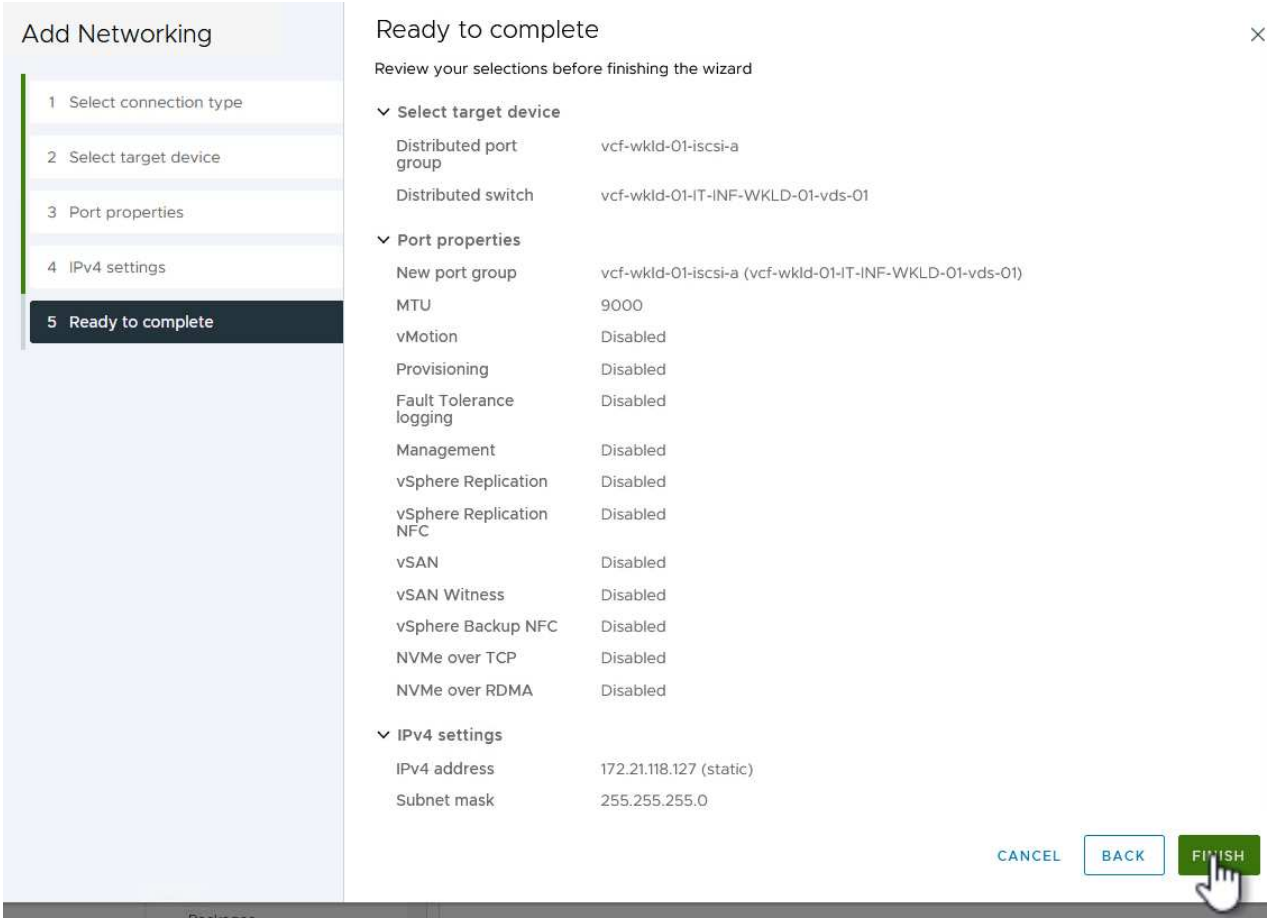
4. Behalten Sie auf der Seite **Porteigenschaften** die Standardeinstellungen bei und klicken Sie auf **Weiter**, um fortzufahren.



5. Geben Sie auf der Seite **IPv4-Einstellungen** die **IP-Adresse** und **Subnetzmaske** ein und geben Sie eine neue Gateway-IP-Adresse an (nur falls erforderlich). Klicken Sie auf **Weiter**, um fortzufahren.



6. Überprüfen Sie Ihre Auswahl auf der Seite **Bereit zum Abschließen** und klicken Sie auf **Fertig**, um den VMkernel-Adapter zu erstellen.



7. Wiederholen Sie diesen Vorgang, um einen VMkernel-Adapter für das zweite iSCSI-Netzwerk zu erstellen.

Bereitstellen und Verwenden von ONTAP Tools zum Konfigurieren von Speicher

Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VCF-Verwaltungsdomänencluster ausgeführt und umfassen die Bereitstellung von ONTAP -Tools, die Erstellung eines vVols iSCSI-Datenspeichers und die Migration von Verwaltungs-VMs in den neuen Datenspeicher.

Für VI-Workloaddomänen werden ONTAP Tools im VCF-Managementcluster installiert, aber beim vCenter registriert, das der VI-Workloaddomäne zugeordnet ist.

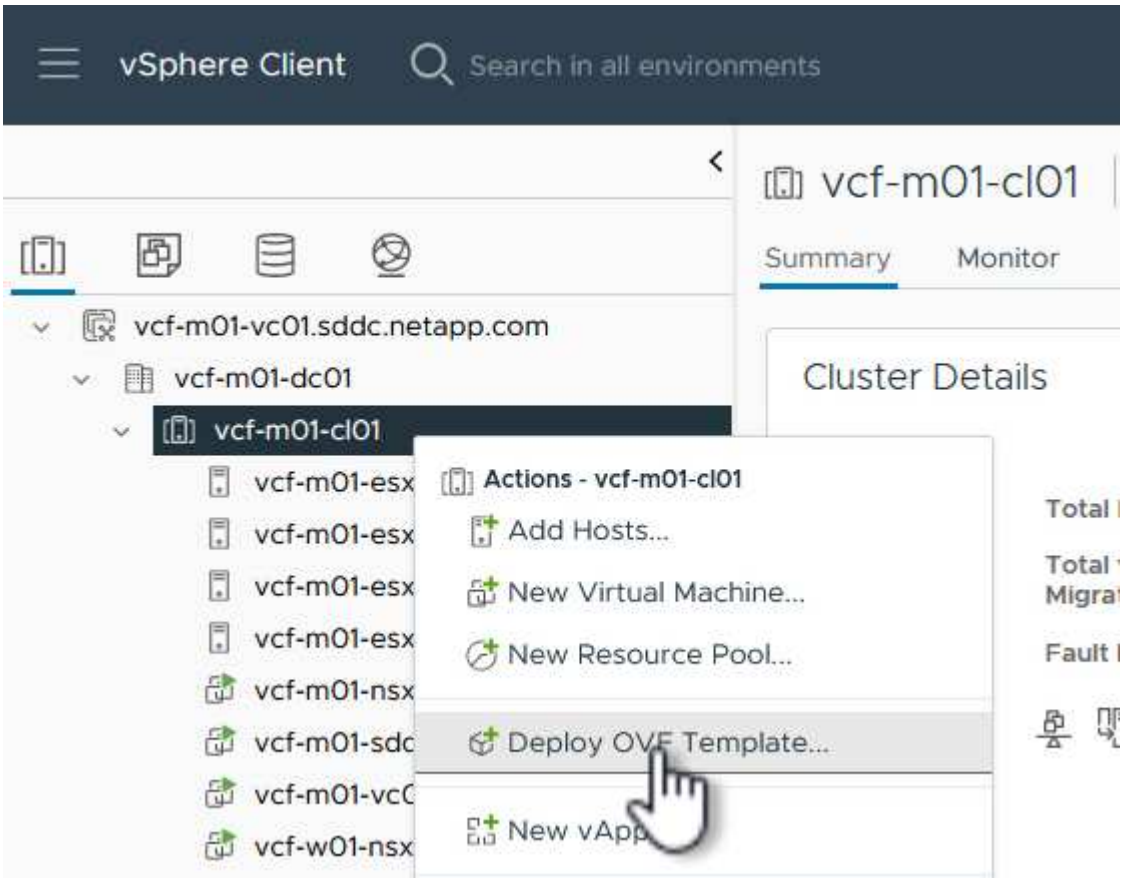
Weitere Informationen zur Bereitstellung und Verwendung von ONTAP Tools in einer Umgebung mit mehreren vCentern finden Sie unter"Voraussetzungen für die Registrierung von ONTAP Tools in einer Umgebung mit mehreren vCenter-Servern" .

Bereitstellen von ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere werden als VM-Appliance bereitgestellt und bieten eine integrierte vCenter-Benutzeroberfläche zur Verwaltung des ONTAP Speichers.

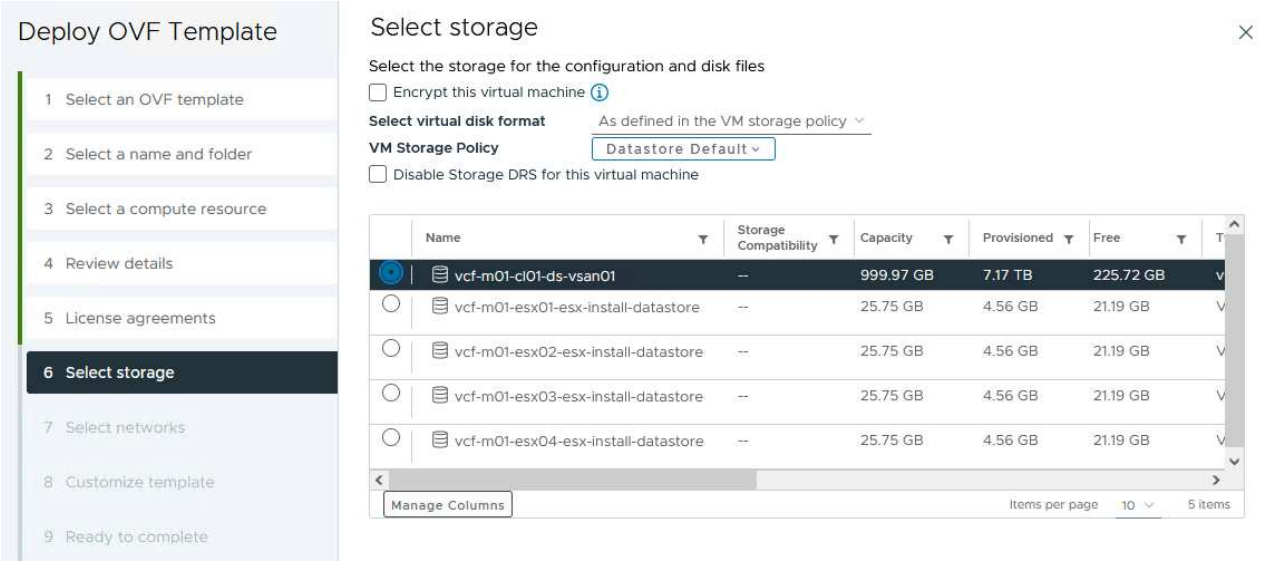
Führen Sie die folgenden Schritte aus, um ONTAP tools for VMware vSphere bereitzustellen:

1. Besorgen Sie sich das OVA-Image der ONTAP -Tools von der"NetApp Support-Site" und in einen lokalen Ordner herunterladen.
2. Melden Sie sich bei der vCenter-Appliance für die VCF-Verwaltungsdomäne an.
3. Klicken Sie in der vCenter-Appliance-Schnittstelle mit der rechten Maustaste auf den Verwaltungscluster und wählen Sie **OVF-Vorlage bereitstellen…**

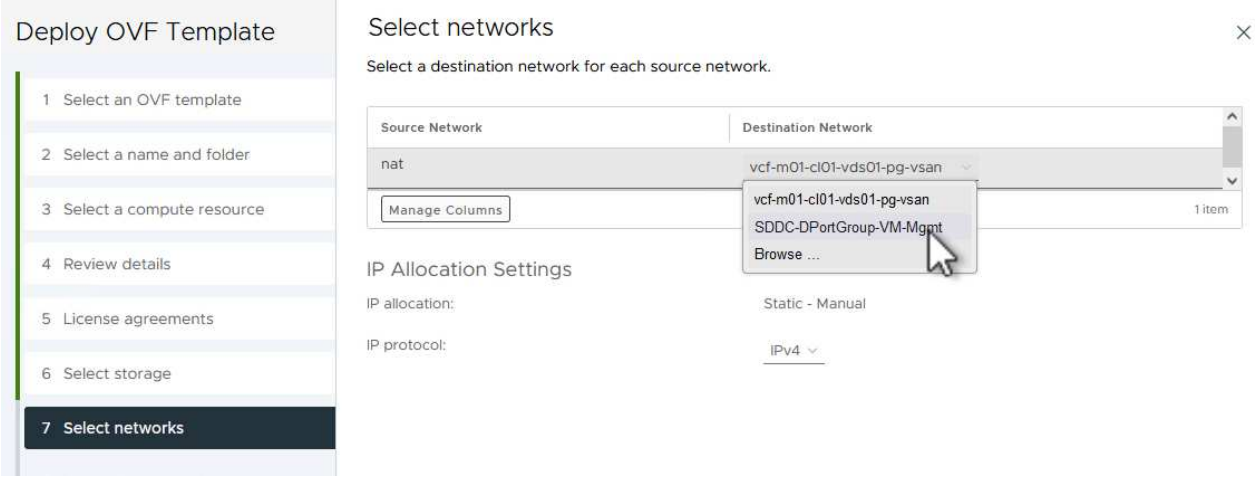


4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei der ONTAP -Tools aus.

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und einen Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie als Speicherort der Konfigurations- und Datenträgerdateien den vSAN-Datenspeicher des VCF-Managementdomänenclusters aus.

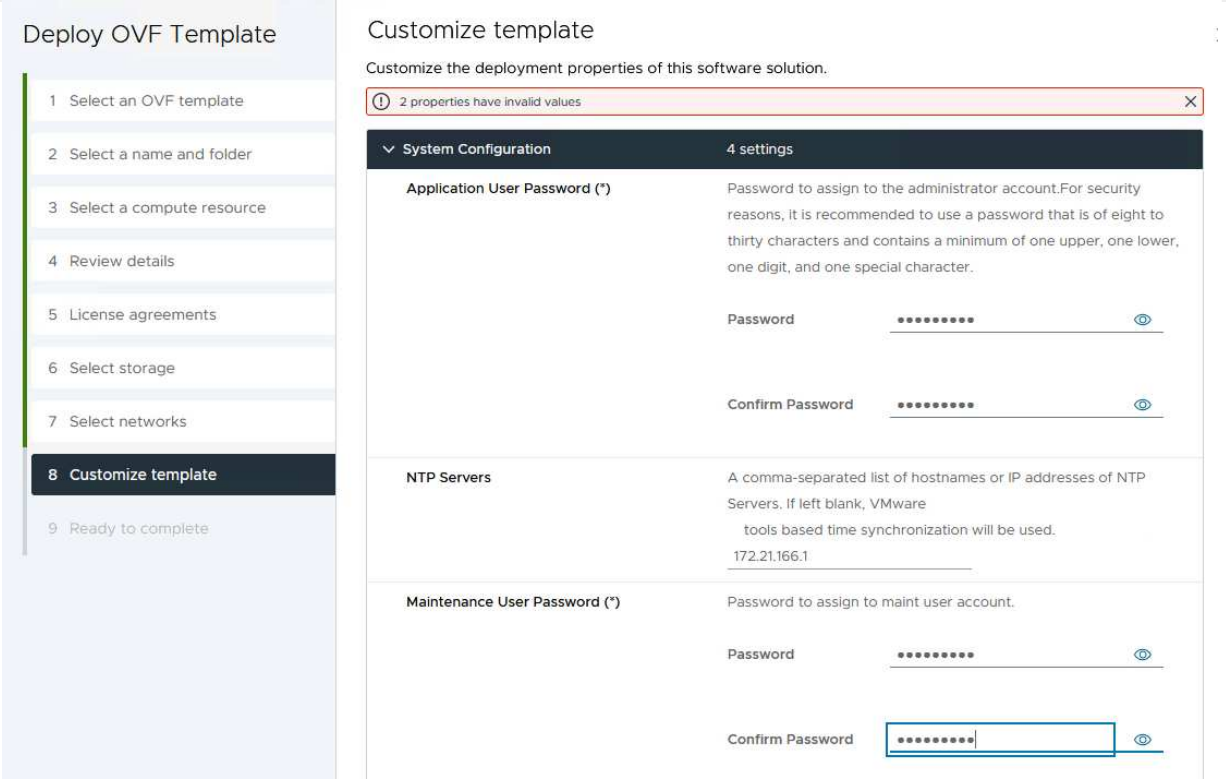


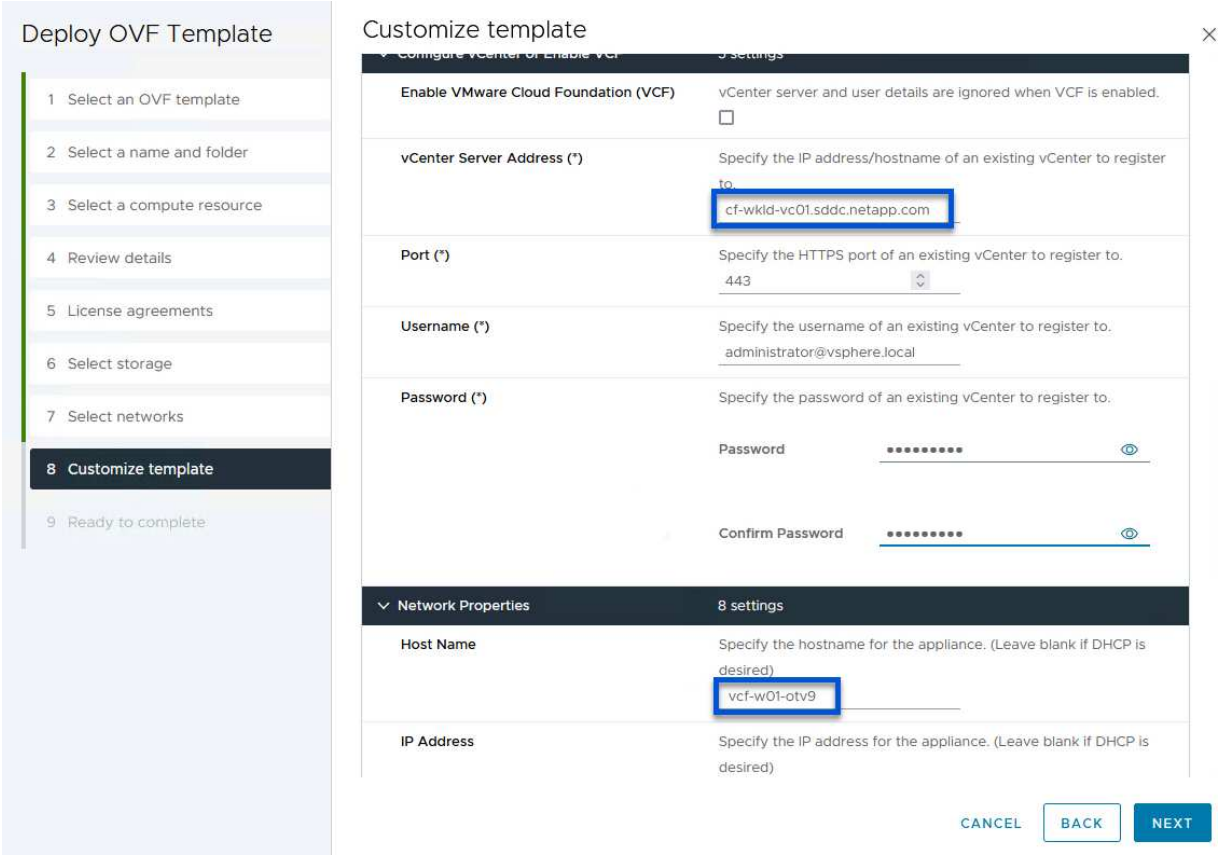
7. Wählen Sie auf der Seite „Netzwerk auswählen“ das für den Verwaltungsverkehr verwendete Netzwerk aus.



8. Geben Sie auf der Seite „Vorlage anpassen“ alle erforderlichen Informationen ein:
   - Für den Administratorzugriff auf ONTAP Tools zu verwendendes Kennwort.
   - IP-Adresse des NTP-Servers.
   - Kennwort für das ONTAP Tools-Wartungskonto.
   - ONTAP Tools Derby DB-Passwort.
   - Aktivieren Sie das Kontrollkästchen **VMware Cloud Foundation (VCF) aktivieren** nicht. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
   - FQDN oder IP-Adresse der vCenter-Appliance für die **VI-Workload-Domäne**
   - Anmeldeinformationen für die vCenter-Appliance der **VI Workload Domain**
   - Geben Sie die erforderlichen Felder für die Netzwerkeigenschaften an.

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

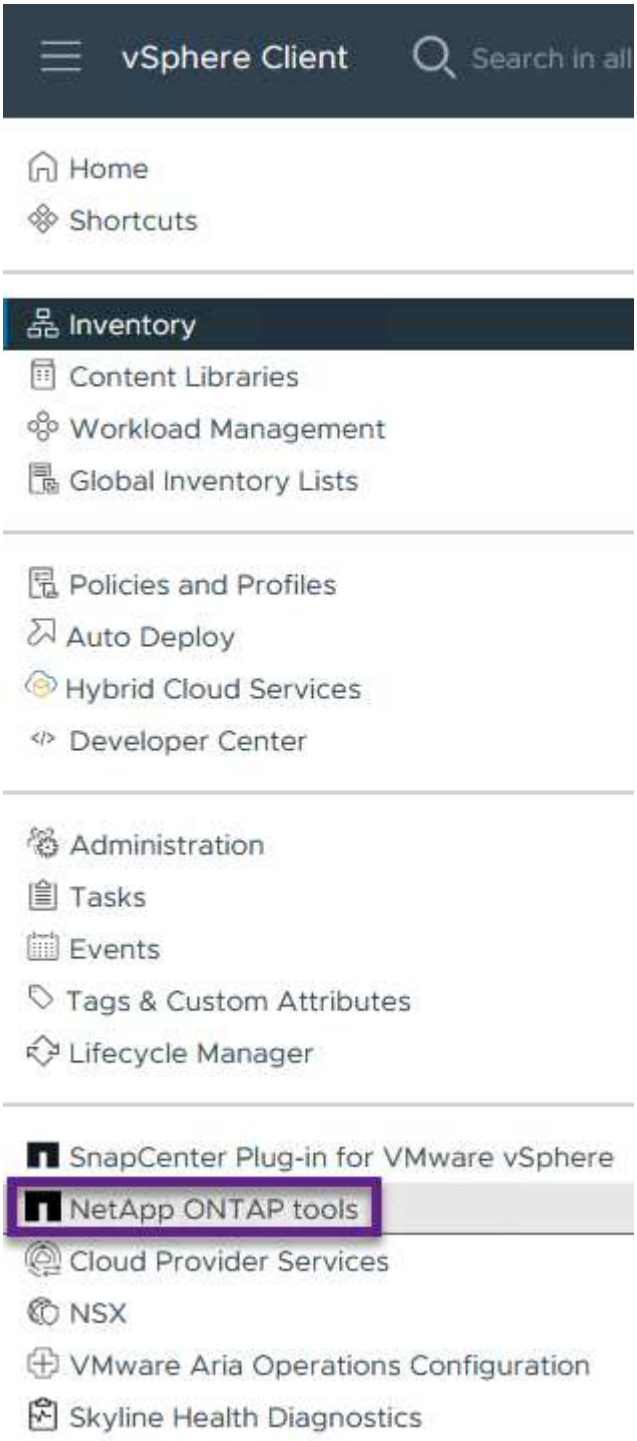




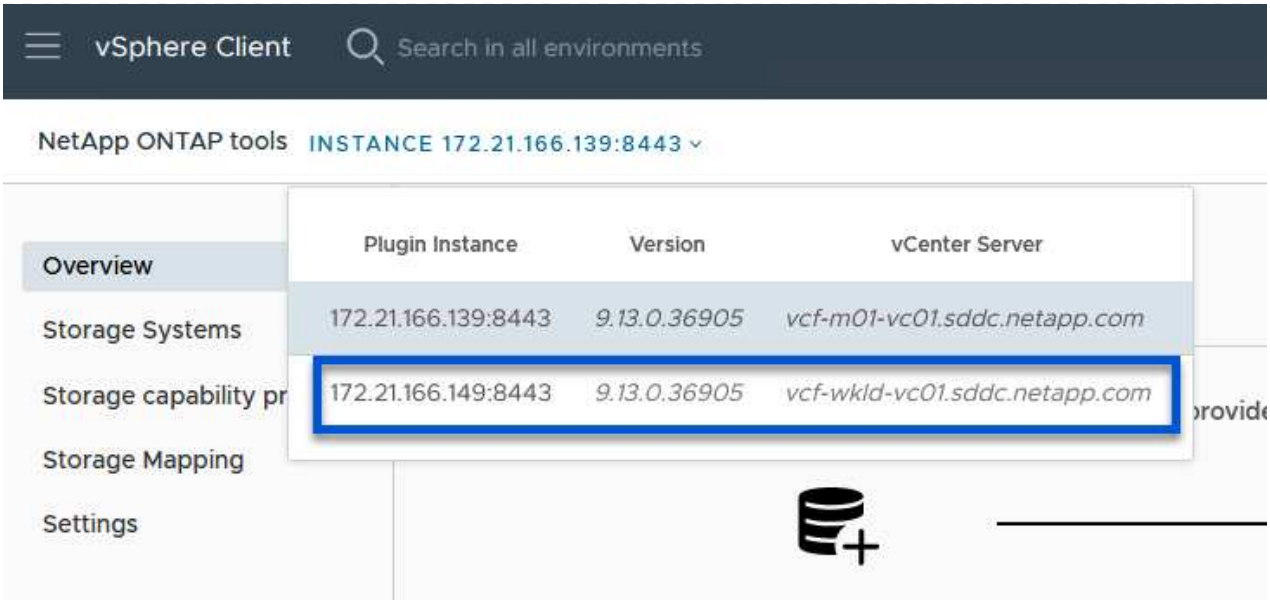
9. Überprüfen Sie alle Informationen auf der Seite „Bereit zum Abschließen“ und klicken Sie auf „Fertig stellen“, um mit der Bereitstellung der ONTAP Tools-Appliance zu beginnen.

Fügen Sie ONTAP Tools ein Speichersystem hinzu.

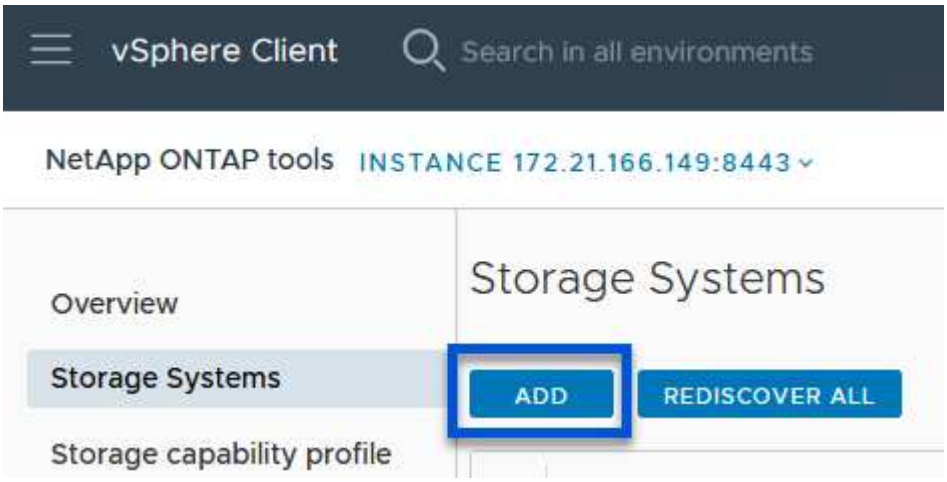
1. Greifen Sie auf NetApp ONTAP Tools zu, indem Sie es im Hauptmenü des vSphere-Clients auswählen.



2. Wählen Sie aus dem Dropdown-Menü **INSTANZ** in der ONTAP Tool-Schnittstelle die ONTAP Tools-Instanz aus, die der zu verwaltenden Workload-Domäne zugeordnet ist.

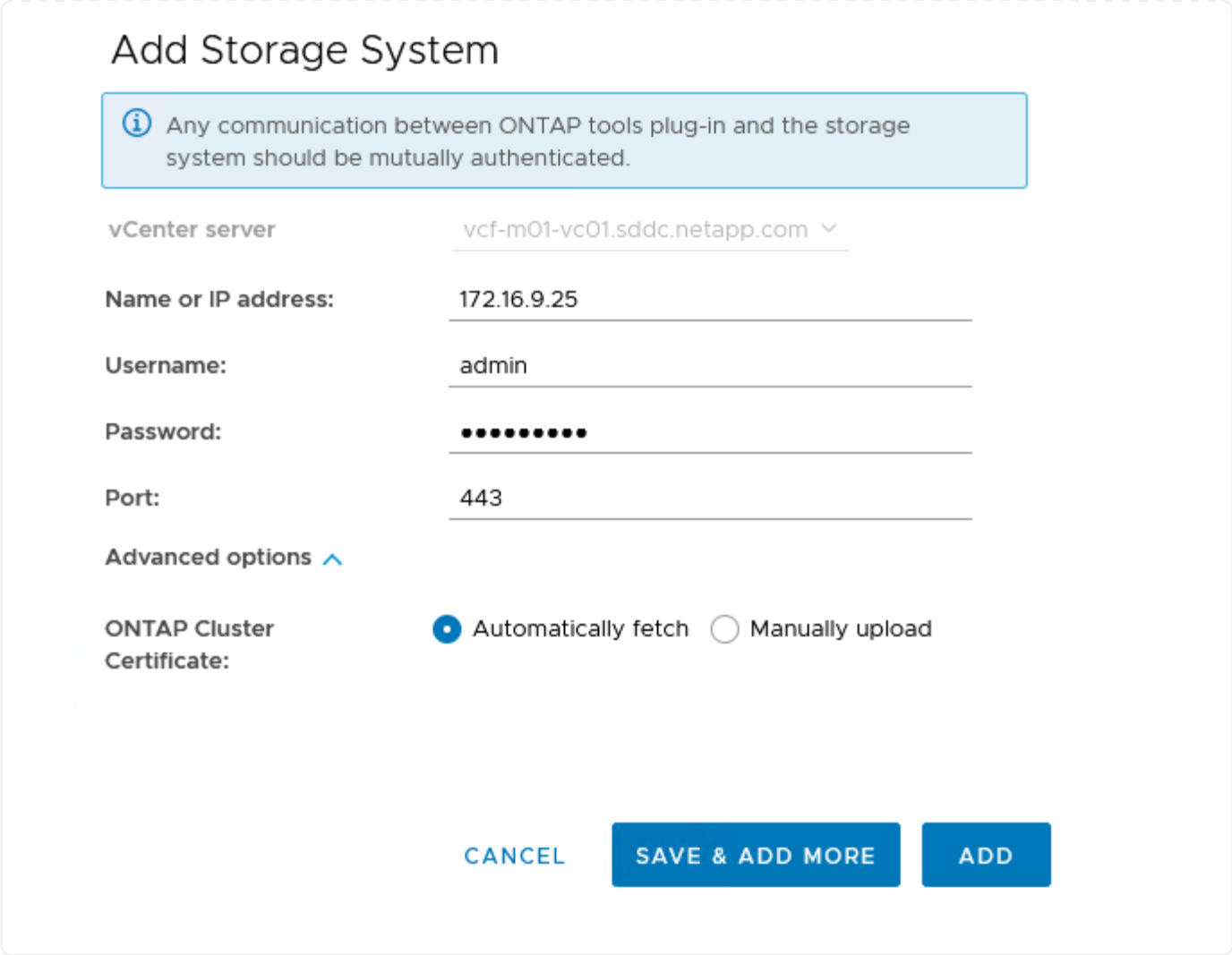


3. Wählen Sie in ONTAP Tools im linken Menü **Storage Systems** aus und drücken Sie dann **Add**.



4. Geben Sie die IP-Adresse, die Anmeldeinformationen des Speichersystems und die Portnummer ein. Klicken Sie auf **Hinzufügen**, um den Erkennungsprozess zu starten.

> vVol erfordert ONTAP Cluster-Anmeldeinformationen anstelle von SVM-Anmeldeinformationen. Weitere Informationen finden Sie unter "Speichersysteme hinzufügen" In der ONTAP Tools-Dokumentation.

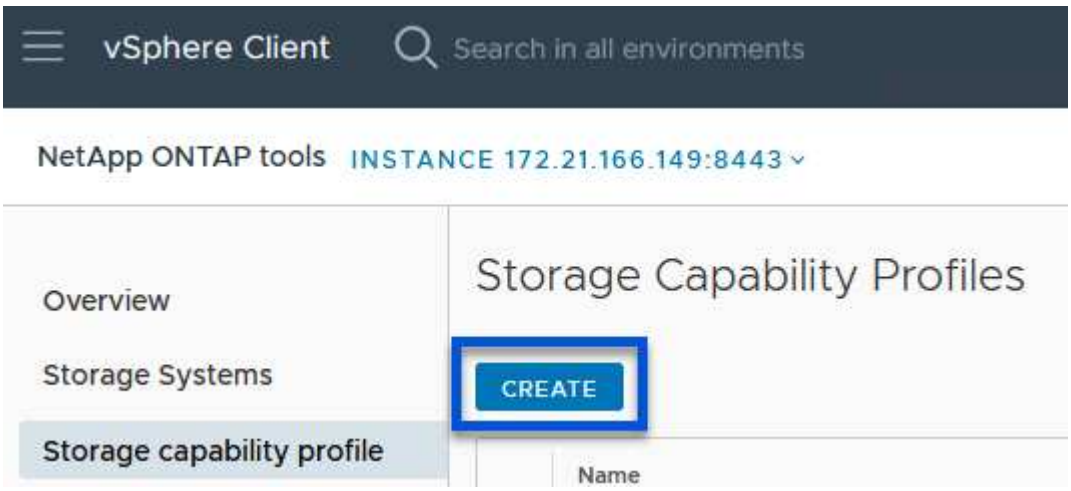

Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Erstellen Sie ein Speicherkapazitätsprofil in ONTAP Tools

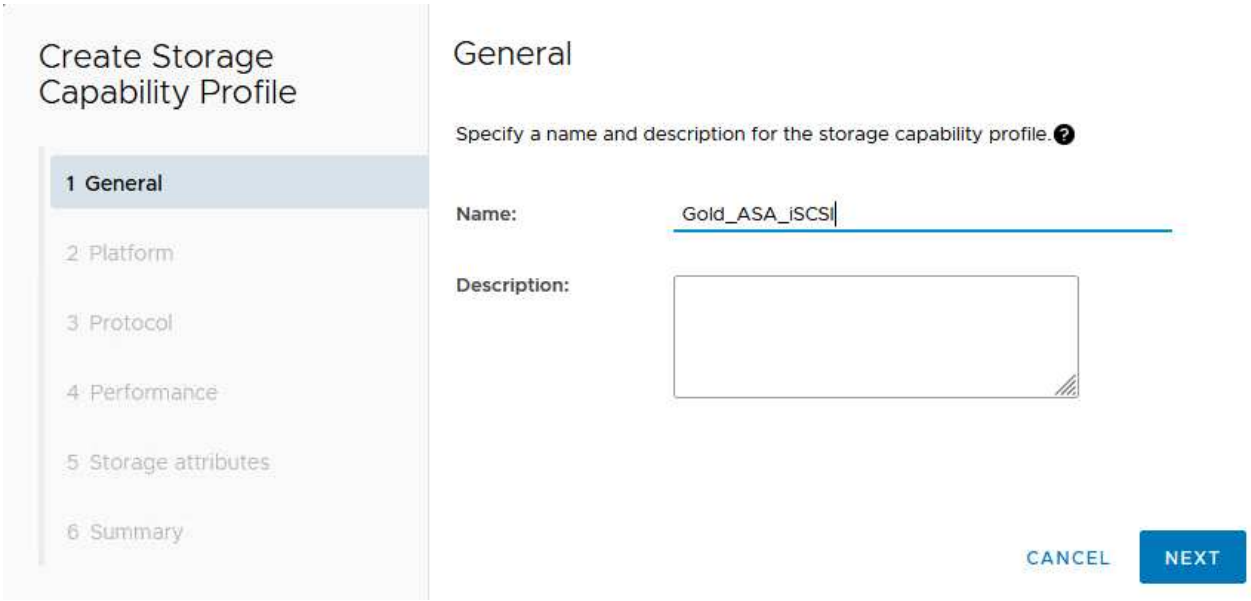
Speicherleistungsprofile beschreiben die Funktionen, die ein Speicherarray oder Speichersystem bietet. Sie enthalten Definitionen der Dienstqualität und werden zur Auswahl von Speichersystemen verwendet, die die im Profil definierten Parameter erfüllen. Es kann eines der bereitgestellten Profile verwendet oder es können neue erstellt werden.

Führen Sie die folgenden Schritte aus, um in ONTAP Tools ein Speicherkapazitätsprofil zu erstellen:

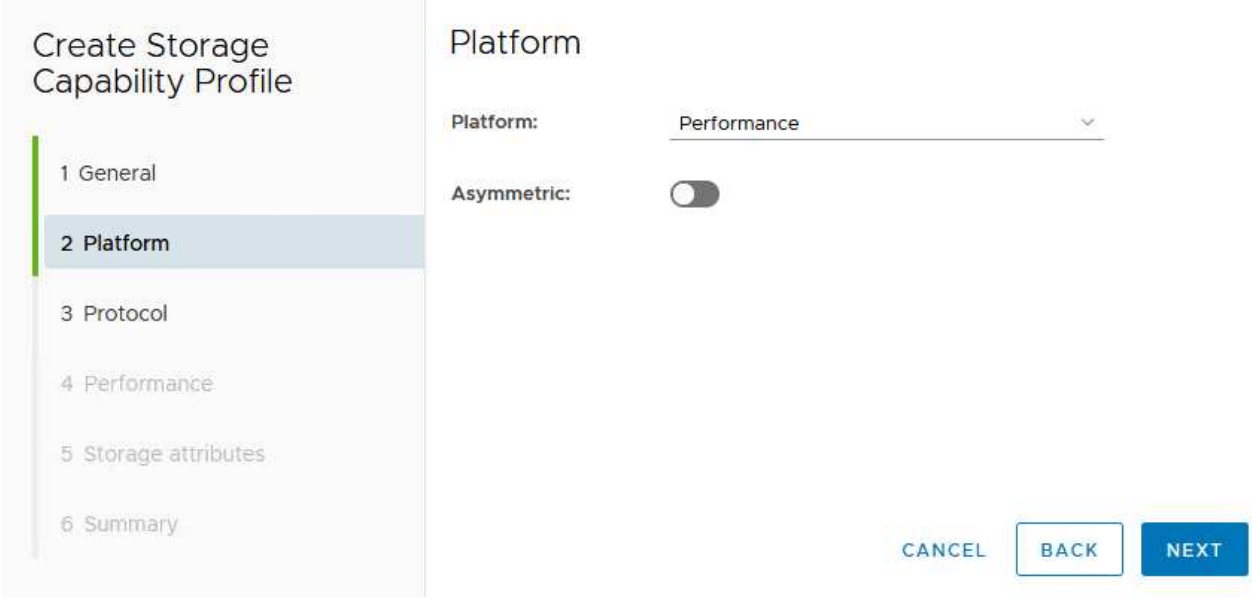
1. Wählen Sie in ONTAP Tools im linken Menü **Storage Capability Profile** aus und drücken Sie dann **Create**.



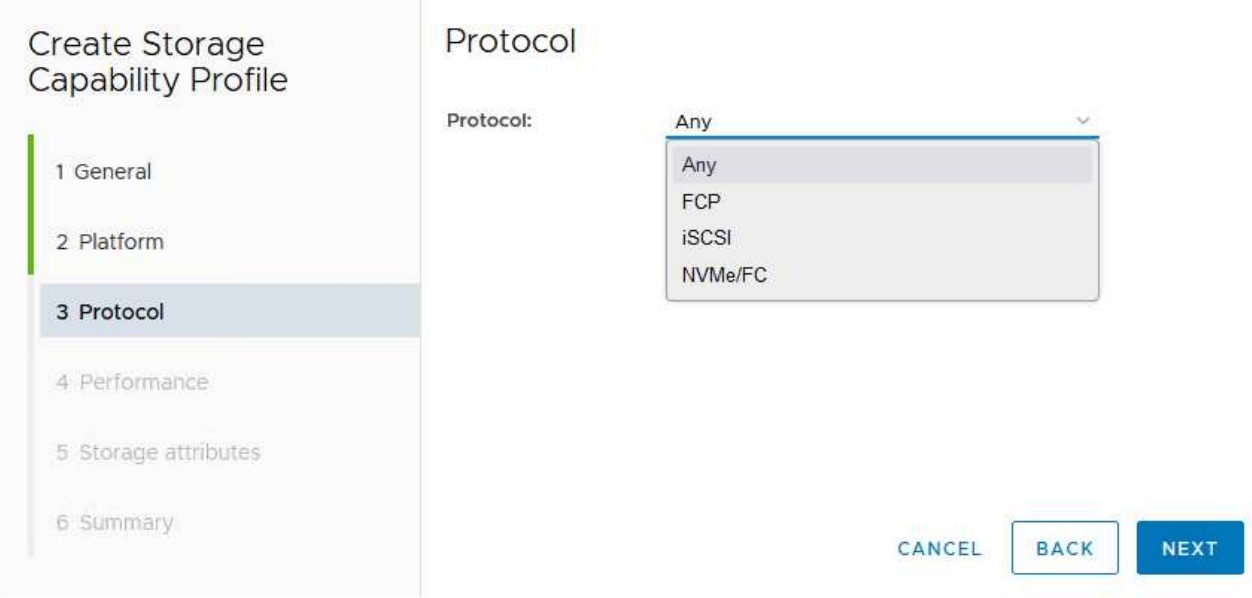
2. Geben Sie im Assistenten **Speicherkapazitätsprofil erstellen** einen Namen und eine Beschreibung des Profils ein und klicken Sie auf **Weiter**.



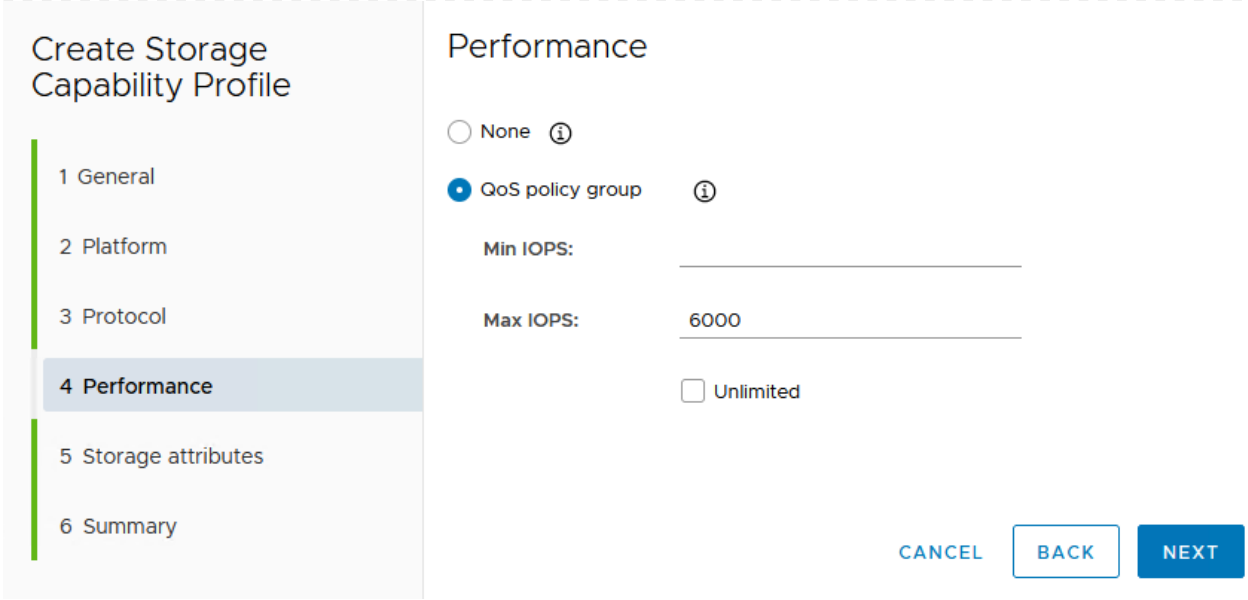
3. Wählen Sie den Plattformtyp aus und legen Sie **Asymmetrisch** auf „Falsch“ fest, um anzugeben, dass das Speichersystem ein All-Flash-SAN-Array sein soll.



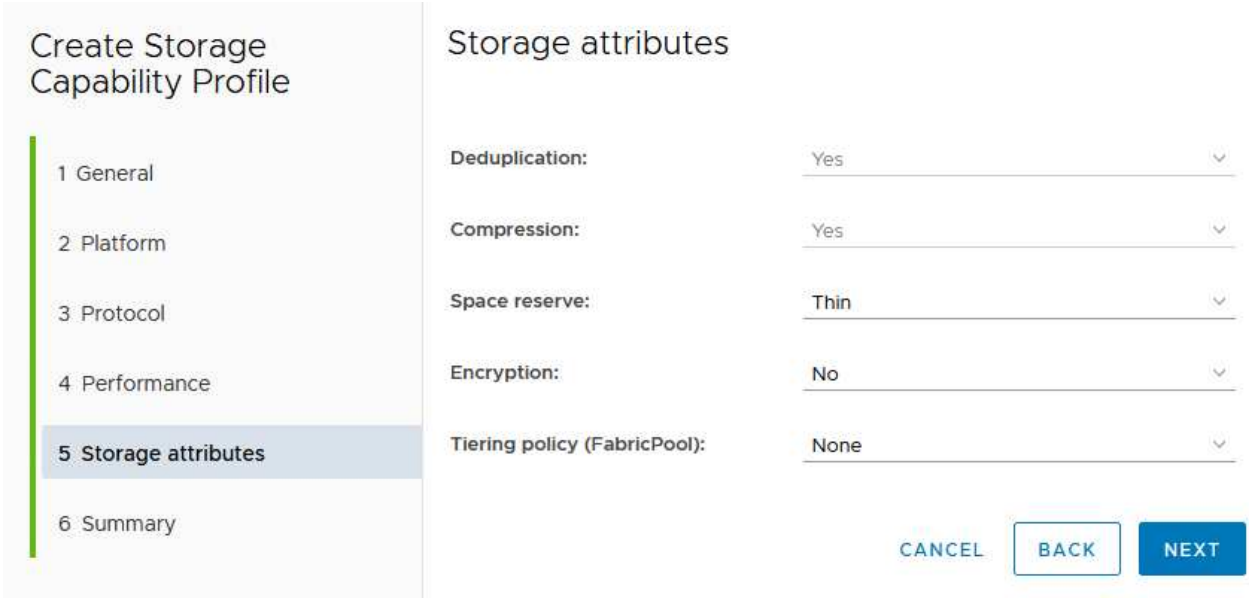
4. Wählen Sie als Nächstes die gewünschte Protokollauswahl oder **Beliebig**, um alle möglichen Protokolle zuzulassen. Klicken Sie auf **Weiter**, um fortzufahren.



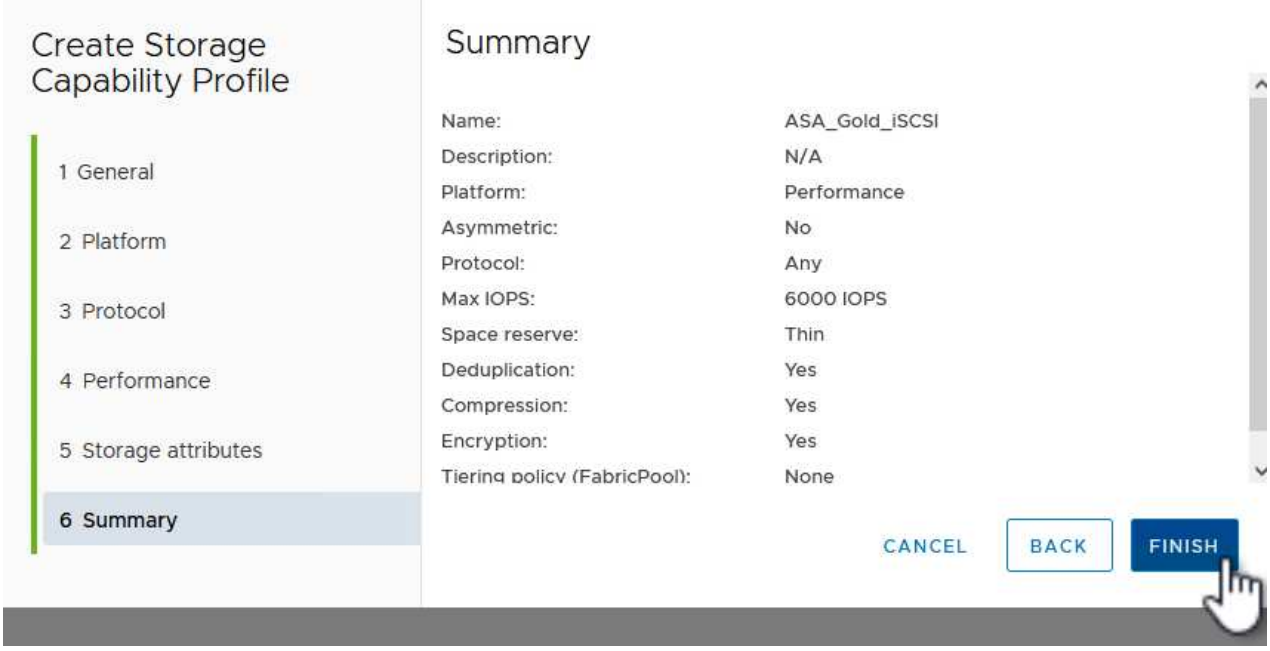
5. Auf der Seite **Leistung** können Sie die Dienstqualität in Form der zulässigen Mindest- und Höchst-IOPs einstellen.



6. Füllen Sie die Seite **Speicherattribute** aus und wählen Sie bei Bedarf Speichereffizienz, Speicherplatzreservierung, Verschlüsselung und Tiering-Richtlinien aus.



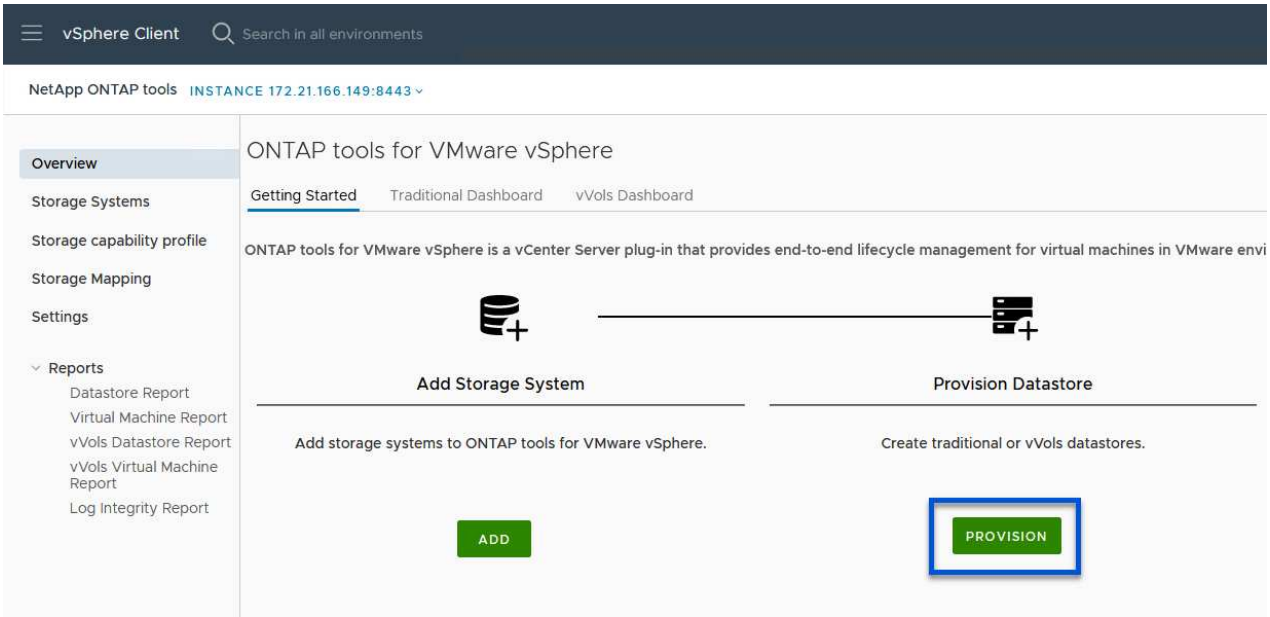
7. Überprüfen Sie abschließend die Zusammenfassung und klicken Sie auf „Fertig“, um das Profil zu erstellen.


Create Storage Capability Profile
1 General
2 Platform
3 Protocol
4 Performance
5 Storage attributes
6 Summary
Summary
Name: ASA_Gold_iSCSI
Description: N/A
Platform: Performance
Asymmetric: No
Protocol: Any
Max IOPS: 6000 IOPS
Space reserve: Thin
Deduplication: Yes
Compression: Yes
Encryption: Yes
Tiering policy (FabricPool): None
CANCEL
BACK
FINISH

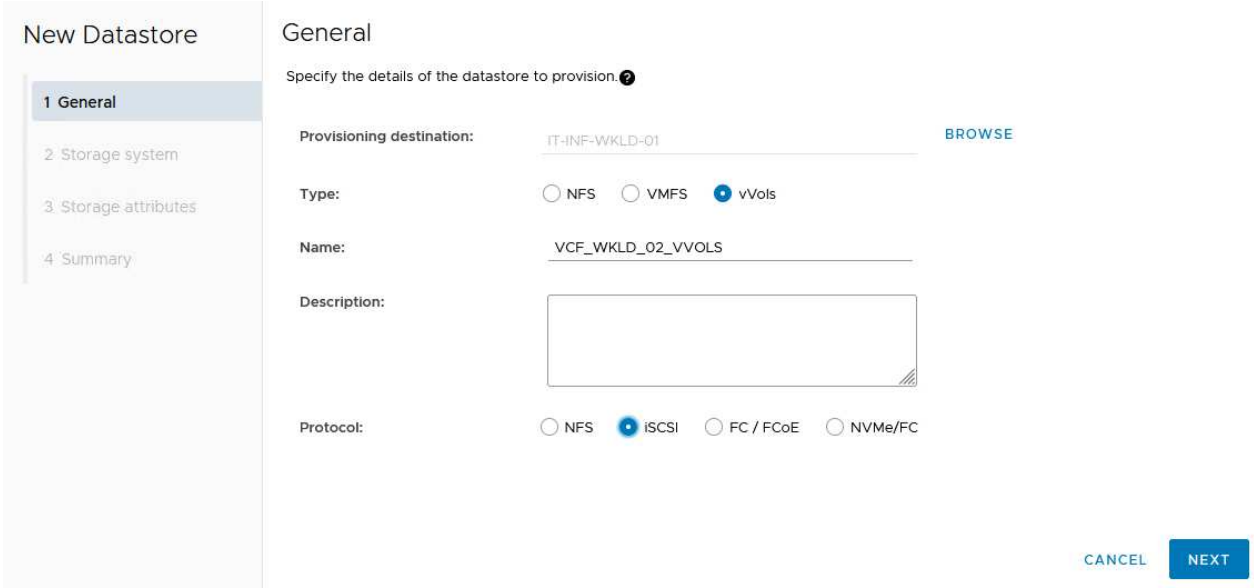
Erstellen Sie einen vVols Datenspeicher in ONTAP Tools

Führen Sie die folgenden Schritte aus, um einen vVols Datenspeicher in ONTAP Tools zu erstellen:

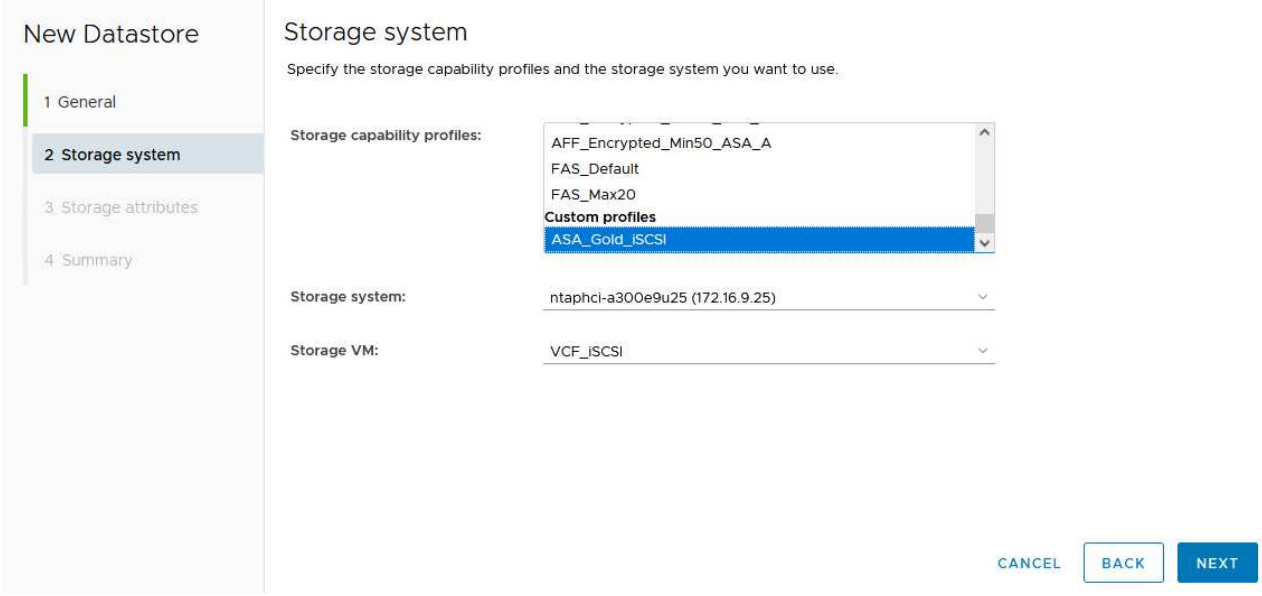
1. Wählen Sie in ONTAP Tools **Übersicht** und klicken Sie auf der Registerkarte **Erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.



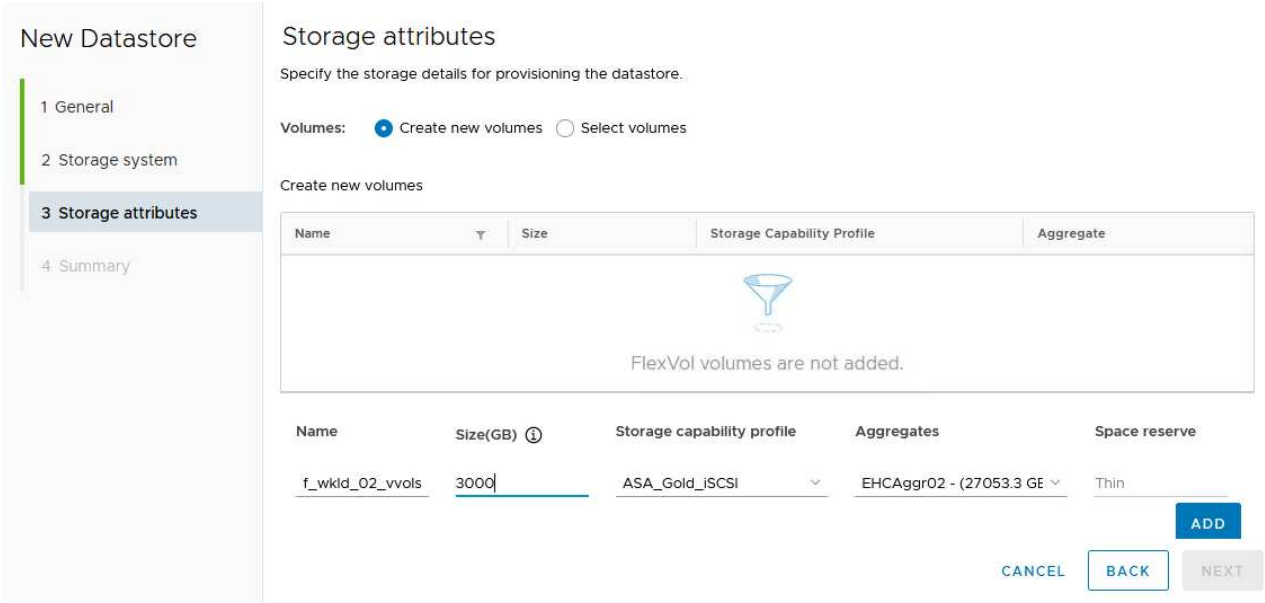
2. Wählen Sie auf der Seite **Allgemein** des Assistenten „Neuer Datenspeicher“ das vSphere-Rechenzentrum oder Clusterziel aus. Wählen Sie * vVols* als Datenspeichertyp, geben Sie einen Namen für den Datenspeicher ein und wählen Sie * iSCSI * als Protokoll. Klicken Sie auf **Weiter**, um fortzufahren.



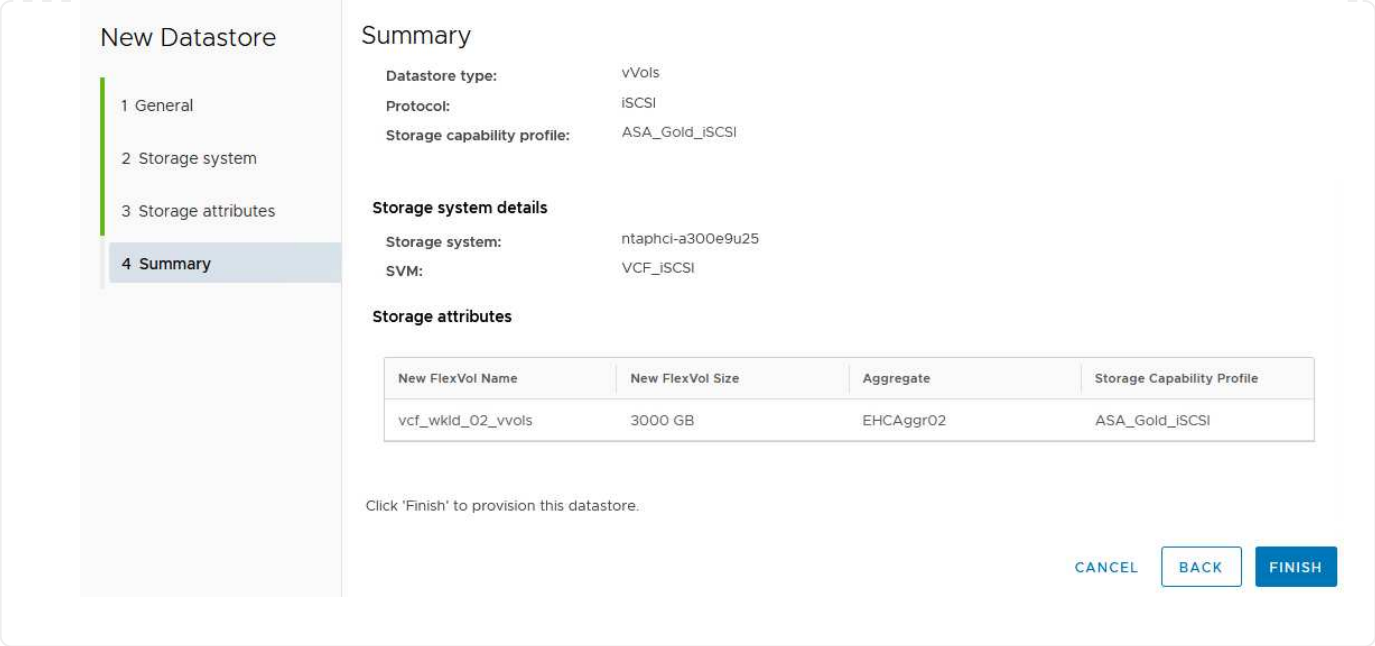
3. Wählen Sie auf der Seite **Speichersystem** ein Speicherfähigkeitsprofil, das Speichersystem und SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.



4. Wählen Sie auf der Seite **Speicherattribute** die Erstellung eines neuen Volumes für den Datenspeicher aus und füllen Sie die Speicherattribute des zu erstellenden Volumes aus. Klicken Sie auf **Hinzufügen**, um das Volume zu erstellen, und dann auf **Weiter**, um fortzufahren.



5. Überprüfen Sie abschließend die Zusammenfassung und klicken Sie auf **Fertig**, um den Erstellungsprozess des vVol-Datenspeichers zu starten.



Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Fügen Sie mithilfe von ONTAP tools for VMware vSphere NFS und vVols als zusätzlichen Speicher zu VI-Workload-Domänen hinzu

In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung von ONTAP Tools für VMware zum Hinzufügen von NFS- und vVols Datenspeichern als zusätzlichen Speicher für eine Workload-Domäne der VMware Cloud Foundation (VCF) Virtual Infrastructure (VI). Dieses Verfahren fasst die Bereitstellung von ONTAP Tools für VMware vSphere, die Konfiguration einer Storage Virtual Machine (SVM) mit logischen NFS-Schnittstellen und die Bereitstellung von NFS- und vVols Datenspeichern zusammen.

NFS wird als Speicherprotokoll für den vVols Datenspeicher verwendet.

Vorteile von NFS

Einfachheit und Benutzerfreundlichkeit: NFS lässt sich unkompliziert einrichten und verwalten und ist daher eine ausgezeichnete Wahl für Umgebungen, in denen eine schnelle und einfache Dateifreigabe erforderlich ist.

Skalierbarkeit: Die Architektur von ONTAP ermöglicht eine effiziente Skalierung von NFS und unterstützt wachsende Datenanforderungen ohne wesentliche Änderungen an der Infrastruktur.

Flexibilität: NFS unterstützt eine breite Palette von Anwendungen und Workloads und ist daher vielseitig für verschiedene Anwendungsfälle geeignet, einschließlich virtualisierter Umgebungen.

Weitere Informationen finden Sie im "NFS v3-Referenzhandbuch für vSphere 8" .

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Erstellen Sie eine Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für NFS-Verkehr.
- Erstellen Sie eine verteilte Portgruppe für das NFS-Netzwerk in der VI-Workloaddomäne.
- Erstellen Sie einen VMkernel-Adapter für NFS auf den ESXi-Hosts für die VI-Workloaddomäne.
- Stellen Sie ONTAP Tools in der VI-Workloaddomäne bereit.
- Erstellen Sie einen neuen NFS-Datenspeicher in der VI-Workloaddomäne.
- Erstellen Sie einen neuen vVols Datenspeicher in der VI-Workloaddomäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF oder FAS Speichersystem mit physischen Datenports auf Ethernet-Switches, die für den Speicherverkehr vorgesehen sind.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf den vSphere-Client kann zugegriffen werden.
- Zuvor wurde eine VI-Workloaddomäne bereitgestellt.

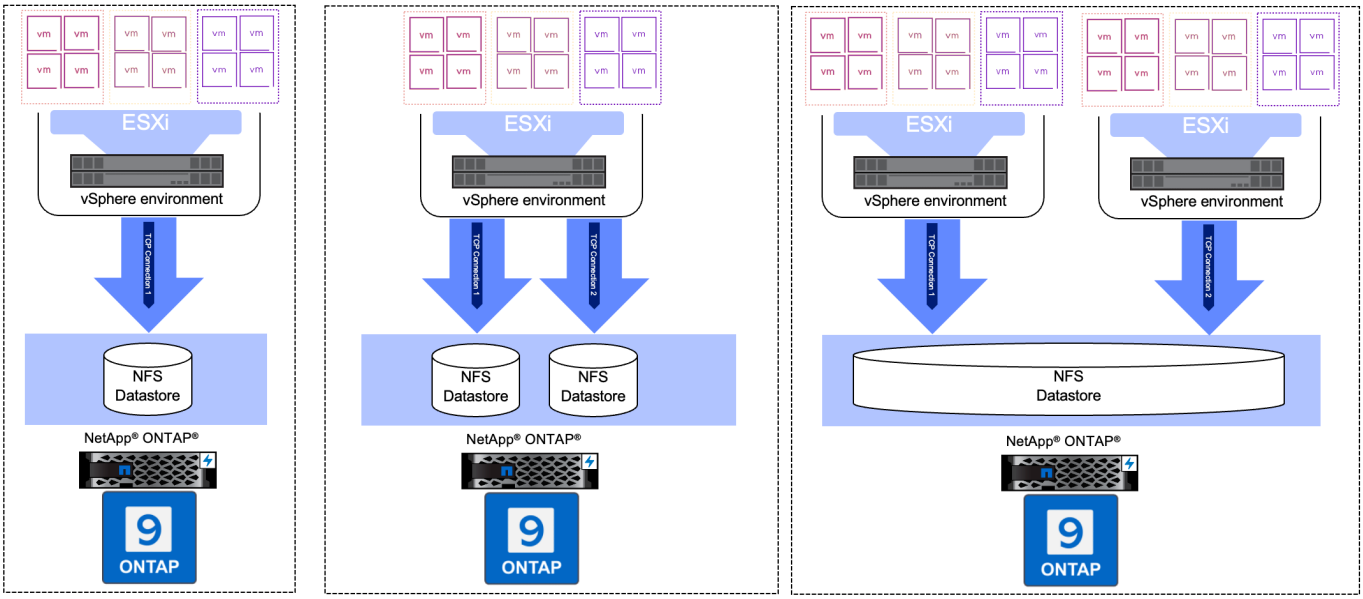
NetApp empfiehlt redundante Netzwerkdesigns für NFS, die Fehlertoleranz für Speichersysteme, Switches, Netzwerkadapter und Hostsysteme bieten. Es ist üblich, NFS je nach den Architekturanforderungen mit einem einzelnen Subnetz oder mehreren Subnetzen bereitzustellen.

Siehe "Best Practices für die Ausführung von NFS mit VMware vSphere" für ausführliche Informationen speziell zu VMware vSphere.

Netzwerkhinweise zur Verwendung von ONTAP mit VMware vSphere finden Sie im "Netzwerkkonfiguration – NFS" Abschnitt der Dokumentation zu NetApp -Unternehmensanwendungen.

Diese Dokumentation veranschaulicht den Vorgang zum Erstellen einer neuen SVM und zum Angeben der IP-Adressinformationen zum Erstellen mehrerer LIFs für NFS-Verkehr. Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie unter"Erstellen Sie eine LIF (Netzwerkschnittstelle)" .

Ausführliche Informationen zur Verwendung von NFS mit vSphere-Clustern finden Sie im"NFS v3-Referenzhandbuch für vSphere 8" .



Bereitstellungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und damit einen vVols und NFS-Datenspeicher in der VCF-Verwaltungsdomäne zu erstellen:

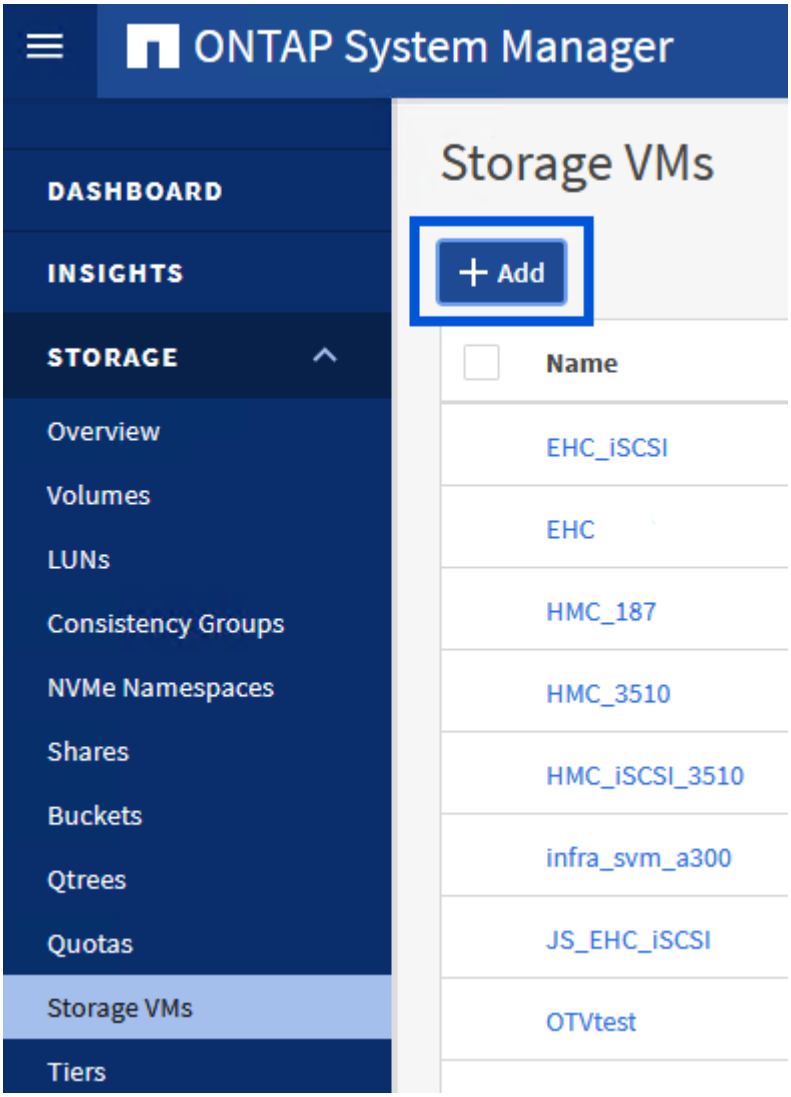
Erstellen Sie SVM und LIFs auf dem ONTAP Speichersystem

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

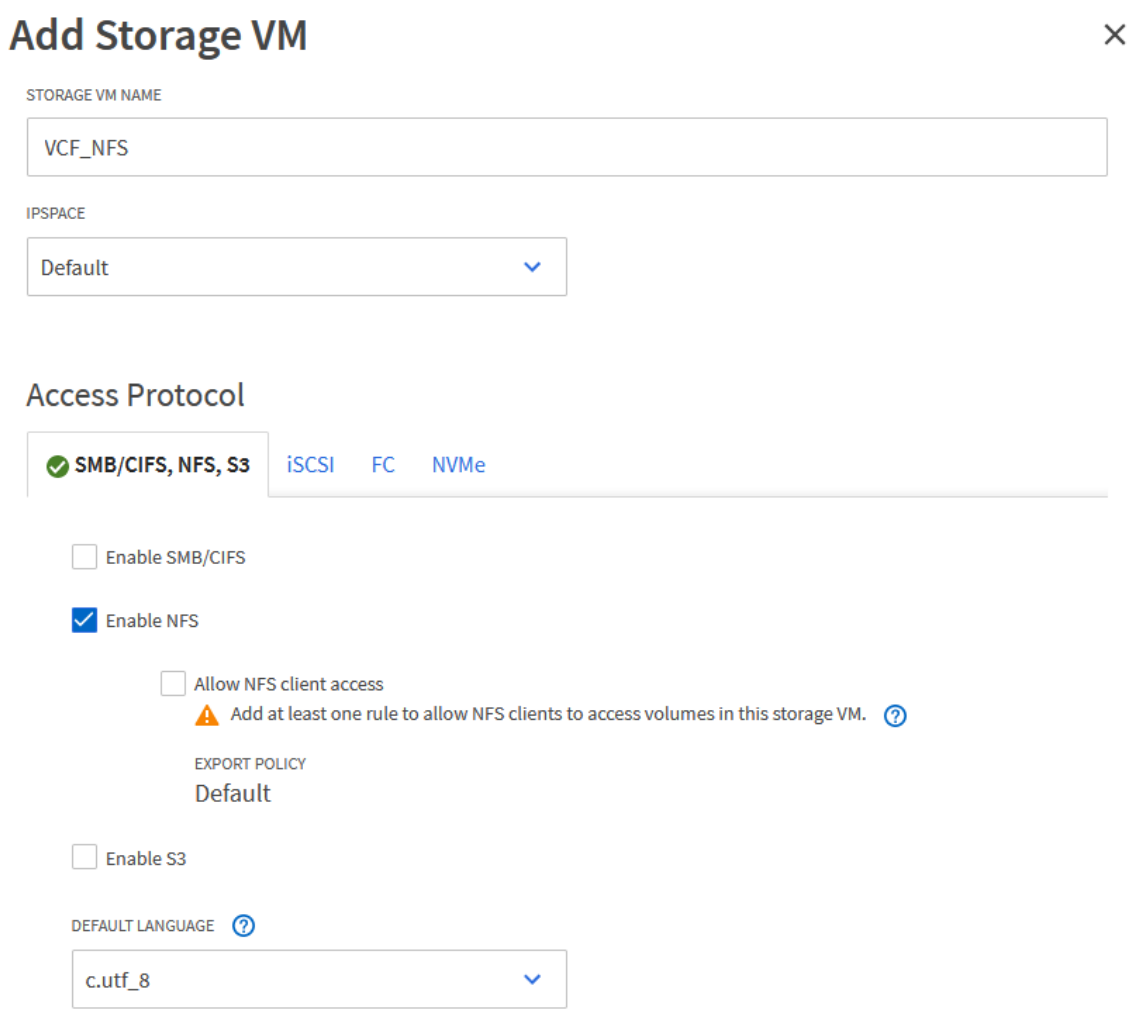
Erstellen der Speicher-VM und LIFs

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für NFS-Verkehr zu erstellen.

1. Navigieren Sie im ONTAP System Manager im linken Menü zu **Storage VMs** und klicken Sie zum Starten auf **+ Hinzufügen**.

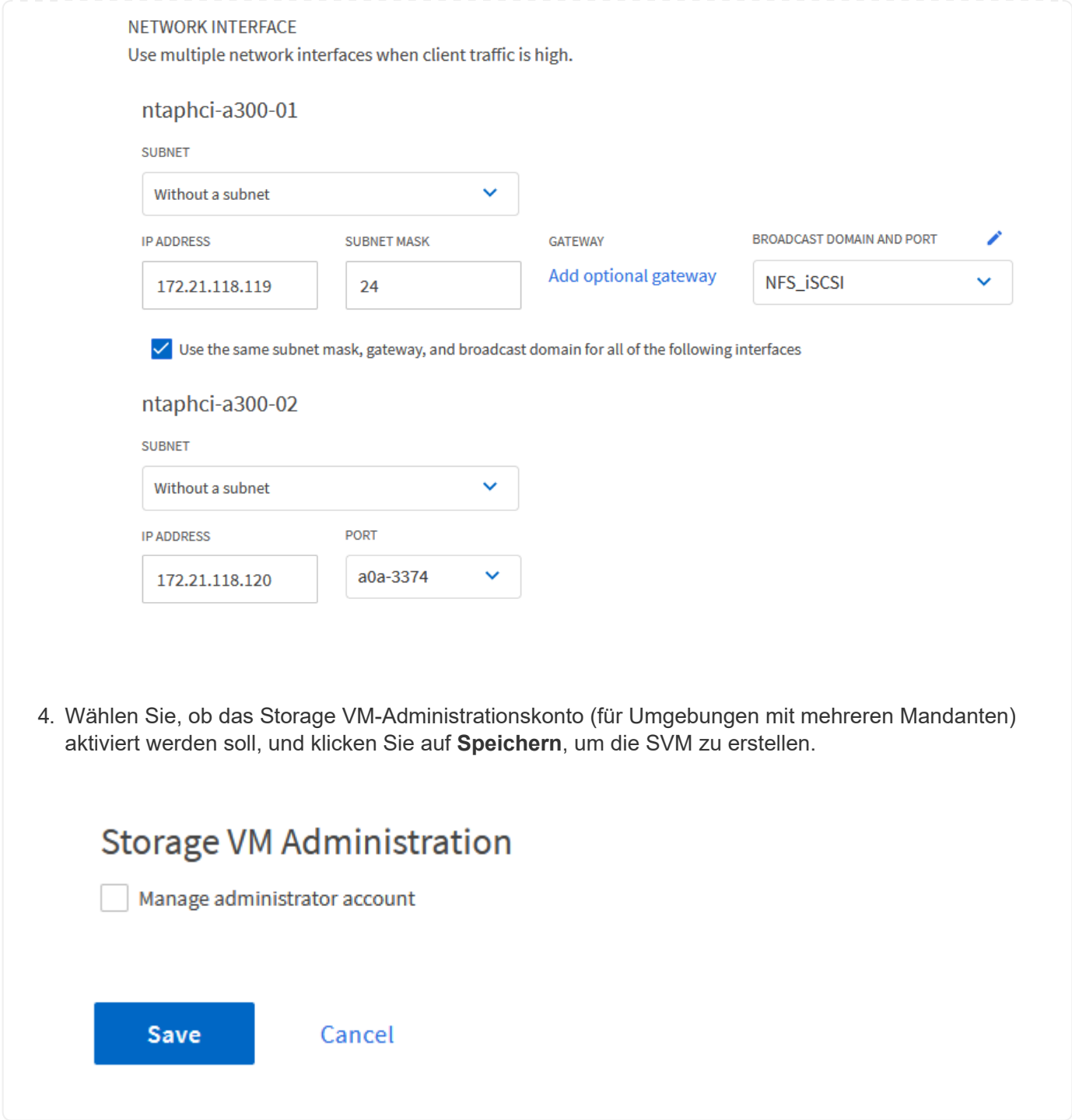


2. Geben Sie im Assistenten **Speicher-VM hinzufügen** einen **Namen** für die SVM ein, wählen Sie den **IP-Bereich** aus und klicken Sie dann unter **Zugriffsprotokoll** auf die Registerkarte **SMB/CIFS, NFS, S3** und aktivieren Sie das Kontrollkästchen **NFS aktivieren**.



Es ist nicht erforderlich, hier die Schaltfläche **NFS-Clientzugriff zulassen** zu aktivieren, da Ontap Tools für VMware vSphere zur Automatisierung des Datenspeicherbereitstellungsprozesses verwendet werden. Dazu gehört die Bereitstellung des Clientzugriffs für die ESXi-Hosts.

3. Geben Sie im Abschnitt **Netzwerkschnittstelle** die **IP-Adresse**, **Subnetzmaske** und **Broadcast-Domäne und -Port** für das erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert werden, um gemeinsame Einstellungen für alle verbleibenden LIFs oder separate Einstellungen zu verwenden.



4. Wählen Sie, ob das Storage VM-Administrationskonto (für Umgebungen mit mehreren Mandanten) aktiviert werden soll, und klicken Sie auf **Speichern**, um die SVM zu erstellen.

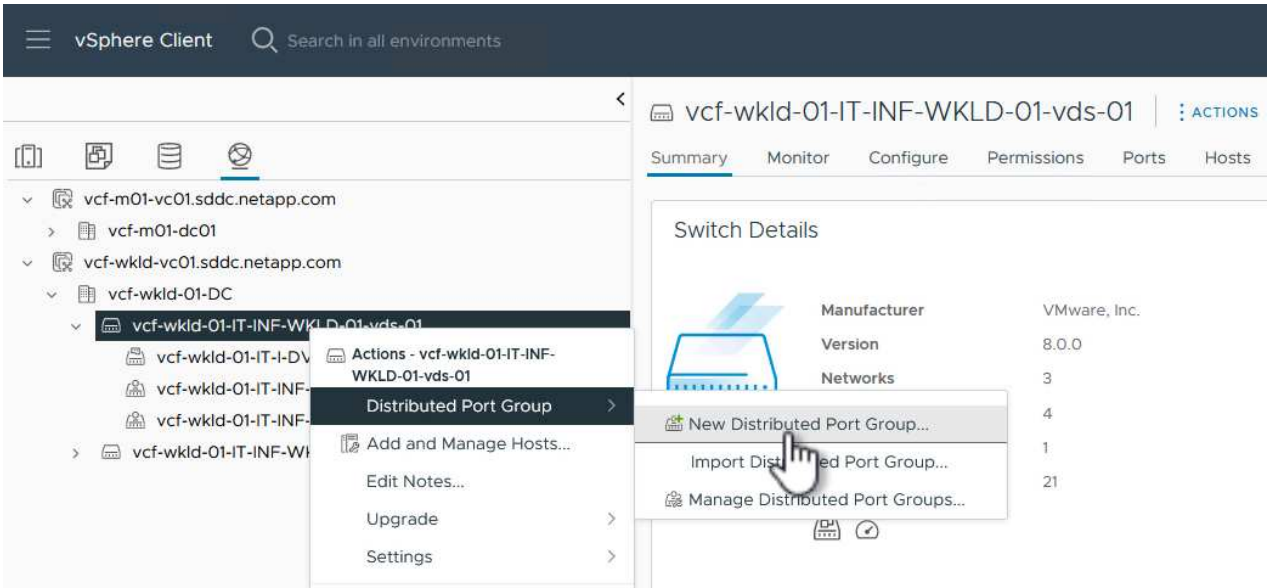
Einrichten des Netzwerks für NFS auf ESXi-Hosts

Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VI Workload Domain-Cluster ausgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client in allen Verwaltungs- und Workloaddomänen gleich ist.

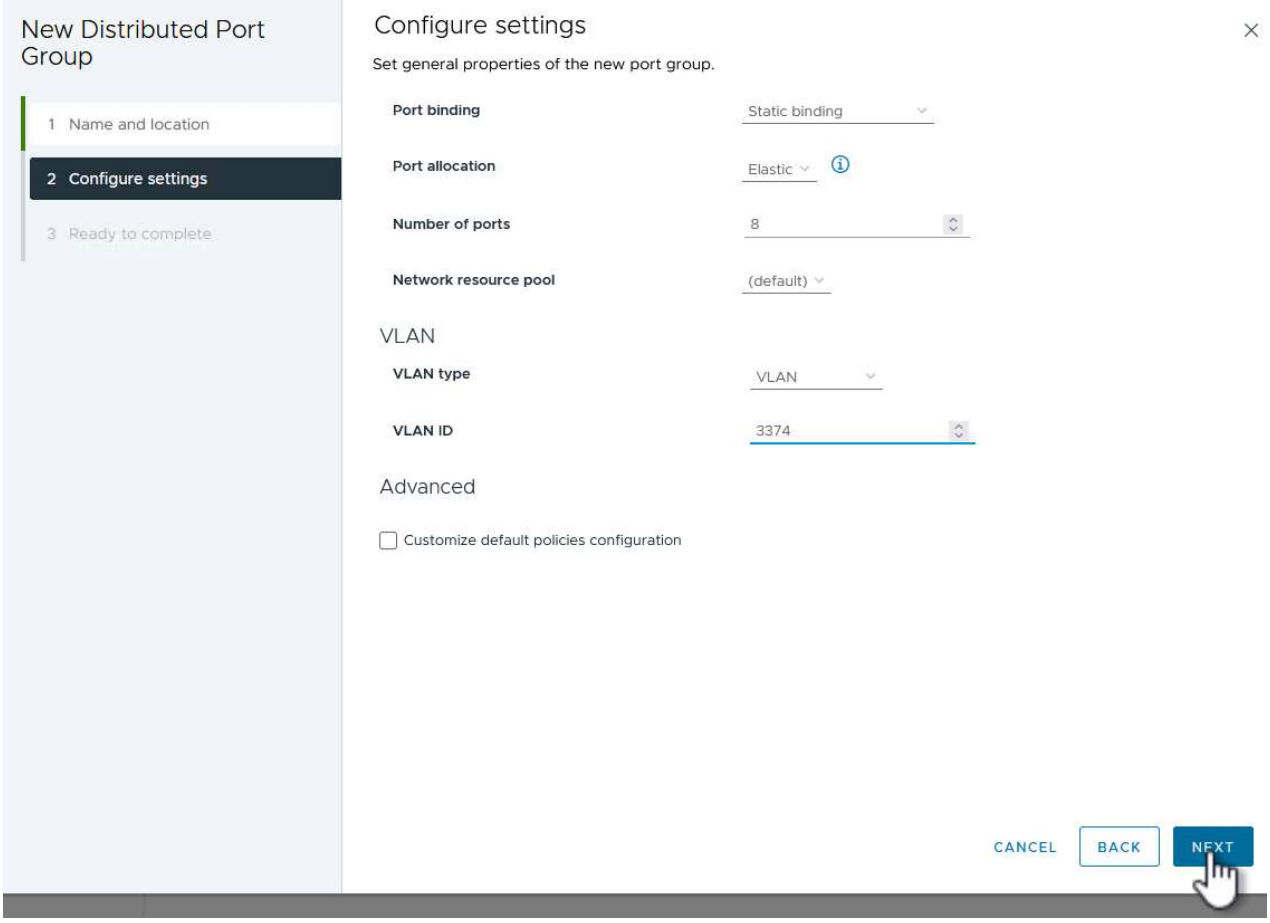
Erstellen Sie eine verteilte Portgruppe für NFS-Verkehr

Führen Sie die folgenden Schritte aus, um eine neue verteilte Portgruppe für das Netzwerk zur Übertragung von NFS-Verkehr zu erstellen:

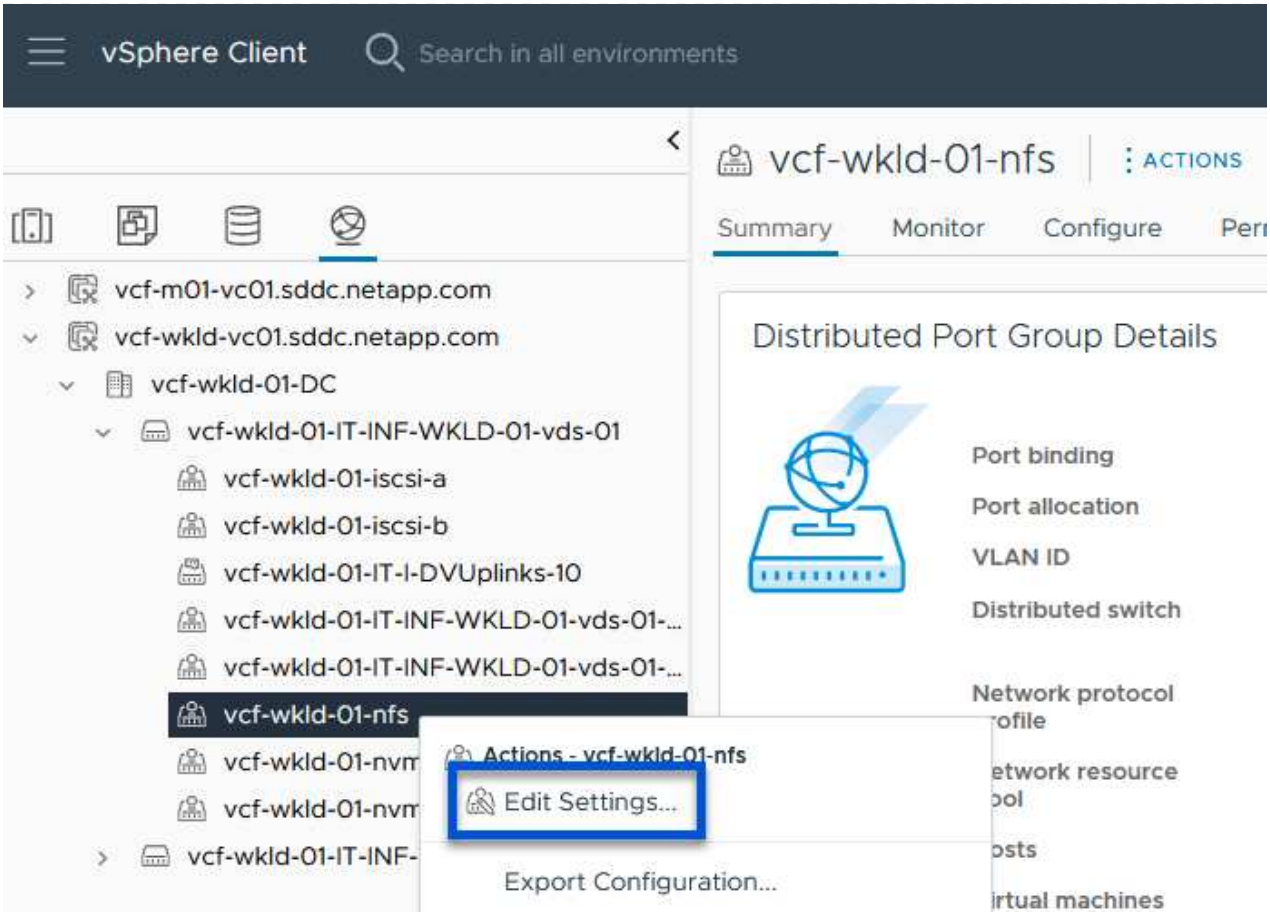
1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workloaddomäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen einer **Neuen verteilten Portgruppe…**.



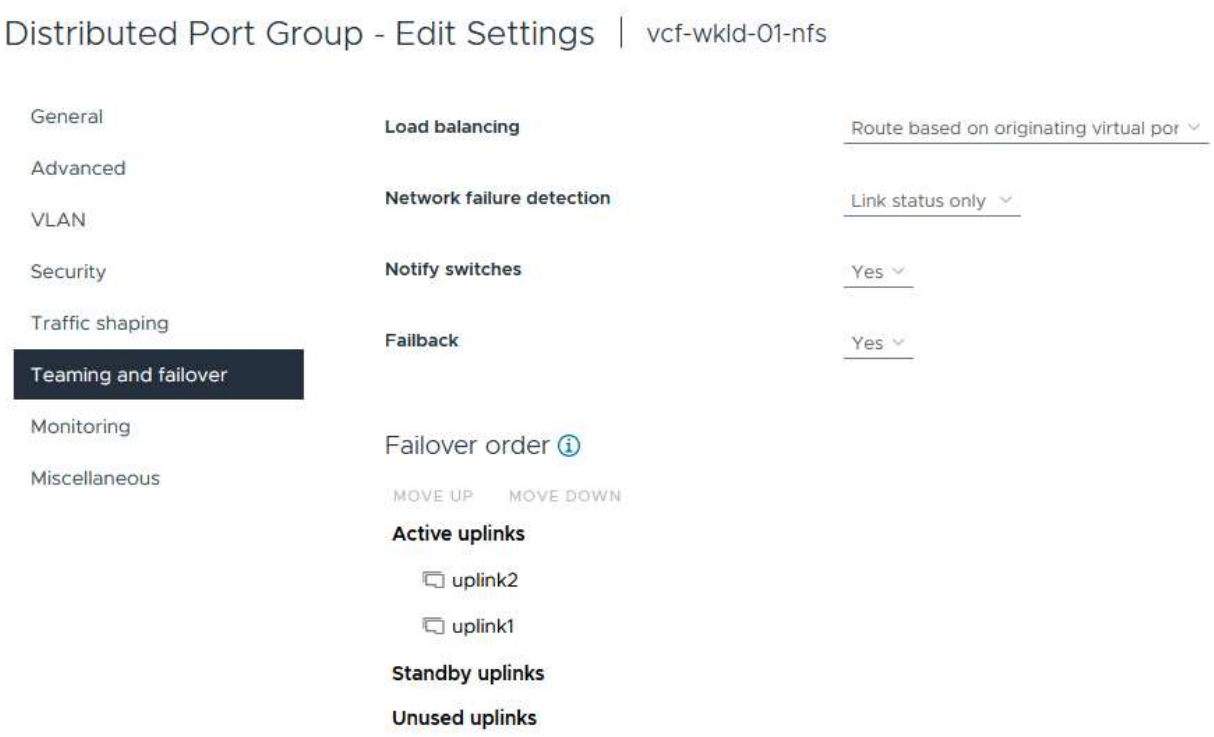
2. Geben Sie im Assistenten **Neue verteilte Portgruppe** einen Namen für die neue Portgruppe ein und klicken Sie auf **Weiter**, um fortzufahren.
3. Füllen Sie auf der Seite **Einstellungen konfigurieren** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige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



4. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Änderungen und klicken Sie auf **Fertig**, um die neue verteilte Portgruppe zu erstellen.
5. Nachdem die Portgruppe erstellt wurde, navigieren Sie zu der Portgruppe und wählen Sie die Aktion „Einstellungen bearbeiten…“ aus.



6. Navigieren Sie auf der Seite **Verteilte Portgruppe – Einstellungen bearbeiten** im linken Menü zu **Teaming und Failover**. Aktivieren Sie die Teambildung für die Uplinks, die für den NFS-Verkehr verwendet werden sollen, indem Sie sicherstellen, dass sie sich gemeinsam im Bereich **Aktive Uplinks** befinden. Verschieben Sie alle nicht verwendeten Uplinks nach unten zu **Ungenutzte Uplinks**.

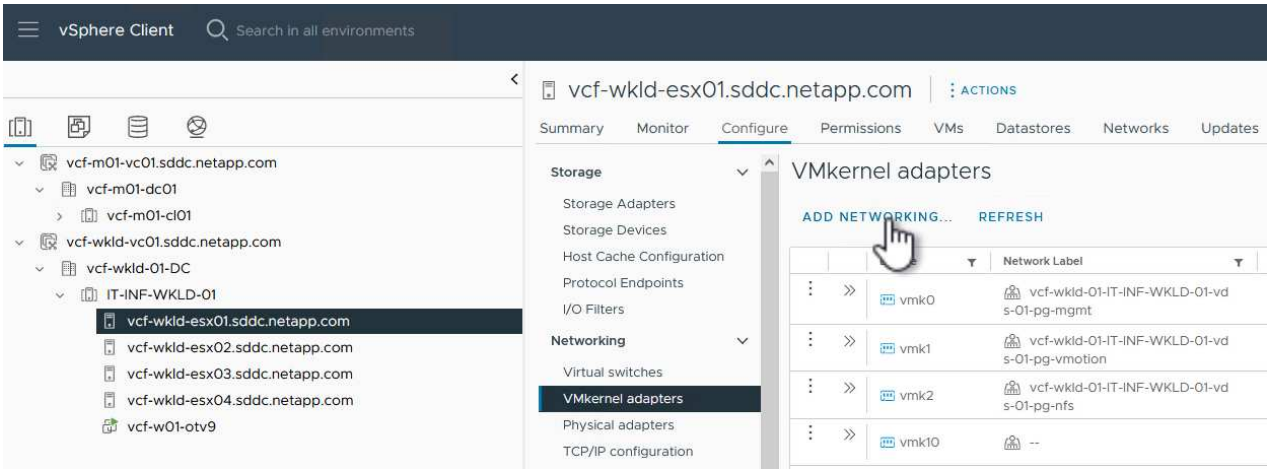


7. Wiederholen Sie diesen Vorgang für jeden ESXi-Host im Cluster.

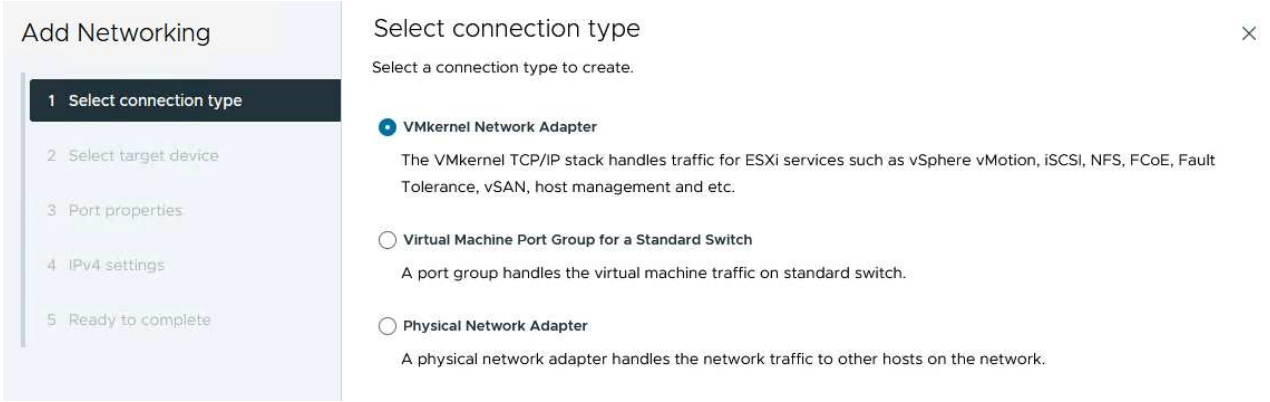
Erstellen Sie auf jedem ESXi-Host einen VMkernel-Adapter

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

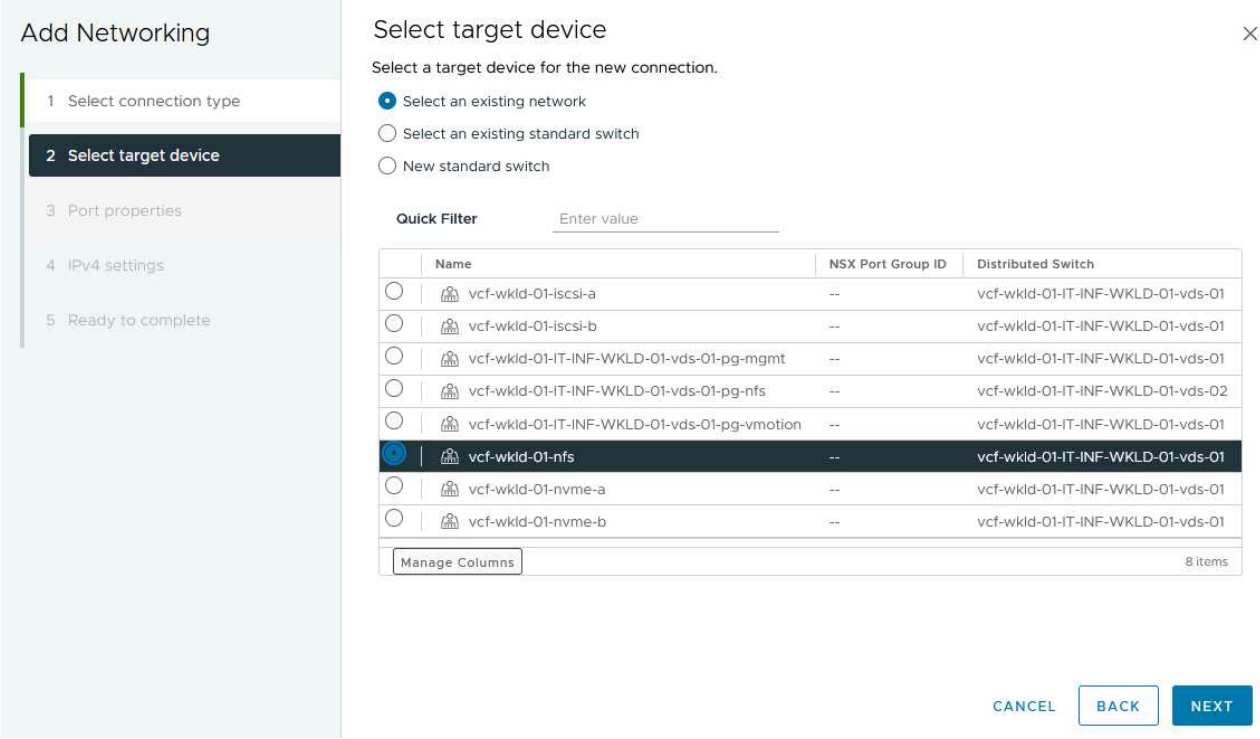
1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts im Workload-Domäneninventar. Wählen Sie auf der Registerkarte **Konfigurieren VMkernel-Adapter** aus und klicken Sie zum Starten auf **Netzwerk hinzufügen…**.



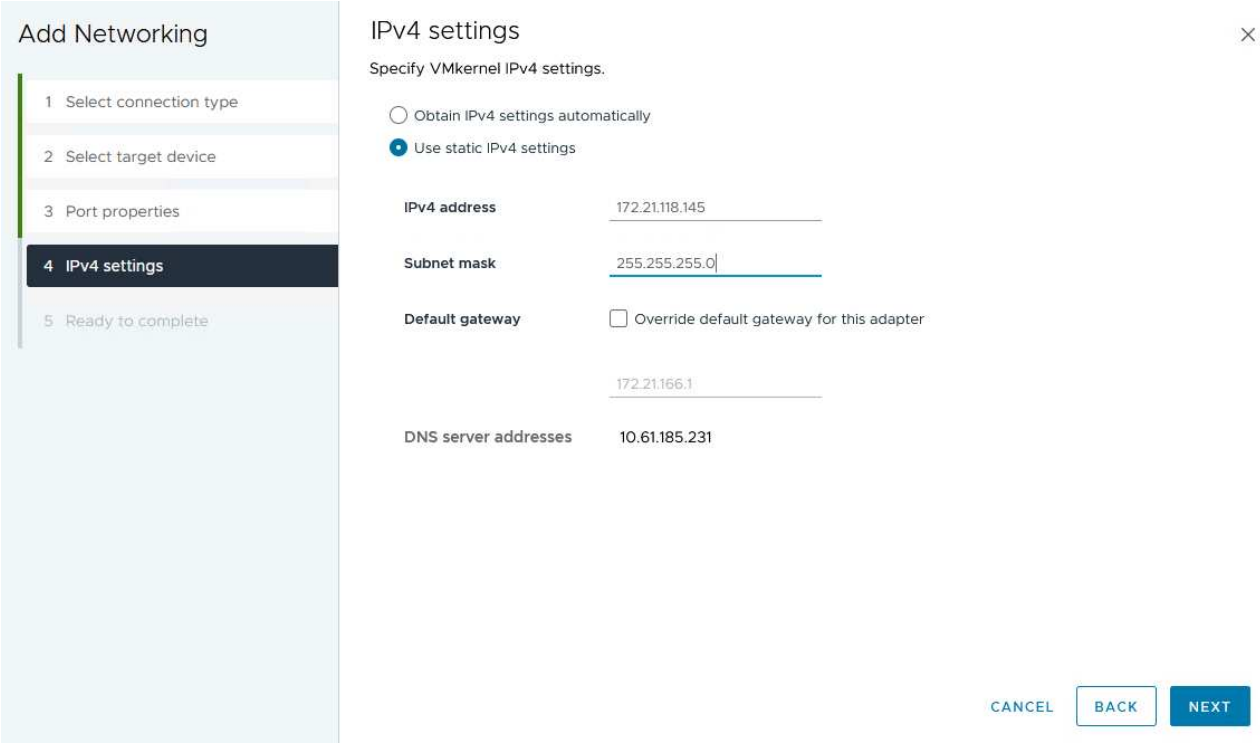
2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel-Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



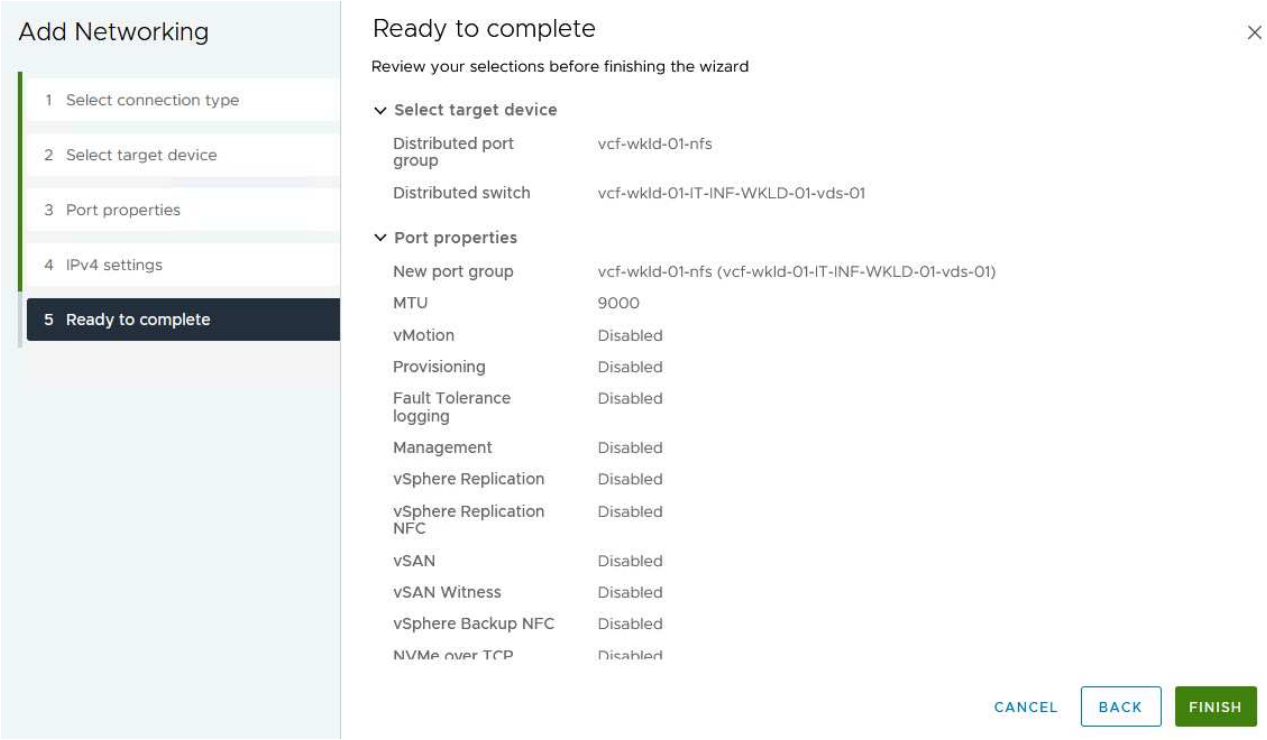
3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für NFS aus.



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



6. Überprüfen Sie Ihre Auswahl auf der Seite **Bereit zum Abschließen** und klicken Sie auf **Fertig**, um den VMkernel-Adapter zu erstellen.



Bereitstellen und Verwenden von ONTAP Tools zum Konfigurieren von Speicher

Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VCF-Verwaltungsdomänencluster ausgeführt und umfassen die Bereitstellung von OTV, die Erstellung eines vVols NFS-Datenspeichers und die Migration von Verwaltungs-VMs in den neuen Datenspeicher.

Für VI-Workloaddomänen wird OTV im VCF-Verwaltungscluster installiert, aber beim vCenter registriert, das der VI-Workloaddomäne zugeordnet ist.

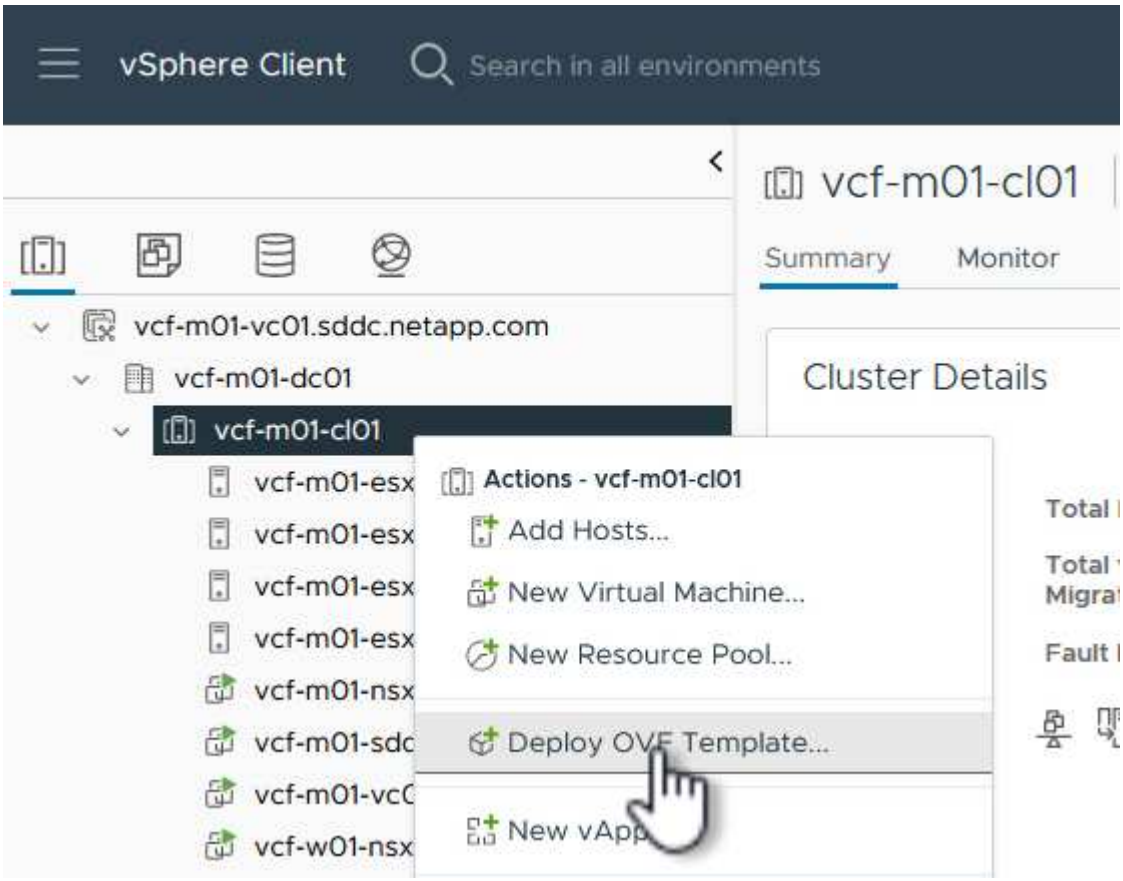
Weitere Informationen zur Bereitstellung und Verwendung von ONTAP Tools in einer Umgebung mit mehreren vCentern finden Sie unter"Voraussetzungen für die Registrierung von ONTAP Tools in einer Umgebung mit mehreren vCenter-Servern" .

Bereitstellen von ONTAP tools for VMware vSphere

ONTAP tools for VMware vSphere (OTV) werden als VM-Appliance bereitgestellt und bieten eine integrierte vCenter-Benutzeroberfläche zur Verwaltung des ONTAP Speichers.

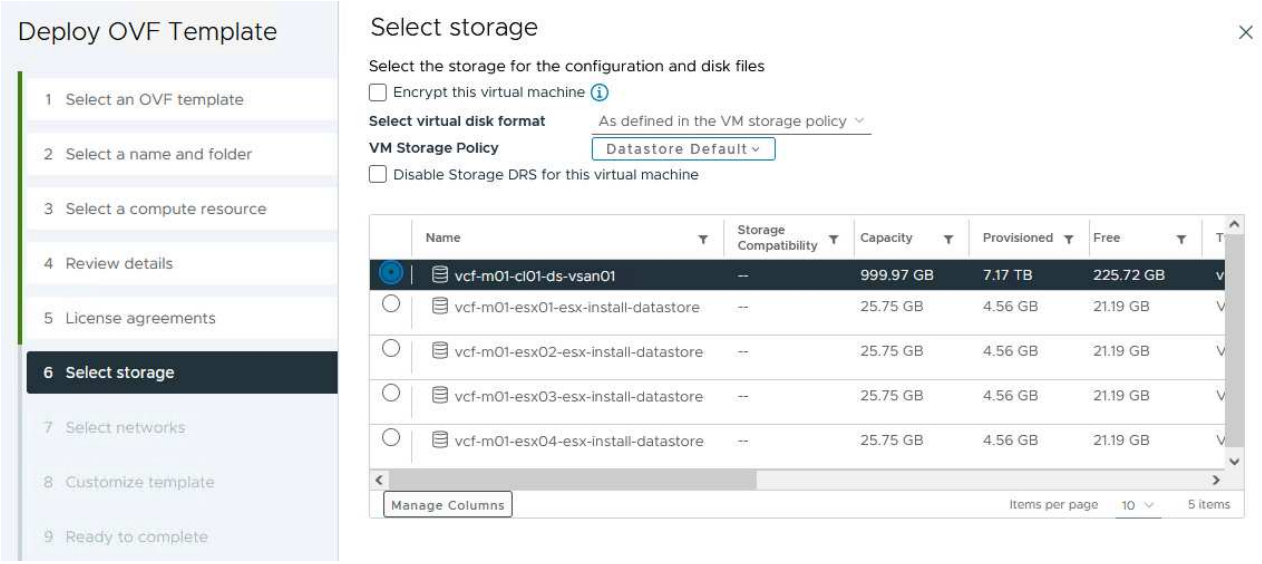
Führen Sie die folgenden Schritte aus, um ONTAP tools for VMware vSphere bereitzustellen:

1. Besorgen Sie sich das OVA-Image der ONTAP -Tools von der"NetApp Support-Site" und in einen lokalen Ordner herunterladen.
2. Melden Sie sich bei der vCenter-Appliance für die VCF-Verwaltungsdomäne an.
3. Klicken Sie in der vCenter-Appliance-Schnittstelle mit der rechten Maustaste auf den Verwaltungscluster und wählen Sie **OVF-Vorlage bereitstellen…**

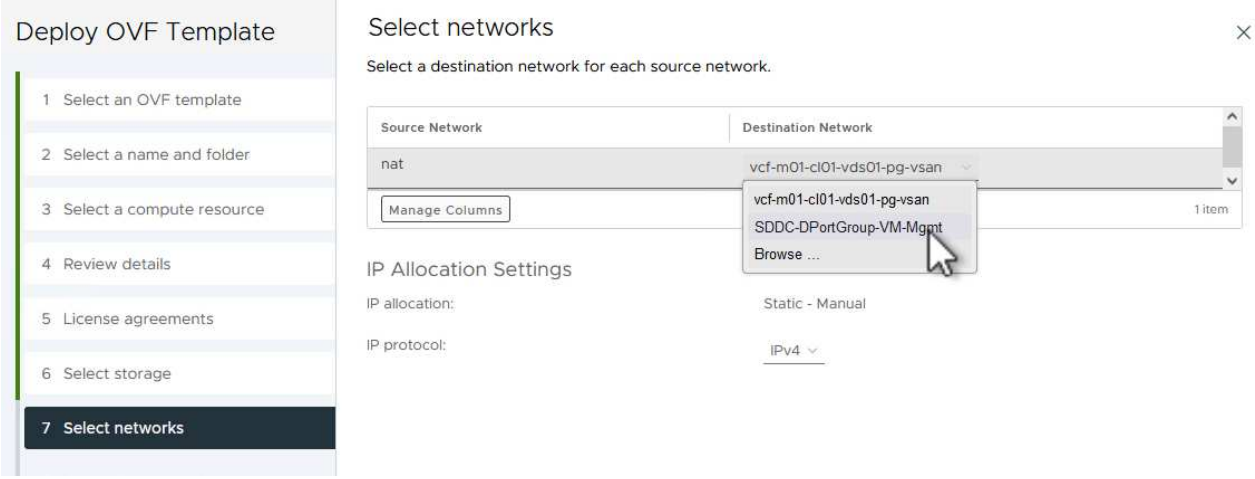


4. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie die im vorherigen Schritt heruntergeladene OVA-Datei der ONTAP -Tools aus.

5. Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und einen Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
6. Wählen Sie als Speicherort der Konfigurations- und Datenträgerdateien den vSAN-Datenspeicher des VCF-Managementdomänenclusters aus.

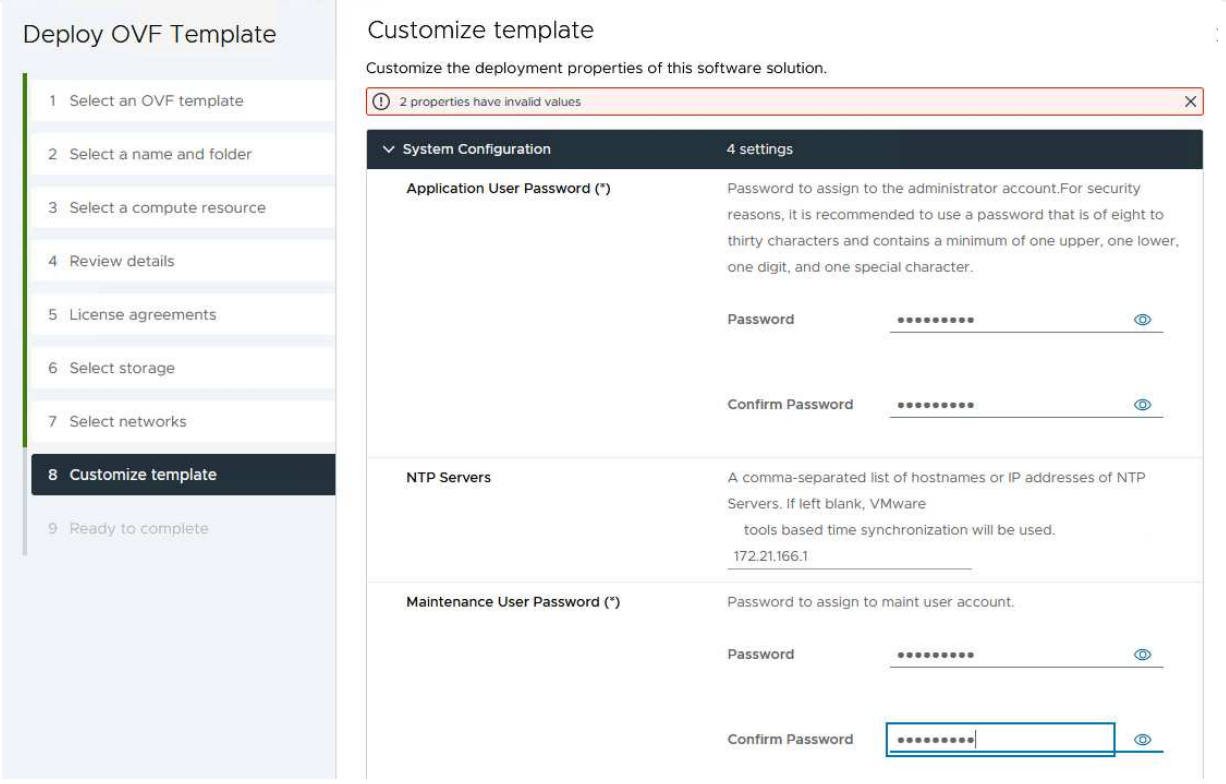


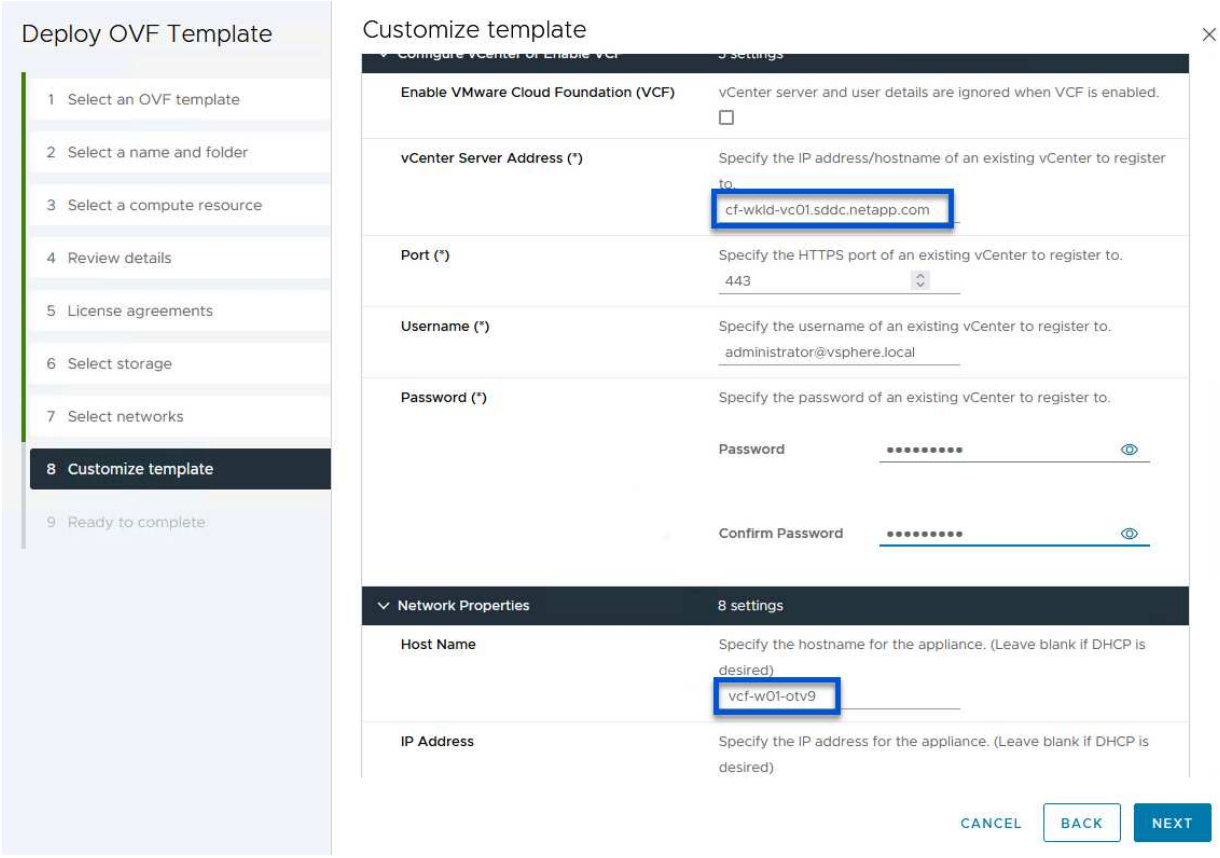
7. Wählen Sie auf der Seite „Netzwerk auswählen“ das für den Verwaltungsverkehr verwendete Netzwerk aus.



8. Geben Sie auf der Seite „Vorlage anpassen“ alle erforderlichen Informationen ein:
   - Für den administrativen Zugriff auf OTV zu verwendendes Passwort.
   - IP-Adresse des NTP-Servers.
   - Passwort für das OTV-Wartungskonto.
   - OTV Derby DB-Passwort.
   - Aktivieren Sie das Kontrollkästchen **VMware Cloud Foundation (VCF) aktivieren** nicht. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
   - FQDN oder IP-Adresse der vCenter-Appliance für die **VI-Workload-Domäne**
   - Anmeldeinformationen für die vCenter-Appliance der **VI Workload Domain**
   - Geben Sie die erforderlichen Felder für die Netzwerkeigenschaften an.

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

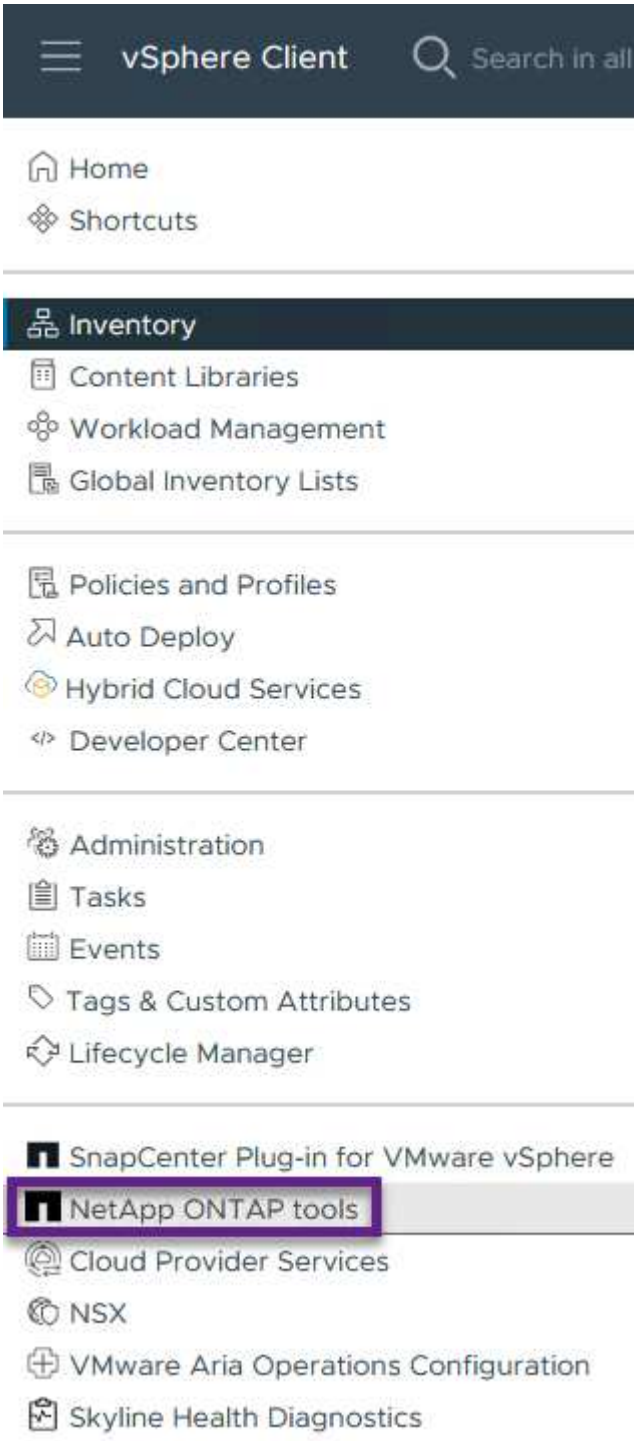




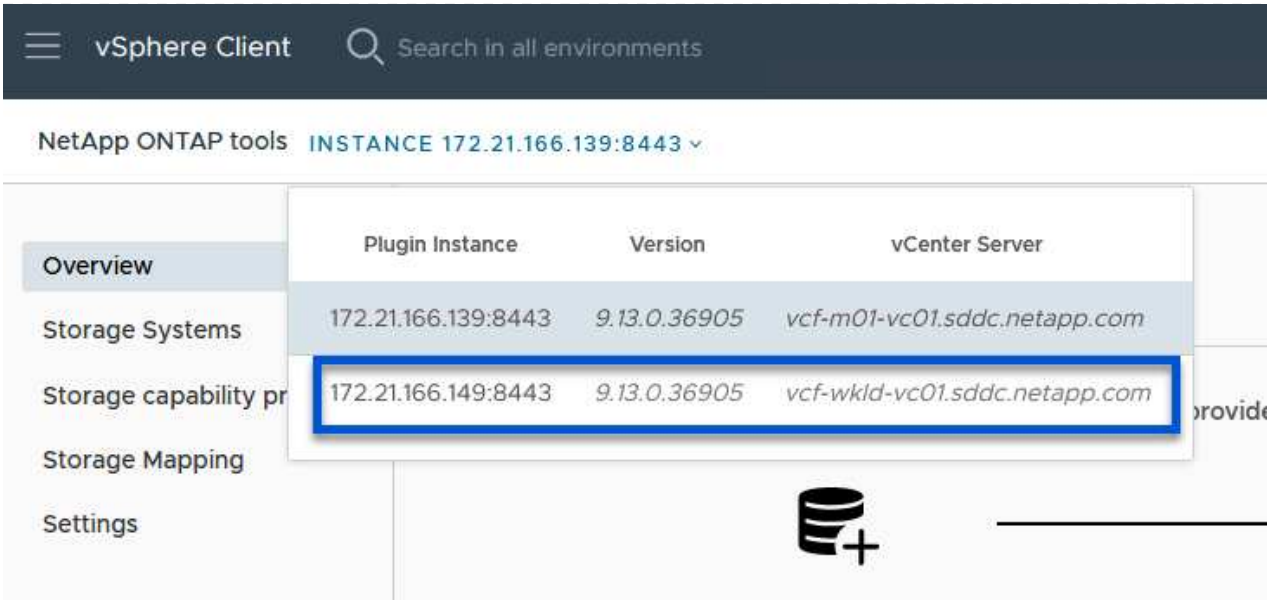
9. Überprüfen Sie alle Informationen auf der Seite „Bereit zum Abschließen“ und klicken Sie auf „Fertig stellen“, um mit der Bereitstellung des OTV-Geräts zu beginnen.

Fügen Sie ONTAP Tools ein Speichersystem hinzu.

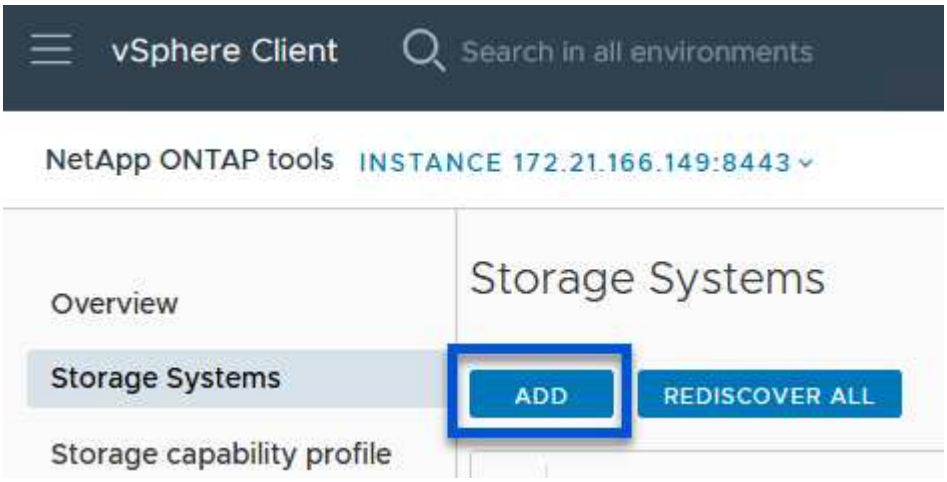
1. Greifen Sie auf NetApp ONTAP Tools zu, indem Sie es im Hauptmenü des vSphere-Clients auswählen.



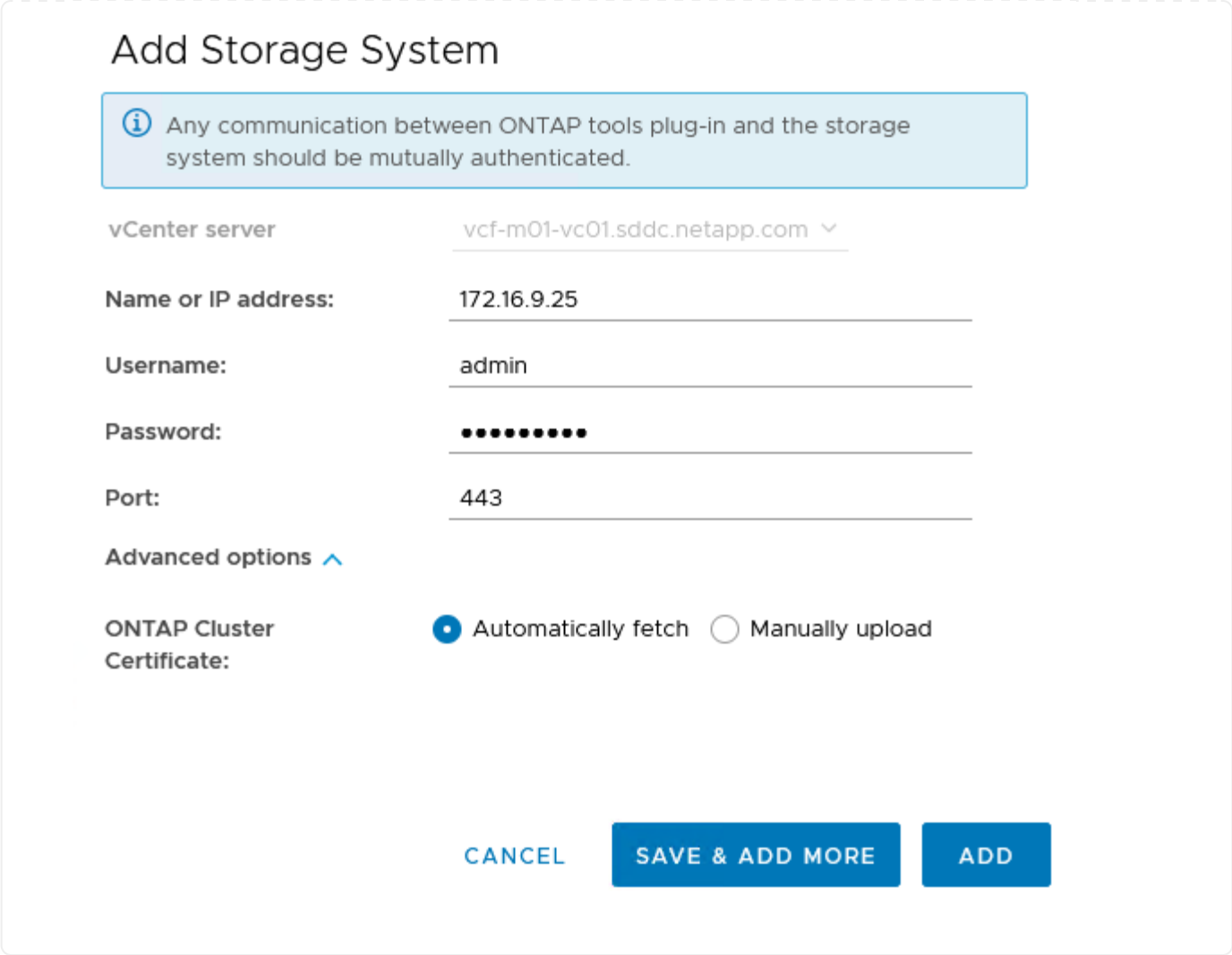
2. Wählen Sie aus dem Dropdown-Menü **INSTANCE** in der ONTAP Tool-Schnittstelle die OTV-Instanz aus, die der zu verwaltenden Workload-Domäne zugeordnet ist.



3. Wählen Sie in ONTAP Tools im linken Menü **Storage Systems** aus und drücken Sie dann **Add**.



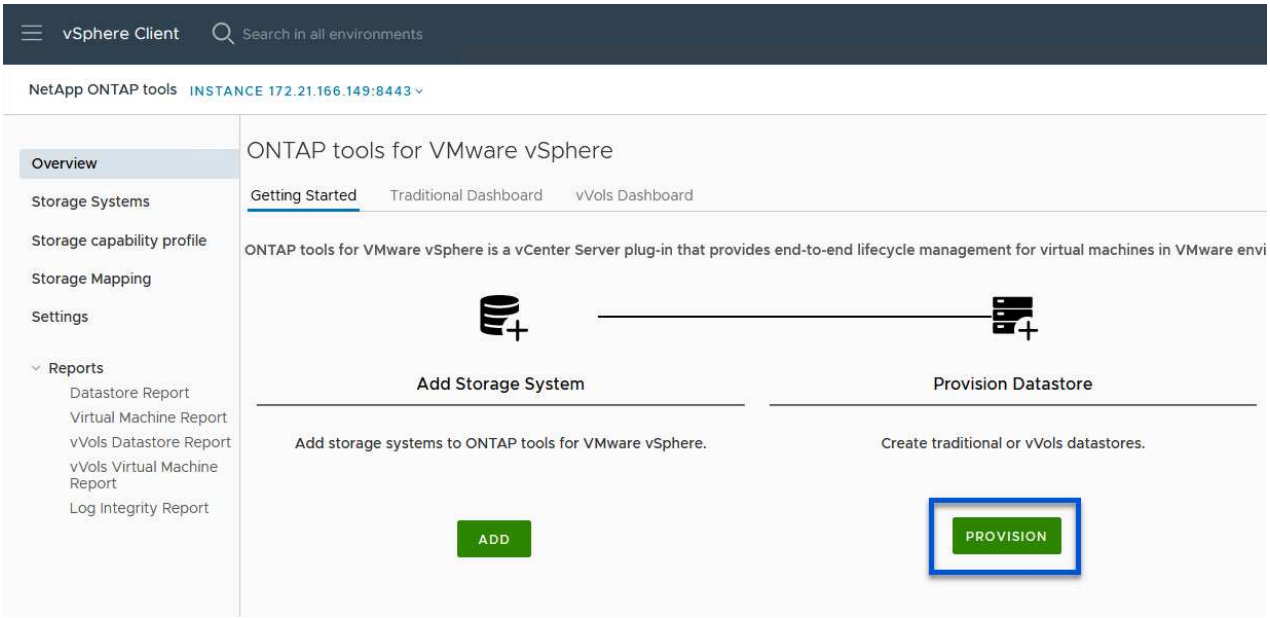
4. Geben Sie die IP-Adresse, die Anmeldeinformationen des Speichersystems und die Portnummer ein. Klicken Sie auf **Hinzufügen**, um den Erkennungsprozess zu starten.


Add Storage System
Any communication between ONTAP tools plug-in and the storage system should be mutually authenticated.
vCenter server
vcf-m01-vc01.sddc.netapp.com
Name or IP address:
172.16.9.25
Username:
admin
Password:
Port:
443
Advanced options
ONTAP Cluster Certificate:
Automatically fetch
Manually upload
CANCEL
SAVE & ADD MORE
ADD

Erstellen Sie einen NFS-Datenspeicher in ONTAP Tools

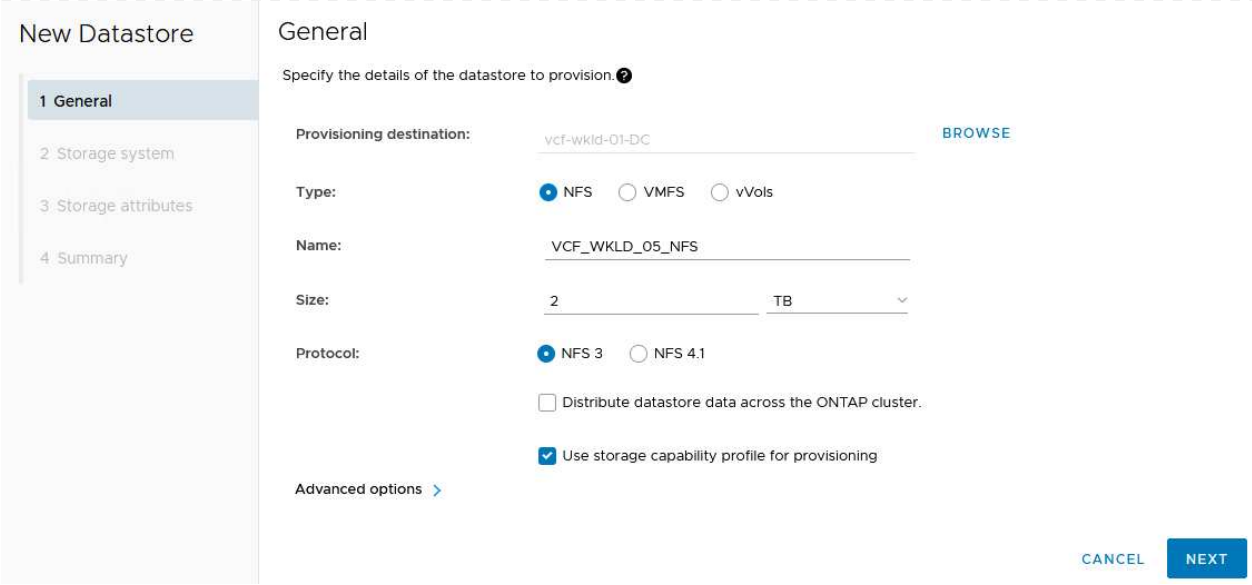
Führen Sie die folgenden Schritte aus, um mithilfe von ONTAP Tools einen ONTAP -Datenspeicher bereitzustellen, der auf NFS ausgeführt wird.

1. Wählen Sie in ONTAP Tools **Übersicht** und klicken Sie auf der Registerkarte **Erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.

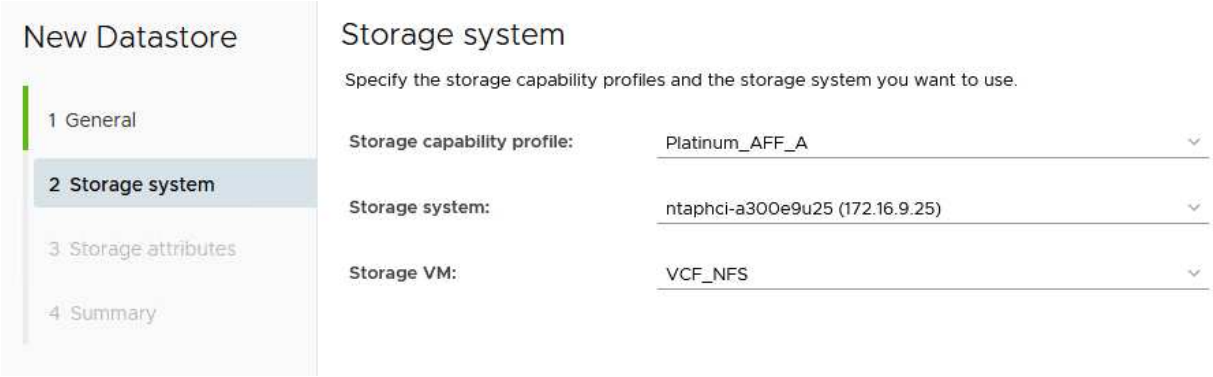


2. Wählen Sie auf der Seite **Allgemein** des Assistenten „Neuer Datenspeicher“ das vSphere-Rechenzentrum oder Clusterziel aus. Wählen Sie **NFS** als Datenspeichertyp, geben Sie einen Namen für den Datenspeicher ein und wählen Sie das Protokoll aus. Wählen Sie, ob Sie FlexGroup -Volumes verwenden möchten und ob Sie für die Bereitstellung eine Speicherkapazitätsdatei verwenden möchten. Klicken Sie auf **Weiter**, um fortzufahren.

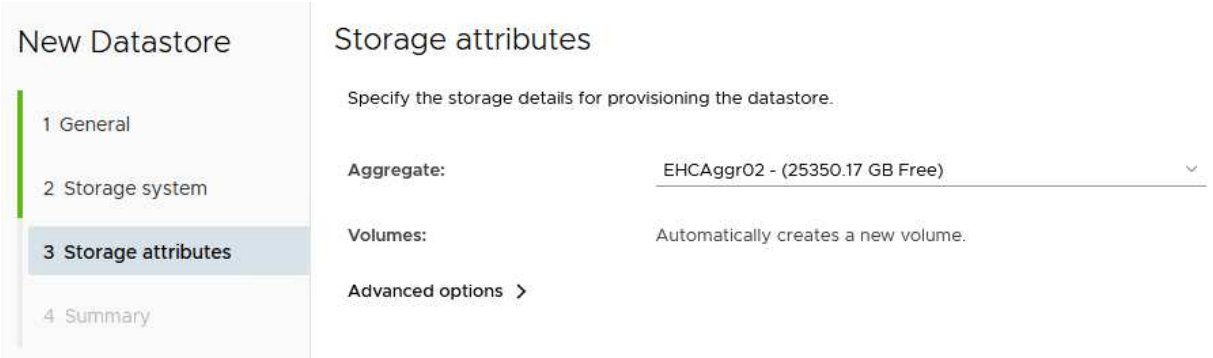
   Hinweis: Wenn Sie „Datastore-Daten im Cluster verteilen“ auswählen, wird das zugrunde liegende Volume als FlexGroup -Volume erstellt, wodurch die Verwendung von Storage Capability Profiles ausgeschlossen wird. Siehe "Unterstützte und nicht unterstützte Konfigurationen für FlexGroup -Volumes" Weitere Informationen zur Verwendung von FlexGroup -Volumes.



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

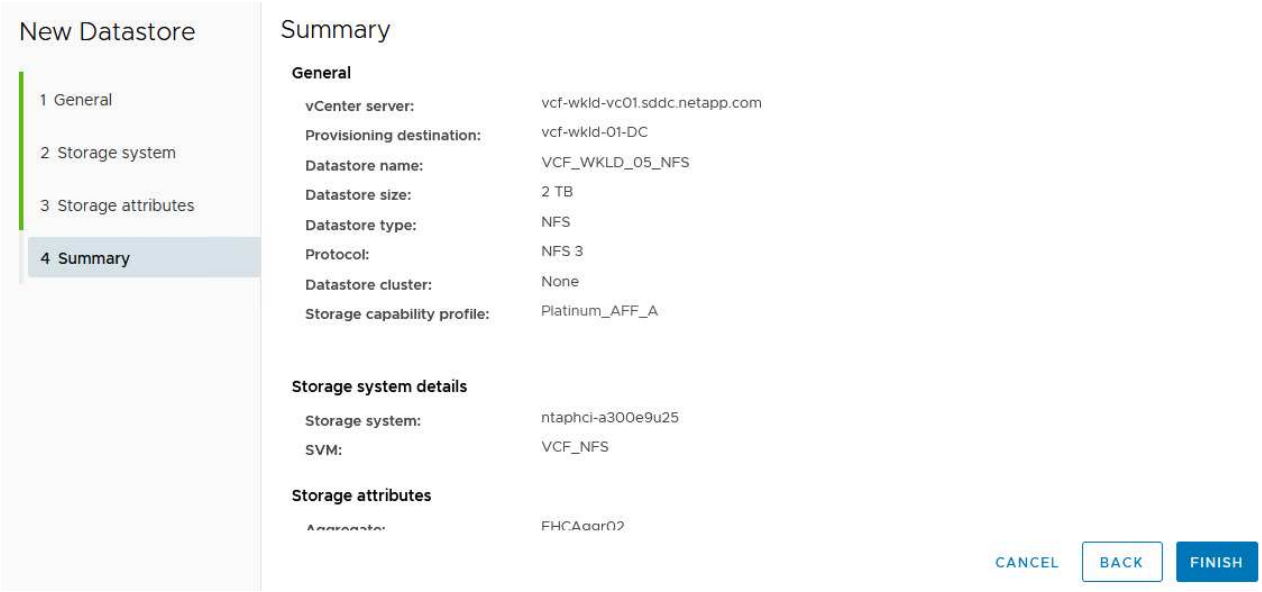


4. Wählen Sie auf der Seite **Speicherattribute** das zu verwendende Aggregat aus und klicken Sie dann auf **Weiter**, um fortzufahren.



5. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf „Fertig stellen“, um mit der

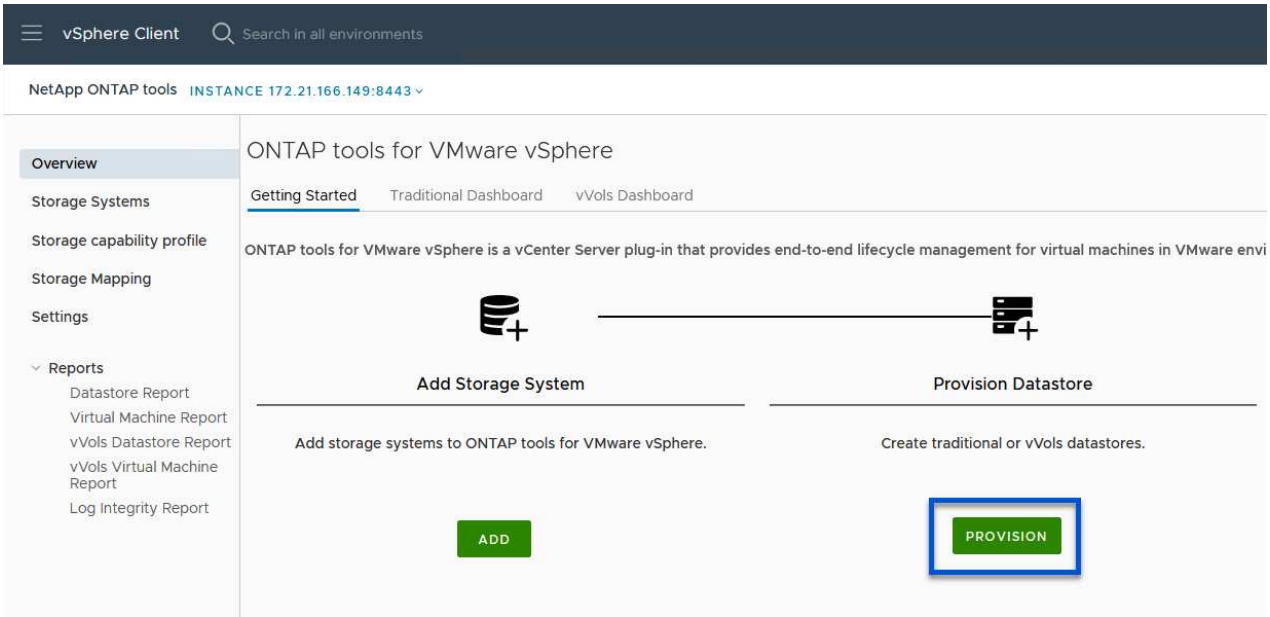
Erstellung des NFS-Datenspeichers zu beginnen.



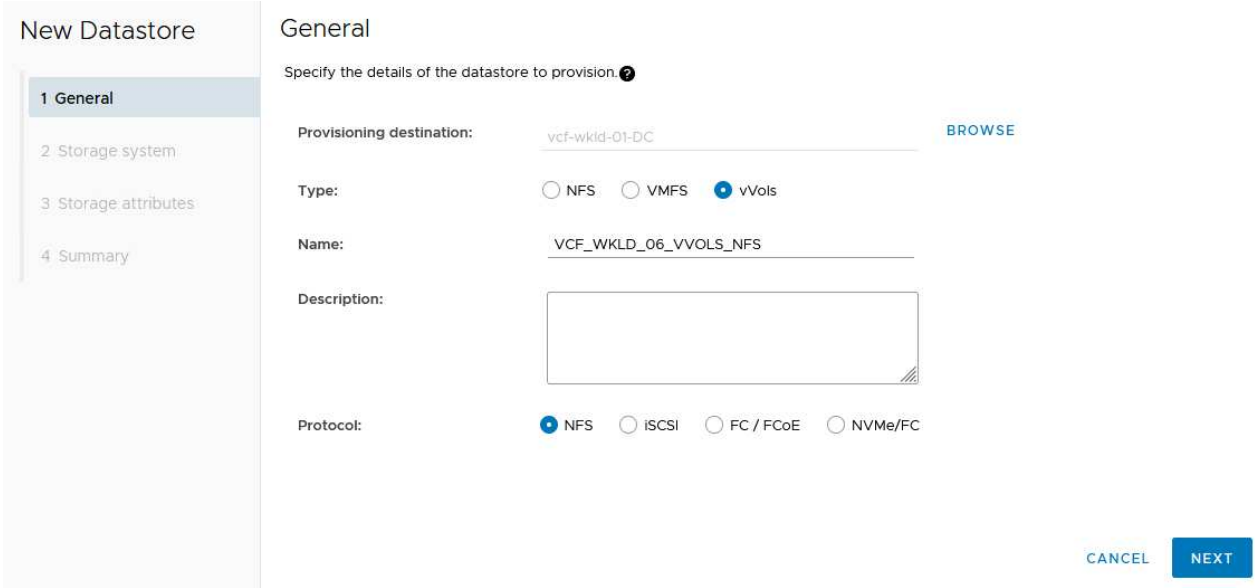
Erstellen Sie einen vVols Datenspeicher in ONTAP Tools

Führen Sie die folgenden Schritte aus, um einen vVols Datenspeicher in ONTAP Tools zu erstellen:

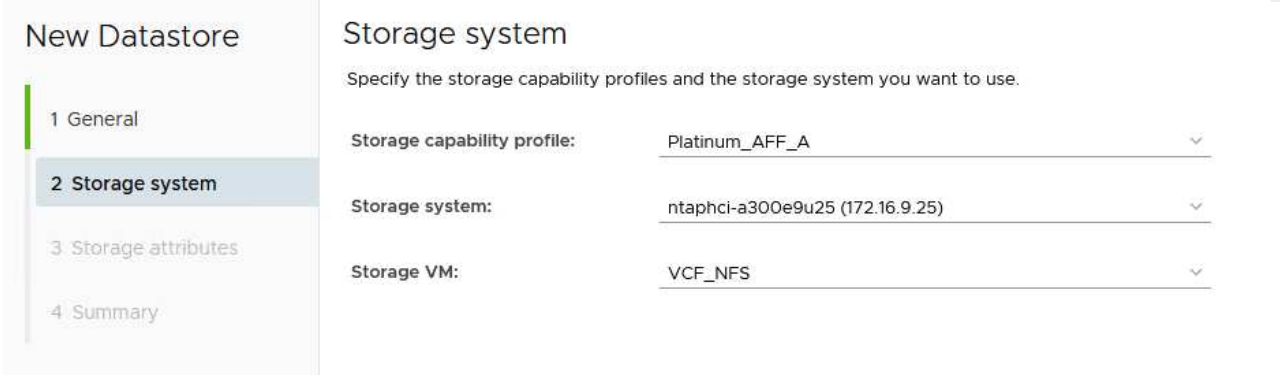
1. Wählen Sie in ONTAP Tools **Übersicht** und klicken Sie auf der Registerkarte **Erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.



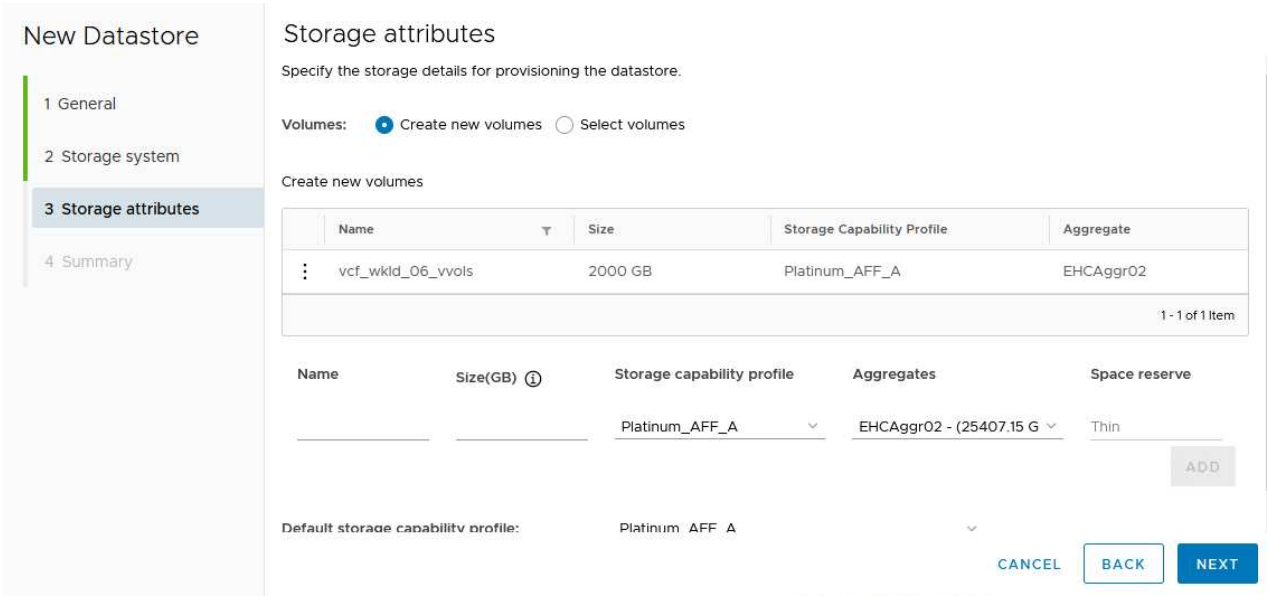
2. Wählen Sie auf der Seite **Allgemein** des Assistenten „Neuer Datenspeicher“ das vSphere-Rechenzentrum oder Clusterziel aus. Wählen Sie * vVols* als Datenspeichertyp, geben Sie einen Namen für den Datenspeicher ein und wählen Sie * NFS * als Protokoll. Klicken Sie auf **Weiter**, um fortzufahren.



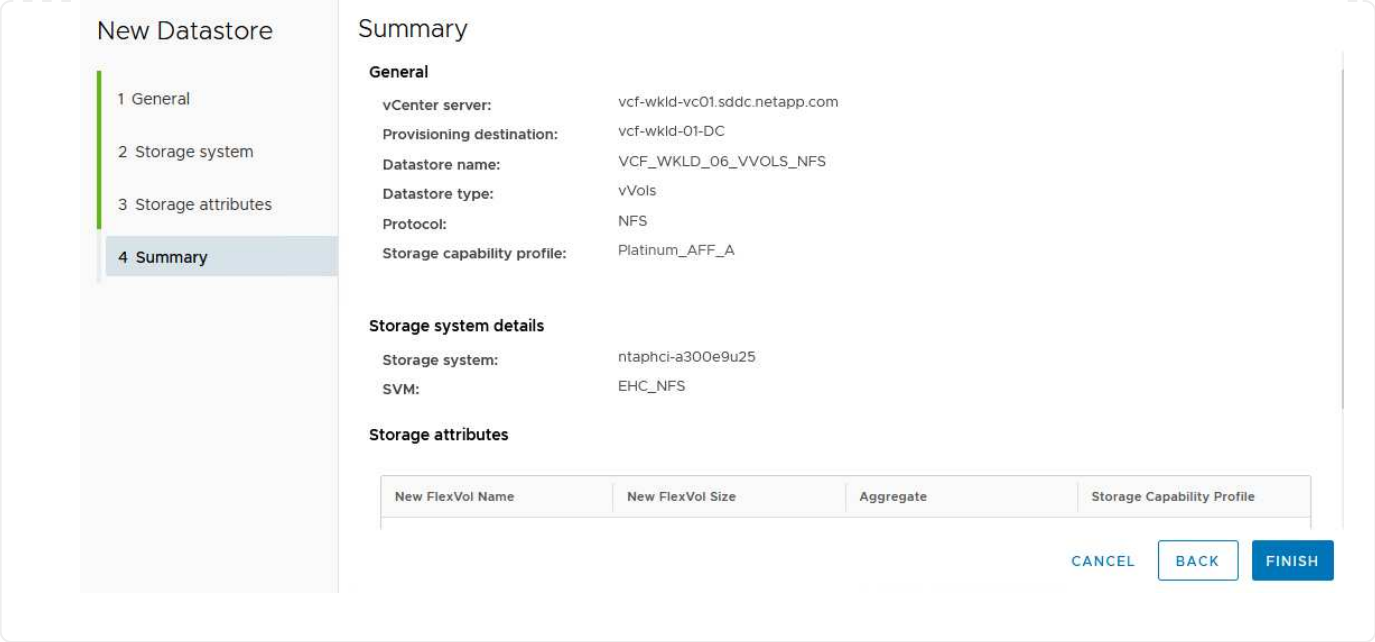
3. Wählen Sie auf der Seite **Speichersystem** ein Speicherfähigkeitsprofil, das Speichersystem und SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.



4. Wählen Sie auf der Seite **Speicherattribute** die Erstellung eines neuen Volumes für den Datenspeicher aus und füllen Sie die Speicherattribute des zu erstellenden Volumes aus. Klicken Sie auf **Hinzufügen**, um das Volume zu erstellen, und dann auf **Weiter**, um fortzufahren.



5. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig**, um den Erstellungsprozess des vVol-Datenspeichers zu starten.



Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Fügen Sie NVMe über TCP als zusätzlichen Speicher zu VI-Workloaddomänen hinzu

In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung von ONTAP Tools für VMware, um NVMe über TCP (NVMe/TCP) als zusätzlichen Speicher für eine Workload-Domäne der VMware Cloud Foundation (VCF) Virtual Infrastructure (VI) zu konfigurieren. Dieses Verfahren fasst das Einrichten einer NVMe/TCP-fähigen Storage Virtual Machine (SVM), das Erstellen von NVMe-Namespaces, das Konfigurieren des ESXi-Hostnetzwerks und das Bereitstellen eines VMFS-Datenspeichers zusammen.

Vorteile von NVMe gegenüber TCP

Hohe Leistung: Bietet außergewöhnliche Leistung mit geringer Latenz und hohen Datenübertragungsraten. Dies ist für anspruchsvolle Anwendungen und umfangreiche Datenoperationen von entscheidender Bedeutung.

Skalierbarkeit: Unterstützt skalierbare Konfigurationen, sodass IT-Administratoren ihre Infrastruktur bei steigendem Datenbedarf nahtlos erweitern können.

Kostengünstig: Läuft über Standard-Ethernet-Switches und ist in TCP-Datagrammen gekapselt. Zur Durchführung ist keine spezielle Ausrüstung erforderlich.

Weitere Informationen zu den Vorteilen von NVMe finden Sie unter "Was ist NVME?"

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

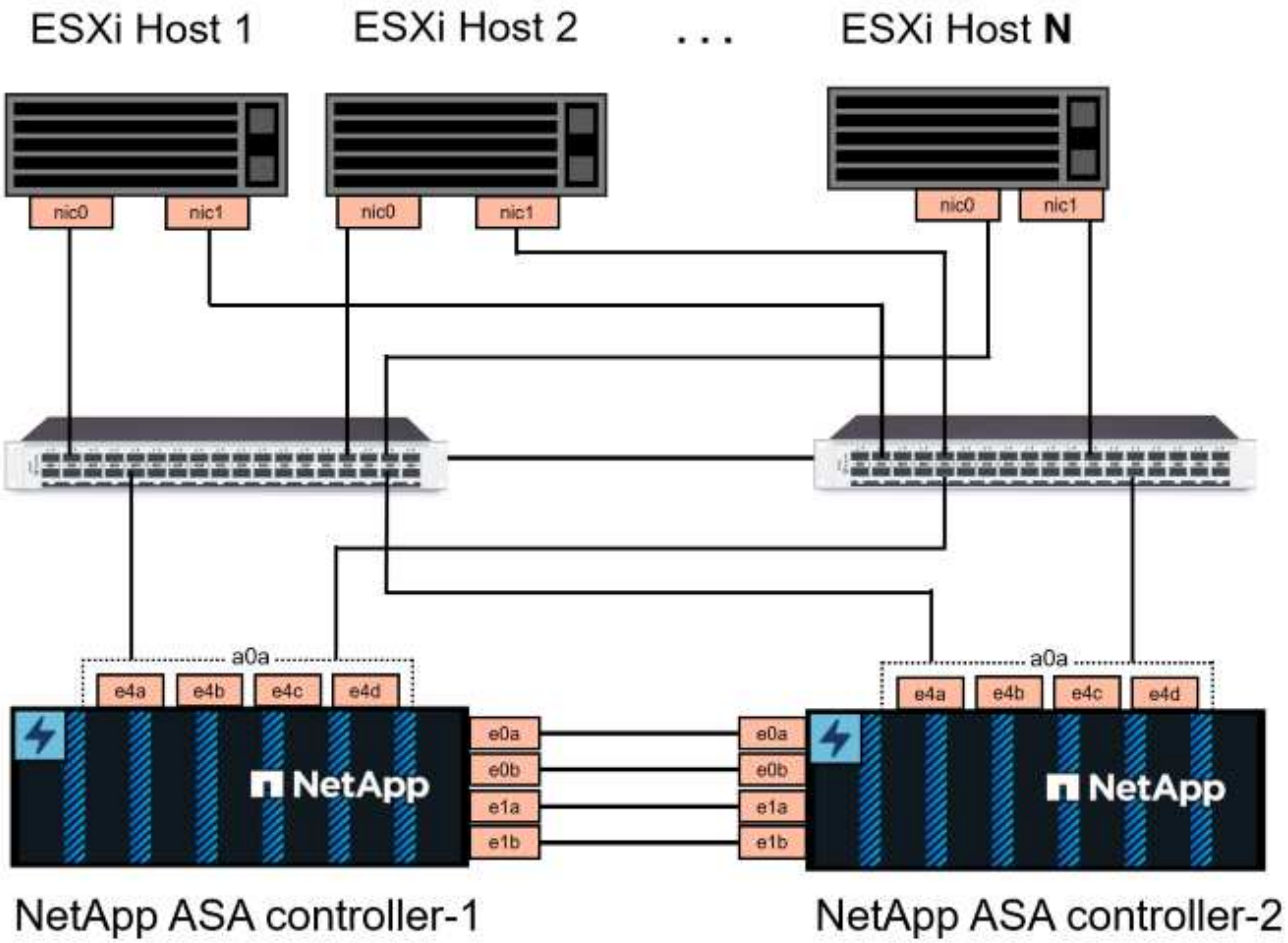
- Erstellen Sie eine Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für NVMe/TCP-Verkehr.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workloaddomäne.
- Erstellen Sie VMkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workloaddomäne.
- Fügen Sie NVMe/TCP-Adapter auf ESXi-Hosts hinzu.
- Stellen Sie einen NVMe/TCP-Datenspeicher bereit.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF oder ASA Speichersystem mit physischen Datenports auf Ethernet-Switches, die für den Speicherverkehr vorgesehen sind.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf den vSphere-Client kann zugegriffen werden.
- Zuvor wurde eine VI-Workloaddomäne bereitgestellt.

NetApp empfiehlt vollständig redundante Netzwerkdesigns für NVMe/TCP. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration, die Fehlertoleranz für Speichersysteme, Switches, Netzwerkadapter und Hostsysteme bietet. Weitere Informationen finden Sie in der NetApp"SAN-Konfigurationsreferenz" für weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp , für alle SVMs in NVMe/TCP-Konfigurationen mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken zu haben.

Diese Dokumentation veranschaulicht den Vorgang zum Erstellen einer neuen SVM und zum Angeben der IP-Adressinformationen zum Erstellen mehrerer LIFs für NVMe/TCP-Verkehr. Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie unter"Erstellen Sie eine LIF (Netzwerkschnittstelle)" .

Weitere Informationen zu NVMe-Designüberlegungen für ONTAP Speichersysteme finden Sie unter"NVMe-Konfiguration, -Unterstützung und -Einschränkungen" .

Bereitstellungsschritte

Führen Sie die folgenden Schritte aus, um einen VMFS-Datenspeicher in einer VCF-Workloaddomäne mithilfe von NVMe/TCP zu erstellen.

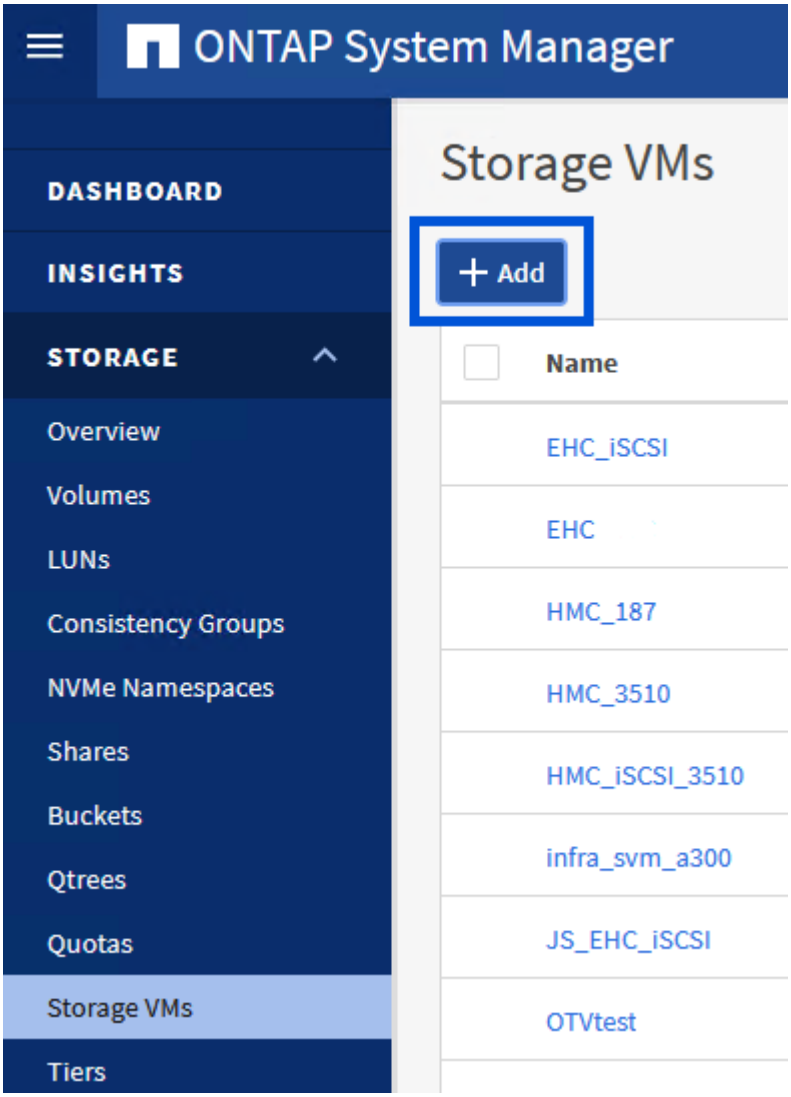
Erstellen Sie SVM, LIFs und NVMe-Namespace auf dem ONTAP Speichersystem

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

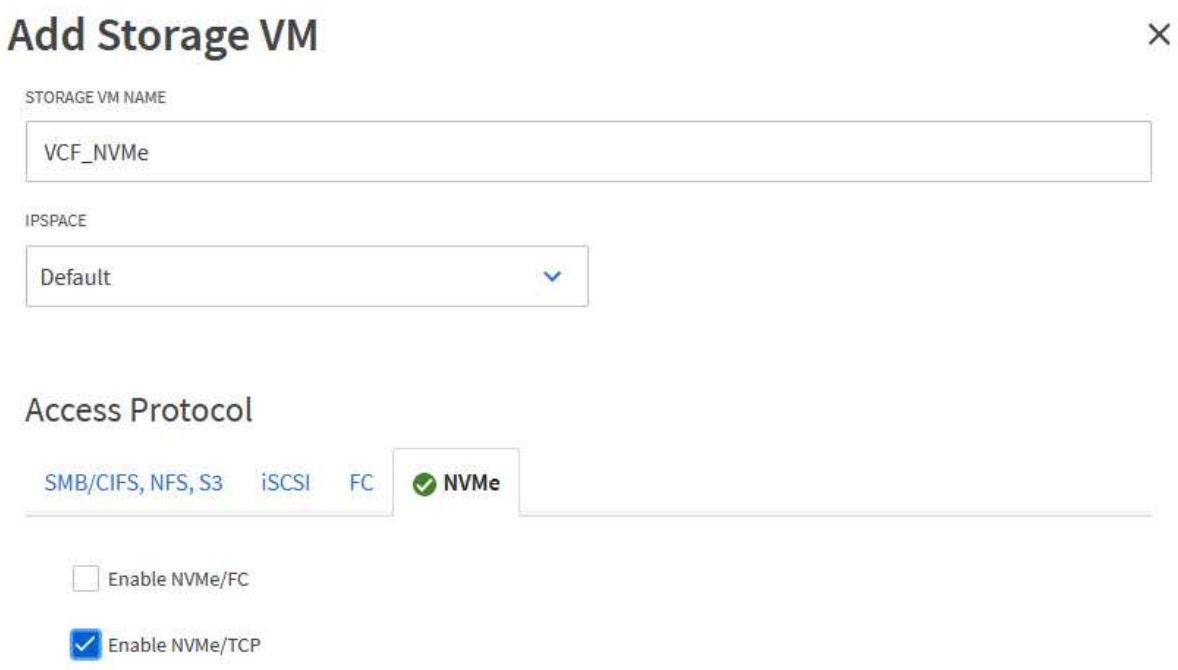
Erstellen der Speicher-VM und LIFs

Führen Sie die folgenden Schritte aus, um eine SVM zusammen mit mehreren LIFs für NVMe/TCP-Verkehr zu erstellen.

1. Navigieren Sie im ONTAP System Manager im linken Menü zu **Storage VMs** und klicken Sie zum Starten auf **+ Hinzufügen**.

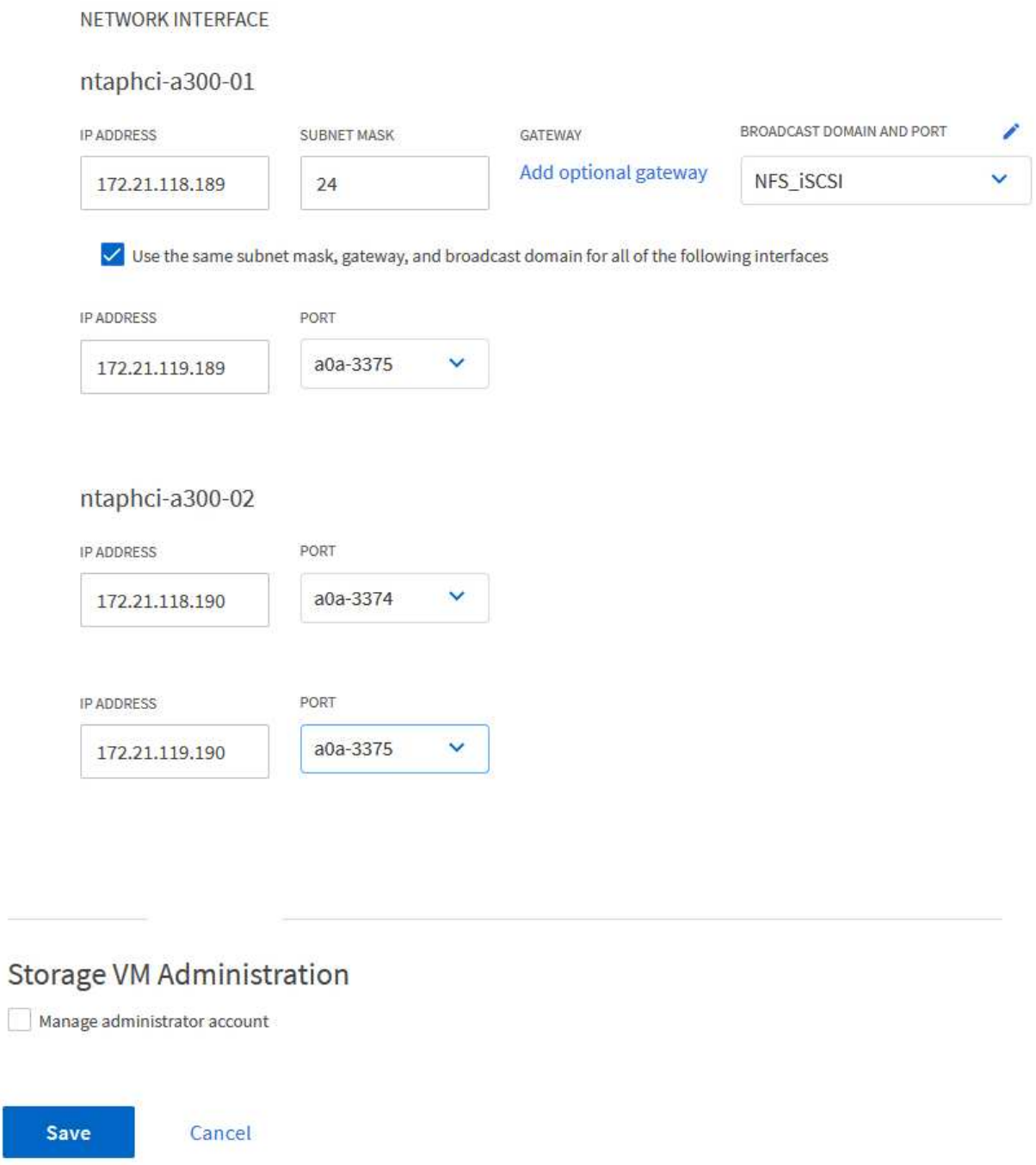


2. Geben Sie im Assistenten **Speicher-VM hinzufügen** einen **Namen** für die SVM ein, wählen Sie den **IP-Bereich** aus und klicken Sie dann unter **Zugriffsprotokoll** auf die Registerkarte **NVMe** und aktivieren Sie das Kontrollkästchen **NVMe/TCP aktivieren**.

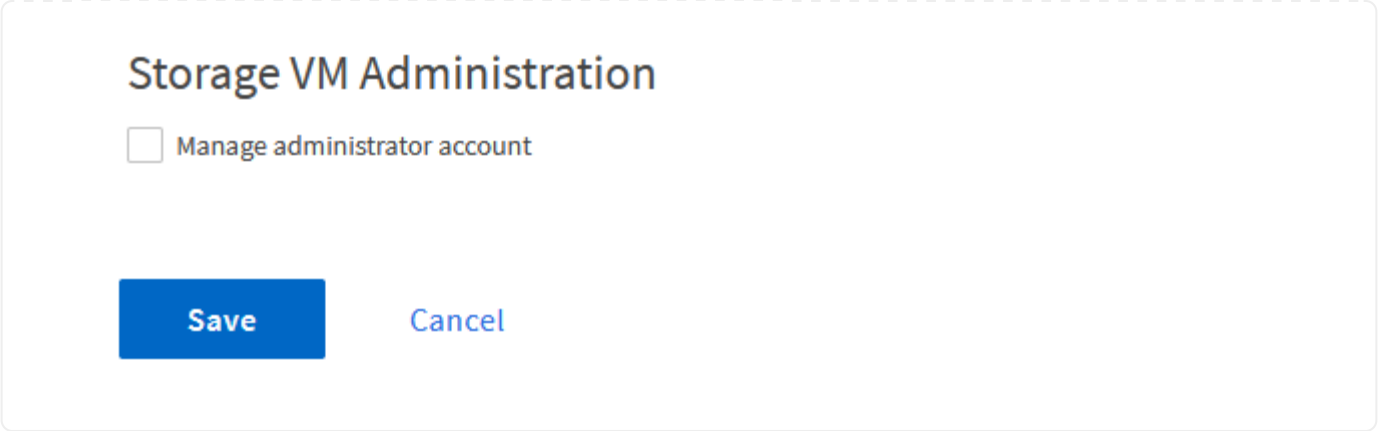


3. Geben Sie im Abschnitt **Netzwerkschnittstelle** die **IP-Adresse**, **Subnetzmaske** und **Broadcast-Domäne und -Port** für das erste LIF ein. Für nachfolgende LIFs kann das Kontrollkästchen aktiviert werden, um gemeinsame Einstellungen für alle verbleibenden LIFs zu verwenden oder separate Einstellungen zu verwenden.

> Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp , für alle SVMs in NVMe/TCP-Konfigurationen mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken zu haben.



4. Wählen Sie, ob das Storage VM-Administrationskonto (für Umgebungen mit mehreren Mandanten) aktiviert werden soll, und klicken Sie auf **Speichern**, um die SVM zu erstellen.


Storage VM Administration
Manage administrator account
Save
Cancel

Erstellen des NVMe-Namespace

NVMe-Namespaces sind analog zu LUNs für iSCSi oder FC. Der NVMe-Namespace muss erstellt werden, bevor ein VMFS-Datenspeicher vom vSphere-Client bereitgestellt werden kann. Um den NVMe-Namespace zu erstellen, muss zunächst der NVMe Qualified Name (NQN) von jedem ESXi-Host im Cluster abgerufen werden. Der NQN wird von ONTAP verwendet, um die Zugriffskontrolle für den Namespace bereitzustellen.

Führen Sie die folgenden Schritte aus, um einen NVMe-Namespace zu erstellen:

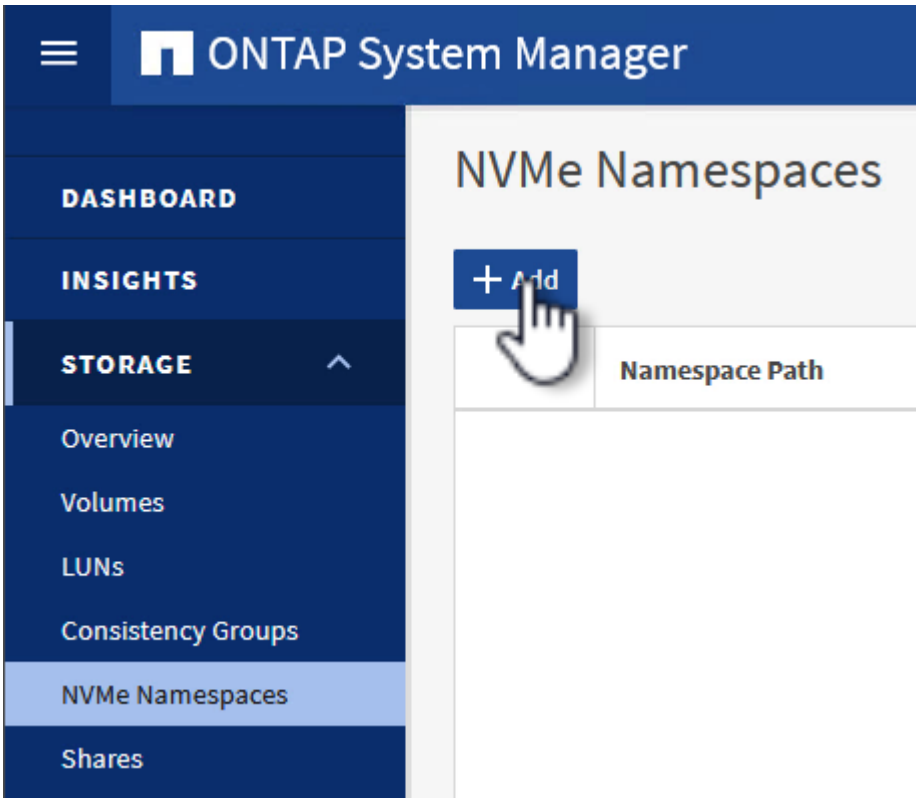
1. Öffnen Sie eine SSH-Sitzung mit einem ESXi-Host im Cluster, um dessen NQN zu erhalten. Verwenden Sie den folgenden Befehl aus der CLI:

   ```
   esxcli nvme info get
   ```

   Es sollte eine Ausgabe ähnlich der folgenden angezeigt werden:

   ```
   Host NQN: nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-esx01
   ```

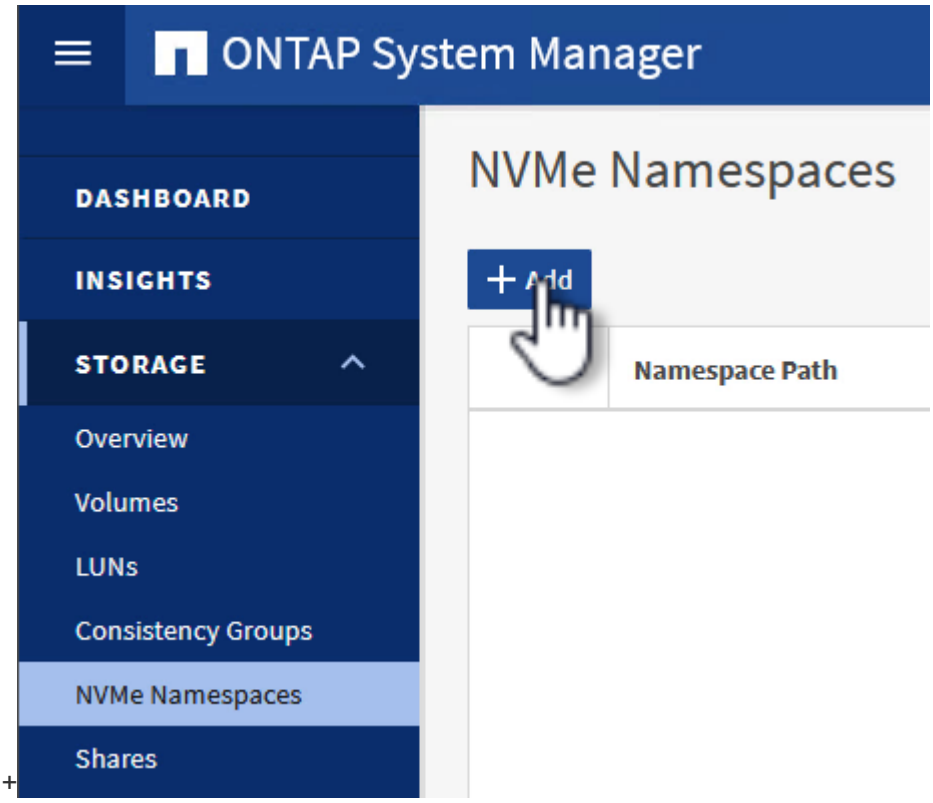
2. Notieren Sie den NQN für jeden ESXi-Host im Cluster
3. Navigieren Sie im ONTAP System Manager im linken Menü zu **NVMe Namespaces** und klicken Sie zum Starten auf **+ Hinzufügen**.



4. Geben Sie auf der Seite **NVMe-Namespace hinzufügen** ein Namenspräfix, die Anzahl der zu

erstellenden Namespaces, die Größe des Namespaces und das Host-Betriebssystem ein, das auf den Namespace zugreifen wird. Erstellen Sie im Abschnitt **Host-NQN** eine durch Kommas getrennte Liste der NQNs, die zuvor von den ESXi-Hosts gesammelt wurden, die auf die Namespaces zugreifen werden.

Klicken Sie auf **Weitere Optionen**, um zusätzliche Elemente wie die Snapshot-Schutzrichtlinie zu konfigurieren. Klicken Sie abschließend auf **Speichern**, um den NVMe-Namespace zu erstellen.



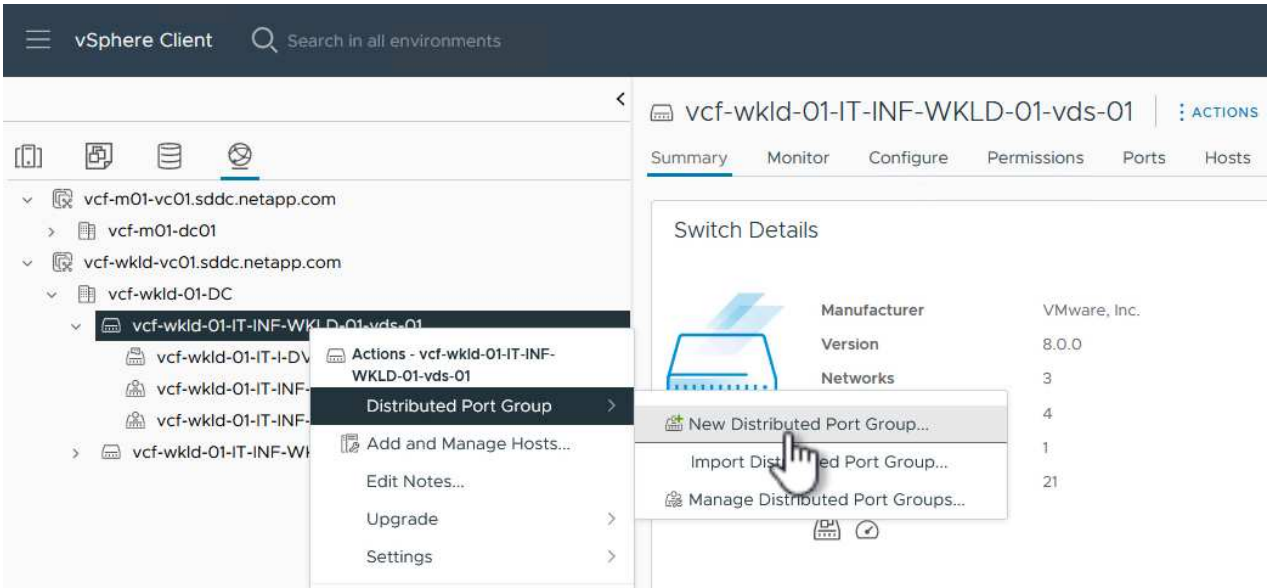
Einrichten von Netzwerk- und NVMe-Softwareadaptern auf ESXi-Hosts

Die folgenden Schritte werden mithilfe des vSphere-Clients auf dem VI-Workload-Domänencluster ausgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client sowohl für die Verwaltungs- als auch für die Workloaddomänen gleich ist.

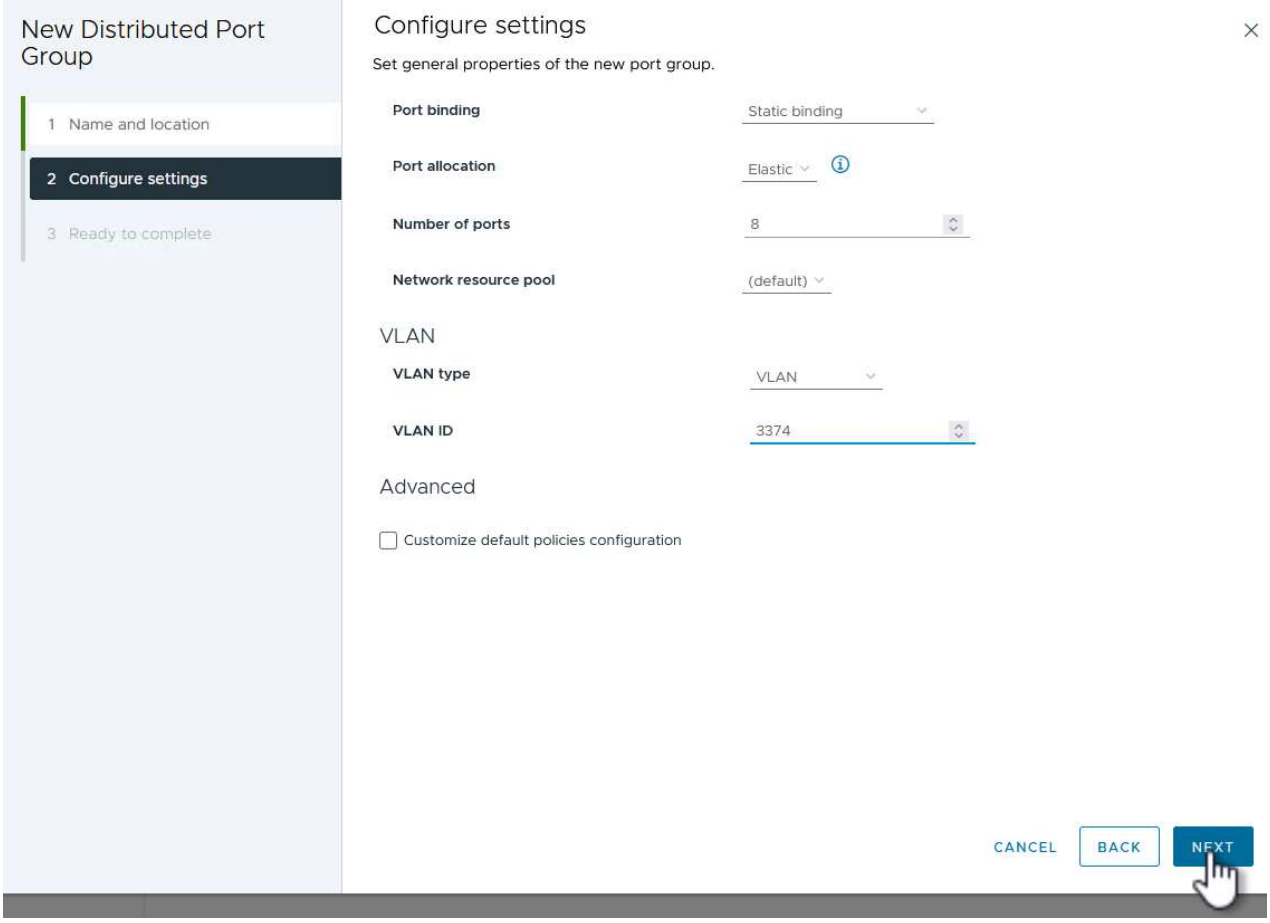
Erstellen Sie verteilte Portgruppen für NVME/TCP-Verkehr

Führen Sie die folgenden Schritte aus, um für jedes NVMe/TCP-Netzwerk eine neue verteilte Portgruppe zu erstellen:

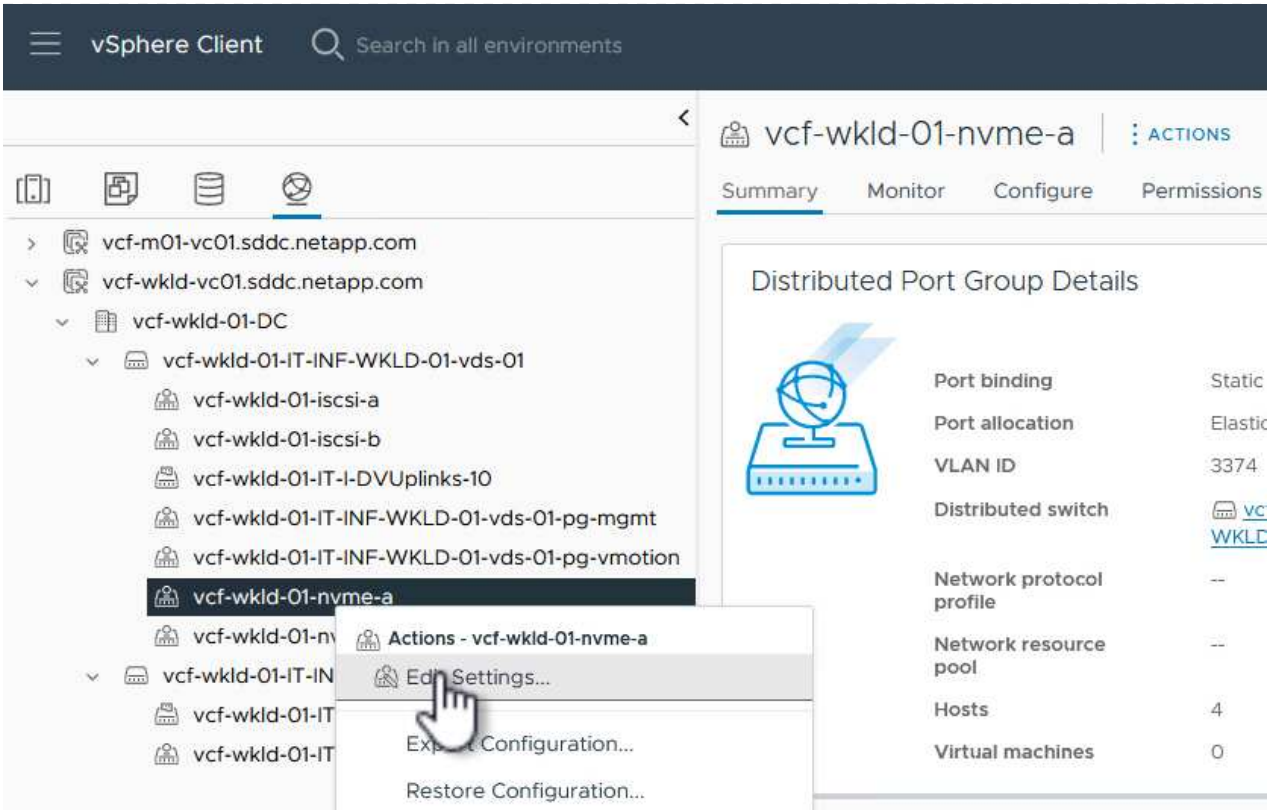
1. Navigieren Sie im vSphere-Client zu **Inventar > Netzwerk** für die Workloaddomäne. Navigieren Sie zum vorhandenen Distributed Switch und wählen Sie die Aktion zum Erstellen einer **Neuen verteilten Portgruppe…**.



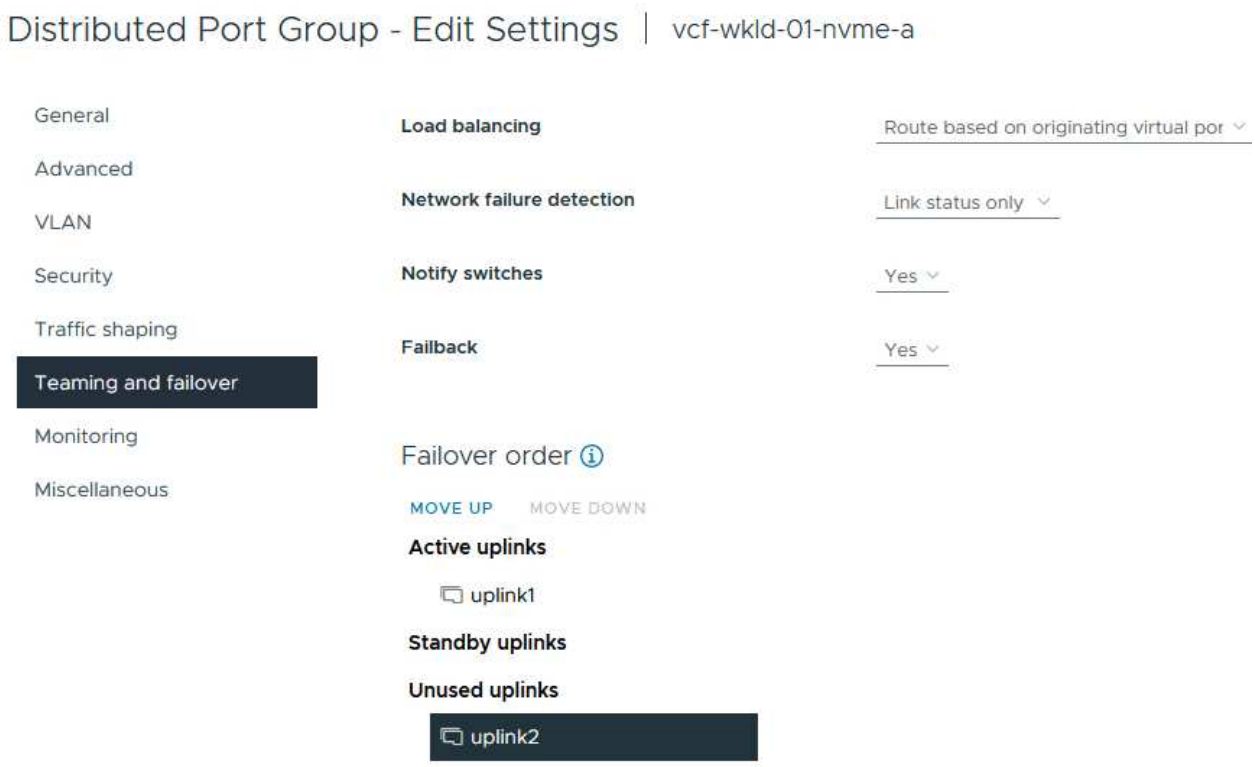
2. Geben Sie im Assistenten **Neue verteilte Portgruppe** einen Namen für die neue Portgruppe ein und klicken Sie auf **Weiter**, um fortzufahren.
3. Füllen Sie auf der Seite **Einstellungen konfigurieren** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige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



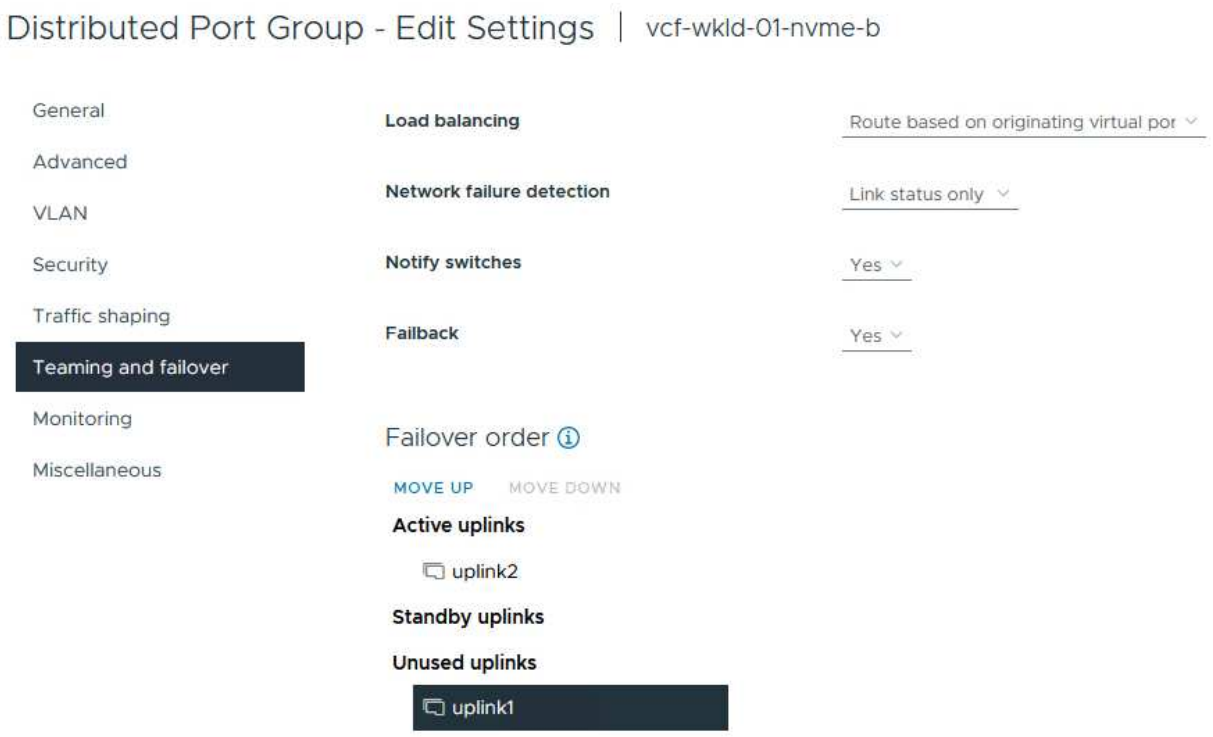
4. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Änderungen und klicken Sie auf **Fertig**, um die neue verteilte Portgruppe zu erstellen.
5. Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete NVMe/TCP-Netzwerk zu erstellen, und stellen Sie sicher, dass Sie die richtige **VLAN-ID** eingegeben haben.
6. Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion „Einstellungen bearbeiten…“ aus.



7. Navigieren Sie auf der Seite **Verteilte Portgruppe – Einstellungen bearbeiten** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **Nicht verwendete Uplinks** zu verschieben.



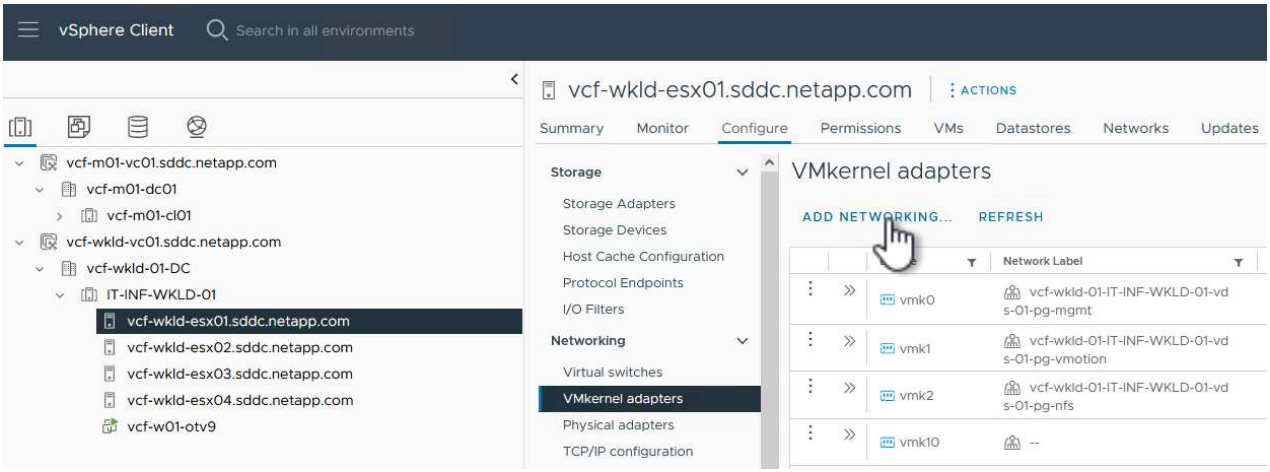
8. Wiederholen Sie diesen Schritt für die zweite NVMe/TCP-Portgruppe. Verschieben Sie dieses Mal jedoch **Uplink1** nach unten zu **Ungenutzte Uplinks**.



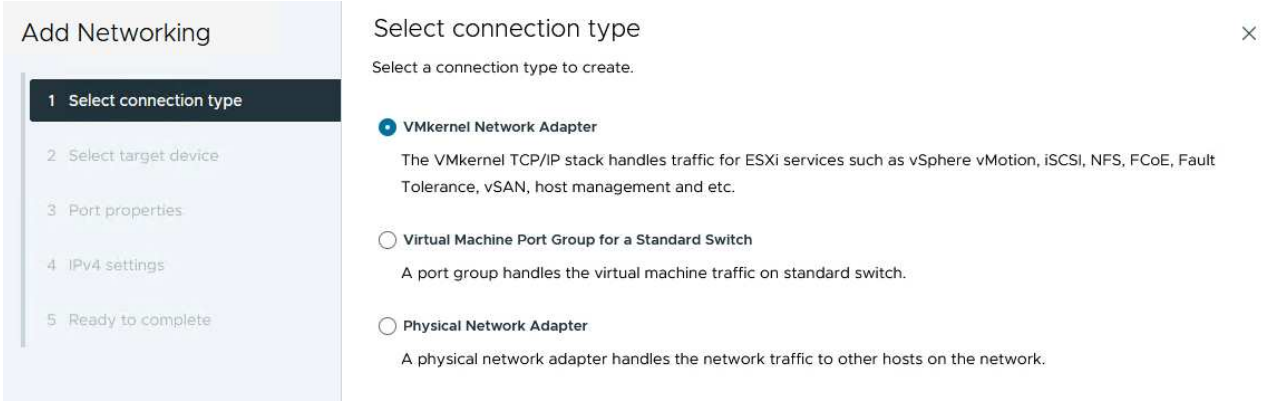
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

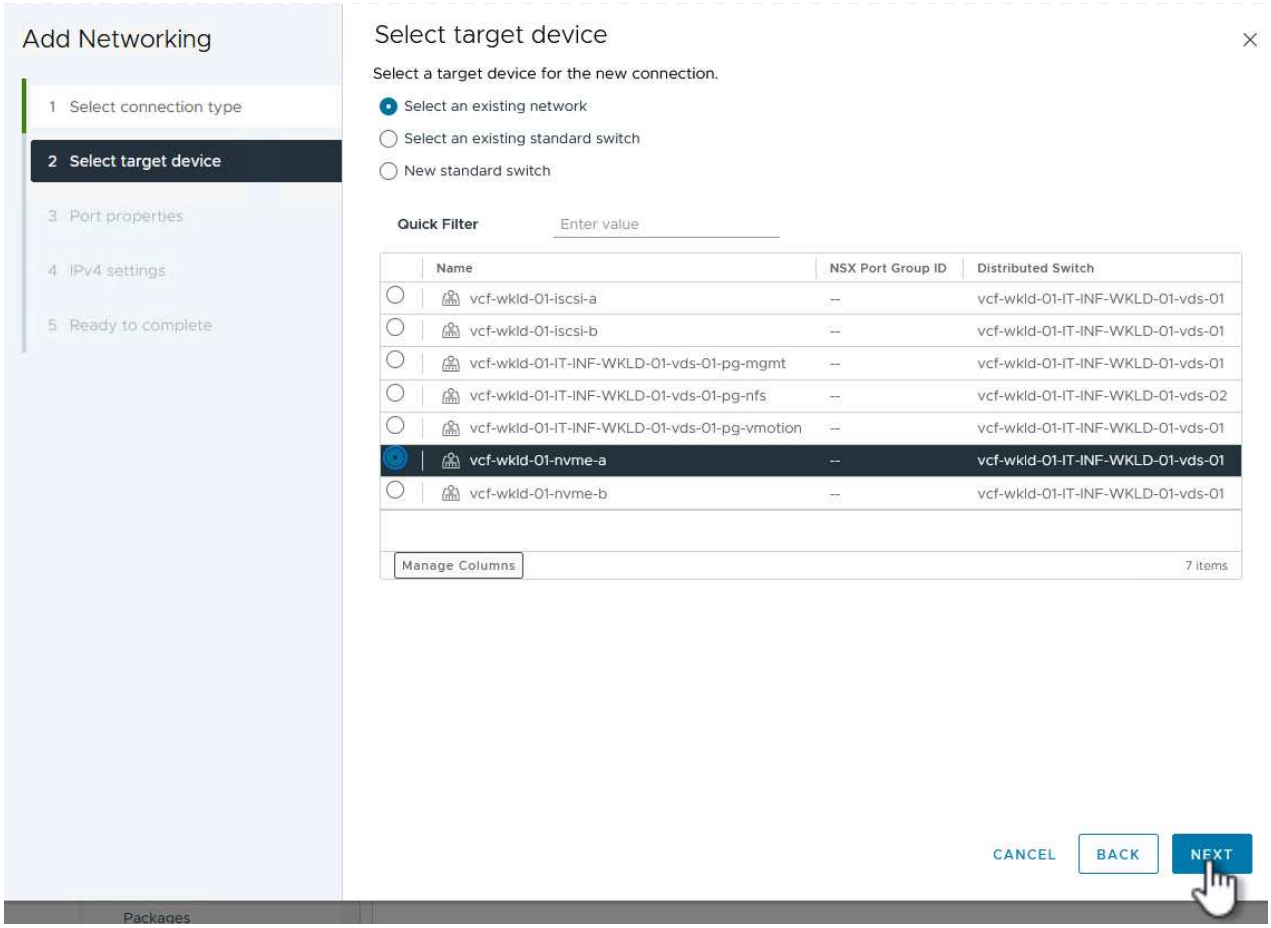
1. Navigieren Sie vom vSphere-Client zu einem der ESXi-Hosts im Workload-Domäneninventar. Wählen Sie auf der Registerkarte **Konfigurieren VMkernel-Adapter** aus und klicken Sie zum Starten auf **Netzwerk hinzufügen…**.



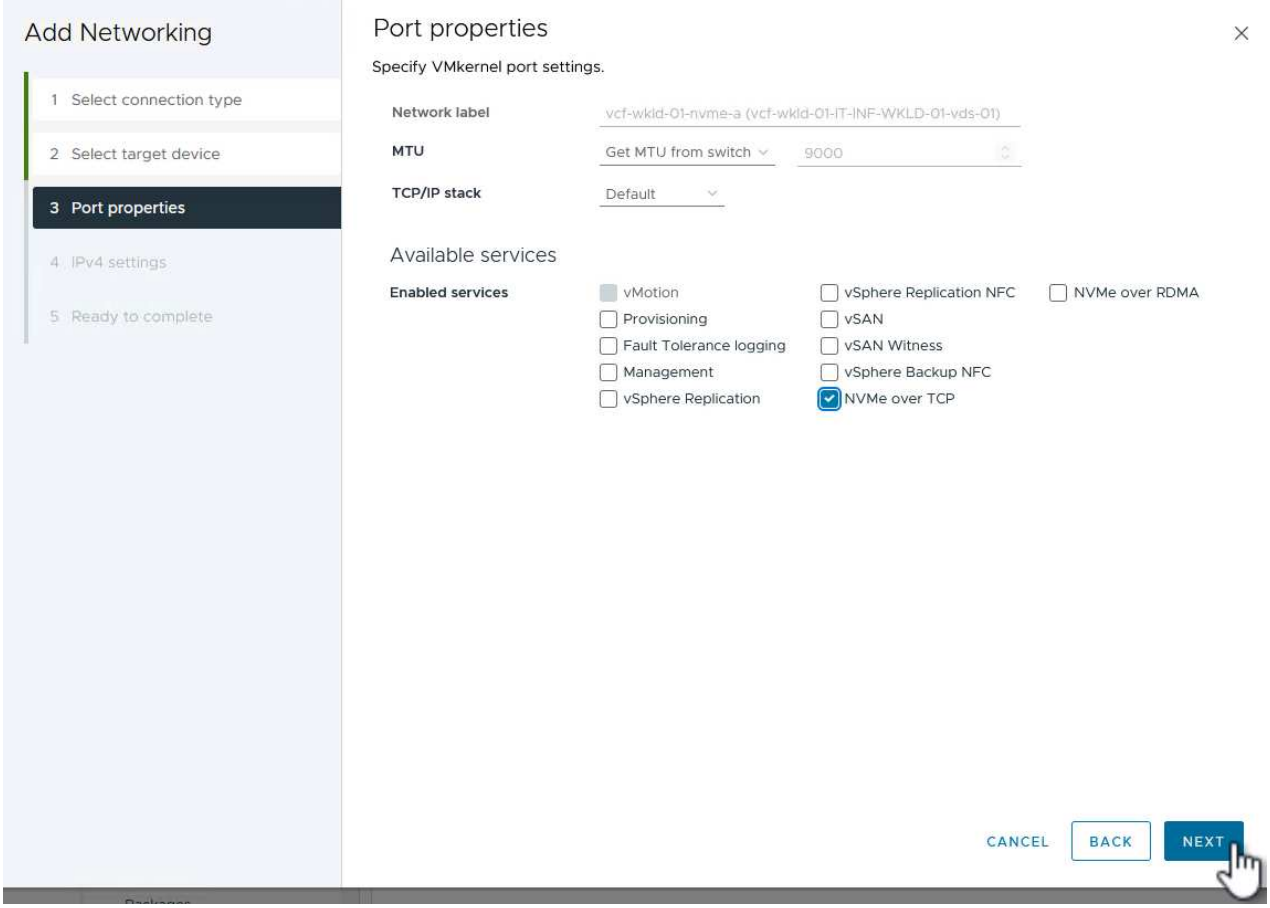
2. Wählen Sie im Fenster **Verbindungstyp auswählen VMkernel-Netzwerkadapter** und klicken Sie auf **Weiter**, um fortzufahren.



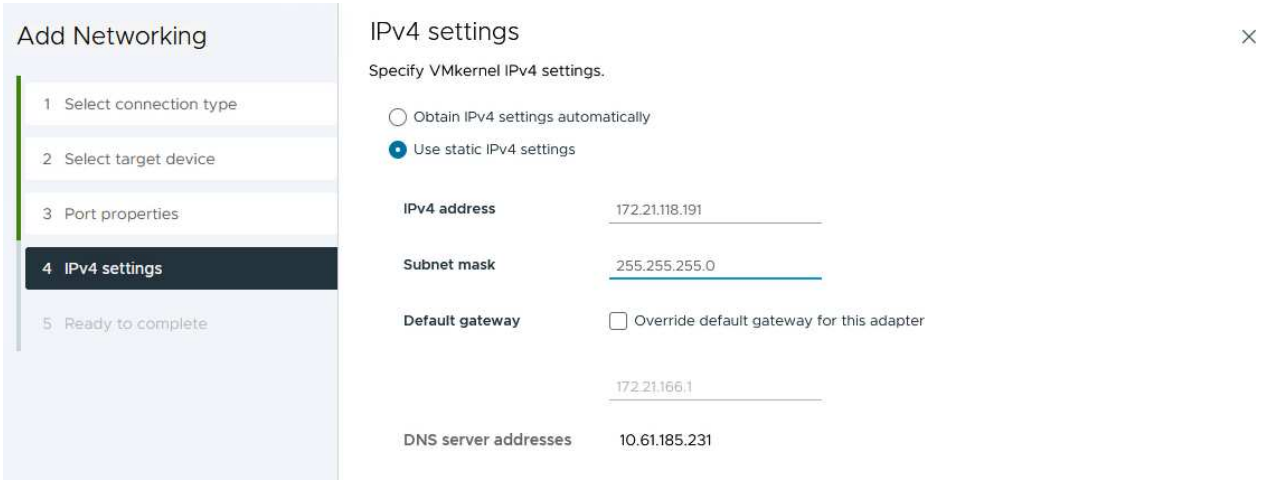
3. Wählen Sie auf der Seite **Zielgerät auswählen** eine der zuvor erstellten verteilten Portgruppen für iSCSI aus.



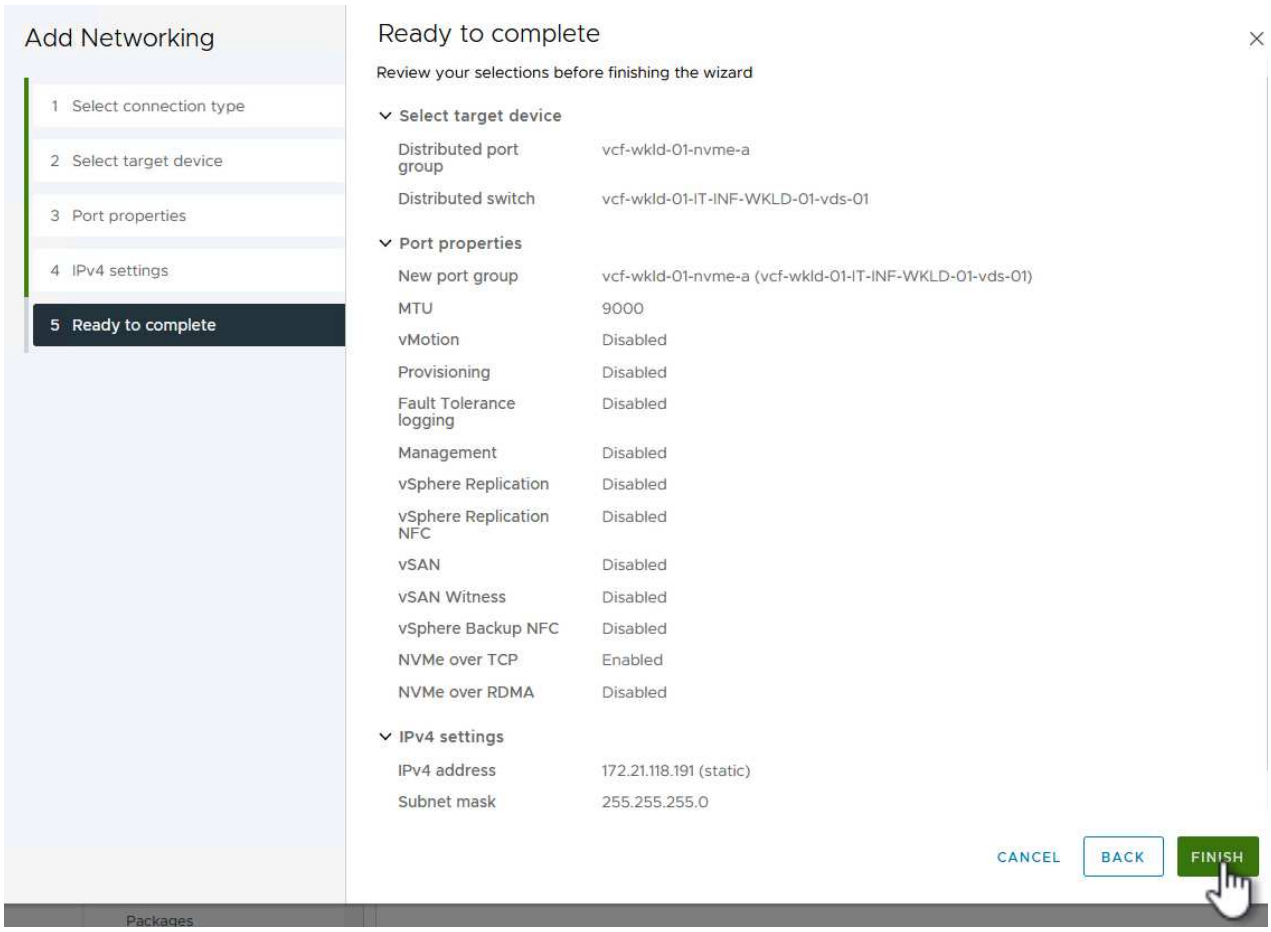
4. Klicken Sie auf der Seite **Porteigenschaften** auf das Kontrollkästchen für **NVMe über TCP** und klicken Sie auf **Weiter**, um fortzufahren.



5. Geben Sie auf der Seite **IPv4-Einstellungen** die **IP-Adresse** und **Subnetzmaske** ein und geben Sie eine neue Gateway-IP-Adresse an (nur falls erforderlich). Klicken Sie auf **Weiter**, um fortzufahren.



6. Überprüfen Sie Ihre Auswahl auf der Seite **Bereit zum Abschließen** und klicken Sie auf **Fertig**, um den VMkernel-Adapter zu erstellen.



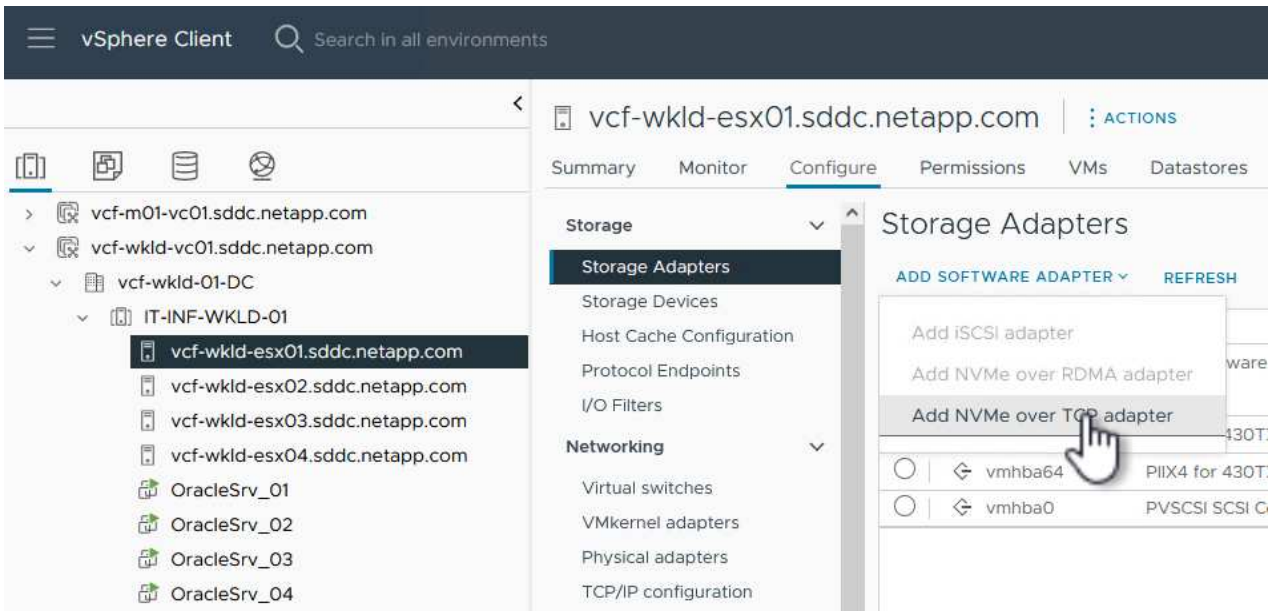
7. Wiederholen Sie diesen Vorgang, um einen VMkernel-Adapter für das zweite iSCSI-Netzwerk zu erstellen.

NVMe-over-TCP-Adapter hinzufügen

Auf jedem ESXi-Host im Workload-Domänencluster muss für jedes eingerichtete NVMe/TCP-Netzwerk, das für Speicherverkehr vorgesehen ist, ein NVMe-over-TCP-Softwareadapter installiert sein.

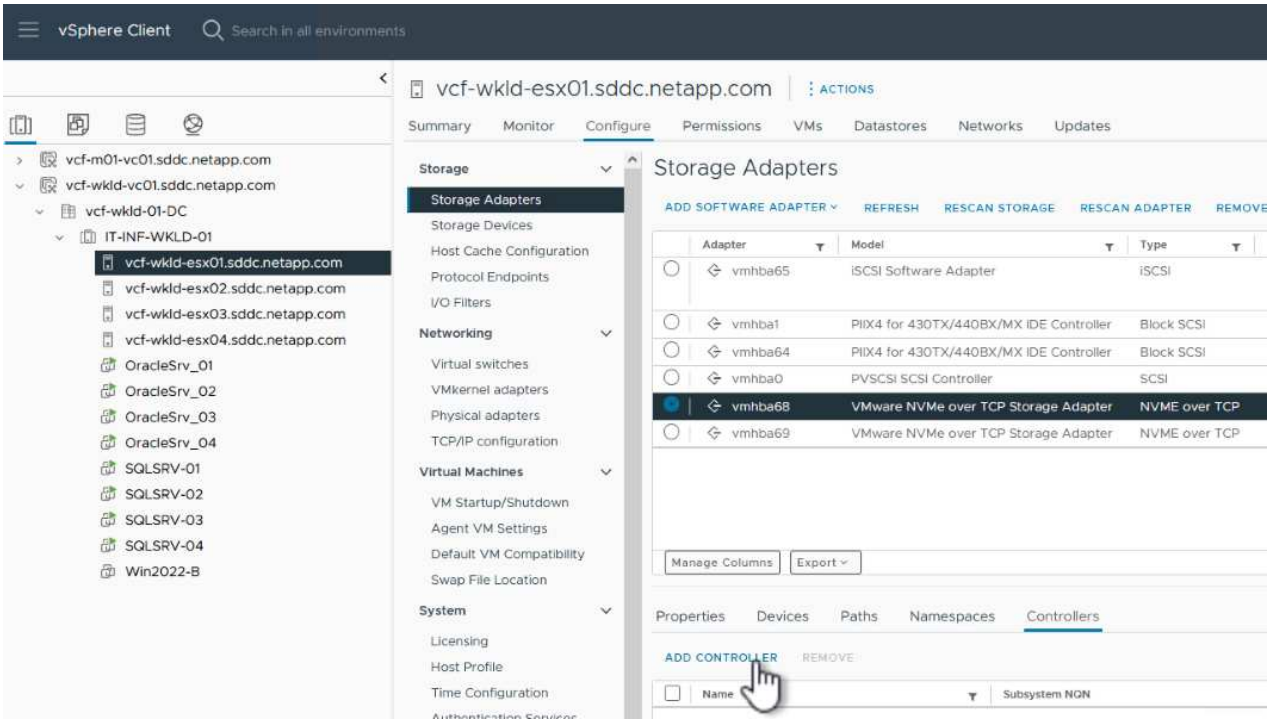
Führen Sie die folgenden Schritte aus, um NVMe-over-TCP-Adapter zu installieren und die NVMe-Controller zu ermitteln:

1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Klicken Sie auf der Registerkarte **Konfigurieren** im Menü auf **Speicheradapter** und wählen Sie dann im Dropdown-Menü **Softwareadapter hinzufügen** die Option **NVMe-over-TCP-Adapter hinzufügen**.

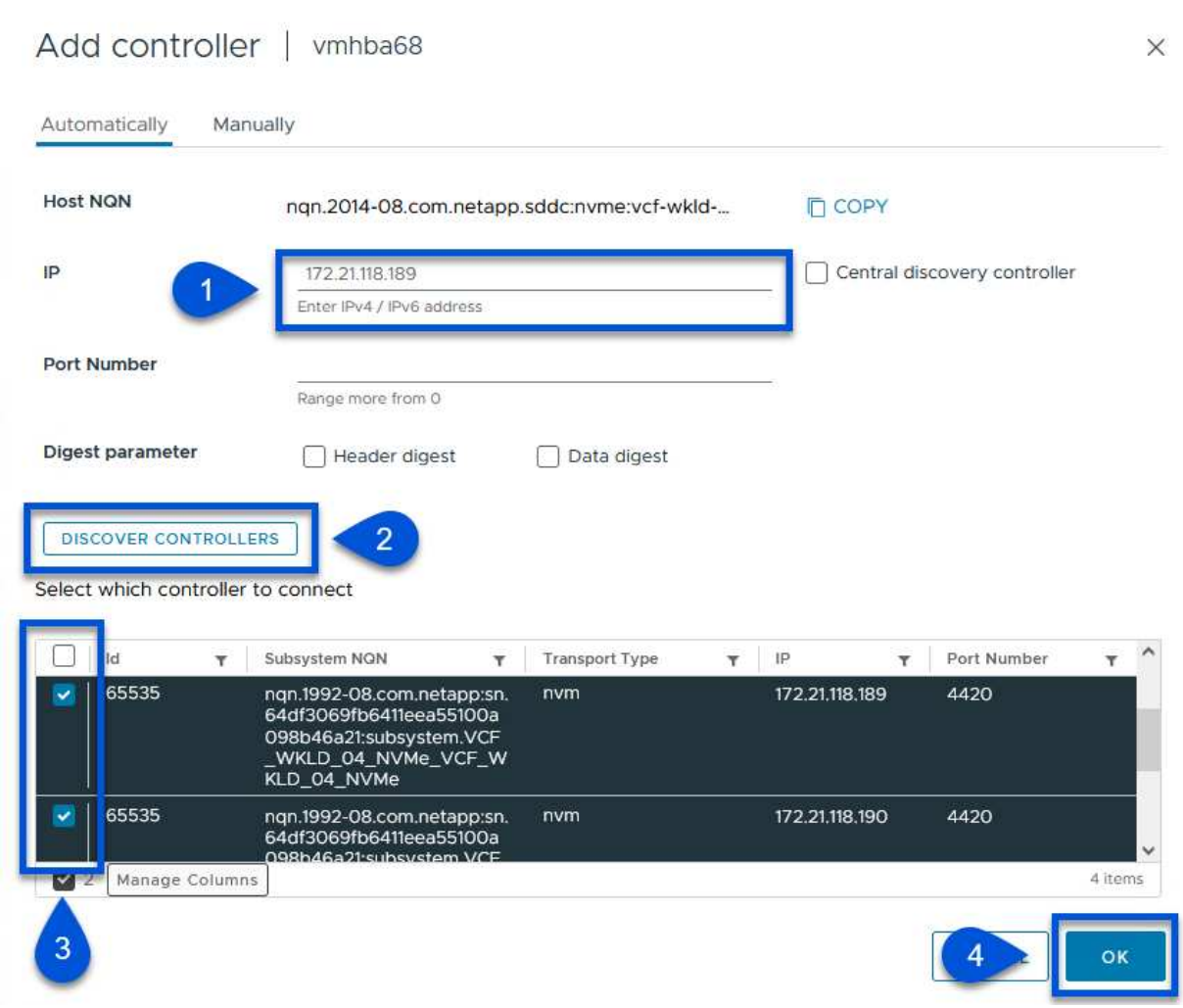


2. Rufen Sie im Fenster **Software-NVMe-over-TCP-Adapter hinzufügen** das Dropdown-Menü **Physischer Netzwerkadapter** auf und wählen Sie den richtigen physischen Netzwerkadapter aus, auf dem der NVMe-Adapter aktiviert werden soll.

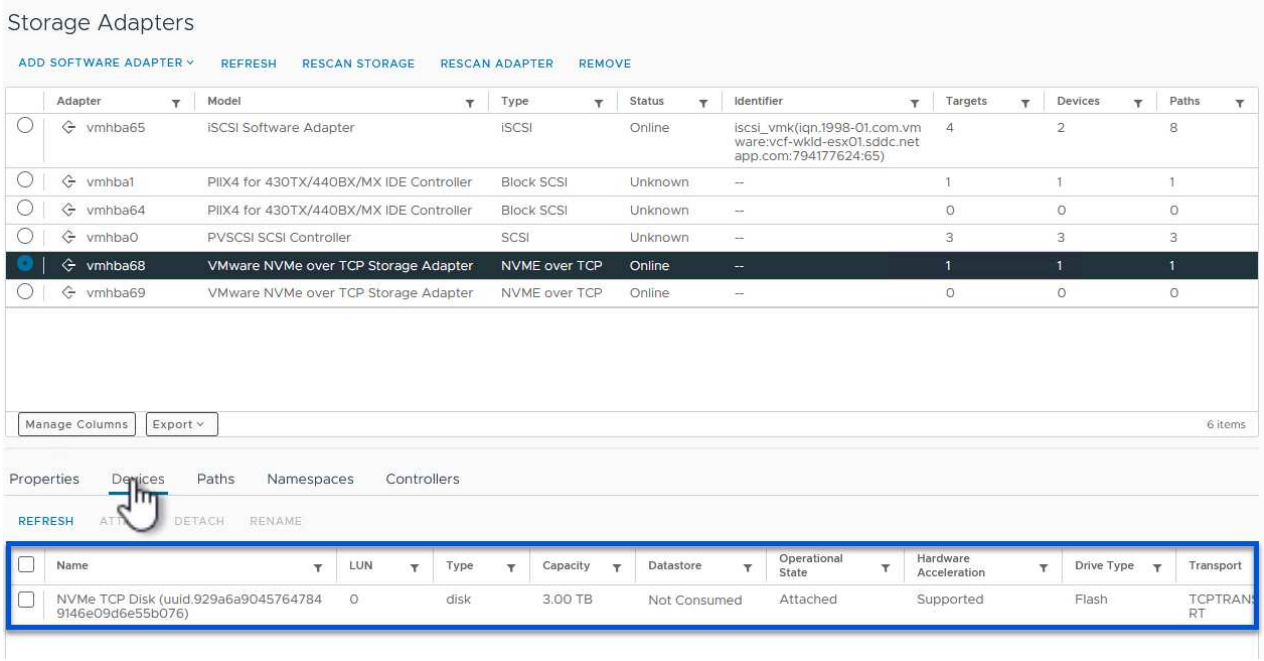
3. Wiederholen Sie diesen Vorgang für das zweite Netzwerk, das NVMe über TCP-Verkehr zugewiesen ist, und weisen Sie den richtigen physischen Adapter zu.
4. Wählen Sie einen der neu installierten NVMe-over-TCP-Adapter aus und wählen Sie auf der Registerkarte **Controller** die Option **Controller hinzufügen**.



5. Wählen Sie im Fenster **Controller hinzufügen** die Registerkarte **Automatisch** und führen Sie die folgenden Schritte aus.
   - Geben Sie eine IP-Adresse für eine der logischen SVM-Schnittstellen im selben Netzwerk ein wie der physische Adapter, der diesem NVMe-over-TCP-Adapter zugewiesen ist.
   - Klicken Sie auf die Schaltfläche **Controller erkennen**.
   - Aktivieren Sie in der Liste der erkannten Controller das Kontrollkästchen für die beiden Controller, deren Netzwerkadressen mit diesem NVMe-over-TCP-Adapter übereinstimmen.
   - Klicken Sie auf die Schaltfläche **OK**, um die ausgewählten Controller hinzuzufügen.



6. Nach einigen Sekunden sollte der NVMe-Namespace auf der Registerkarte „Geräte“ angezeigt werden.

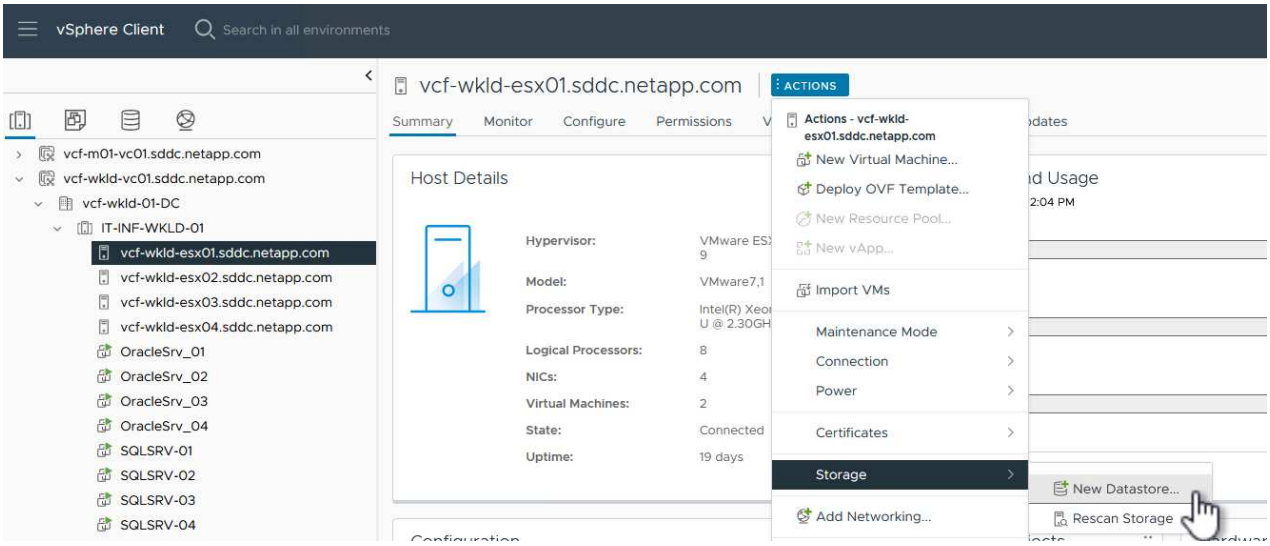


7. Wiederholen Sie diesen Vorgang, um einen NVMe-over-TCP-Adapter für das zweite für NVMe/TCP-Verkehr eingerichtete Netzwerk zu erstellen.

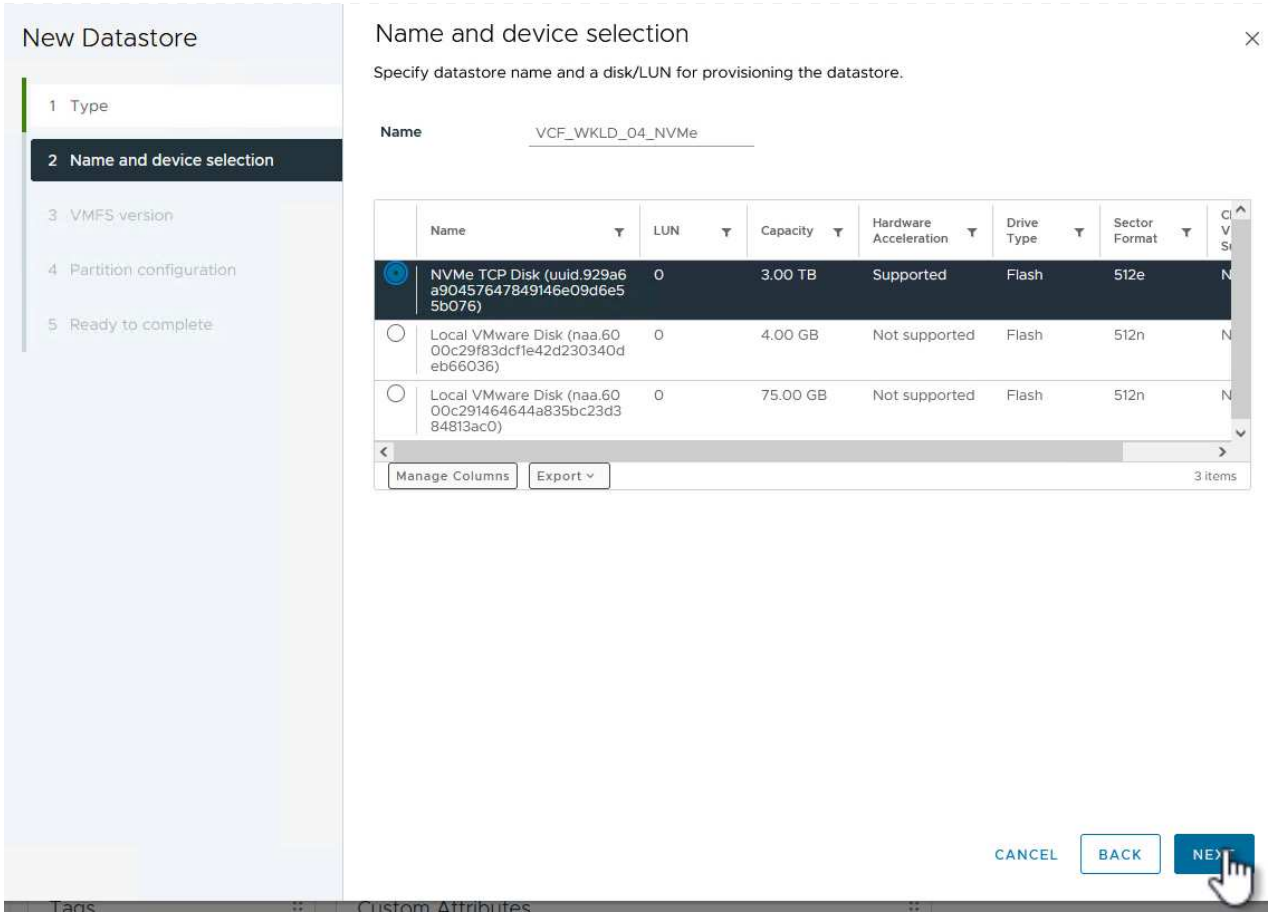
Bereitstellen eines NVMe-über-TCP-Datenspeichers

Führen Sie die folgenden Schritte aus, um einen VMFS-Datenspeicher im NVMe-Namespace zu erstellen:

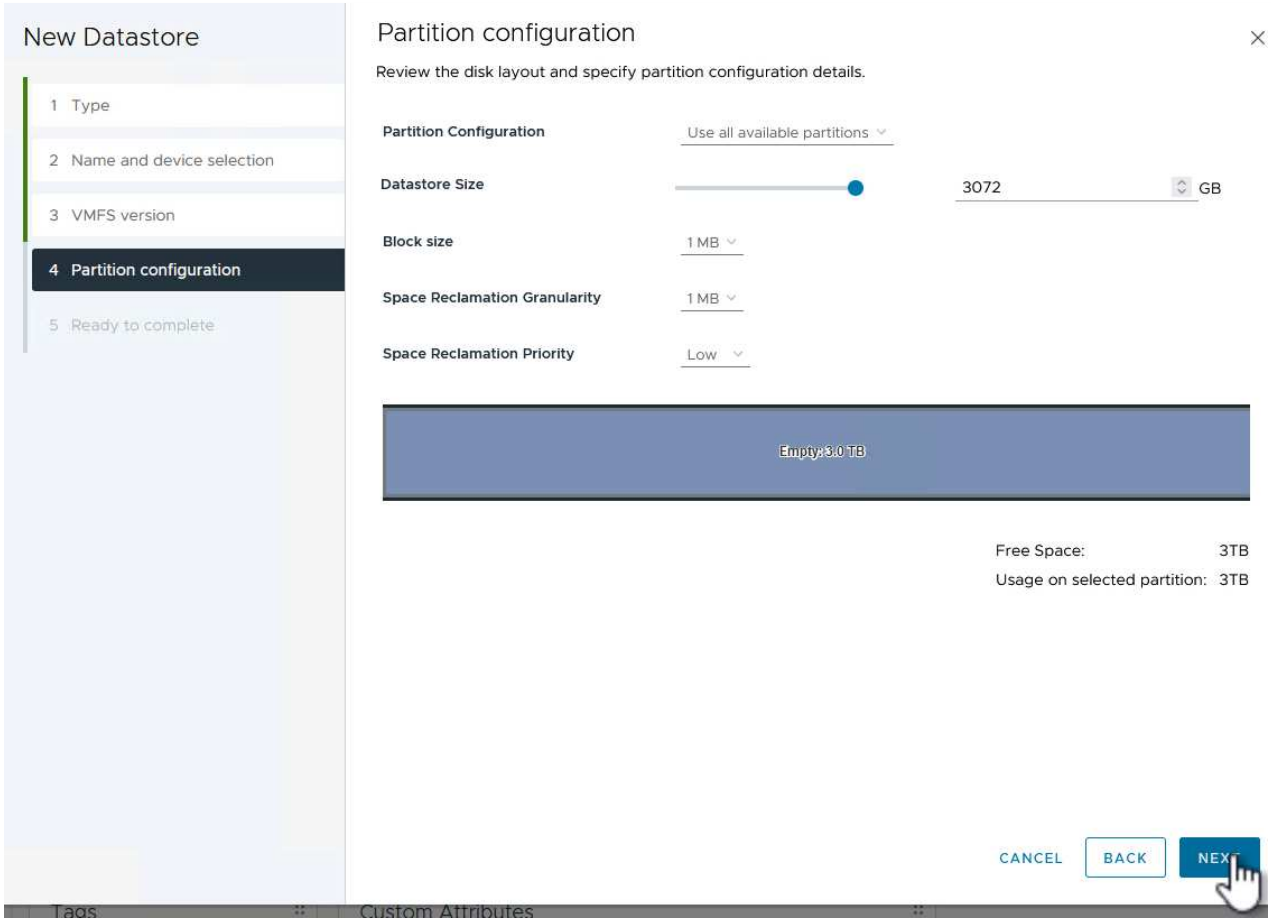
1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Wählen Sie im Menü **Aktionen** die Option **Speicher > Neuer Datenspeicher…**.



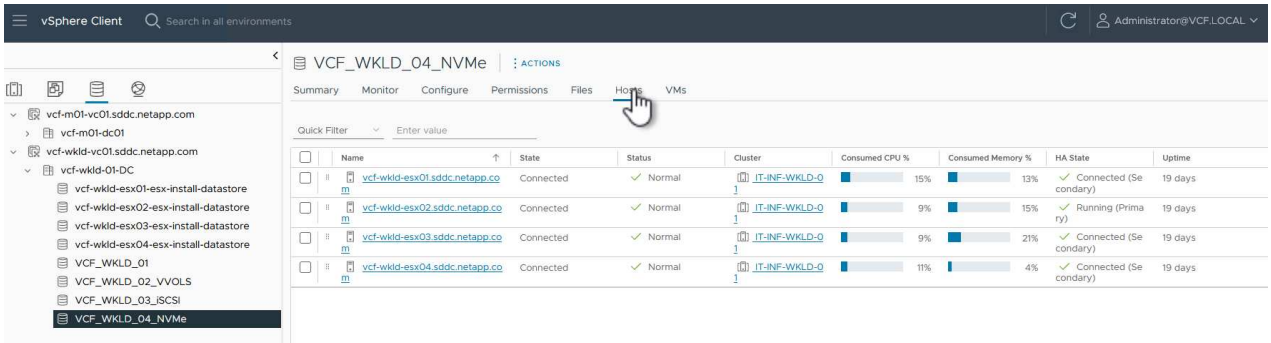
2. Wählen Sie im Assistenten **Neuer Datenspeicher** als Typ **VMFS** aus. Klicken Sie auf **Weiter**, um fortzufahren.
3. Geben Sie auf der Seite **Namens- und Geräteauswahl** einen Namen für den Datenspeicher ein und wählen Sie den NVMe-Namespace aus der Liste der verfügbaren Geräte aus.



4. Wählen Sie auf der Seite **VMFS-Version** die VMFS-Version für den Datenspeicher aus.
5. Nehmen Sie auf der Seite **Partitionskonfiguration** die gewünschten Änderungen am Standardpartitionsschema vor. Klicken Sie auf **Weiter**, um fortzufahren.



6. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Zusammenfassung und klicken Sie auf **Fertig**, um den Datenspeicher zu erstellen.
7. Navigieren Sie zum neuen Datenspeicher im Inventar und klicken Sie auf die Registerkarte **Hosts**. Bei korrekter Konfiguration sollten alle ESXi-Hosts im Cluster aufgelistet sein und Zugriff auf den neuen Datenspeicher haben.



Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Fügen Sie einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher zu VI-Workload-Domänen hinzu

In diesem Anwendungsfall beschreiben wir das Verfahren zum Konfigurieren eines VMFS-Datenspeichers mit Fiber Channel (FC) als zusätzlichen Speicher für eine VMware Cloud Foundation (VCF) Virtual Infrastructure (VI)-Workloaddomäne. Dieses Verfahren fasst die Bereitstellung von ONTAP Tools für VMware vSphere, die Registrierung des VI-Workload-vCenter-Servers, die Definition des Speicher-Backends und die Bereitstellung des FC-Datenspeichers zusammen.

Vorteile von Fibre Channel

Hohe Leistung: FC bietet Hochgeschwindigkeitsdatenübertragungsraten und ist daher ideal für Anwendungen, die einen schnellen und zuverlässigen Zugriff auf große Datenmengen erfordern.

Geringe Latenz: Sehr geringe Latenz, die für leistungssensible Anwendungen wie Datenbanken und virtualisierte Umgebungen entscheidend ist.

Zuverlässigkeit: FC-Netzwerke sind für ihre Robustheit und Zuverlässigkeit bekannt und verfügen über Funktionen wie integrierte Redundanz und Fehlerkorrektur.

Dedizierte Bandbreite: FC bietet dedizierte Bandbreite für Speicherverkehr und reduziert so das Risiko einer Netzwerküberlastung.

Weitere Informationen zur Verwendung von Fibre Channel mit NetApp -Speichersystemen finden Sie unter "SAN-Bereitstellung mit FC" .

Szenarioübersicht

Der VCF-Zusatzdatenspeicher wird im Rahmen der Day-2-Operationen mithilfe von vCenter bereitgestellt. Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Bereitstellung von ONTAP -Tools in der Verwaltungsdomäne
- Registrieren Sie VI-Workload-vCenter-Server bei ONTAP -Tools
- Definieren Sie das Storage-Backend im ONTAP -Tools-Plugin für VMware vSphere
- Bereitstellen von VMFS auf FC-Transport

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP AFF oder ASA Speichersystem mit FC-Ports, die mit FC-Switches verbunden sind.
- SVM mit FC-Lifs erstellt.
- vSphere mit FC-HBAs, die mit FC-Switches verbunden sind.
- Auf FC-Switches ist eine einzelne Initiator-Ziel-Zonierung konfiguriert.

> Verwenden Sie in der Zonenkonfiguration die logische SVM FC-Schnittstelle anstelle physischer FC-Ports auf ONTAP -Systemen.

NetApp empfiehlt Multipath für FC-LUNs.

Ausführliche Informationen zur Konfiguration von Fibre Channel auf ONTAP Speichersystemen finden Sie unter "SAN-Speicherverwaltung" in der ONTAP 9-Dokumentation.

Weitere Informationen zur Verwendung von VMFS mit ONTAP Speichersystemen finden Sie im"Bereitstellungshandbuch für VMFS" .

Bereitstellungsschritte für die VI-Workloaddomäne

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und damit einen VMFS-Datenspeicher in der VCF VI-Workloaddomäne zu erstellen:

- "Registrieren Sie VI Workload vCenter, um das vCenter-Plugin zu aktivieren"
- "Definieren Sie das Speicher-Backend mithilfe der vSphere-Clientschnittstelle"
- "Bereitstellen von VMFS auf FC"

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Videodemo für diese Lösung

VMFS(FC)-Datenspeicher als zusätzlicher Speicher für die VCF-Verwaltungsdomäne

Schützen Sie VCF mit SnapCenter

Erfahren Sie mehr über den Schutz von VCF-Workload-Domänen mit dem SnapCenter -Plug-in für VMware vSphere

Informieren Sie sich über die NetApp -Lösungen, die Sie zum Schutz von VMware Cloud Foundation (VCF)-Workloads mit dem SnapCenter Plug-in for VMware vSphere verwenden können. Dieses Plug-in vereinfacht die Sicherung und Wiederherstellung, gewährleistet anwendungskonsistente Sicherungen und optimiert den Speicher mit den Effizienztechnologien von NetApp.

Es unterstützt automatisierte Arbeitsabläufe und skalierbare Vorgänge und bietet gleichzeitig eine nahtlose Integration mit dem vSphere-Client. Mit der SnapMirror -Replikation, die eine sekundäre Sicherung vor Ort oder in der Cloud ermöglicht, bietet es robusten Datenschutz und betriebliche Effizienz in virtualisierten Umgebungen.

Weitere Einzelheiten finden Sie in den folgenden Lösungen.

- "Schützen der VCF-Workloaddomäne"
- "Schützen Sie mehrere VCF-Workloaddomänen"
- "Schützen Sie die VCF-Workload-Domäne mit NVMe"
- "3-2-1-Datenschutz für VMware mit SnapCenter -Plug-in und BlueXP backup and recovery für VMs"

Schützen Sie eine VCF-Workloaddomäne mit dem SnapCenter -Plug-in für VMware vSphere

In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung des SnapCenter -Plug-Ins für VMware vSphere zum Sichern und Wiederherstellen von VMs und Datenspeichern in einer VMware Cloud Foundation (VCF)-Workloaddomäne. Dieses Verfahren fasst die Bereitstellung des SnapCenter -Plug-Ins für VMware vSphere, das Hinzufügen von Speichersystemen, das Erstellen von Sicherungsrichtlinien und das Durchführen von Wiederherstellungen von VMs und Dateien zusammen.

iSCSI wird in dieser Lösung als Speicherprotokoll für den VMFS-Datenspeicher verwendet.

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Stellen Sie das SnapCenter Plug-in for VMware vSphere (SCV) in der VI-Workloaddomäne bereit.
- Fügen Sie SCV Speichersysteme hinzu.
- Erstellen Sie Sicherungsrichtlinien in SCV.
- Erstellen Sie Ressourcengruppen in SCV.
- Verwenden Sie SCV, um Datenspeicher oder bestimmte VMs zu sichern.
- Verwenden Sie SCV, um VMs an einem anderen Speicherort im Cluster wiederherzustellen.
- Verwenden Sie SCV, um Dateien in einem Windows-Dateisystem wiederherzustellen.

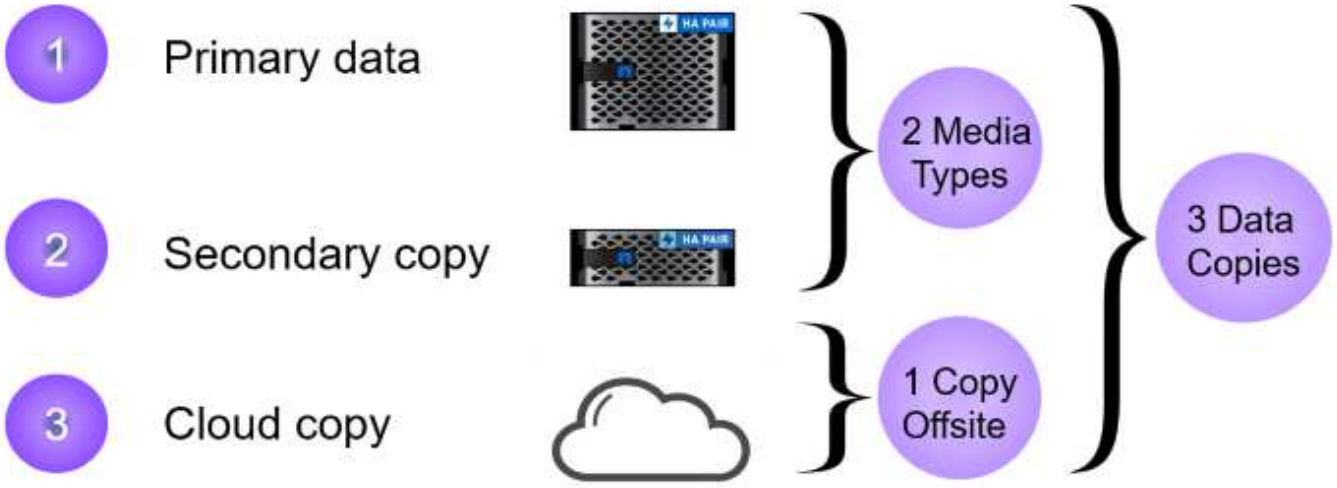
Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA -Speichersystem mit iSCSI VMFS-Datenspeichern, die dem Workload-Domänencluster zugewiesen sind.
- Ein sekundäres ONTAP Speichersystem, das für den Empfang sekundärer Backups mit SnapMirror konfiguriert ist.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf den vSphere-Client kann zugegriffen werden.
- Zuvor wurde eine VI-Workloaddomäne bereitgestellt.
- Auf dem Cluster, den SCV schützen soll, sind virtuelle Maschinen vorhanden.

Informationen zum Konfigurieren von iSCSI-VMFS-Datenspeichern als zusätzlicher Speicher finden Sie unter "**iSCSI als zusätzlicher Speicher für Managementdomänen mit ONTAP Tools für VMware**" in dieser Dokumentation. Der Prozess zur Verwendung von OTV zum Bereitstellen von Datenspeichern ist für Verwaltungs- und Workloaddomänen identisch.

> Zusätzlich zur Replikation von mit SCV erstellten Backups auf sekundären Speicher können mithilfe von NetApp BlueXP backup and recovery für VMs externe Kopien der Daten auf Objektspeicher bei einem der drei (3) führenden Cloud-Anbieter erstellt werden. Weitere Informationen finden Sie in der Lösung"3-2-1-Datenschutz für VMware mit SnapCenter -Plug-in und BlueXP backup and recovery für VMs" .



Bereitstellungsschritte

Führen Sie die folgenden Schritte aus, um das SnapCenter -Plug-in bereitzustellen und damit Sicherungen zu erstellen und VMs und Datenspeicher wiederherzustellen:

Bereitstellen und Verwenden von SCV zum Schutz von Daten in einer VI-Workloaddomäne

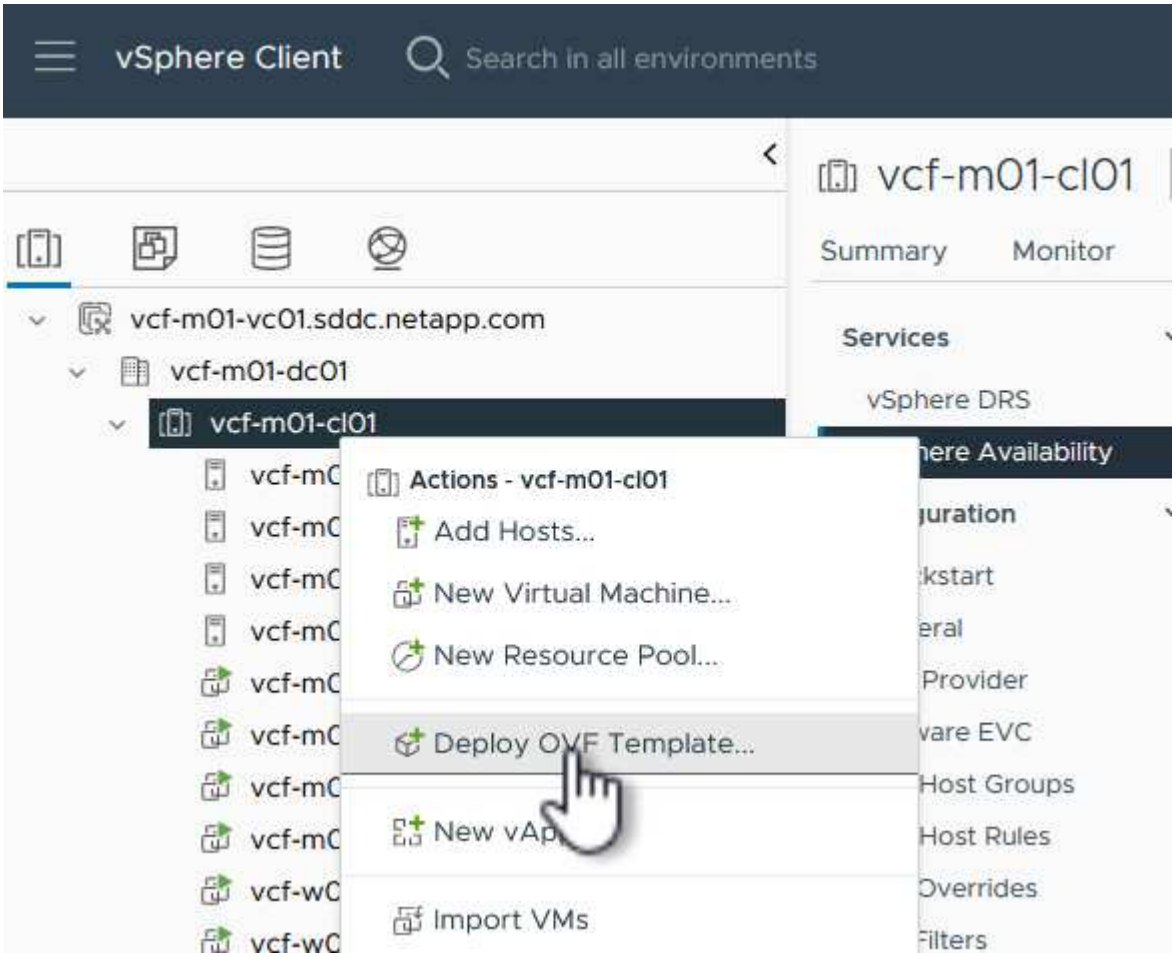
Führen Sie die folgenden Schritte aus, um SCV bereitzustellen, zu konfigurieren und zum Schutz von Daten in einer VI-Workloaddomäne zu verwenden:

Bereitstellen des SnapCenter Plug-in for VMware vSphere

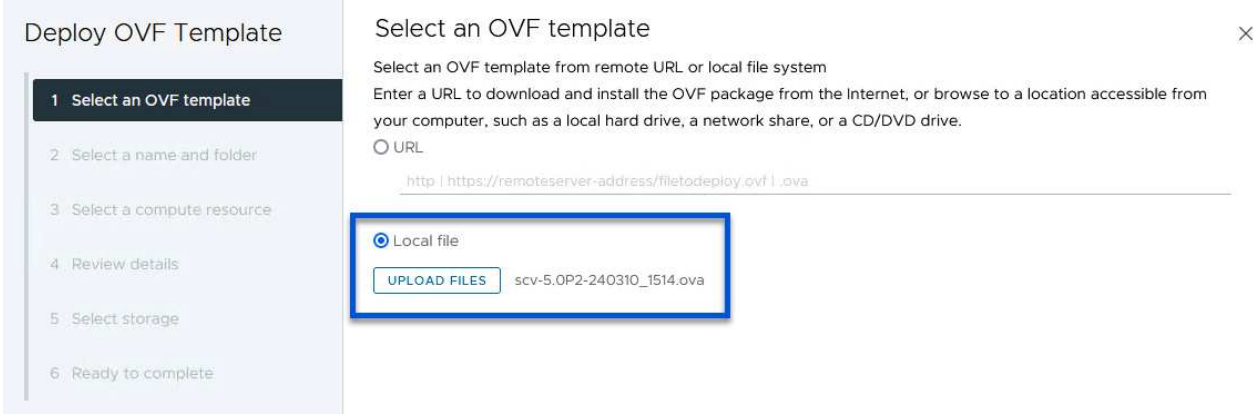
Das SnapCenter Plug-in wird in der VCF-Verwaltungsdomäne gehostet, ist aber beim vCenter für die VI-Workloaddomäne registriert. Für jede vCenter-Instanz ist eine SCV-Instanz erforderlich. Bedenken Sie, dass eine Workload-Domäne mehrere Cluster umfassen kann, die von einer einzigen vCenter-Instanz verwaltet werden.

Führen Sie vom vCenter-Client aus die folgenden Schritte aus, um SCV in der VI-Workloaddomäne bereitzustellen:

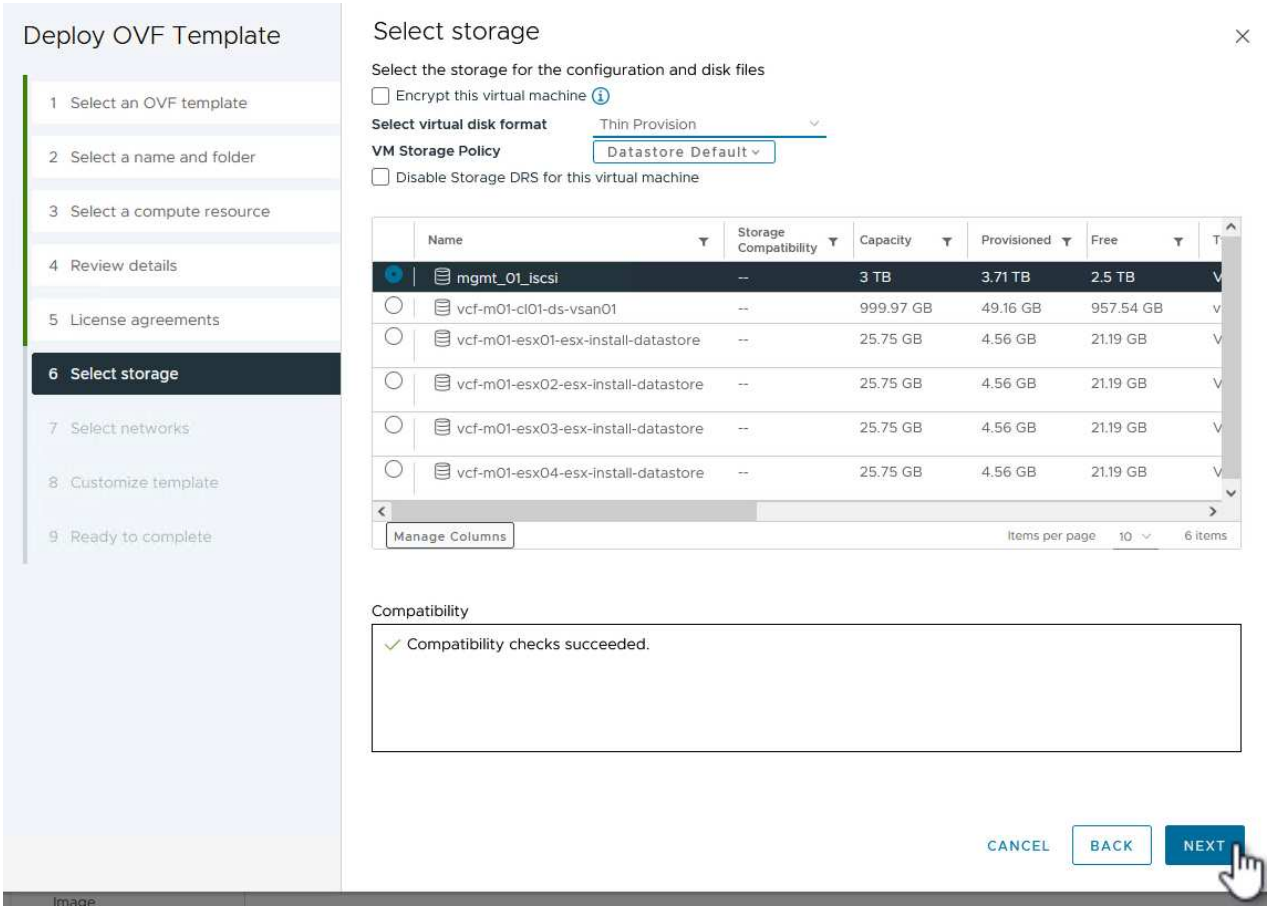
1. Laden Sie die OVA-Datei für die SCV-Bereitstellung aus dem Downloadbereich der NetApp Support-Site herunter"**HIER**" .
2. Wählen Sie im vCenter-Client der Verwaltungsdomäne „OVF-Vorlage bereitstellen…“ aus.



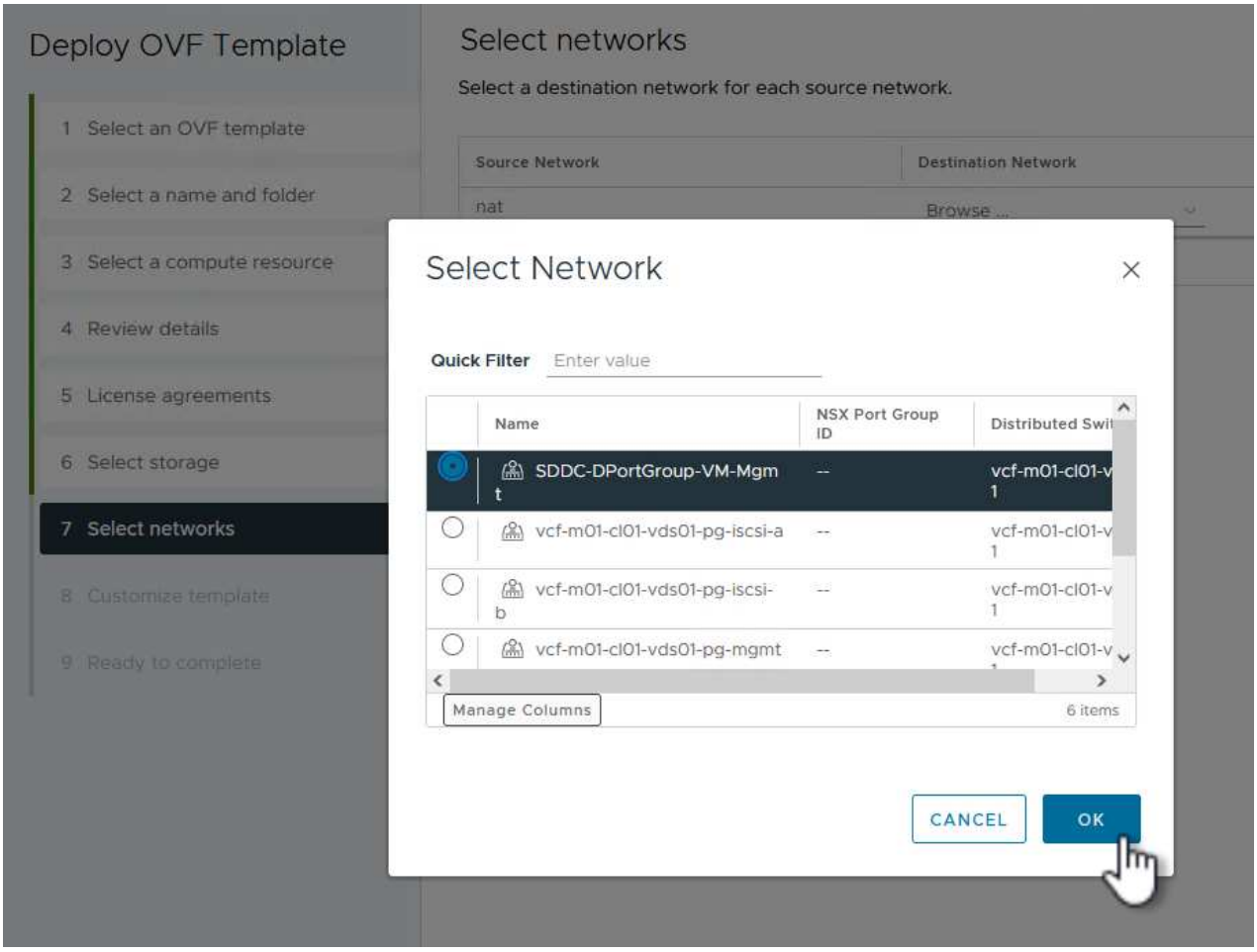
3. Klicken Sie im Assistenten **OVF-Vorlage bereitstellen** auf das Optionsfeld **Lokale Datei** und wählen Sie dann das Hochladen der zuvor heruntergeladenen OVF-Vorlage aus. Klicken Sie auf **Weiter**, um fortzufahren.



4. Geben Sie auf der Seite **Name und Ordner auswählen** einen Namen für die SCV-Datenbroker-VM und einen Ordner in der Verwaltungsdomäne an. Klicken Sie auf **Weiter**, um fortzufahren.
5. Wählen Sie auf der Seite **Wählen Sie eine Rechenressource aus** den Verwaltungsdomänencluster oder einen bestimmten ESXi-Host innerhalb des Clusters aus, auf dem die VM installiert werden soll.
6. Überprüfen Sie die Informationen zur OVF-Vorlage auf der Seite **Details überprüfen** und stimmen Sie den Lizenzbedingungen auf der Seite **Lizenzvereinbarungen** zu.
7. Wählen Sie auf der Seite **Speicher auswählen** den Datenspeicher aus, in dem die VM installiert werden soll, und wählen Sie das **virtuelle Datenträgerformat** und die **VM-Speicherrichtlinie** aus. Bei dieser Lösung wird die VM auf einem iSCSI-VMFS-Datenspeicher installiert, der sich auf einem ONTAP -Speichersystem befindet, wie zuvor in einem separaten Abschnitt dieser Dokumentation beschrieben. Klicken Sie auf **Weiter**, um fortzufahren.



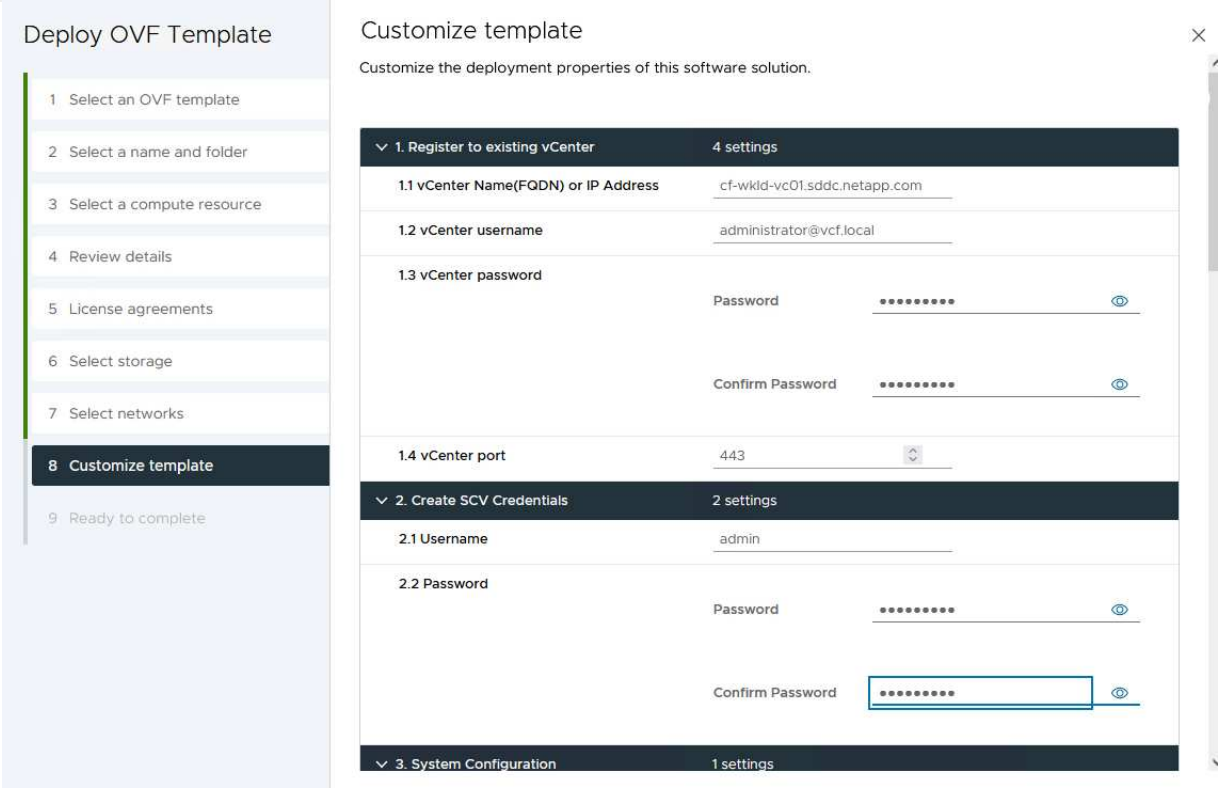
8. Wählen Sie auf der Seite **Netzwerk auswählen** das Verwaltungsnetzwerk aus, das mit der vCenter-Appliance der Workload-Domäne und den primären und sekundären ONTAP Speichersystemen kommunizieren kann.

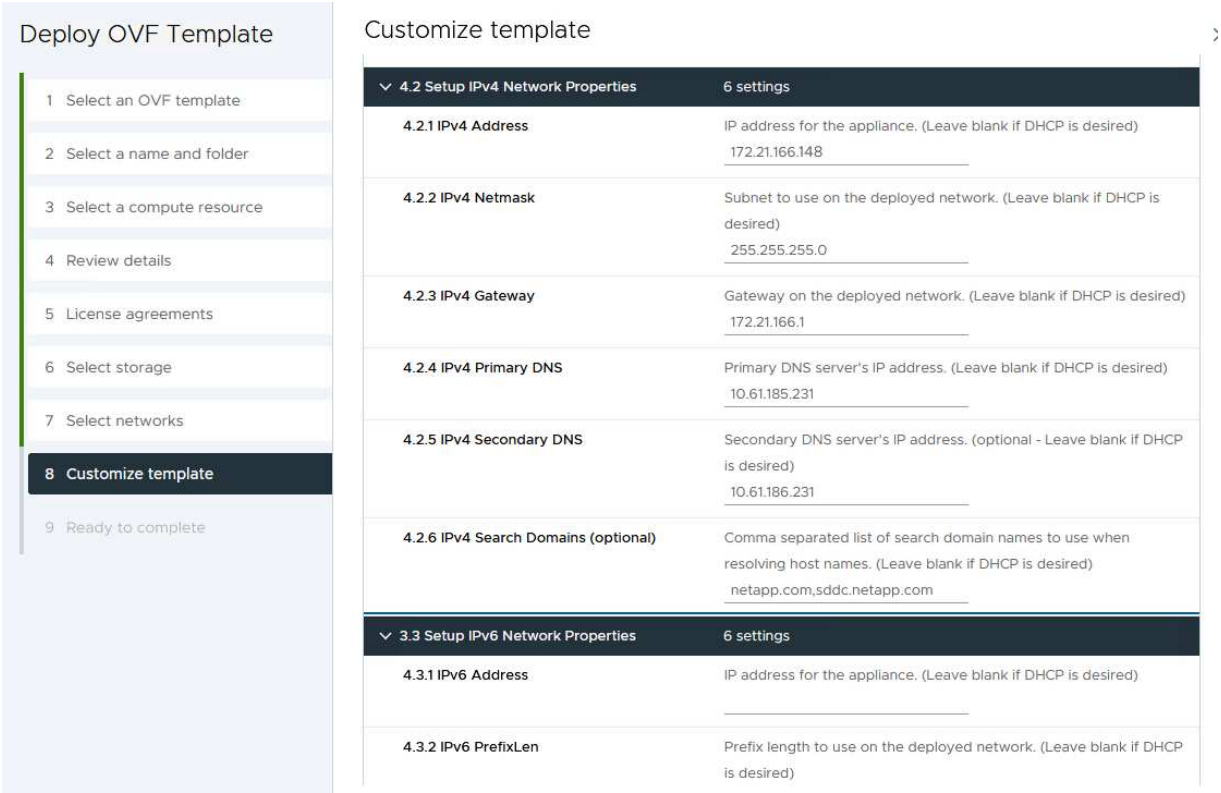


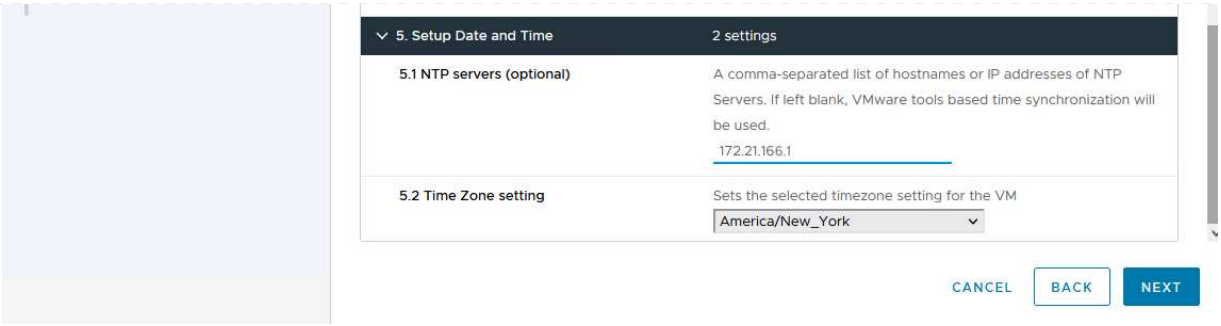
9. Geben Sie auf der Seite **Vorlage anpassen** alle für die Bereitstellung erforderlichen Informationen ein:

   - FQDN oder IP und Anmeldeinformationen für die vCenter-Appliance der Workloaddomäne.
   - Anmeldeinformationen für das SCV-Administratorkonto.
   - Anmeldeinformationen für das SCV-Wartungskonto.
   - Details zu den IPv4-Netzwerkeigenschaften (IPv6 kann ebenfalls verwendet werden).
   - Datums- und Uhrzeiteinstellungen.

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


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
Customize the deployment properties of this software solution.
1. Register to existing vCenter
4 settings
1.1 vCenter Name(FQDN) or IP Address
cf-wkld-vc01.sddc.netapp.com
1.2 vCenter username
administrator@vcf.local
1.3 vCenter password
Password
Confirm Password
1.4 vCenter port
443
2. Create SCV Credentials
2 settings
2.1 Username
admin
2.2 Password
Password
Confirm Password
3. System Configuration
1 settings


Deploy OVF Template
1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 License agreements
6 Select storage
7 Select networks
8 Customize template
9 Ready to complete
Customize template
4.2 Setup IPv4 Network Properties
6 settings
4.2.1 IPv4 Address
IP address for the appliance. (Leave blank if DHCP is desired)
172.21.166.148
4.2.2 IPv4 Netmask
Subnet to use on the deployed network. (Leave blank if DHCP is desired)
255.255.255.0
4.2.3 IPv4 Gateway
Gateway on the deployed network. (Leave blank if DHCP is desired)
172.21.166.1
4.2.4 IPv4 Primary DNS
Primary DNS server's IP address. (Leave blank if DHCP is desired)
10.61.185.231
4.2.5 IPv4 Secondary DNS
Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired)
10.61.186.231
4.2.6 IPv4 Search Domains (optional)
Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired)
netapp.com,sddc.netapp.com
3.3 Setup IPv6 Network Properties
6 settings
4.3.1 IPv6 Address
IP address for the appliance. (Leave blank if DHCP is desired)
4.3.2 IPv6 PrefixLen
Prefix length to use on the deployed network. (Leave blank if DHCP is desired)

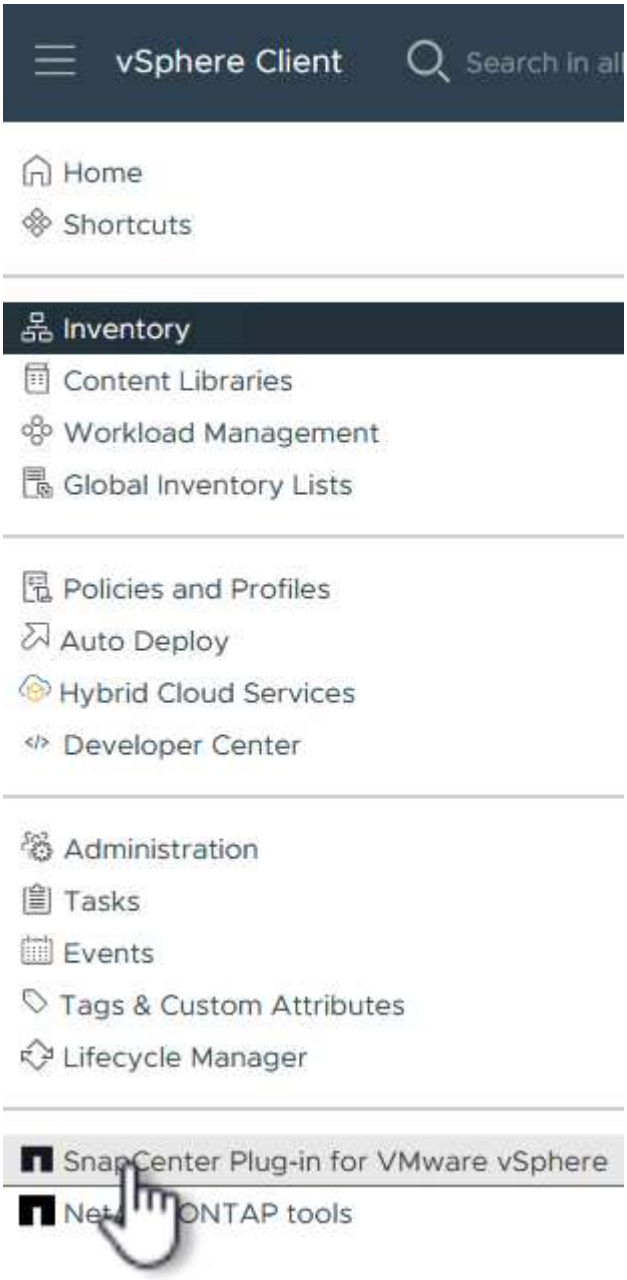


10. Überprüfen Sie abschließend auf der Seite **Bereit zum Abschließen** alle Einstellungen und klicken Sie auf „Fertig stellen“, um die Bereitstellung zu starten.

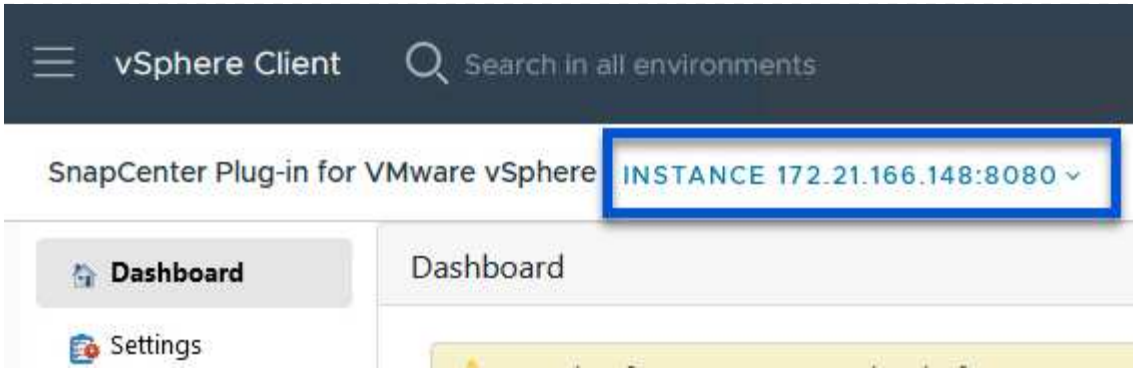
Speichersysteme zu SCV hinzufügen

Sobald das SnapCenter -Plug-in installiert ist, führen Sie die folgenden Schritte aus, um Speichersysteme zu SCV hinzuzufügen:

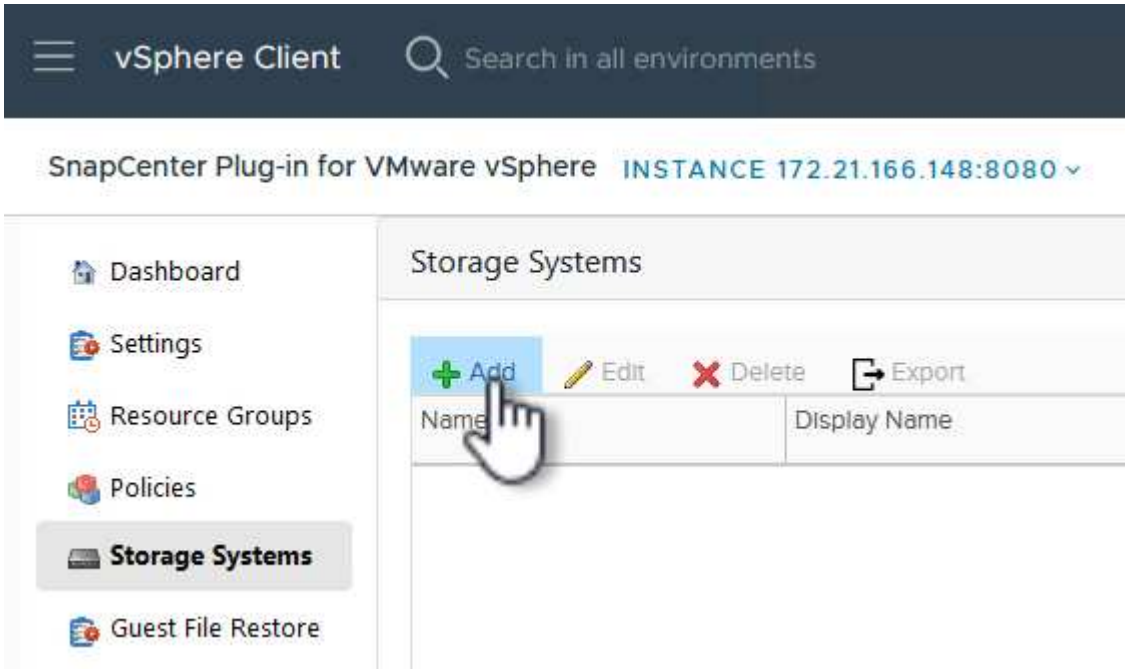
1. Auf SCV kann über das Hauptmenü im vSphere-Client zugegriffen werden.



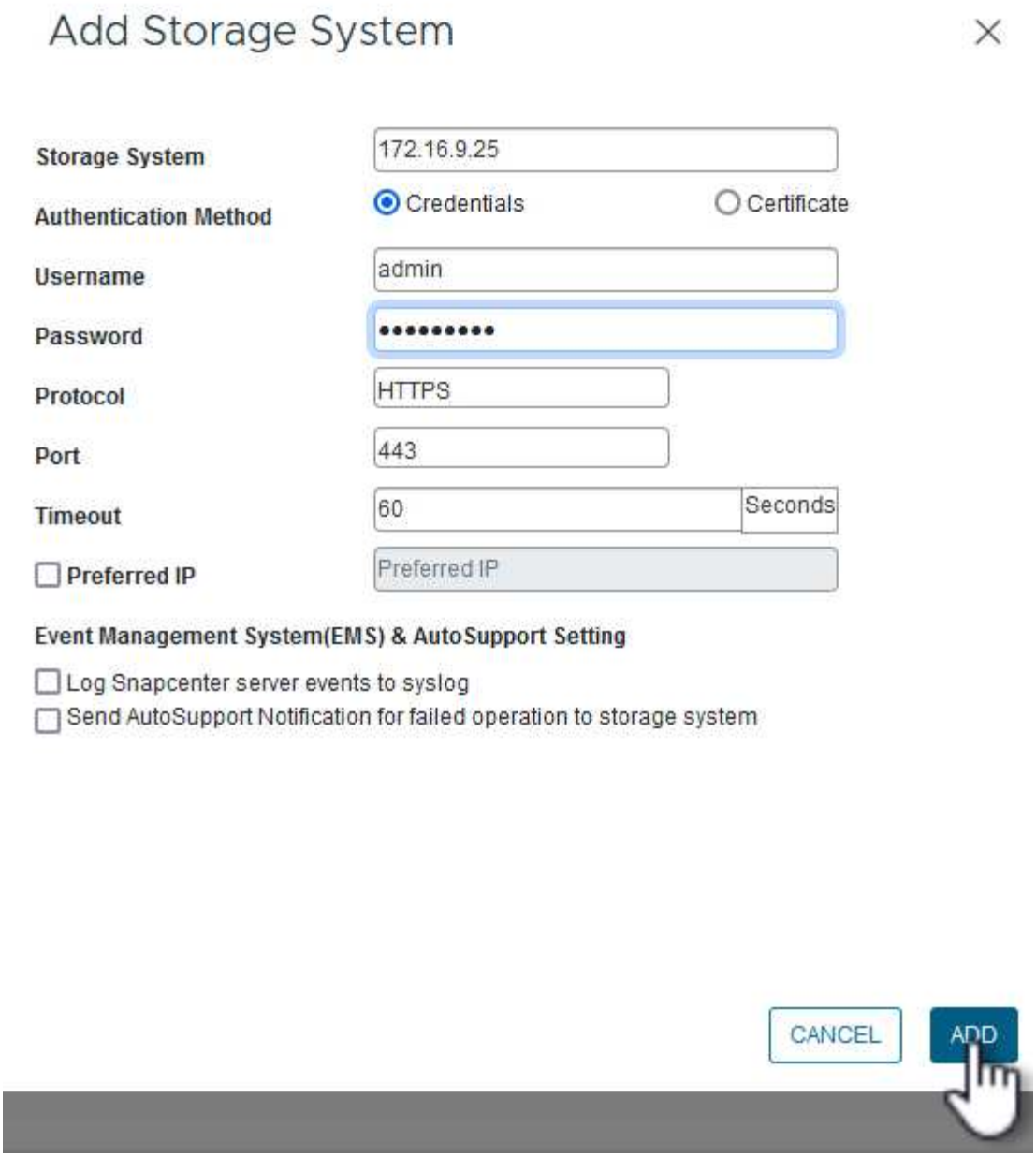
2. Wählen Sie oben in der SCV-Benutzeroberfläche die richtige SCV-Instanz aus, die dem zu schützenden vSphere-Cluster entspricht.



3. Navigieren Sie im linken Menü zu **Speichersysteme** und klicken Sie auf **Hinzufügen**, um zu beginnen.



4. Geben Sie im Formular **Speichersystem hinzufügen** die IP-Adresse und Anmeldeinformationen des hinzuzufügenden ONTAP -Speichersystems ein und klicken Sie auf **Hinzufügen**, um die Aktion abzuschließen.



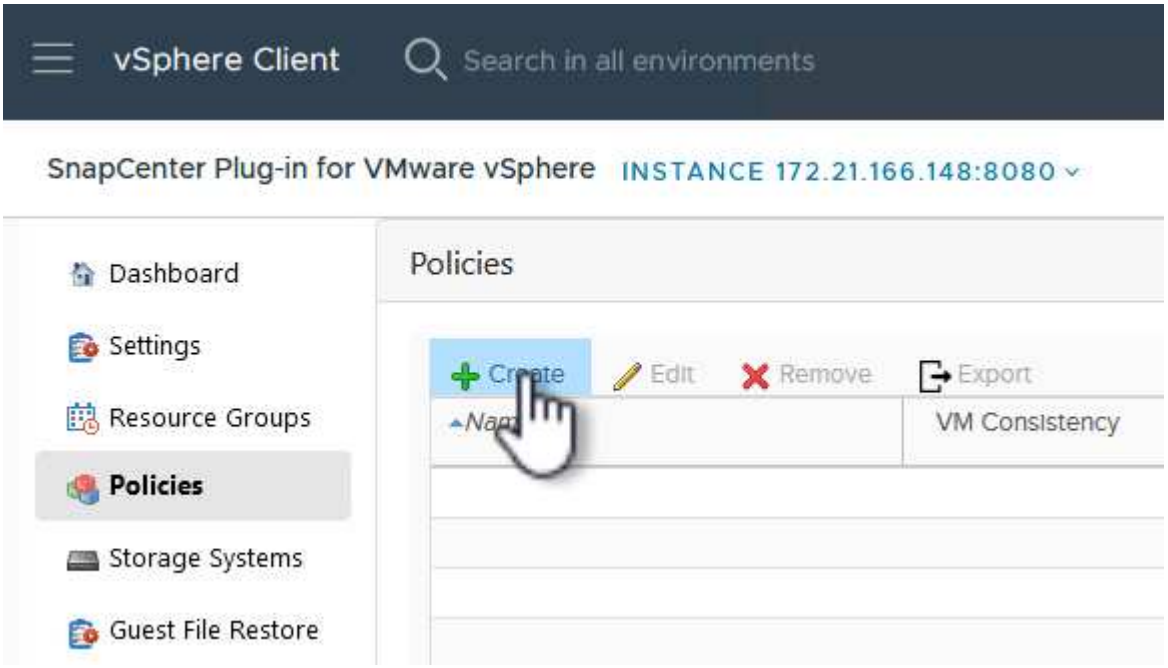
5. Wiederholen Sie diesen Vorgang für alle weiteren zu verwaltenden Speichersysteme, einschließlich aller Systeme, die als sekundäre Sicherungsziele verwendet werden sollen.

Konfigurieren von Sicherungsrichtlinien in SCV

Weitere Informationen zum Erstellen von SCV-Sicherungsrichtlinien finden Sie unter"Erstellen Sie Sicherungsrichtlinien für VMs und Datenspeicher" .

Führen Sie die folgenden Schritte aus, um eine neue Sicherungsrichtlinie zu erstellen:

1. Wählen Sie im linken Menü **Richtlinien** aus und klicken Sie auf **Erstellen**, um zu beginnen.



2. Geben Sie im Formular **Neue Sicherungsrichtlinie** einen **Namen** und eine **Beschreibung** für die Richtlinie, die **Häufigkeit**, mit der die Sicherungen durchgeführt werden, und den **Aufbewahrungszeitraum** an, der angibt, wie lange die Sicherung aufbewahrt wird.

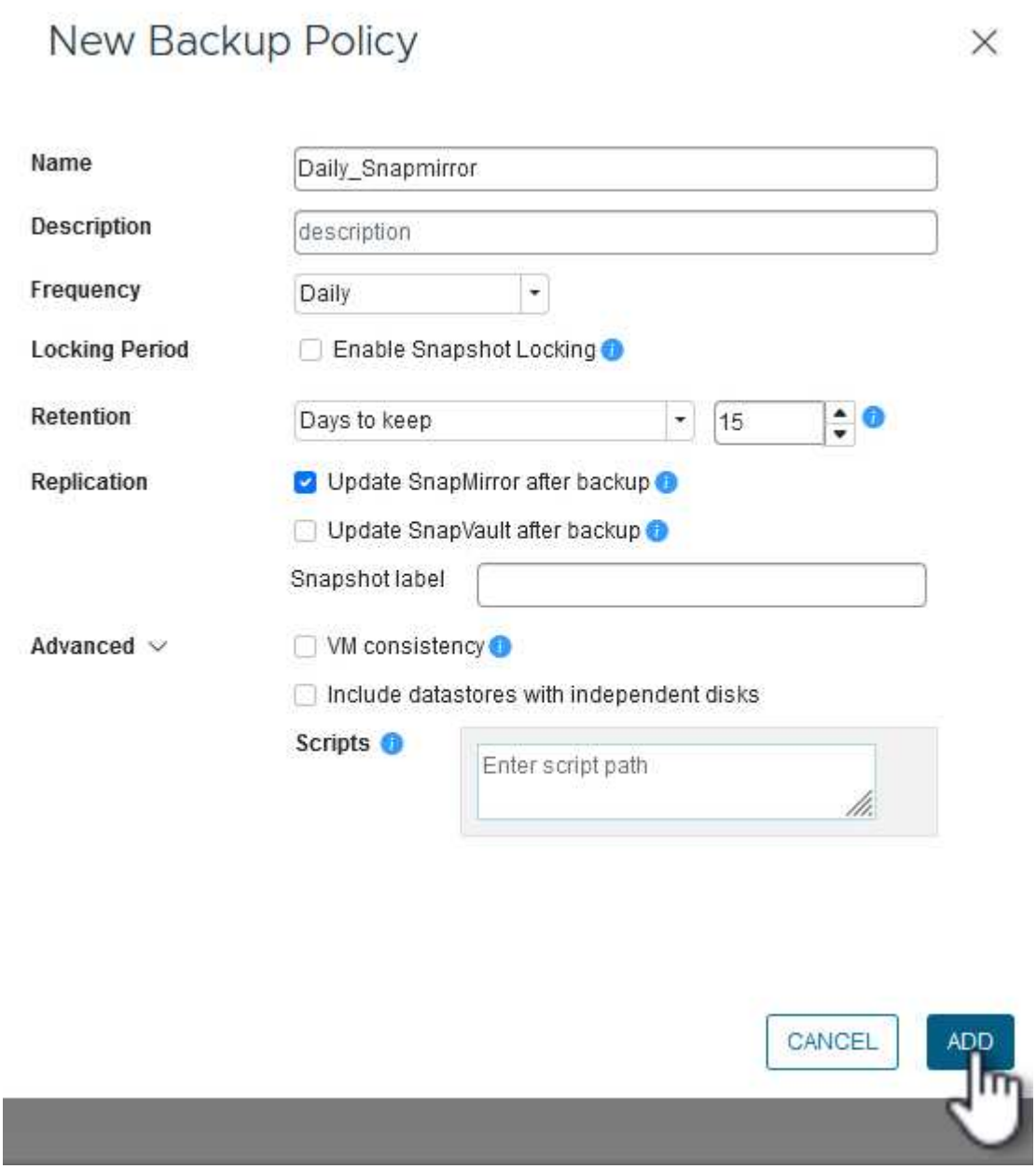
   Sperrzeitraum ermöglicht der ONTAP SnapLock -Funktion das Erstellen manipulationssicherer Snapshots und die Konfiguration des Sperrzeitraums.

   Für **Replikation** Wählen Sie diese Option aus, um die zugrunde liegenden SnapMirror oder SnapVault -Beziehungen für das ONTAP Speichervolume zu aktualisieren.

   > Die Replikation von SnapMirror und SnapVault ähnelt sich darin, dass beide die ONTAP SnapMirror -Technologie nutzen, um Speichervolumes asynchron auf ein sekundäres Speichersystem zu replizieren und so den Schutz und die Sicherheit zu erhöhen. Bei SnapMirror -Beziehungen regelt der in der SCV-Sicherungsrichtlinie angegebene Aufbewahrungsplan die Aufbewahrung sowohl für das primäre als auch für das sekundäre Volume. Mit SnapVault -Beziehungen kann auf dem sekundären Speichersystem ein separater Aufbewahrungsplan für längerfristige oder unterschiedliche Aufbewahrungspläne eingerichtet werden. In diesem Fall wird die Snapshot-Bezeichnung in der SCV-Sicherungsrichtlinie und in der mit dem sekundären Volume verknüpften Richtlinie angegeben, um zu identifizieren, auf welche Volumes der unabhängige Aufbewahrungszeitplan angewendet werden soll.

   Wählen Sie alle weiteren erweiterten Optionen aus und klicken Sie auf **Hinzufügen**, um die Richtlinie

zu erstellen.

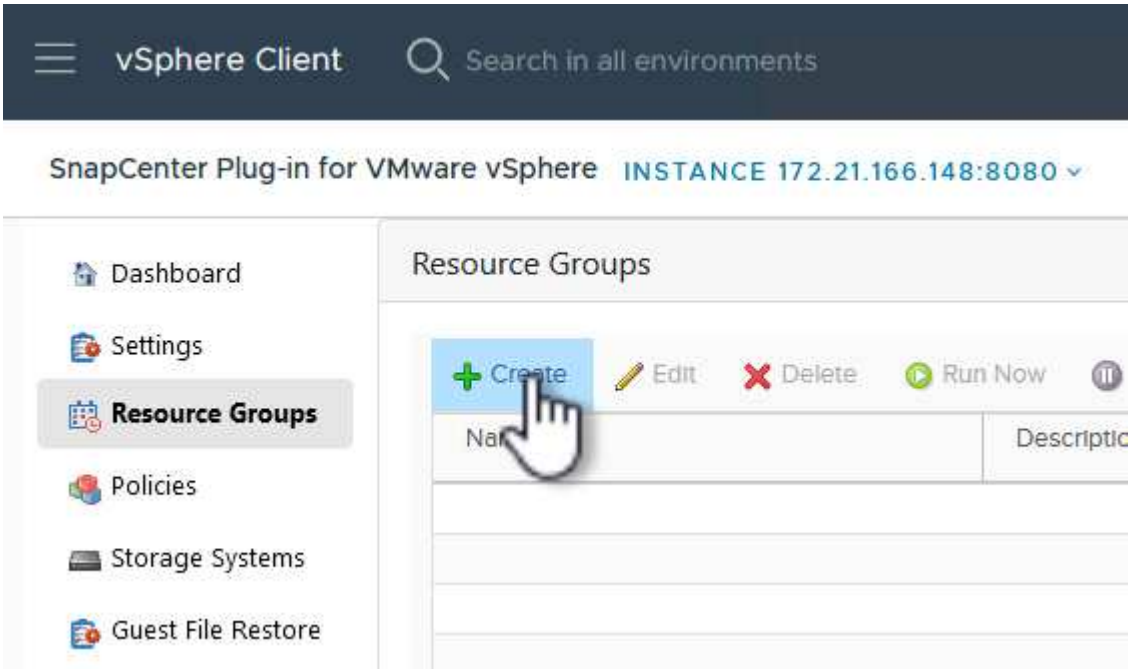


Erstellen von Ressourcengruppen in SCV

Weitere Informationen zum Erstellen von SCV-Ressourcengruppen finden Sie unter"Erstellen von Ressourcengruppen" .

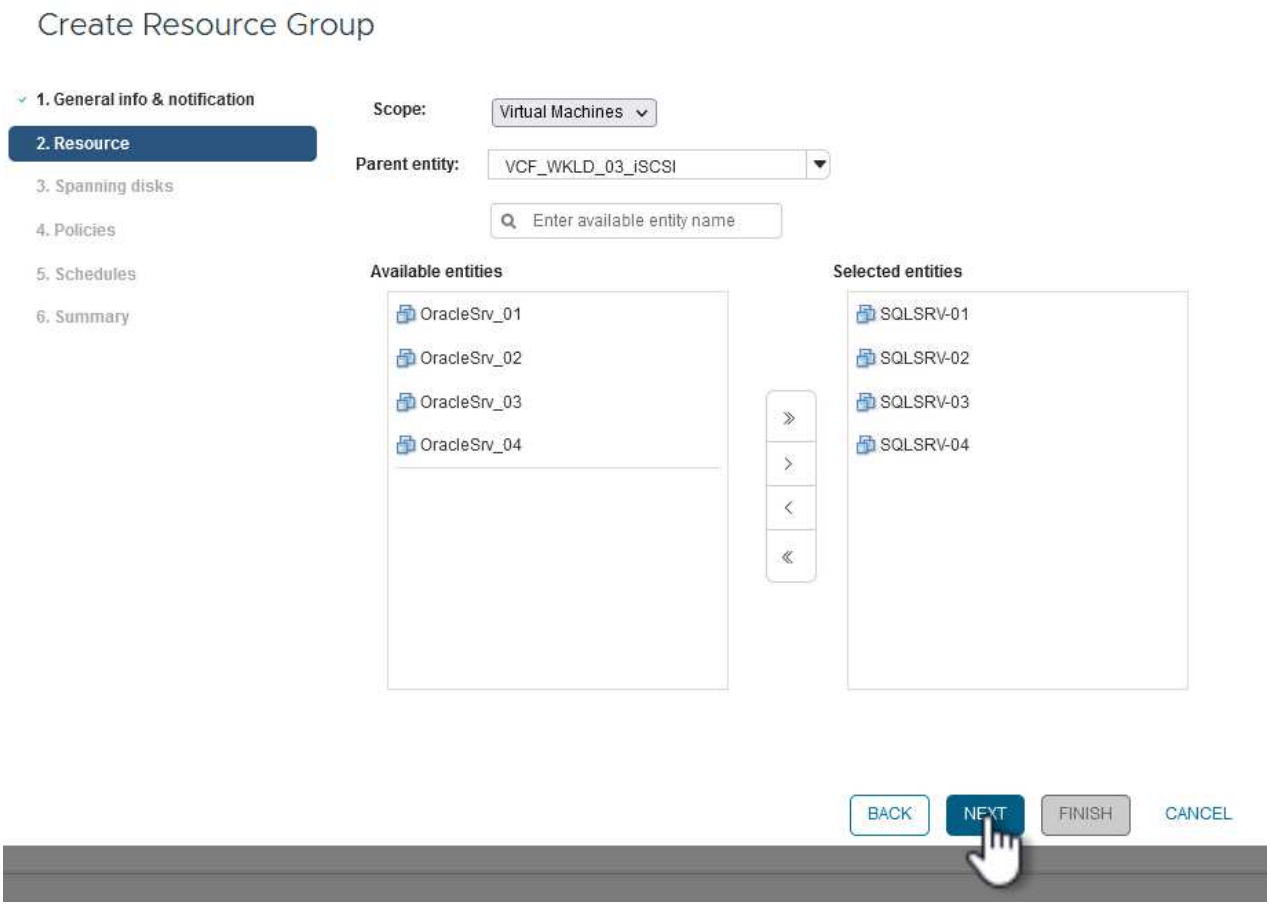
Führen Sie die folgenden Schritte aus, um eine neue Ressourcengruppe zu erstellen:

1. Wählen Sie im linken Menü **Ressourcengruppen** aus und klicken Sie auf **Erstellen**, um zu beginnen.

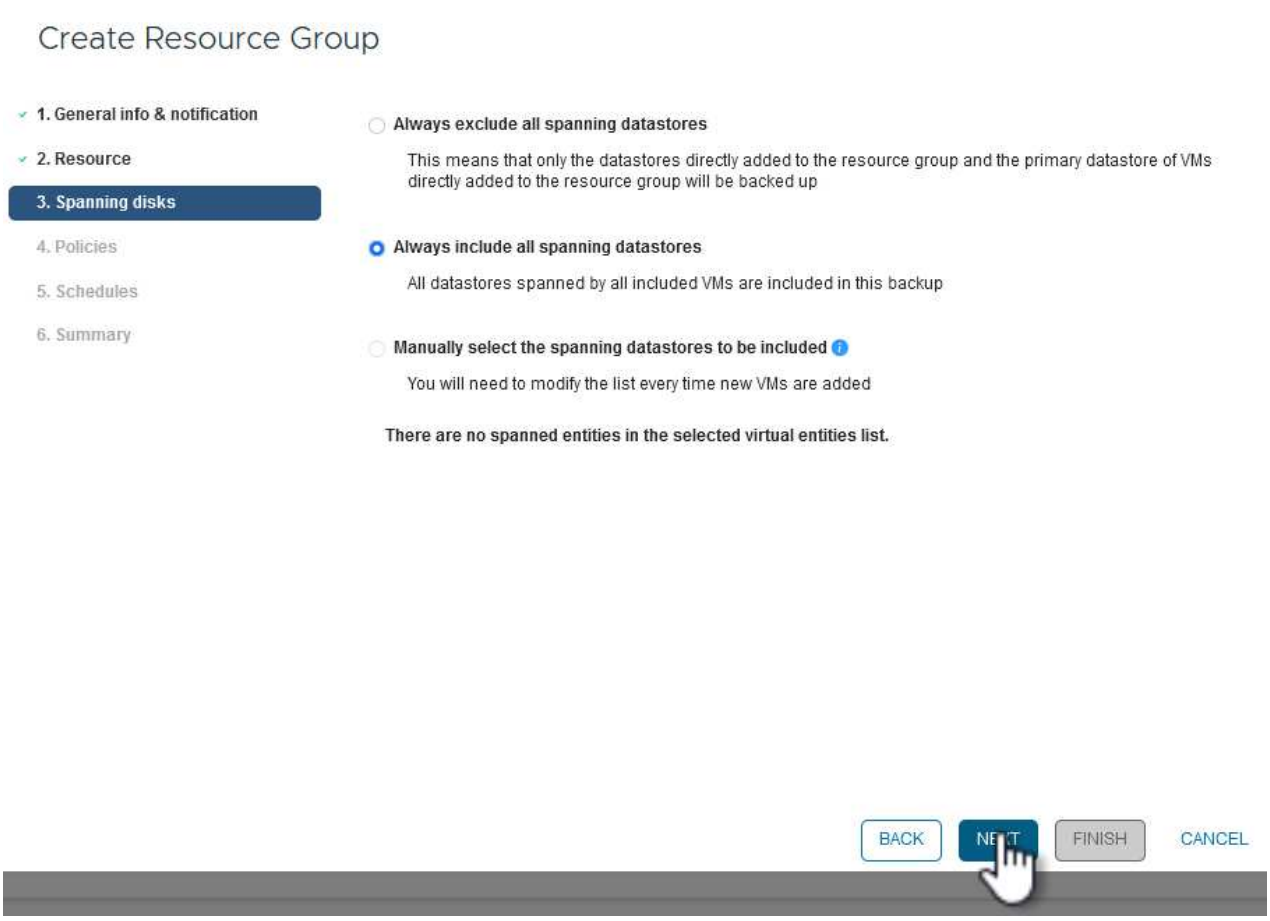


2. Geben Sie auf der Seite **Allgemeine Informationen und Benachrichtigungen** einen Namen für die Ressourcengruppe, Benachrichtigungseinstellungen und alle zusätzlichen Optionen für die Benennung der Snapshots an.
3. Wählen Sie auf der Seite **Ressource** die zu schützenden Datenspeicher und VMs in der Ressourcengruppe aus. Klicken Sie auf **Weiter**, um fortzufahren.

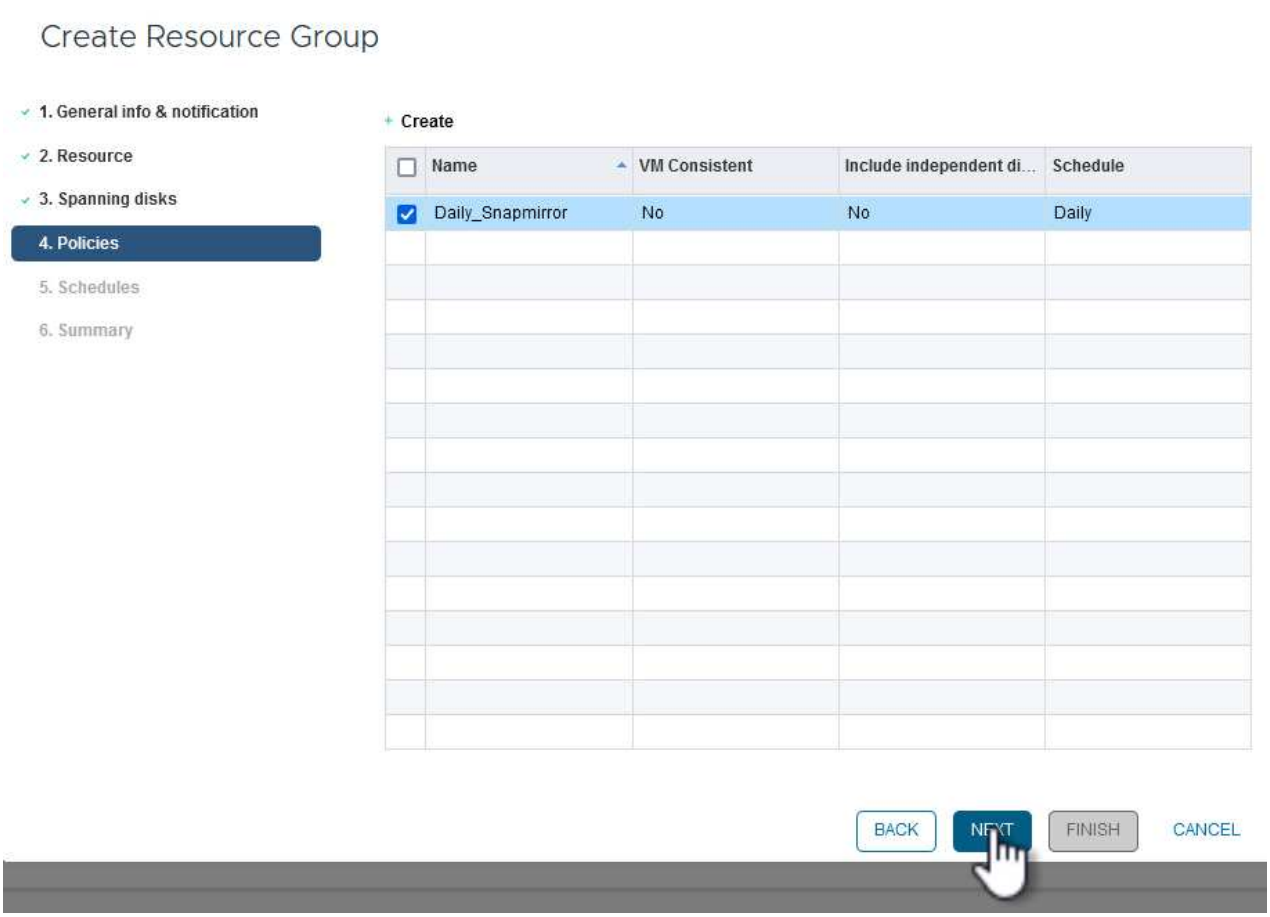
> Auch wenn nur bestimmte VMs ausgewählt werden, wird immer der gesamte Datenspeicher gesichert. Dies liegt daran, dass ONTAP Snapshots des Volumes erstellt, auf dem der Datenspeicher gehostet wird. Beachten Sie jedoch, dass die Auswahl nur bestimmter VMs für die Sicherung die Möglichkeit zur Wiederherstellung auf nur diese VMs einschränkt.



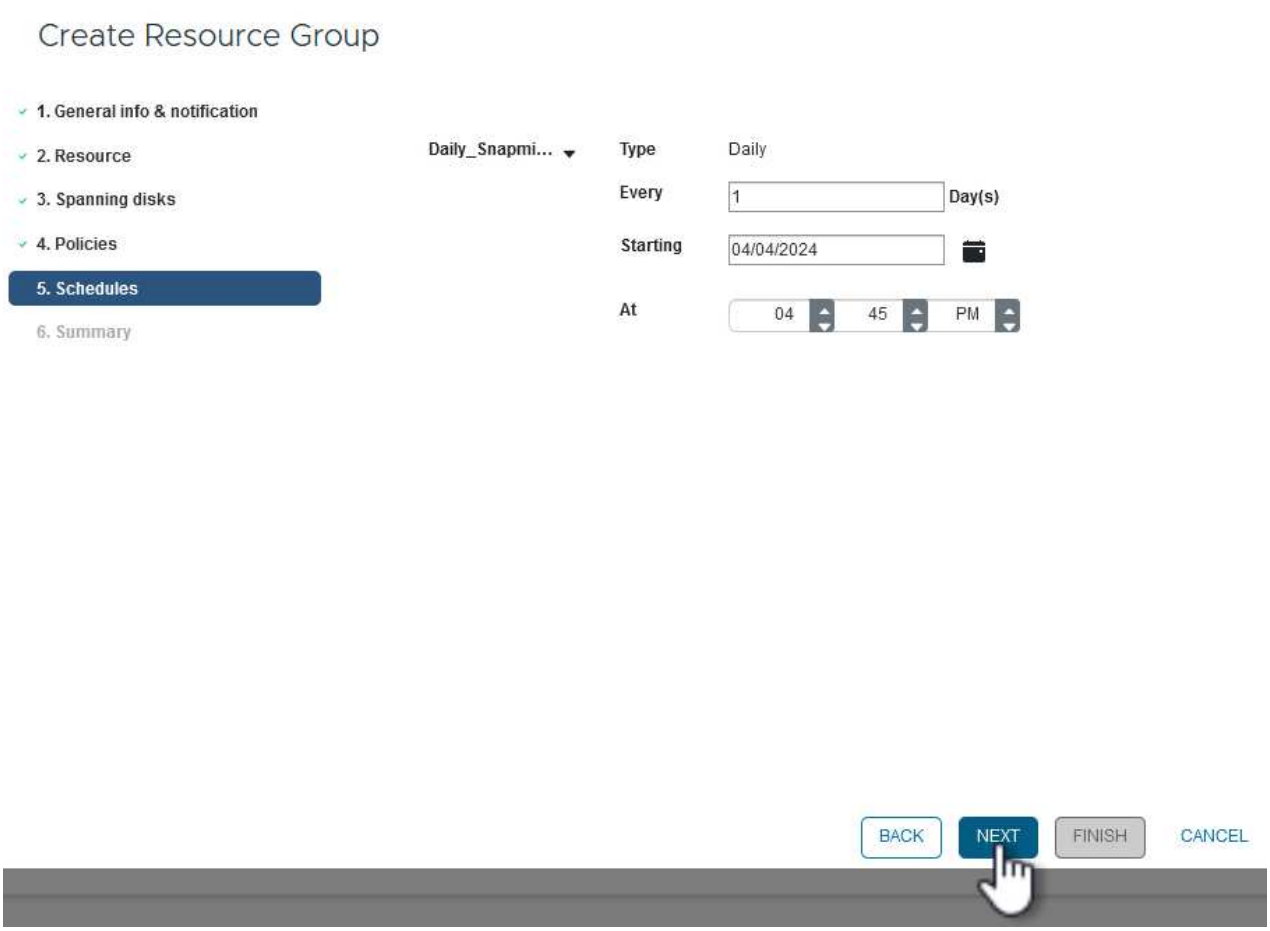
4. Wählen Sie auf der Seite **Spanning Disks** die Option für den Umgang mit VMs mit VMDKs aus, die sich über mehrere Datenspeicher erstrecken. Klicken Sie auf **Weiter**, um fortzufahren.



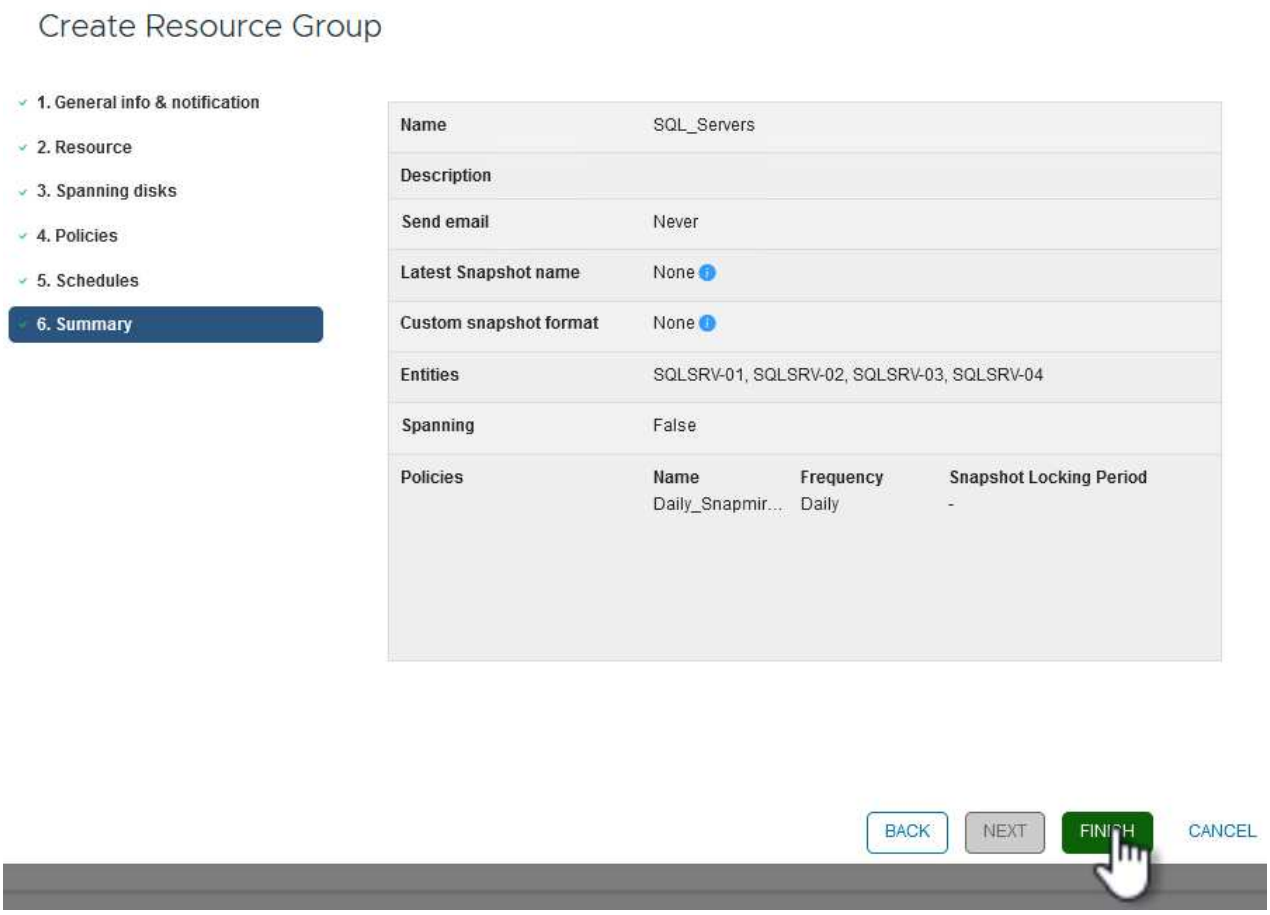
5. Wählen Sie auf der Seite **Richtlinien** eine oder mehrere zuvor erstellte Richtlinien aus, die mit dieser Ressourcengruppe verwendet werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.



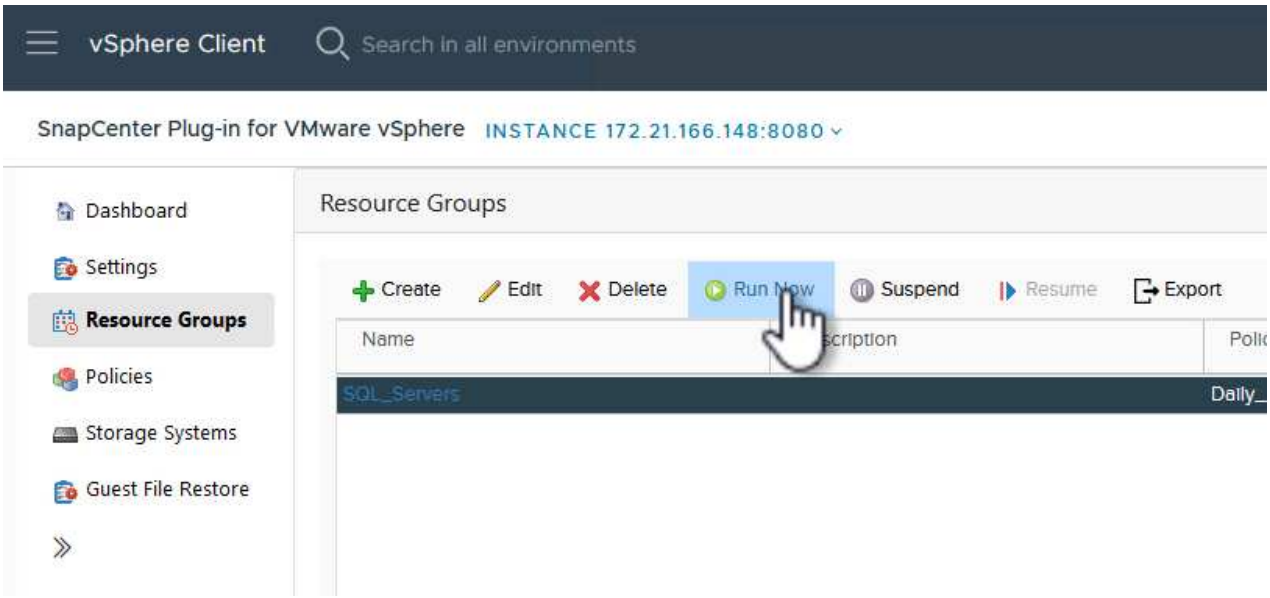
6. Legen Sie auf der Seite **Zeitpläne** fest, wann die Sicherung ausgeführt werden soll, indem Sie die Wiederholung und die Tageszeit konfigurieren. Klicken Sie auf **Weiter**, um fortzufahren.



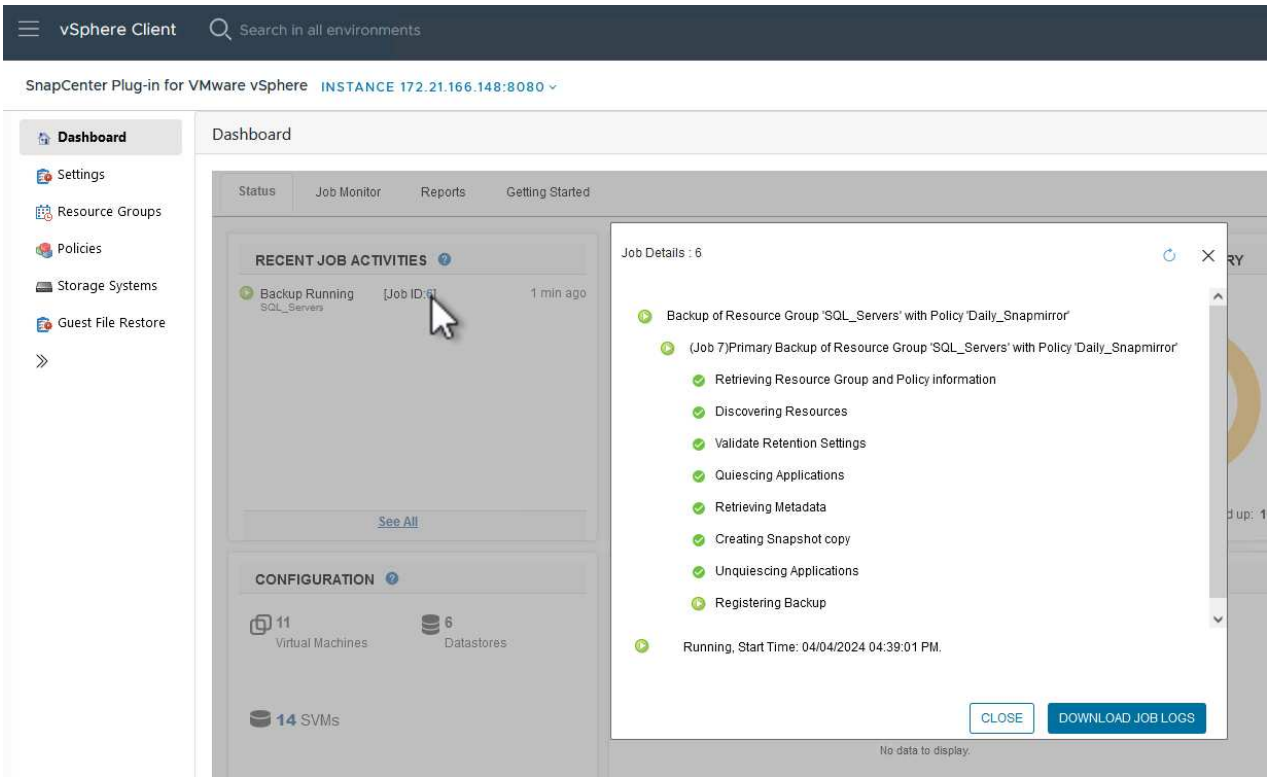
7. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig**, um die Ressourcengruppe zu erstellen.



8. Klicken Sie nach der Erstellung der Ressourcengruppe auf die Schaltfläche **Jetzt ausführen**, um die erste Sicherung auszuführen.



9. Navigieren Sie zum **Dashboard** und klicken Sie unter **Letzte Jobaktivitäten** auf die Zahl neben **Job-ID**, um den Job-Monitor zu öffnen und den Fortschritt des laufenden Jobs anzuzeigen.



Verwenden Sie SCV zum Wiederherstellen von VMs, VMDKs und Dateien

Das SnapCenter -Plug-in ermöglicht die Wiederherstellung von VMs, VMDKs, Dateien und Ordnern aus primären oder sekundären Backups.

VMs können auf dem ursprünglichen Host oder auf einem alternativen Host im selben vCenter Server oder auf einem alternativen ESXi-Host wiederhergestellt werden, der vom selben vCenter oder einem beliebigen vCenter im verknüpften Modus verwaltet wird.

vVol-VMs können auf dem ursprünglichen Host wiederhergestellt werden.

VMDKs in herkömmlichen VMs können entweder im Original oder in einem alternativen Datenspeicher wiederhergestellt werden.

VMDKs in vVol-VMs können im ursprünglichen Datenspeicher wiederhergestellt werden.

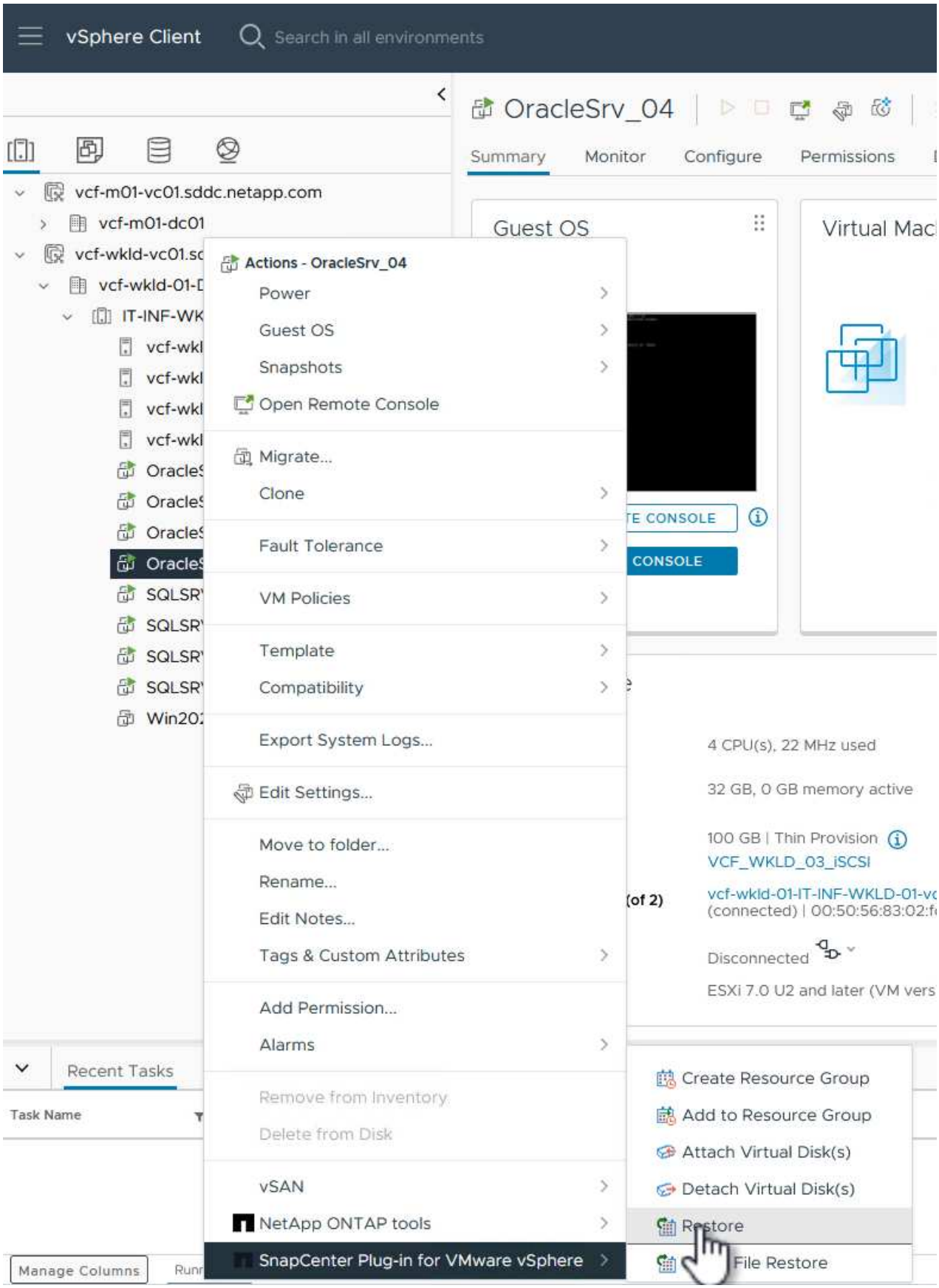
Einzelne Dateien und Ordner können in einer Gastdateiwiederherstellungssitzung wiederhergestellt werden. Dabei wird eine Sicherungskopie einer virtuellen Festplatte angehängt und anschließend werden die ausgewählten Dateien oder Ordner wiederhergestellt.

Führen Sie die folgenden Schritte aus, um VMs, VMDKs oder einzelne Ordner wiederherzustellen.

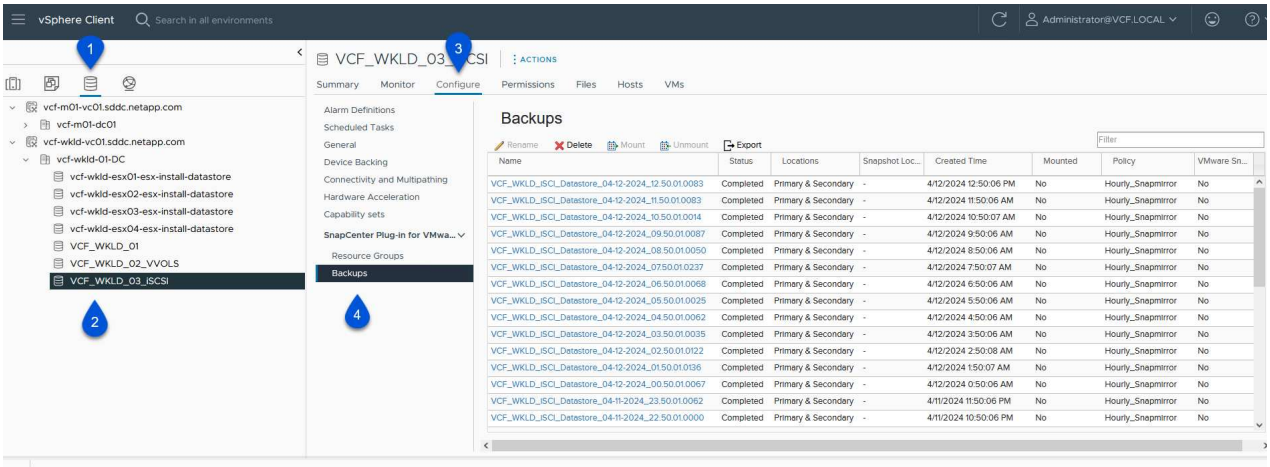
Wiederherstellen von VMs mit dem SnapCenter -Plug-in

Führen Sie die folgenden Schritte aus, um eine VM mit SCV wiederherzustellen:

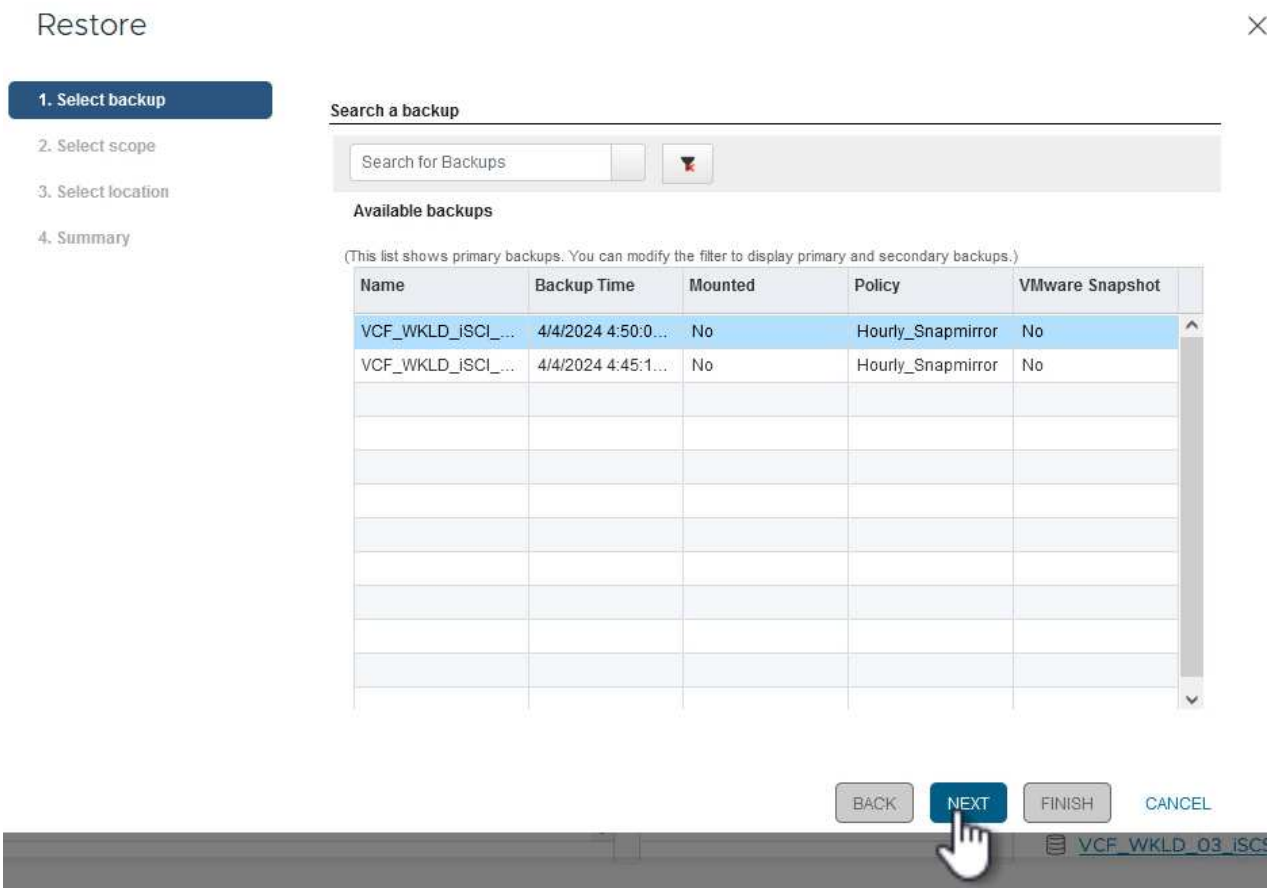
1. Navigieren Sie im vSphere-Client zu der wiederherzustellenden VM, klicken Sie mit der rechten Maustaste und navigieren Sie zu * SnapCenter Plug-in for VMware vSphere*. Wählen Sie im Untermenü **Wiederherstellen**.


vSphere Client
Search in all environments
OracleSrv_04
Summary
Monitor
Configure
Permissions
vcf-m01-vc01.sddc.netapp.com
vcf-m01-dc01
vcf-wkld-vc01.sc
vcf-wkld-01-D
IT-INF-WK
vcf-wkl
vcf-wkl
vcf-wkl
vcf-wkl
Oracle
Oracle
Oracle
Oracle
SQLSR
SQLSR
SQLSR
SQLSR
Win20
Guest OS
Virtual Mac
TE CONSOLE
CONSOLE
Actions - OracleSrv_04
Power
Guest OS
Snapshots
Open Remote Console
Migrate...
Clone
Fault Tolerance
VM Policies
Template
Compatibility
Export System Logs...
Edit Settings...
Move to folder...
Rename...
Edit Notes...
Tags & Custom Attributes
Add Permission...
Alarms
Remove from Inventory
Delete from Disk
vSAN
NetApp ONTAP tools
SnapCenter Plug-in for VMware vSphere
4 CPU(s), 22 MHz used
32 GB, 0 GB memory active
100 GB | Thin Provision
VCF_WKLD_03_iSCSI
(of 2)
vcf-wkld-01-IT-INF-WKLD-01-vc
(connected) | 00:50:56:83:02:f
Disconnected
ESXi 7.0 U2 and later (VM vers
Recent Tasks
Task Name
Manage Columns
Create Resource Group
Add to Resource Group
Attach Virtual Disk(s)
Detach Virtual Disk(s)
Restore
File Restore

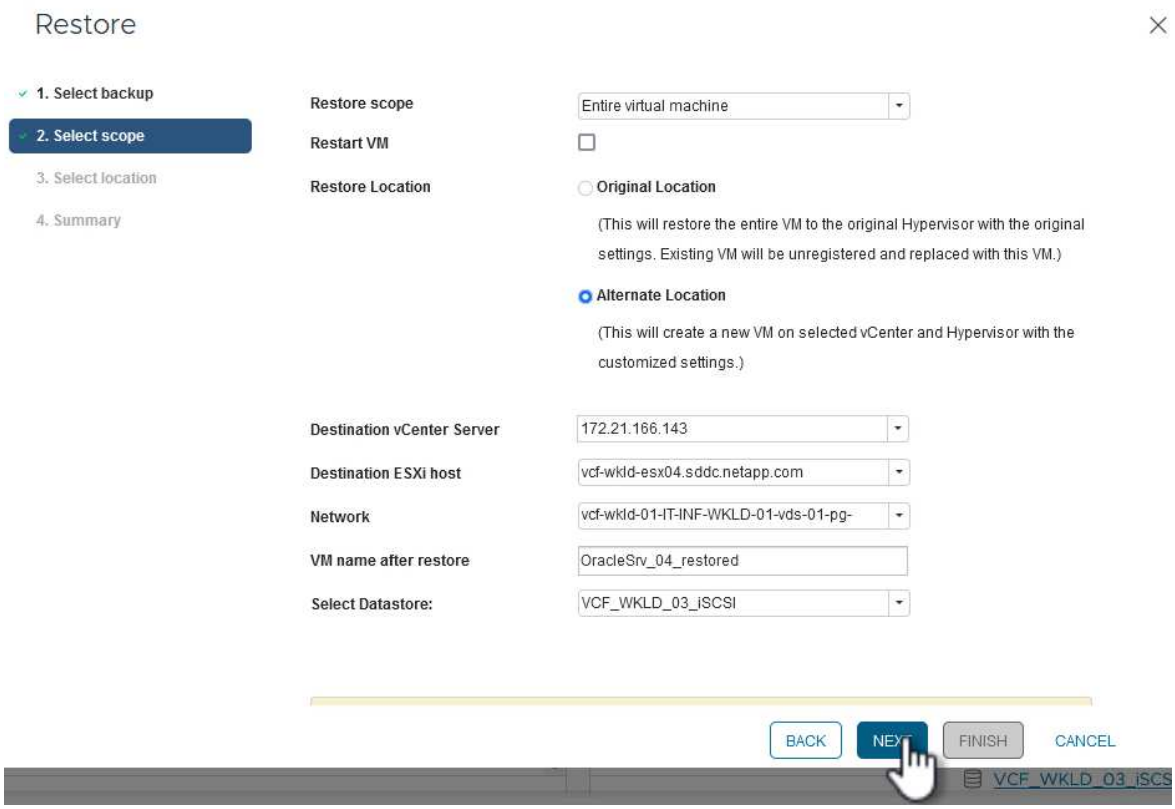
Alternativ können Sie zum Datenspeicher im Inventar navigieren und dann unter der Registerkarte **Konfigurieren** zu * SnapCenter Plug-in for VMware vSphere > Backups* gehen. Wählen Sie aus dem ausgewählten Backup die wiederherzustellenden VMs aus.



2. Wählen Sie im Assistenten **Wiederherstellen** die zu verwendende Sicherung aus. Klicken Sie auf **Weiter**, um fortzufahren.

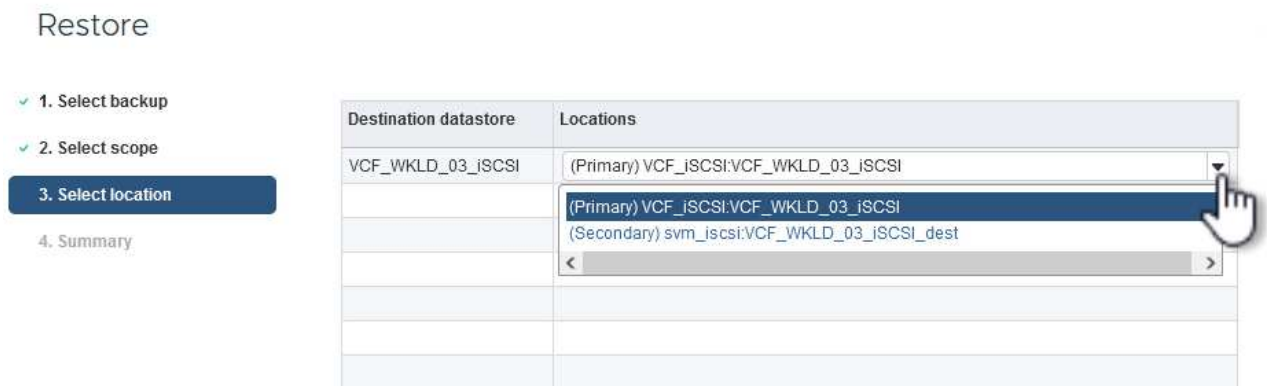


3. Füllen Sie auf der Seite **Bereich auswählen** alle erforderlichen Felder aus:
    - **Wiederherstellungsbereich** – Wählen Sie diese Option aus, um die gesamte virtuelle Maschine wiederherzustellen.
    - **VM neu starten** – Wählen Sie, ob die VM nach der Wiederherstellung gestartet werden soll.
    - **Speicherort wiederherstellen** – Wählen Sie, ob die Wiederherstellung am ursprünglichen Speicherort oder an einem anderen Speicherort erfolgen soll. Wählen Sie bei der Auswahl eines alternativen Standorts die Optionen aus den einzelnen Feldern aus:
        - **Ziel-vCenter-Server** – lokales vCenter oder alternatives vCenter im verknüpften Modus
        - **Ziel-ESXi-Host**
        - **Netzwerk**
        - **VM-Name nach der Wiederherstellung**
        - **Datenspeicher auswählen:**

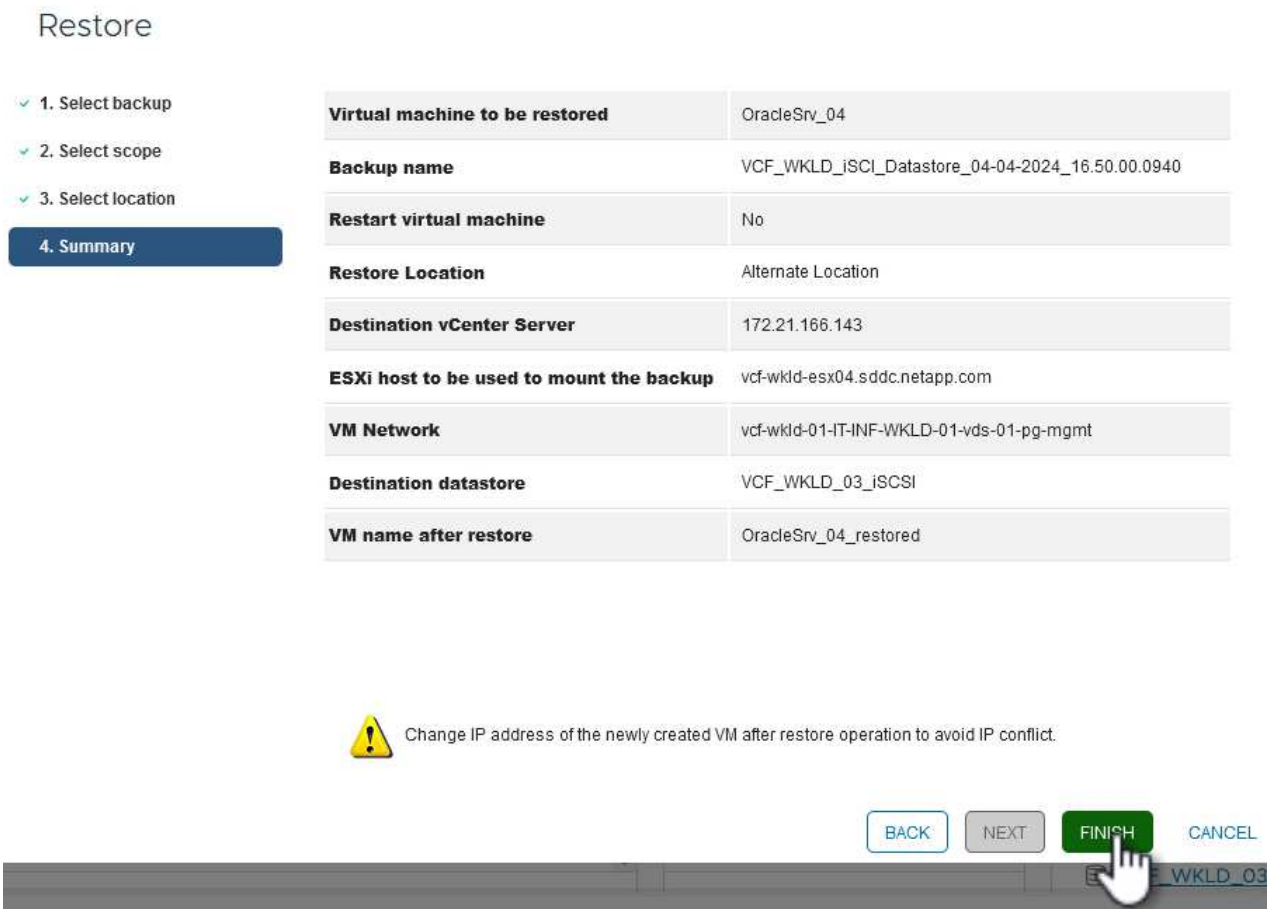


Klicken Sie auf **Weiter**, um fortzufahren.

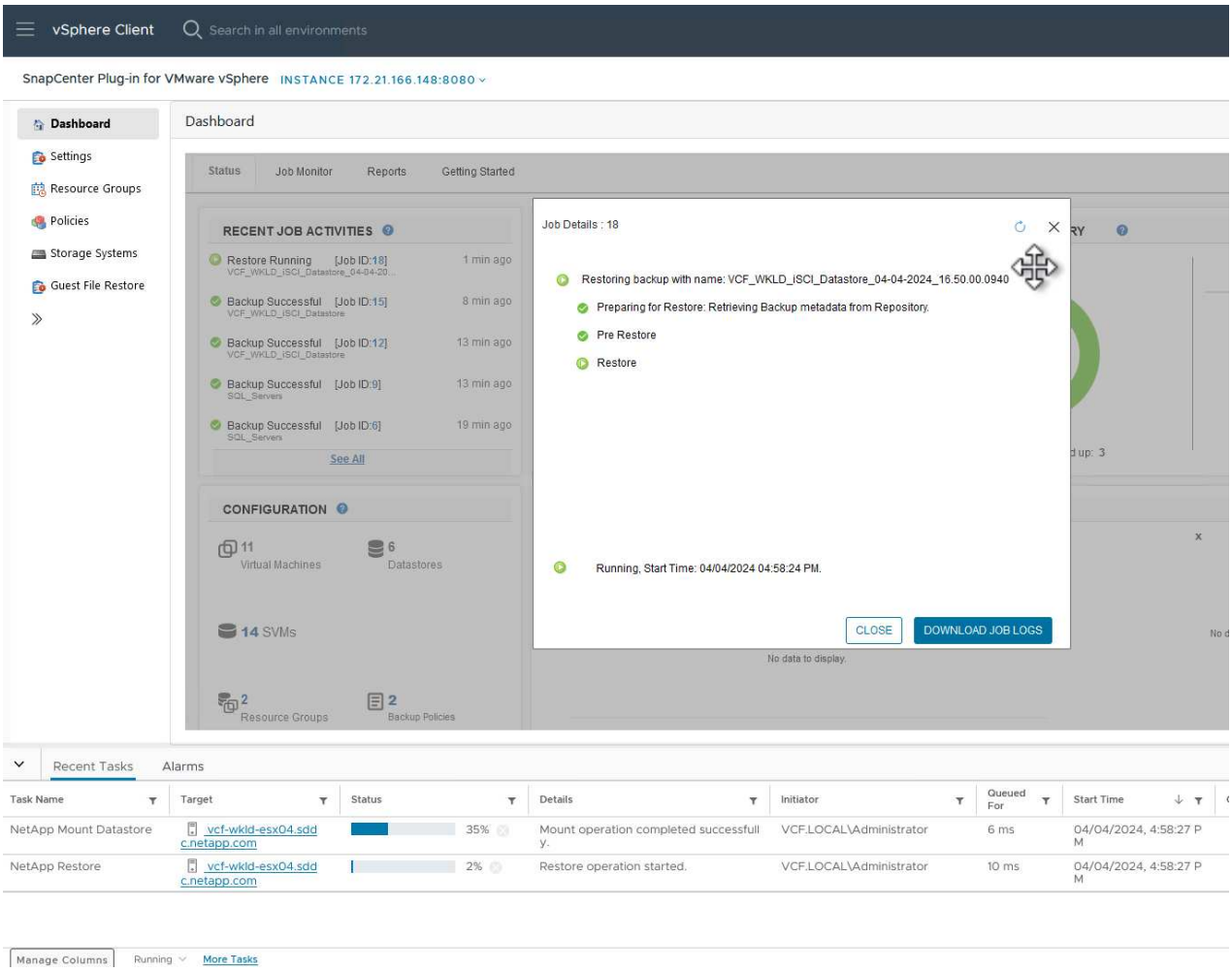
4. Wählen Sie auf der Seite **Speicherort auswählen** aus, ob die VM vom primären oder sekundären ONTAP Speichersystem wiederhergestellt werden soll. Klicken Sie auf **Weiter**, um fortzufahren.



5. Überprüfen Sie abschließend die **Zusammenfassung** und klicken Sie auf **Fertig**, um den Wiederherstellungsauftrag zu starten.



6. Der Fortschritt des Wiederherstellungsjobs kann im Bereich **Letzte Aufgaben** im vSphere-Client und im Job-Monitor in SCV überwacht werden.

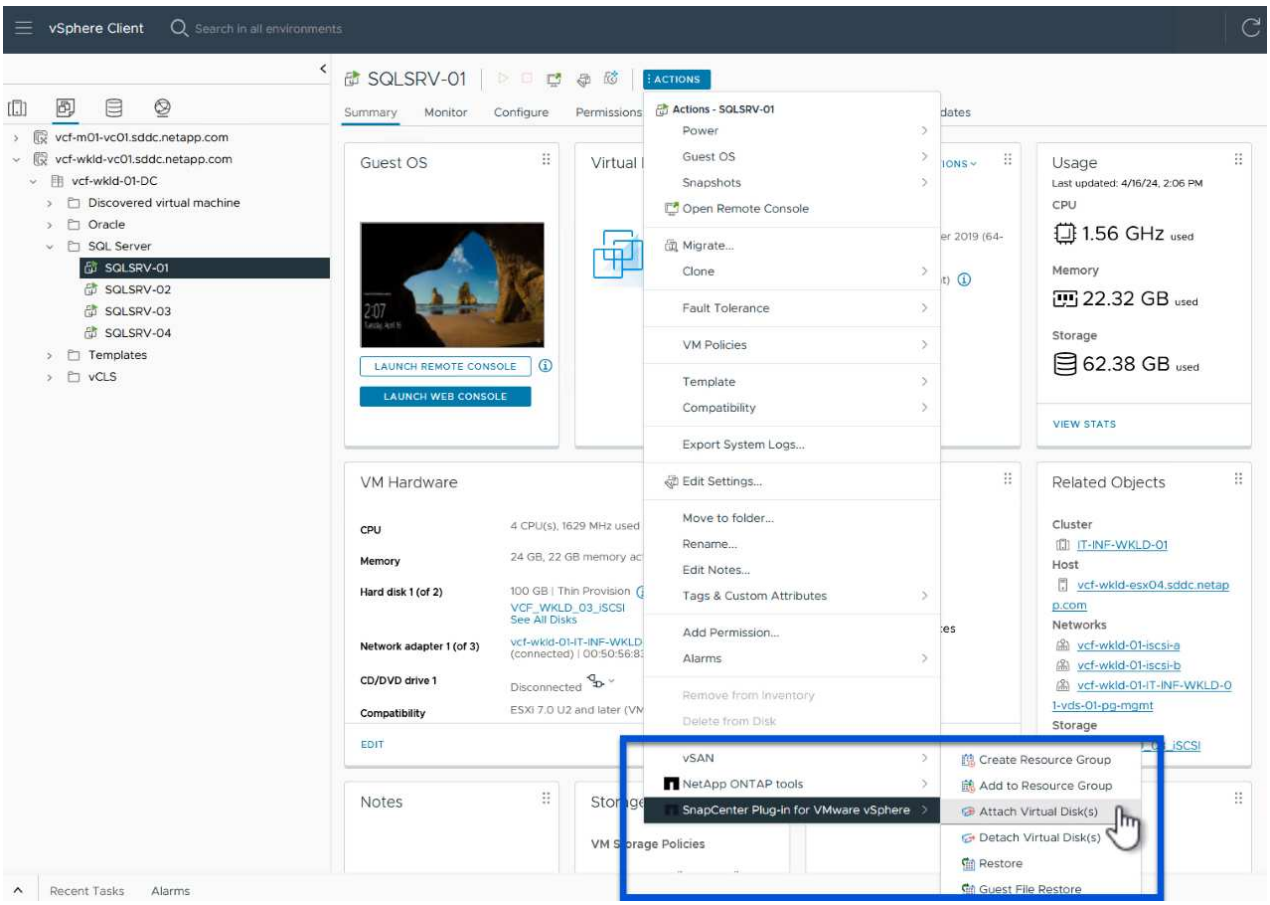

vSphere Client
Search in all environments
SnapCenter Plug-in for VMware vSphere
INSTANCE 172.21.166.148:8080
Dashboard
Settings
Resource Groups
Policies
Storage Systems
Guest File Restore
Dashboard
Status
Job Monitor
Reports
Getting Started
RECENT JOB ACTIVITIES
Restore Running [Job ID:18] 1 min ago
Backup Successful [Job ID:15] 8 min ago
Backup Successful [Job ID:12] 13 min ago
Backup Successful [Job ID:9] 13 min ago
Backup Successful [Job ID:6] 19 min ago
See All
CONFIGURATION
11 Virtual Machines
6 Datastores
14 SVMs
2 Resource Groups
2 Backup Policies
Job Details : 18
Restoring backup with name: VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Preparing for Restore: Retrieving Backup metadata from Repository.
Pre Restore
Restore
Running, Start Time: 04/04/2024 04:58:24 PM.
CLOSE
DOWNLOAD JOB LOGS
No data to display.
Recent Tasks
Alarms
Task Name
Target
Status
Details
Initiator
Queued For
Start Time
NetApp Mount Datastore
vcf-wkld-esx04.sddc.netapp.com
35%
Mount operation completed successfully.
VCF.LOCAL\Administrator
6 ms
04/04/2024, 4:58:27 PM
NetApp Restore
vcf-wkld-esx04.sddc.netapp.com
2%
Restore operation started.
VCF.LOCAL\Administrator
10 ms
04/04/2024, 4:58:27 PM
Manage Columns
Running
More Tasks

Wiederherstellen von VMDKs mit dem SnapCenter -Plug-in

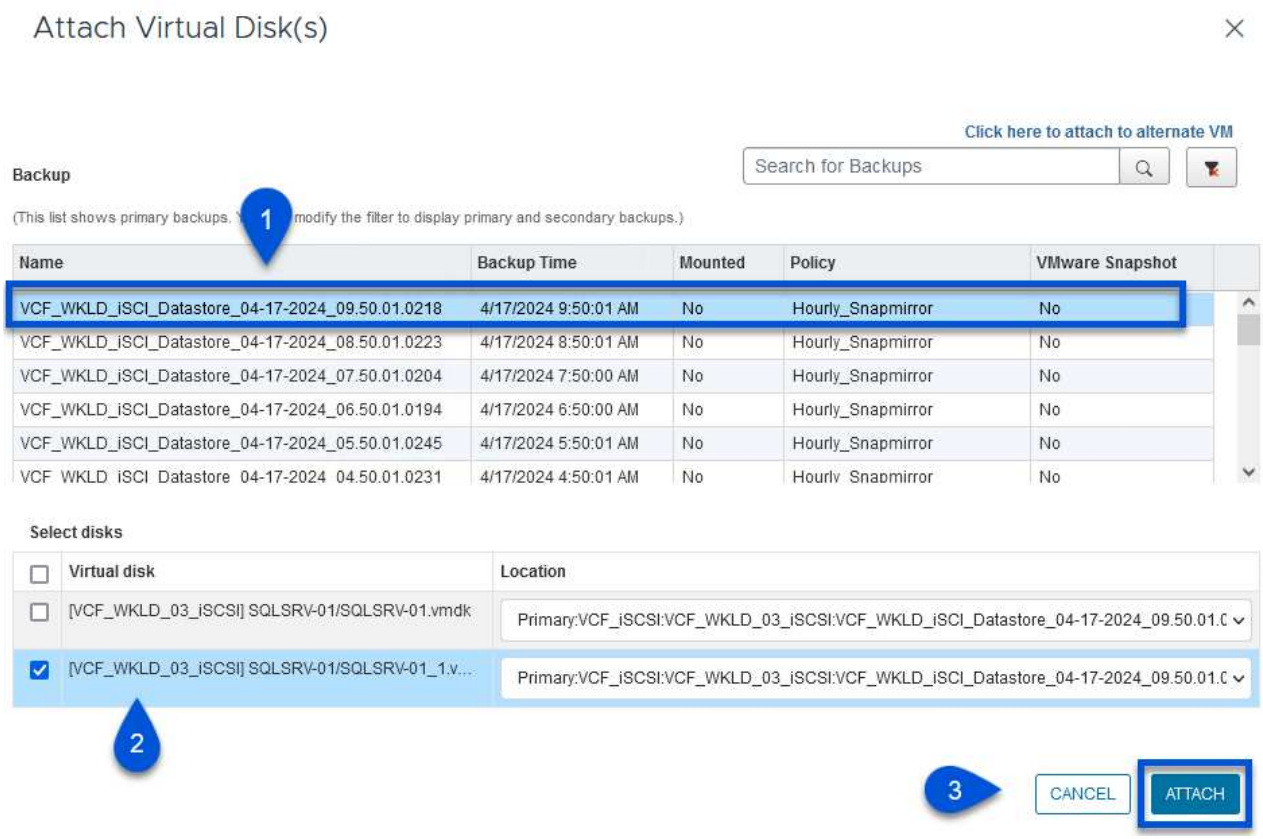
ONTAP Tools ermöglicht die vollständige Wiederherstellung von VMDKs an ihrem ursprünglichen Speicherort oder die Möglichkeit, ein VMDK als neue Festplatte an ein Hostsystem anzuschließen. In diesem Szenario wird ein VMDK an einen Windows-Host angeschlossen, um auf das Dateisystem zuzugreifen.

Um ein VMDK aus einer Sicherung anzuhängen, führen Sie die folgenden Schritte aus:

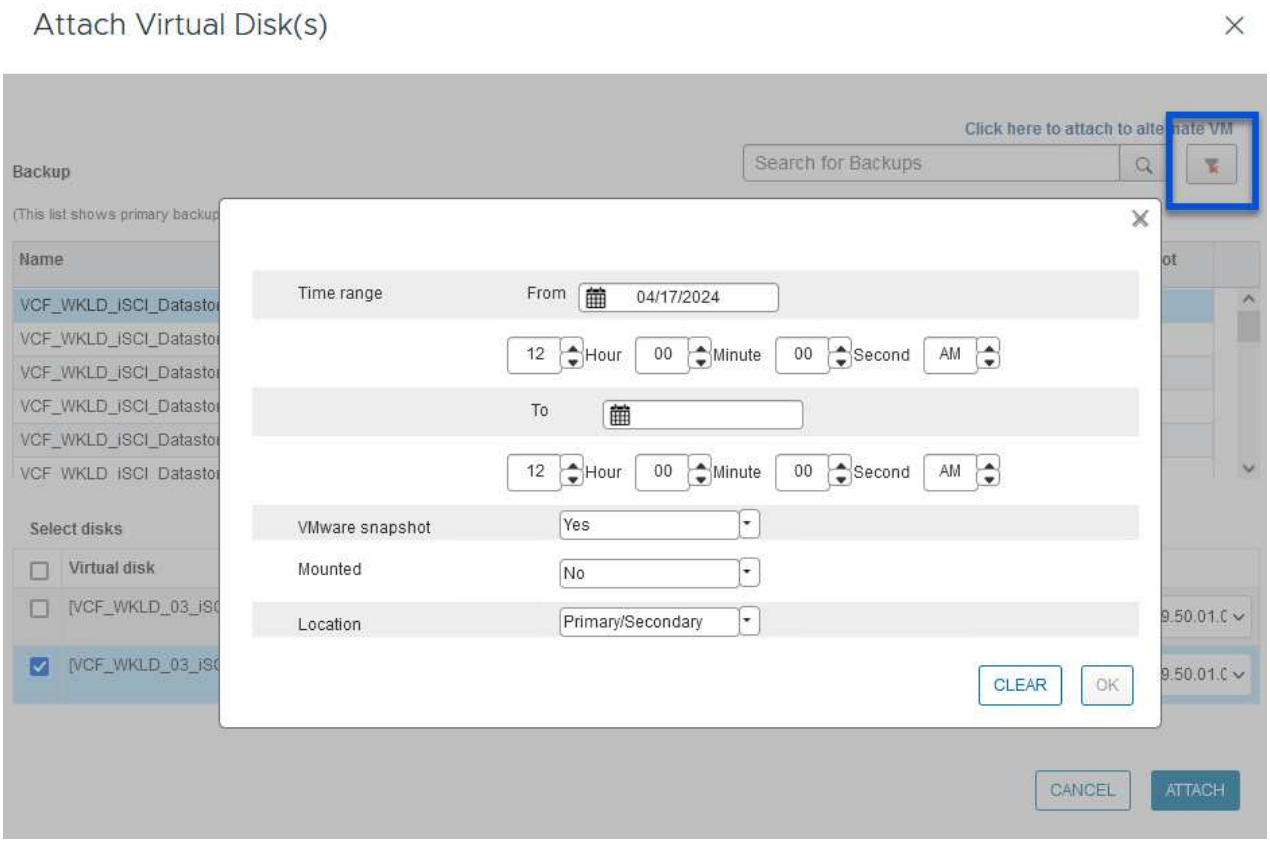
1. Navigieren Sie im vSphere-Client zu einer VM und wählen Sie im Menü **Aktionen** die Option * SnapCenter Plug-in for VMware vSphere > Virtuelle Festplatte(n) anhängen*.



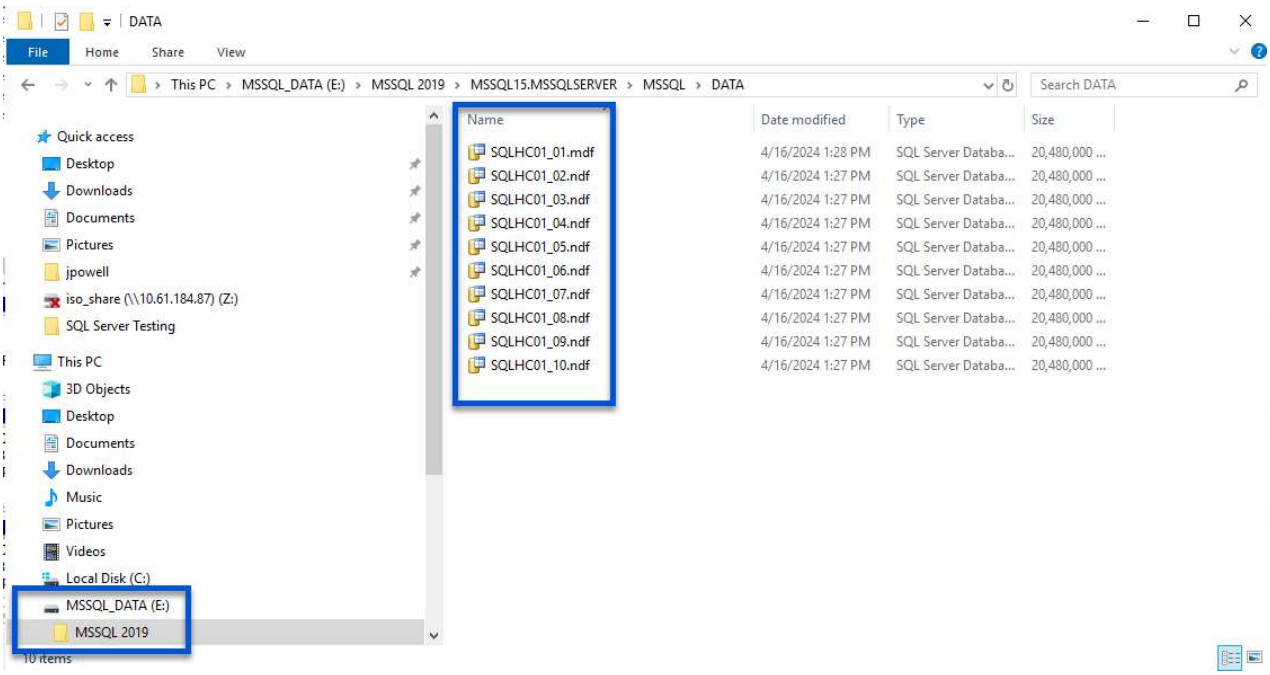
2. Wählen Sie im Assistenten **Virtuelle Festplatte(n) anhängen** die zu verwendende Sicherungsinstanz und die jeweilige anzuhängende VMDK aus.



Mithilfe von Filteroptionen können Backups gesucht und Backups sowohl von primären als auch von sekundären Speichersystemen angezeigt werden.



3. Nachdem Sie alle Optionen ausgewählt haben, klicken Sie auf die Schaltfläche **Anhängen**, um den Wiederherstellungsprozess zu starten und das VMDK an den Host anzuhängen.
4. Sobald der Anschlussvorgang abgeschlossen ist, kann vom Betriebssystem des Hostsystems auf die Festplatte zugegriffen werden. In diesem Fall hat SCV die Festplatte mit ihrem NTFS-Dateisystem an das Laufwerk E: unseres Windows SQL-Servers angeschlossen und die SQL-Datenbankdateien im Dateisystem sind über den Datei-Explorer zugänglich.



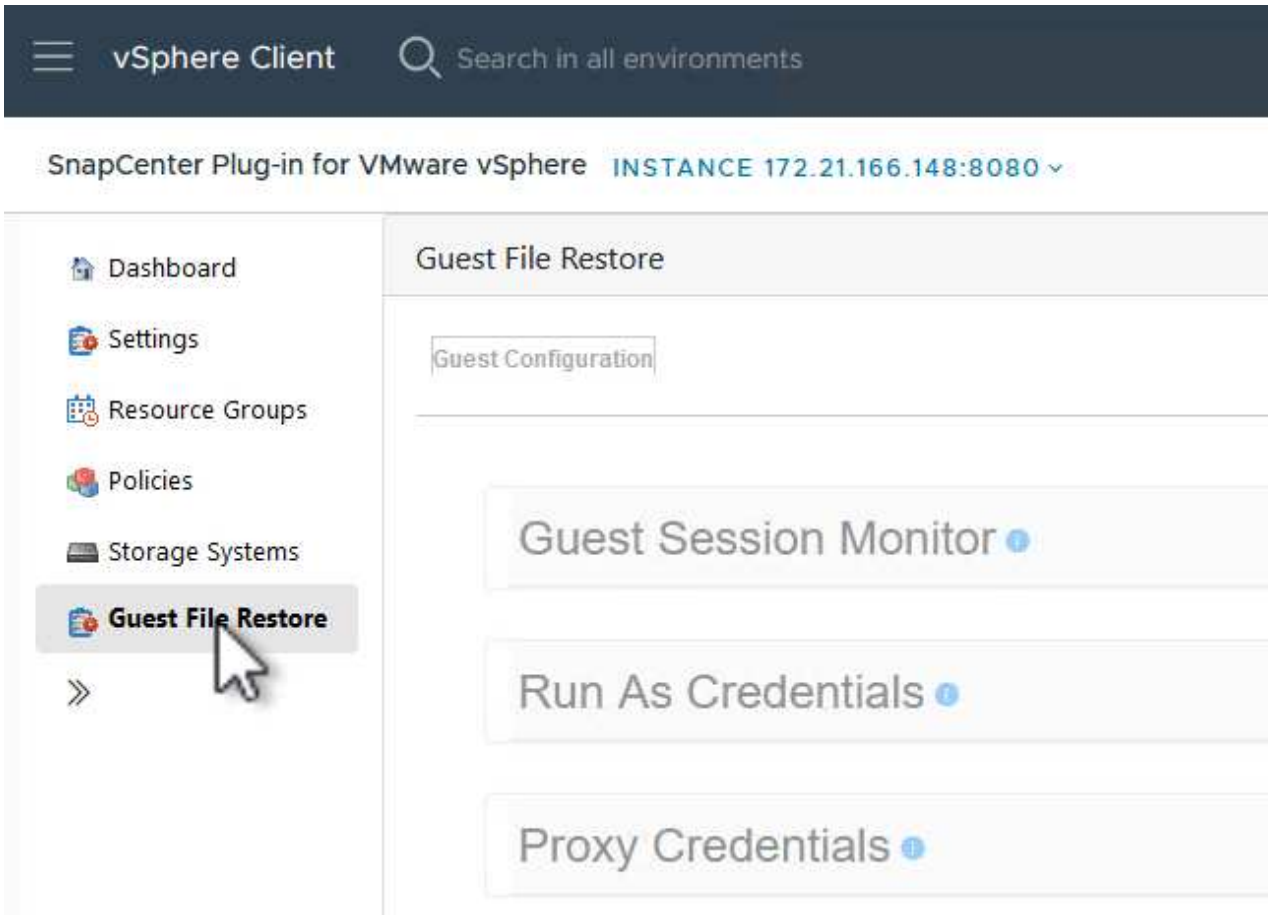
Wiederherstellung des Gastdateisystems mit dem SnapCenter -Plug-in

ONTAP Tools bietet die Möglichkeit, Gastdateisysteme von einem VMDK auf Windows Server-Betriebssystemen wiederherzustellen. Dies wird zentral über die SnapCenter Plug-in-Schnittstelle durchgeführt.

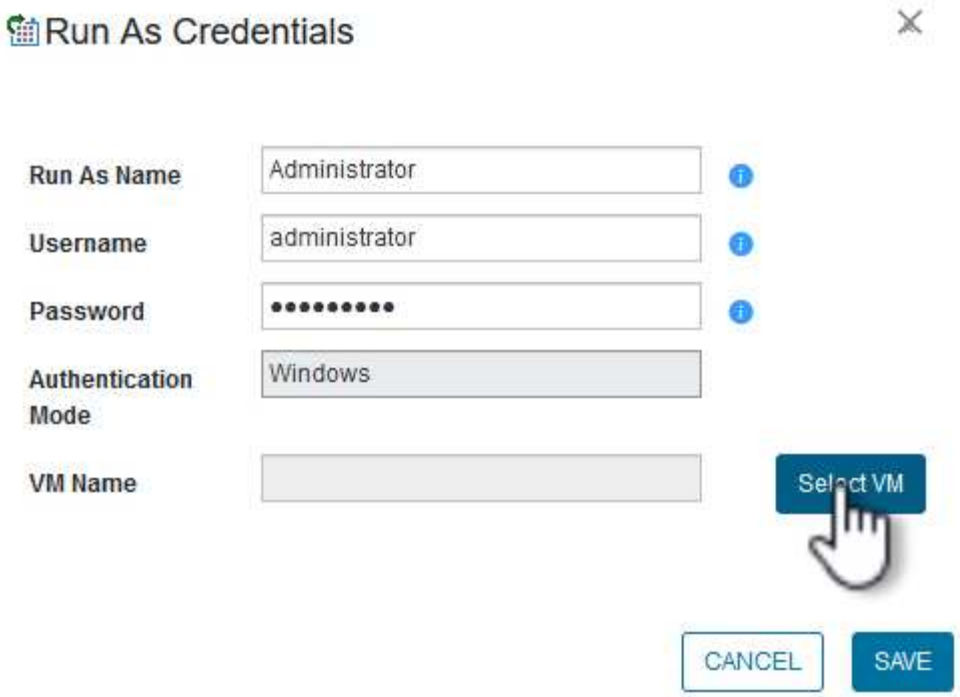
Ausführliche Informationen finden Sie unter"Wiederherstellen von Gastdateien und -ordnern" auf der SCV-Dokumentationsseite.

Führen Sie die folgenden Schritte aus, um eine Gastdateisystemwiederherstellung für ein Windows-System durchzuführen:

1. Der erste Schritt besteht darin, „Run As“-Anmeldeinformationen zu erstellen, um Zugriff auf das Windows-Hostsystem zu gewähren. Navigieren Sie im vSphere-Client zur CSV-Plugin-Oberfläche und klicken Sie im Hauptmenü auf **Guest File Restore**.

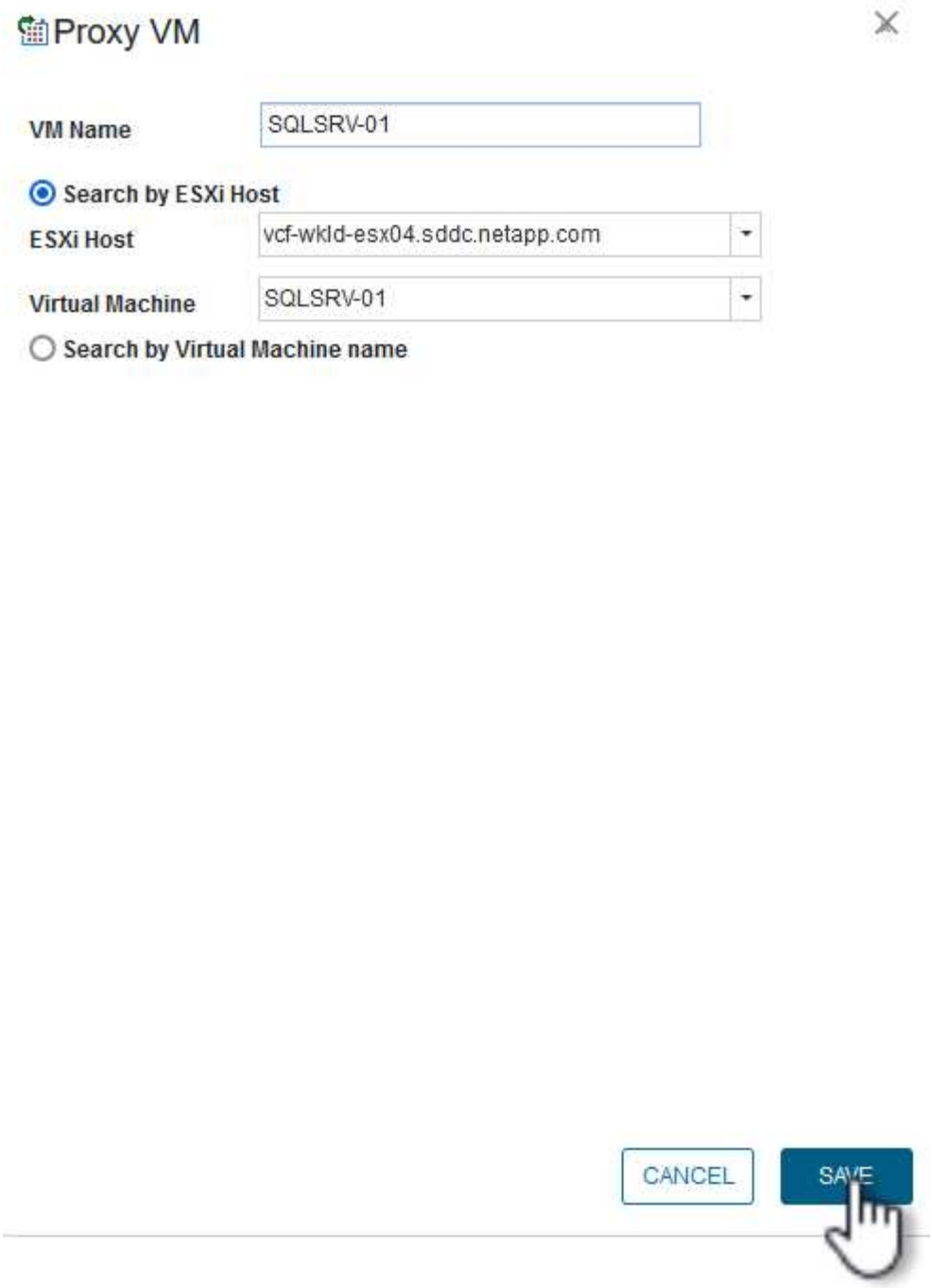


2. Klicken Sie unter **Anmeldeinformationen für „Ausführen als“** auf das Symbol **+**, um das Fenster **Anmeldeinformationen für „Ausführen als“** zu öffnen.
3. Geben Sie einen Namen für den Anmeldeinformationsdatensatz sowie einen Administratorbenutzernamen und ein Kennwort für das Windows-System ein und klicken Sie dann auf die Schaltfläche **VM auswählen**, um eine optionale Proxy-VM auszuwählen, die für die Wiederherstellung verwendet werden

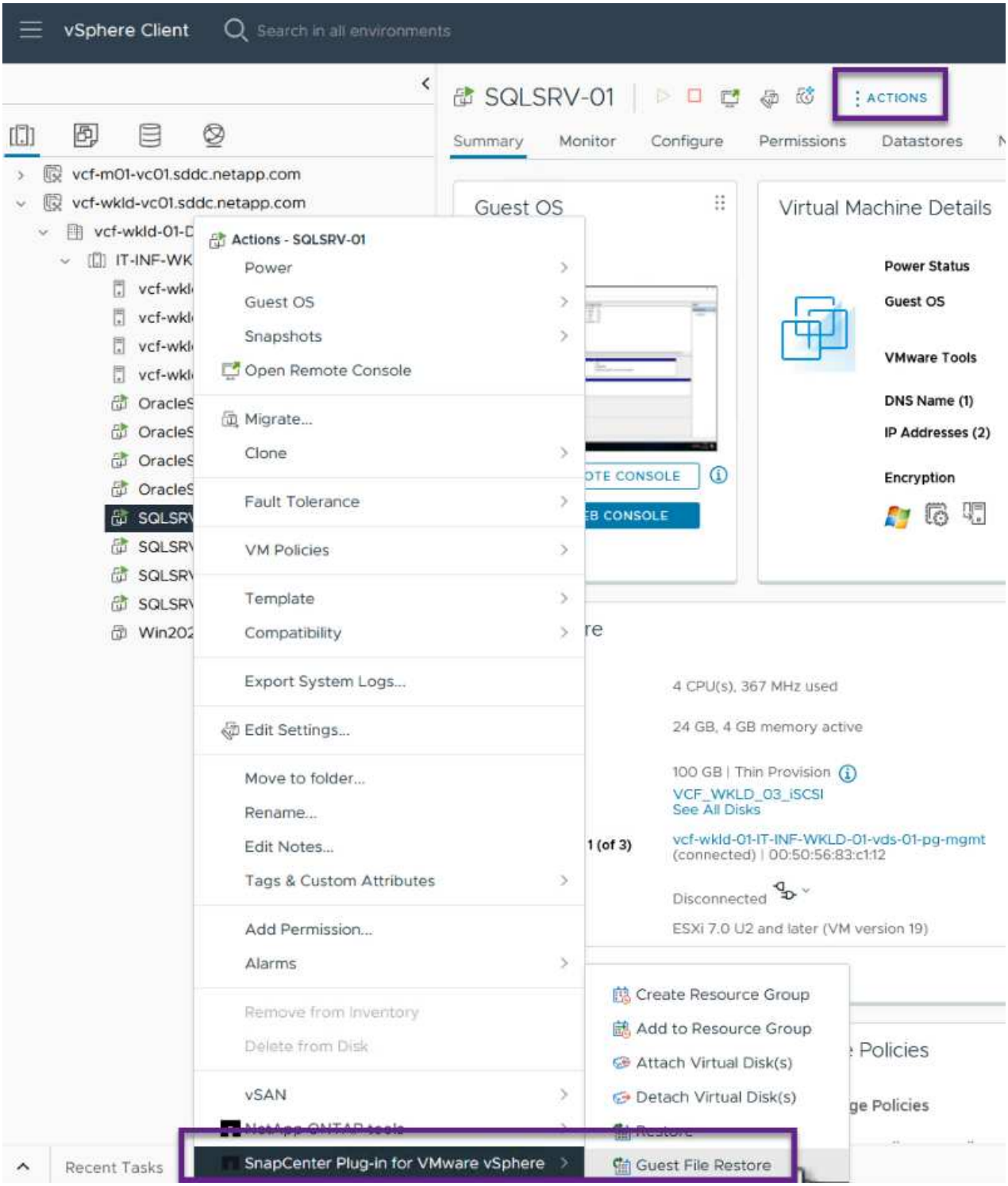


soll.

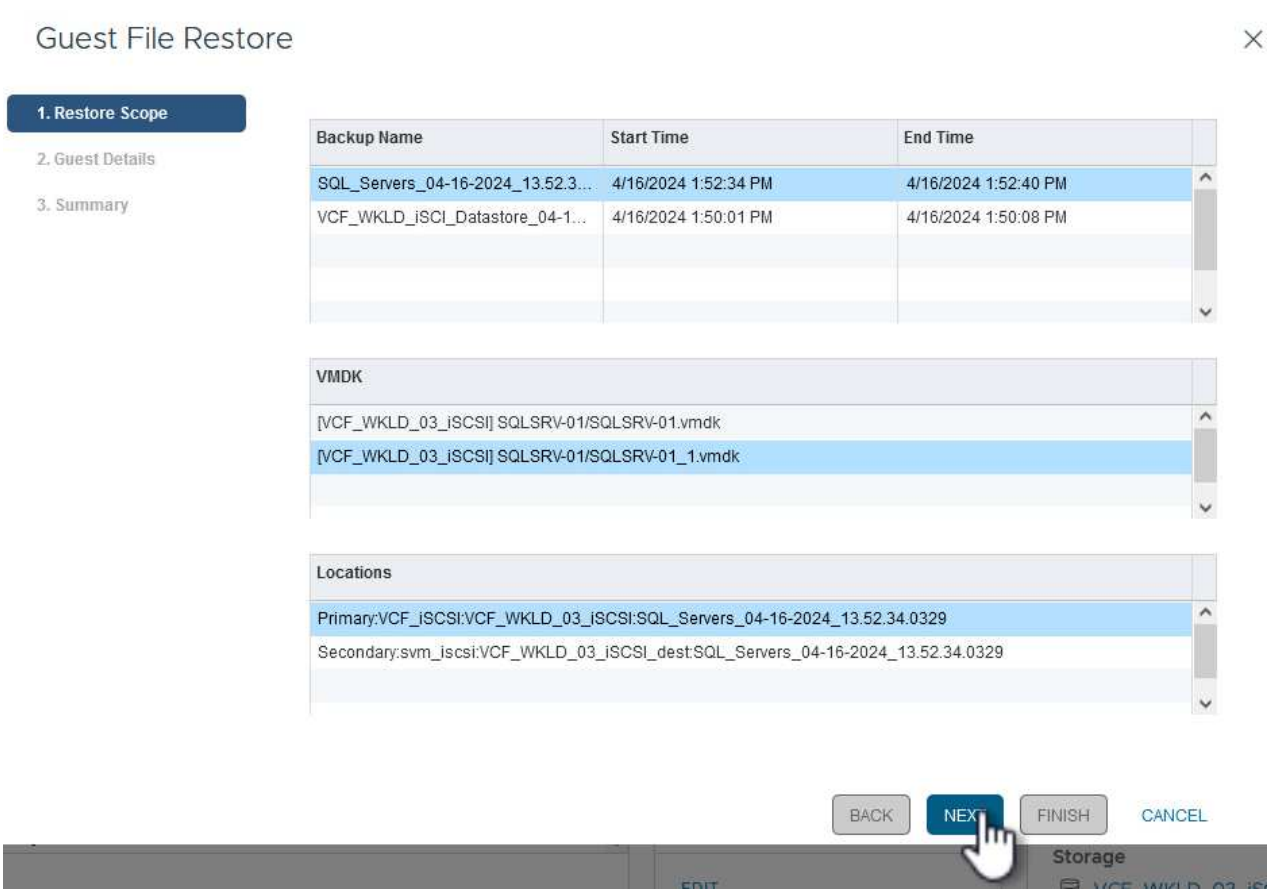
4. Geben Sie auf der Seite „Proxy-VM“ einen Namen für die VM ein und suchen Sie sie, indem Sie nach dem ESXi-Host oder dem Namen suchen. Klicken Sie nach der Auswahl auf **Speichern**.



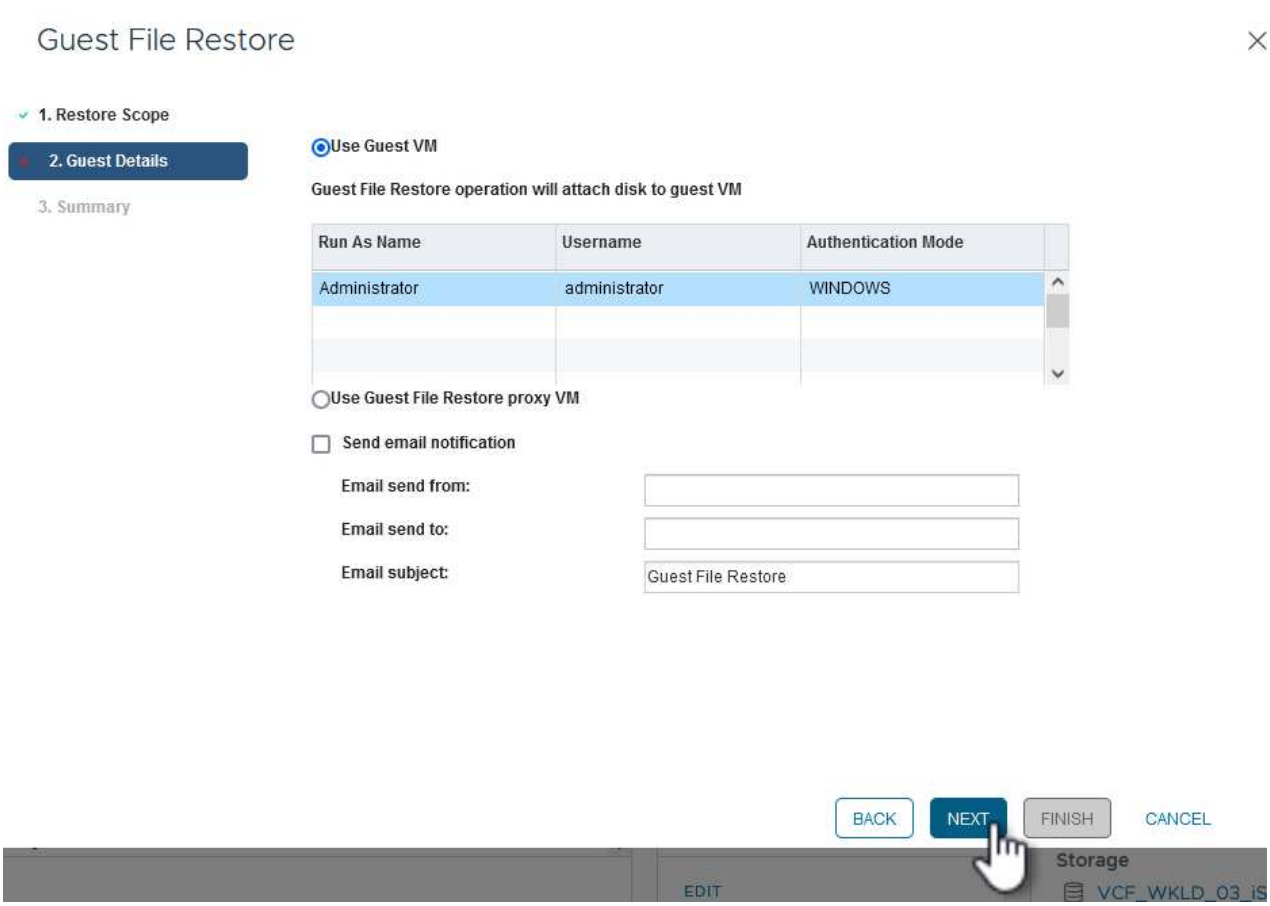
5. Klicken Sie im Fenster **Run As Credentials** erneut auf **Speichern**, um das Speichern des Datensatzes abzuschließen.
6. Navigieren Sie als Nächstes zu einer VM im Inventar. Wählen Sie im Menü **Aktionen** oder durch Rechtsklick auf die VM * SnapCenter Plug-in for VMware vSphere > Gastdateiwiederherstellung* aus.



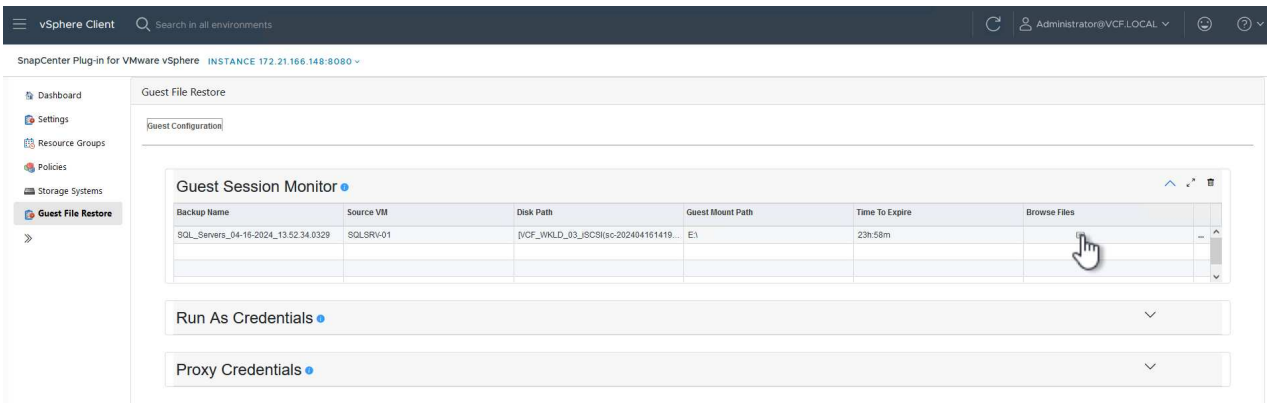
7. Wählen Sie auf der Seite **Wiederherstellungsbereich** des Assistenten **Gastdateiwiederherstellung** die Sicherung aus, aus der die Wiederherstellung erfolgen soll, das jeweilige VMDK und den Speicherort (primär oder sekundär), aus dem das VMDK wiederhergestellt werden soll. Klicken Sie auf **Weiter**, um fortzufahren.



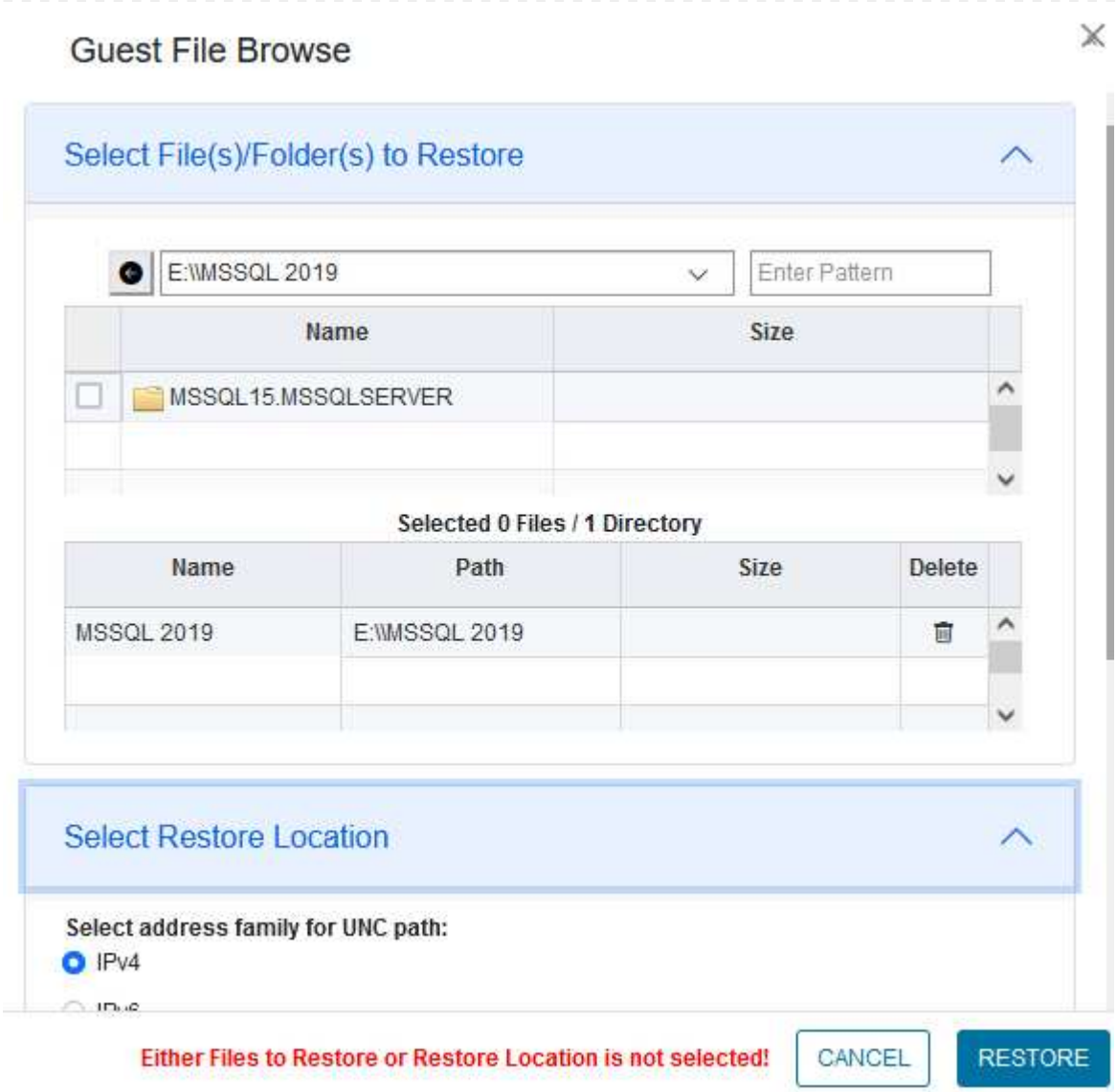
8. Wählen Sie auf der Seite **Gastdetails** aus, ob Sie für die Wiederherstellung **Gast-VM** oder **Gues File Restore-Proxy-VM verwenden** verwenden möchten. Füllen Sie hier bei Bedarf auch die Einstellungen für E-Mail-Benachrichtigungen aus. Klicken Sie auf **Weiter**, um fortzufahren.

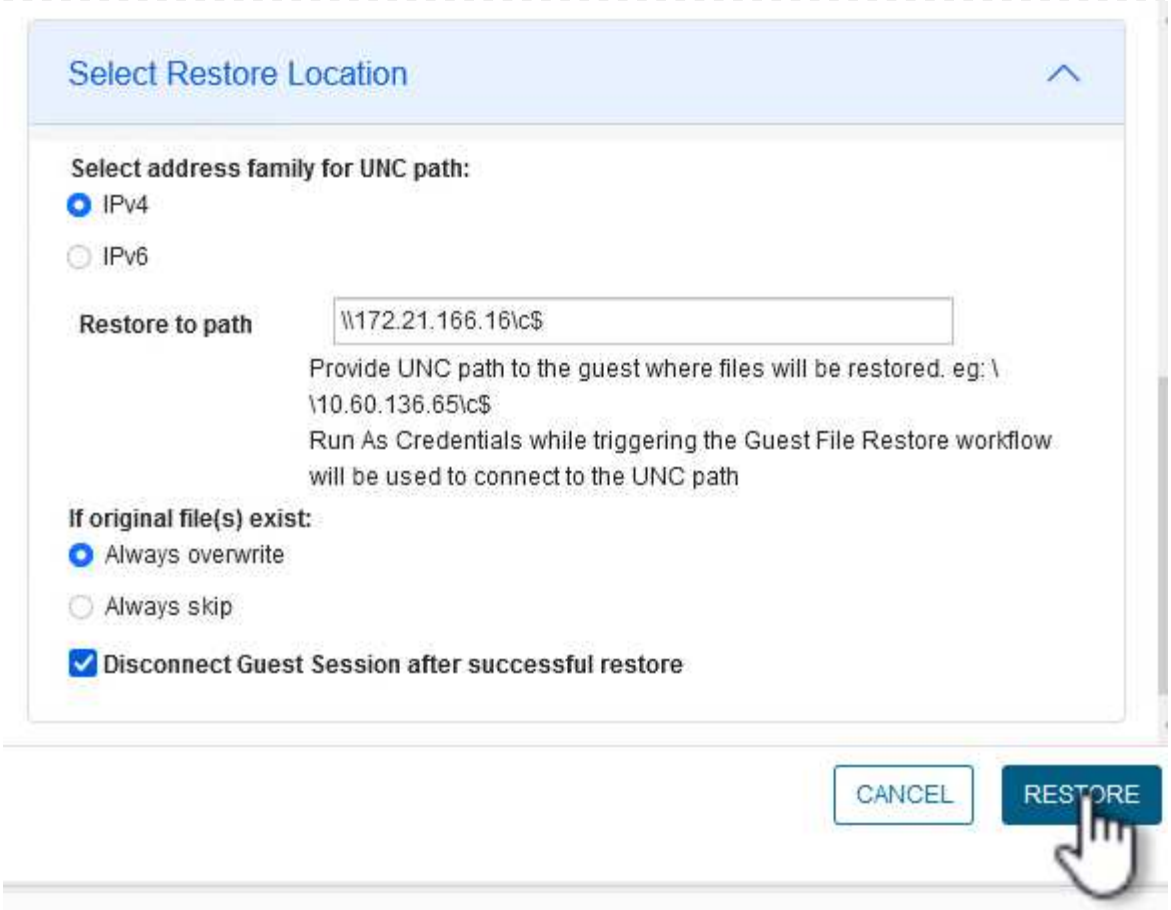


9. Überprüfen Sie abschließend die Seite **Zusammenfassung** und klicken Sie auf **Fertig**, um die Sitzung zur Wiederherstellung des Gastdateisystems zu starten.
10. Navigieren Sie zurück in der SnapCenter -Plug-in-Oberfläche erneut zu **Guest File Restore** und zeigen Sie die laufende Sitzung unter **Guest Session Monitor** an. Klicken Sie auf das Symbol unter **Dateien durchsuchen**, um fortzufahren.



11. Wählen Sie im Assistenten **Guest File Browse** den Ordner oder die Dateien aus, die wiederhergestellt werden sollen, und den Speicherort im Dateisystem, an dem sie wiederhergestellt werden sollen. Klicken Sie abschließend auf **Wiederherstellen**, um den **Wiederherstellungs** -Prozess zu starten.


Guest File Browse
Select File(s)/Folder(s) to Restore
E:\\MSSQL 2019
Enter Pattern
Name
Size
MSSQL15.MSSQLSERVER
Selected 0 Files / 1 Directory
Name
Path
Size
Delete
MSSQL 2019
E:\\MSSQL 2019
Select Restore Location
Select address family for UNC path:
IPv4
Either Files to Restore or Restore Location is not selected!
CANCEL
RESTORE



12. Der Wiederherstellungsjob kann über den Aufgabenbereich des vSphere-Clients überwacht werden.

Weitere Informationen

Informationen zur Konfiguration von VCF finden Sie unter "VMware Cloud Foundation-Dokumentation" .

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im "ONTAP 9 Dokumentation" Center.

Informationen zur Verwendung des SnapCenter Plug-in for VMware vSphere finden Sie im "SnapCenter Plug-in for VMware vSphere Dokumentation" .

Schützen Sie VCF-Verwaltungs- und Workloaddomänen mit dem SnapCenter -Plug -in für VMware vSphere

Verwenden Sie das SnapCenter Plug-in for VMware vSphere, um mehrere VCF-Domänen zu schützen. Dieses Verfahren umfasst das Einrichten des Plug-Ins für jede Domäne, das Konfigurieren von Sicherungsrichtlinien und das Durchführen von Wiederherstellungsvorgängen.

Mithilfe von VMware Cloud Foundation (VCF)-Workloaddomänen können Unternehmen Ressourcen logisch in verschiedene Domänen aufteilen, um unterschiedliche Workloads zu gruppieren und die Sicherheit und Fehlertoleranz zu verbessern.

Einführung

Domänen können unabhängig skaliert werden, bestimmte Konformitäten erfüllen und Multitenancy bieten. Der Datenschutz für VMware Cloud Foundation (VCF) ist ein entscheidender Aspekt, um die Verfügbarkeit, Integrität und Wiederherstellbarkeit von Daten in der gesamten Verwaltungsdomäne und den Workload-Domänen sicherzustellen. Das NetApp SnapCenter Plug-in for VMware vSphere (SCV) ist ein leistungsstarkes Tool, das die Datenschutzfunktionen von NetApp in VMware-Umgebungen integriert. Es vereinfacht die Sicherung, Wiederherstellung und das Klonen von virtuellen VMware vSphere-Maschinen (VMs), die auf NetApp -Speicher gehostet werden.

Dieses Dokument enthält Bereitstellungsschritte zum Schutz mehrerer VCF-Domänen mit SCV.

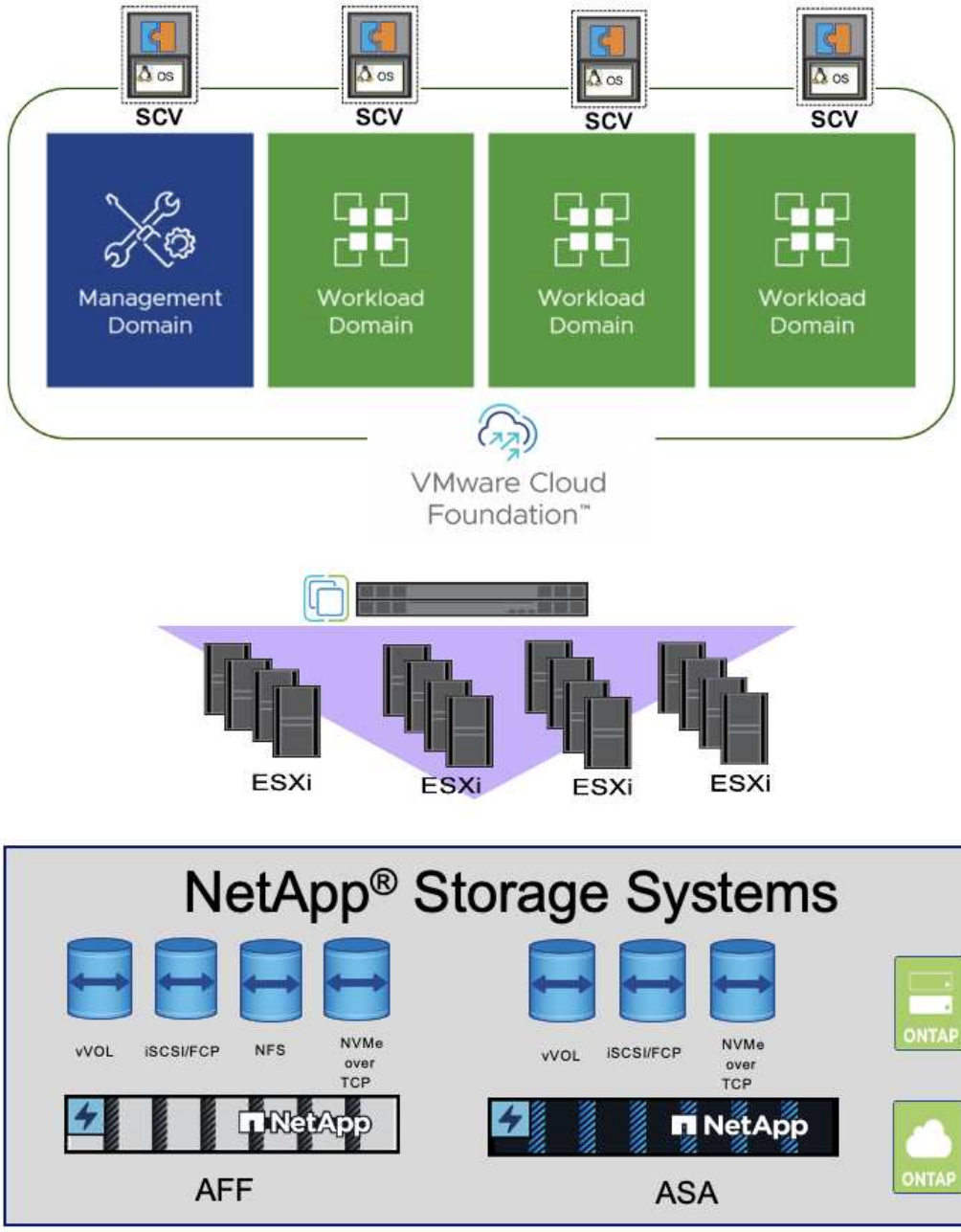
Publikum

Lösungsarchitekten oder Speicheradministratoren, die Datenschutz und Notfallwiederherstellung für VMware VCF-Workloaddomänen sicherstellen.

Architekturübersicht

SCV wird als virtuelle Linux-Appliance mithilfe einer OVA-Datei bereitgestellt, um schnelle, platzsparende, absturzkonsistente und VM-konsistente Sicherungs- und Wiederherstellungsvorgänge für VMs, Datenspeicher sowie Dateien und Ordner bereitzustellen. SCV verwendet eine Remote-Plug-In-Architektur. Es wurden mehrere SCVs bereitgestellt und auf der VCF-Verwaltungsdomäne vCenter gehostet. Zwischen SCV- und VCF-Domäne besteht eine Eins-zu-eins-Beziehung, daher ist für die VCF-Verwaltungsdomäne und jede Workloaddomäne ein SCV erforderlich.

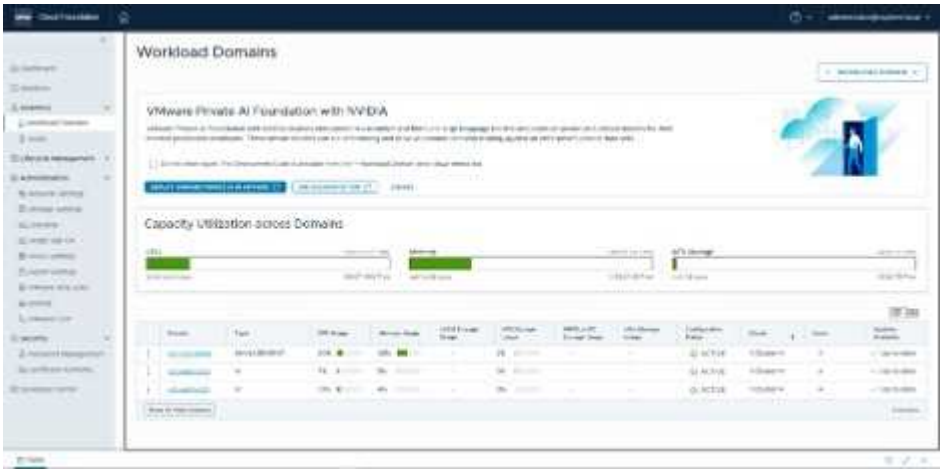
Daten, die sich auf primären ONTAP FAS, AFF oder All SAN Array (ASA)-Systemen befinden und auf sekundäre ONTAP FAS, AFF oder ASA Systeme repliziert werden. SCV arbeitet auch mit SnapCenter Server zusammen, um anwendungsbasierte Sicherungs- und Wiederherstellungsvorgänge in VMware-Umgebungen für anwendungsspezifische SnapCenter -Plug-Ins zu unterstützen. Weitere Informationen finden Sie unter"SnapCenter Plug-in for VMware vSphere Dokumentation."



Die 3-2-1-Backup-Regel ist eine Datenschutzstrategie, bei der drei Kopien der Daten erstellt, auf zwei verschiedenen Medientypen gespeichert und eine Kopie extern aufbewahrt wird. BlueXP backup and recovery ist ein Cloud-basiertes Tool für die Datenverwaltung, das eine einzige Kontrollebene für eine breite Palette von Backup- und Wiederherstellungsvorgängen sowohl in lokalen als auch in Cloud-Umgebungen bietet. Teil der BlueXP backup and recovery Suite NetApp BlueXP ist eine Funktion, die sich in SCV (vor Ort) integrieren lässt, um eine Kopie der Daten auf den Objektspeicher in der Cloud zu erweitern. Dadurch wird eine dritte Kopie der Daten außerhalb des Standorts erstellt, die aus den Backups des primären oder sekundären Speichers stammt. Mit BlueXP backup and recovery können Sie ganz einfach Speicherrichtlinien einrichten, die Kopien Ihrer Daten von einem dieser beiden lokalen Standorte übertragen. Weitere Einzelheiten finden Sie unter"3-2-1-Datenschutz für VMware mit SnapCenter -Plug-in und BlueXP backup and recovery für VMs" .

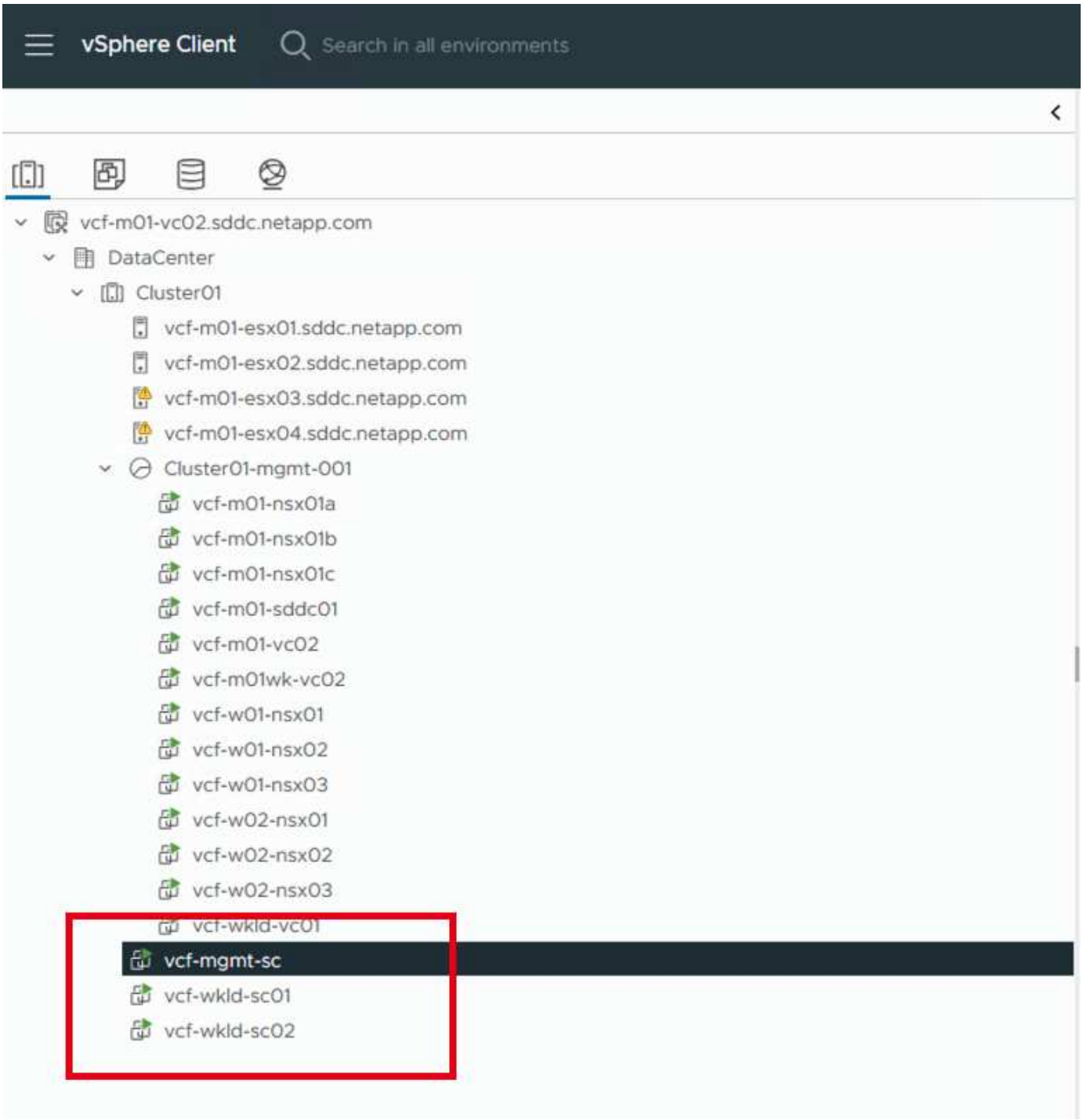
Bereitstellen eines VCF mit Verwaltungsdomäne und mehreren Workloaddomänen

Eine VCF-Workloaddomäne ist eine Gruppe von ESXi-Hosts mit einem oder mehreren vSphere-Clustern, die vom SDDC Manager bereitgestellt werden und anwendungsbereit sind. In einem VCF-Beispiel unten wurden eine Verwaltungsdomäne und zwei Workloaddomänen bereitgestellt. Weitere Informationen zur Bereitstellung von VCF mit NetApp -Speicher finden Sie unter"Dokumentation zur NetApp VCF-Bereitstellung."



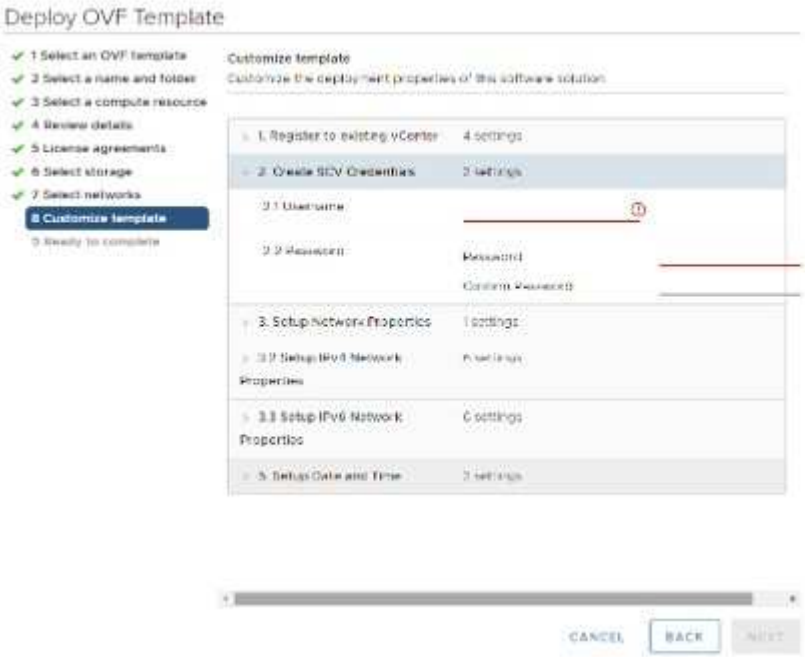
SCV-Bereitstellung, Konfiguration und Wiederherstellungsschritte

Basierend auf der Anzahl der Workloaddomänen und der Verwaltungsdomäne müssen mehrere SCVs bereitgestellt werden. Mit zwei Workloaddomänen und einer Verwaltungsdomäne zeigt das folgende Beispiel, dass drei SCVs auf der VCF-Verwaltungsdomäne vCenter bereitgestellt werden.


vSphere Client
Search in all environments
vcf-m01-vc02.sddc.netapp.com
DataCenter
Cluster01
vcf-m01-esx01.sddc.netapp.com
vcf-m01-esx02.sddc.netapp.com
vcf-m01-esx03.sddc.netapp.com
vcf-m01-esx04.sddc.netapp.com
Cluster01-mgmt-001
vcf-m01-nsx01a
vcf-m01-nsx01b
vcf-m01-nsx01c
vcf-m01-sddc01
vcf-m01-vc02
vcf-m01wk-vc02
vcf-w01-nsx01
vcf-w01-nsx02
vcf-w01-nsx03
vcf-w02-nsx01
vcf-w02-nsx02
vcf-w02-nsx03
vcf-wkld-vc01
vcf-mgmt-sc
vcf-wkld-sc01
vcf-wkld-sc02

SCV für die Verwaltungsdomäne und jede Workloaddomäne bereitstellen

1. "Laden Sie die Open Virtual Appliance (OVA) herunter."
2. Melden Sie sich mit dem vSphere-Client beim vCenter Server an. Navigieren Sie zu Verwaltung > Zertifikate > Zertifikatsverwaltung. Fügen Sie vertrauenswürdige Stammzertifikate hinzu und installieren Sie jedes Zertifikat im Ordner „Certs“. Sobald die Zertifikate installiert sind, kann OVA überprüft und bereitgestellt werden.
3. Melden Sie sich beim vCenter der VCF-Workloaddomäne an und stellen Sie die OVF-Vorlage bereit, um den VMware-Bereitstellungsassistenten zu

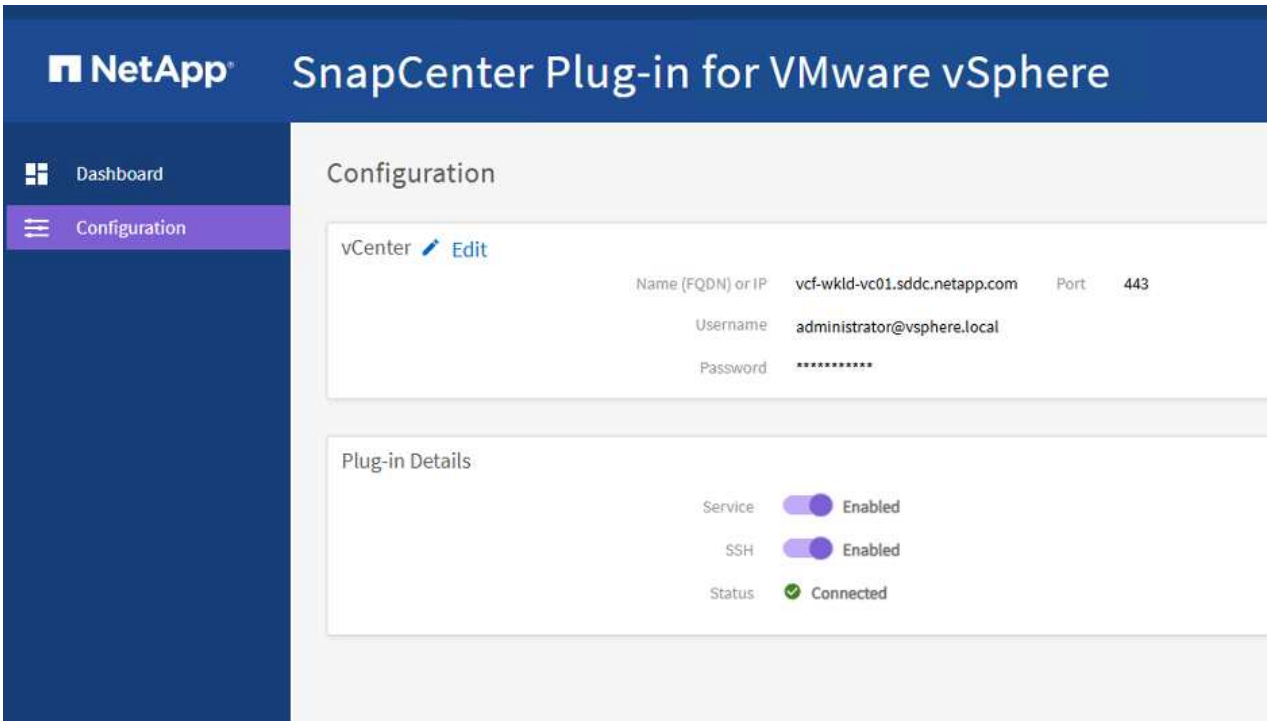


   starten.

4. Schalten Sie OVA ein, um SCV zu starten, und klicken Sie dann auf „VMware-Tools installieren“.
5. Generieren Sie das MFA-Token aus der OVA-Konsole, Systemkonfigurationsmenü.

```
System Configuration Menu:
--------------------------
   1 ) Reboot virtual machine
   2 ) Shut down virtual machine
   3 ) Change 'maint' user password
   4 ) Change time zone
   5 ) Change NTP server
   6 ) Enable SSH access
   7 ) Increase jail disk size (/jail)
   8 ) Upgrade
   9 ) Install VMware Tools
  10 ) Generate MFA Token

   b ) Back
   x ) Exit

Enter your choice: 10


Generating MFA Token... Your MFA Token is : 435164

Press ENTER to continue._
```

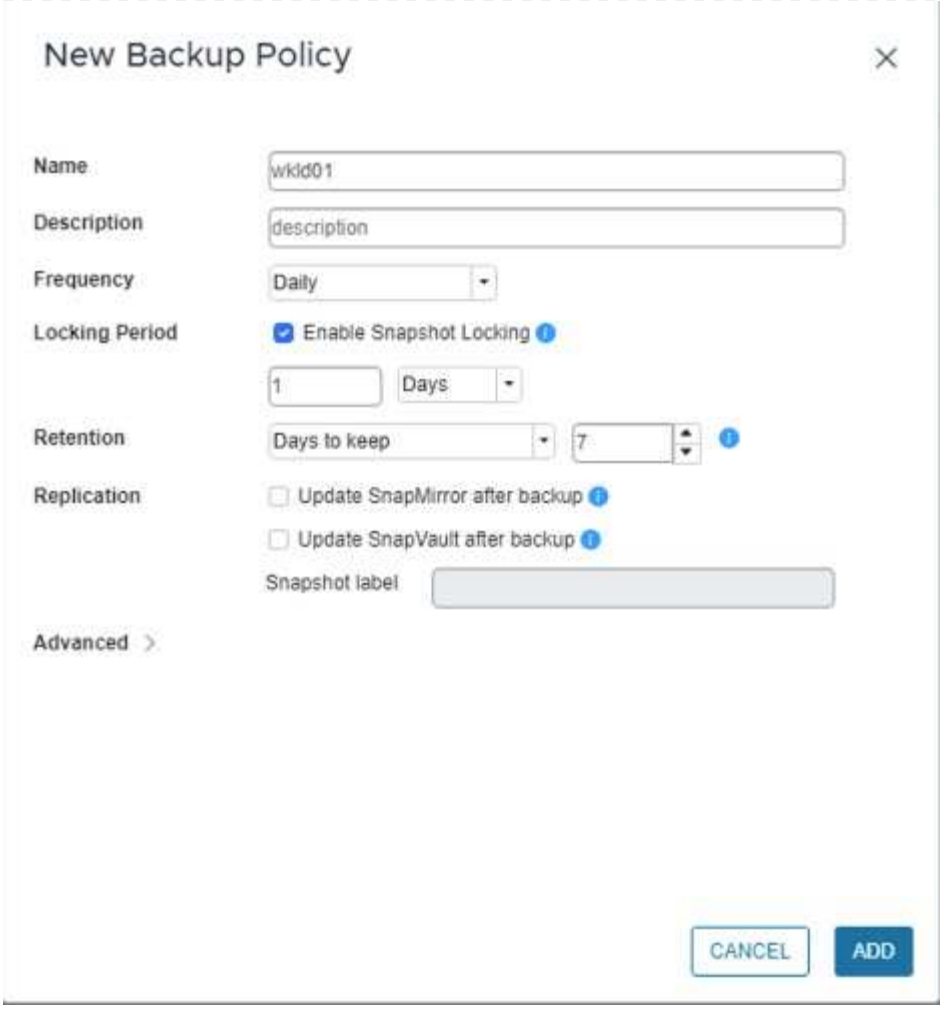
6. Melden Sie sich bei der SCV-Verwaltungs-GUI mit dem zum Zeitpunkt der Bereitstellung festgelegten Administratorbenutzernamen und -kennwort sowie dem mithilfe der Wartungskonsole generierten MFA-Token an.
   `https://<appliance-IP-address>:8080` um auf die Verwaltungs-GUI zuzugreifen.



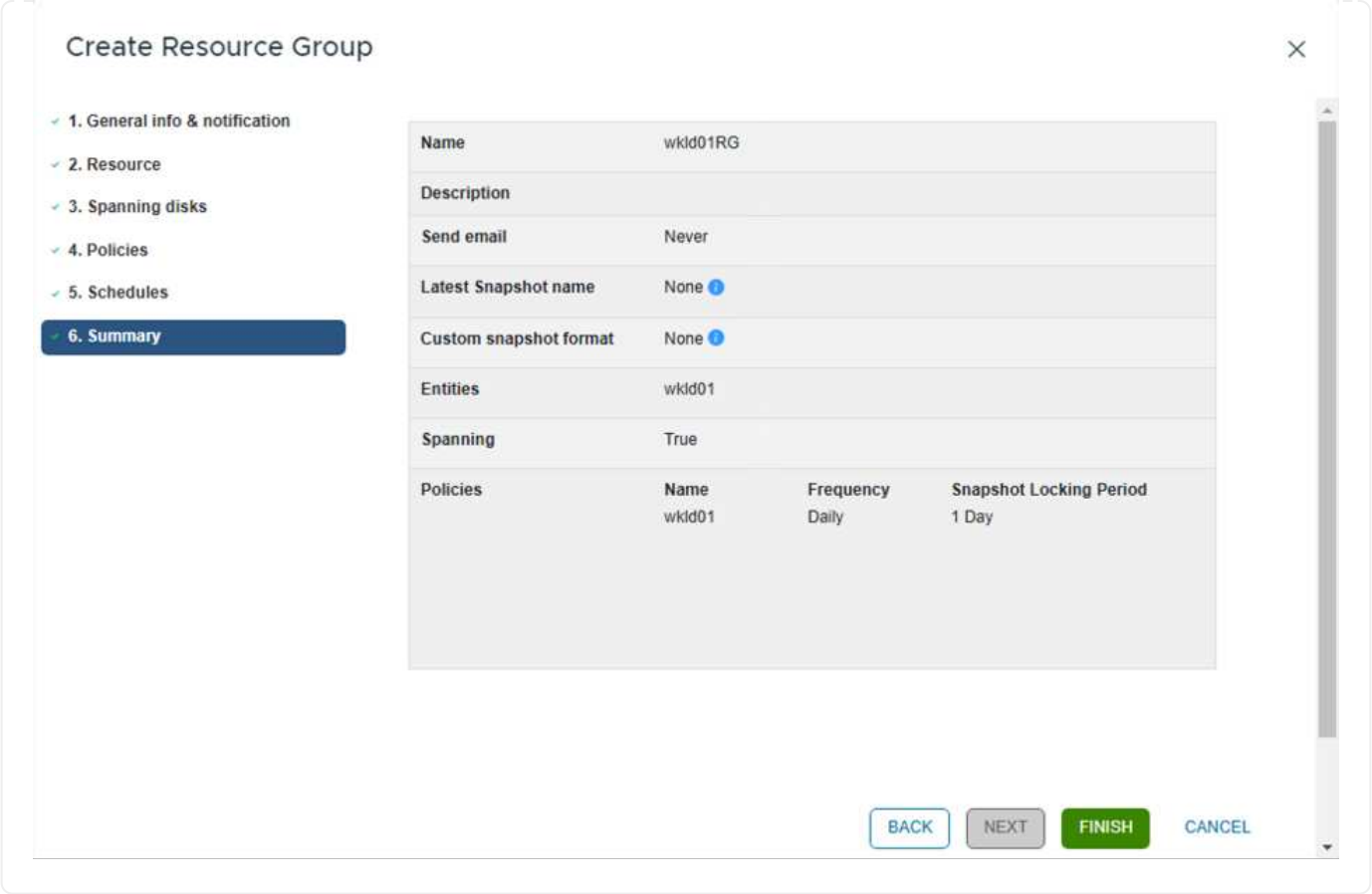
SCV konfigurieren

Um VMs zu sichern oder wiederherzustellen, fügen Sie zunächst die Speichercluster oder VMs hinzu, die die Datenspeicher hosten, erstellen Sie dann Sicherungsrichtlinien für die Aufbewahrung und Häufigkeit und richten Sie eine Ressourcengruppe zum Schutz der Ressourcen
ein.

1. Melden Sie sich beim vCenter-Webclient an, klicken Sie in der Symbolleiste auf „Menü“, wählen Sie „SnapCenter Plug-in for VMware vSphere“ und „Speicher hinzufügen“ aus. Klicken Sie im linken Navigationsbereich des SCV-Plug-Ins auf „Speichersysteme“ und wählen Sie dann die Option „Hinzufügen“ aus. Geben Sie im Dialogfeld „Speichersystem hinzufügen“ die grundlegenden SVM- oder Clusterinformationen ein und wählen Sie „Hinzufügen“ aus. Geben Sie die IP-Adresse des NetApp -Speichers ein und melden Sie sich an.
2. Um eine neue Sicherungsrichtlinie zu erstellen, klicken Sie im linken Navigationsbereich des SCV-Plug-Ins auf „Richtlinien“ und wählen Sie „Neue Richtlinie“ aus. Geben Sie auf der Seite „Neue Sicherungsrichtlinie“ die Richtlinienkonfigurationsinformationen ein und klicken Sie auf „Hinzufügen“.



3. Klicken Sie im linken Navigationsbereich des SCV-Plug-Ins auf „Ressourcengruppen“ und wählen Sie dann „Erstellen“ aus. Geben Sie auf jeder Seite des Assistenten „Ressourcengruppe erstellen“ die erforderlichen Informationen ein, wählen Sie VMs und Datenspeicher aus, die in die Ressourcengruppe aufgenommen werden sollen, und wählen Sie dann die Sicherungsrichtlinien aus, die auf die Ressourcengruppe angewendet werden sollen, und geben Sie den Sicherungszeitplan an.

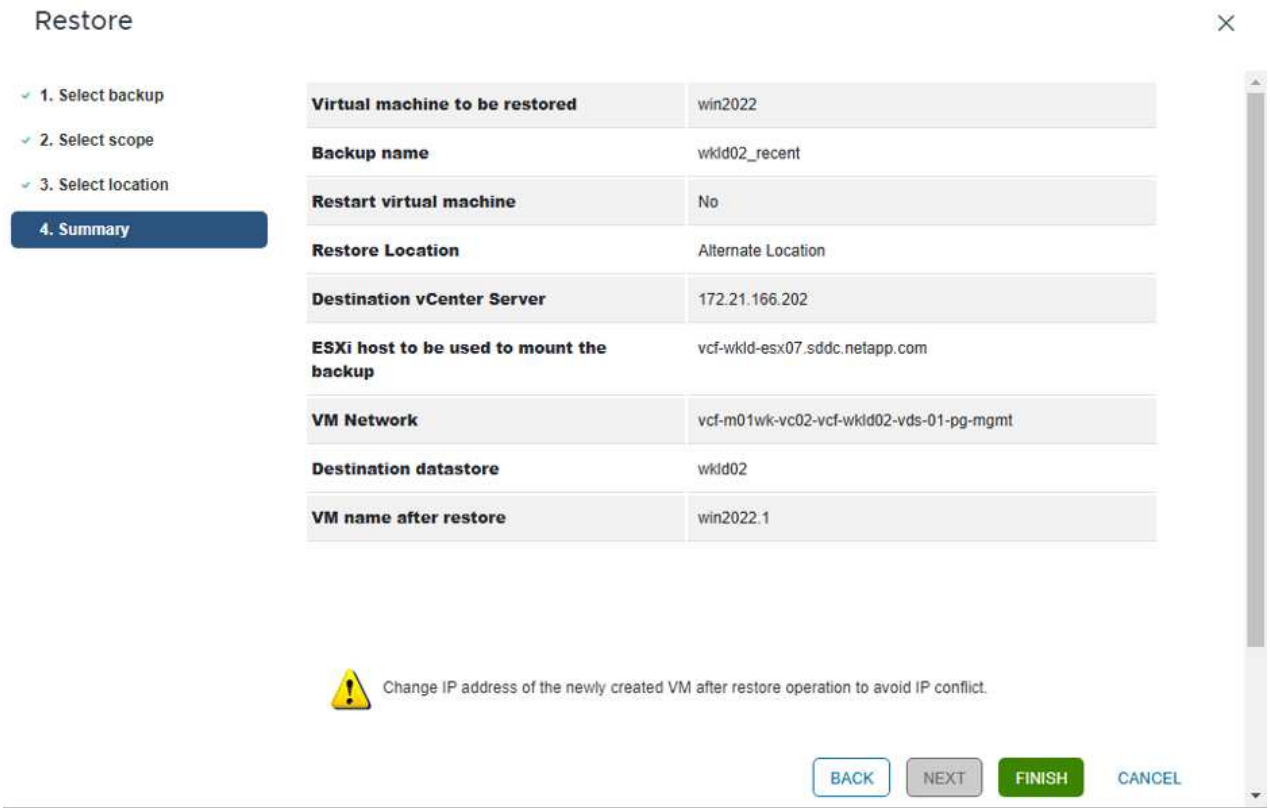

Create Resource Group
1. General info & notification
2. Resource
3. Spanning disks
4. Policies
5. Schedules
6. Summary
Name
wkld01RG
Description
Send email
Never
Latest Snapshot name
None
Custom snapshot format
None
Entities
wkld01
Spanning
True
Policies
Name
wkld01
Frequency
Daily
Snapshot Locking Period
1 Day
BACK
NEXT
FINISH
CANCEL

Wiederherstellen von VM- und Datei- oder Ordner-Backups

VMs, VMDKs, Dateien und Ordner aus Backups können wiederhergestellt werden. Die VM kann auf dem ursprünglichen Host oder einem alternativen Host im selben vCenter-Server oder auf einem alternativen ESXi-Host wiederhergestellt werden, der vom selben vCenter verwaltet wird. Sie können einen herkömmlichen Datenspeicher aus einer Sicherung mounten, wenn Sie auf Dateien in der Sicherung zugreifen möchten. Sie können das Backup entweder auf demselben ESXi-Host mounten, auf dem das Backup erstellt wurde, oder auf einem alternativen ESXi-Host, der über denselben VM-Typ und dieselben Hostkonfigurationen verfügt. Sie können einen Datenspeicher mehrmals auf einem Host mounten. Einzelne Dateien und Ordner können auch in einer Dateiwiederherstellungssitzung des Gastes wiederhergestellt werden, bei der eine Sicherungskopie einer virtuellen Festplatte angehängt und dann die ausgewählten Dateien oder Ordner wiederhergestellt werden. Auch Dateien und Ordner können wiederhergestellt werden.

VM-Wiederherstellungsschritte

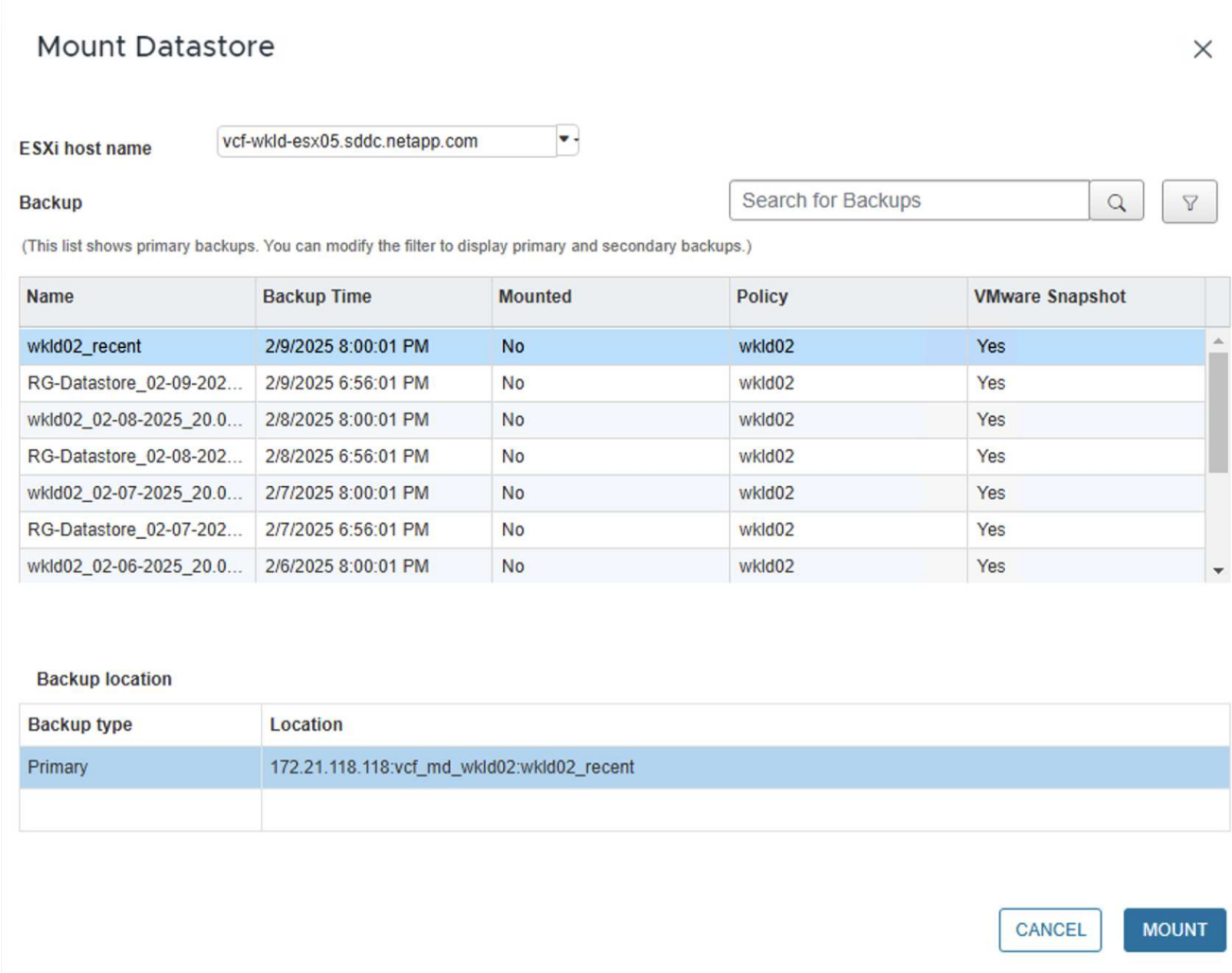
1. Klicken Sie in der GUI des VMware vSphere-Clients in der Symbolleiste auf „Menü“ und wählen Sie „VMs und Vorlagen“ aus der Dropdownliste aus. Klicken Sie mit der rechten Maustaste auf eine VM und wählen Sie „SnapCenter Plug-in for VMware vSphere“ aus der Dropdownliste aus. Wählen Sie dann „Wiederherstellen“ aus der sekundären Dropdownliste aus, um den Assistenten zu starten.
2. Wählen Sie im Wiederherstellungsassistenten den Sicherungs-Snapshot aus, den Sie wiederherstellen möchten, und wählen Sie im Feld „Wiederherstellungsbereich“ die Option „Gesamte virtuelle Maschine“ aus. Wählen Sie den Wiederherstellungsort aus und geben Sie dann die Zielinformationen ein, unter denen die Sicherung bereitgestellt werden soll. Wählen Sie auf der Seite „Speicherort auswählen“ den Speicherort für den wiederhergestellten Datenspeicher aus. Überprüfen Sie die Seite „Zusammenfassung“ und klicken Sie auf „Fertig stellen“.



3. Überwachen Sie den Vorgangsfortschritt, indem Sie unten auf dem Bildschirm auf „Letzte Aufgaben“ klicken.

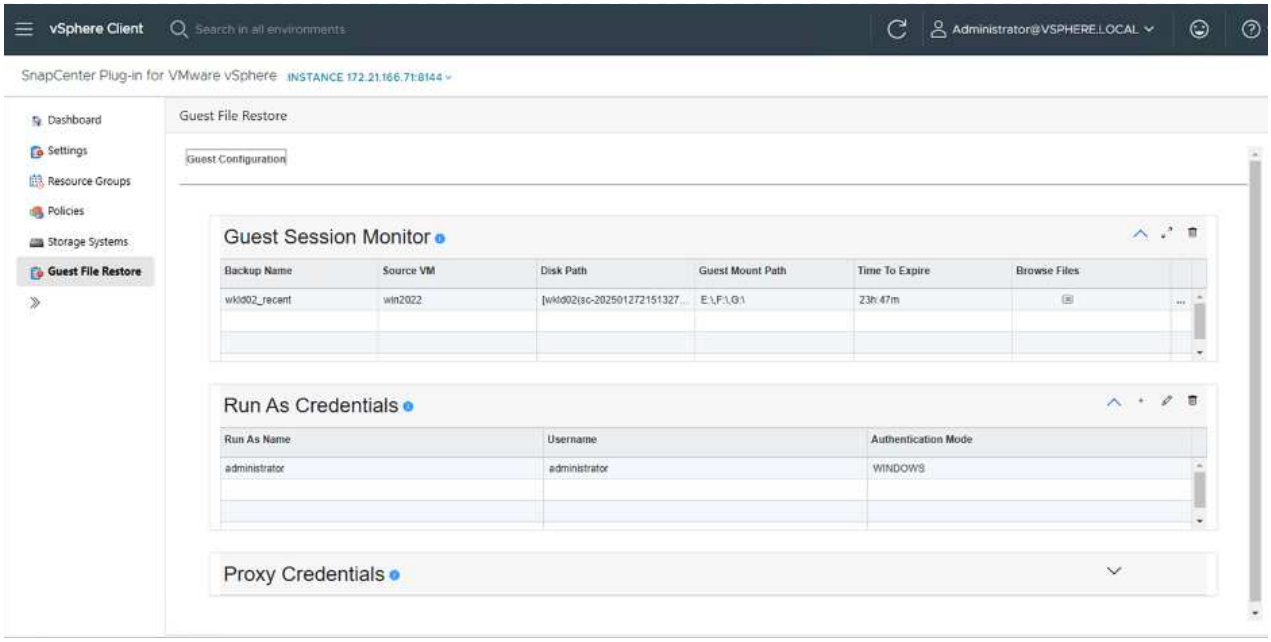
Schritte zur Datenspeicherwiederherstellung

1. Klicken Sie mit der rechten Maustaste auf einen Datenspeicher und wählen Sie „SnapCenter Plug-in for VMware vSphere“ > „Backup mounten“.
2. Wählen Sie auf der Seite „Datenspeicher bereitstellen“ eine Sicherung und einen Sicherungsspeicherort (primär oder sekundär) aus und klicken Sie dann auf „Befestigen“.

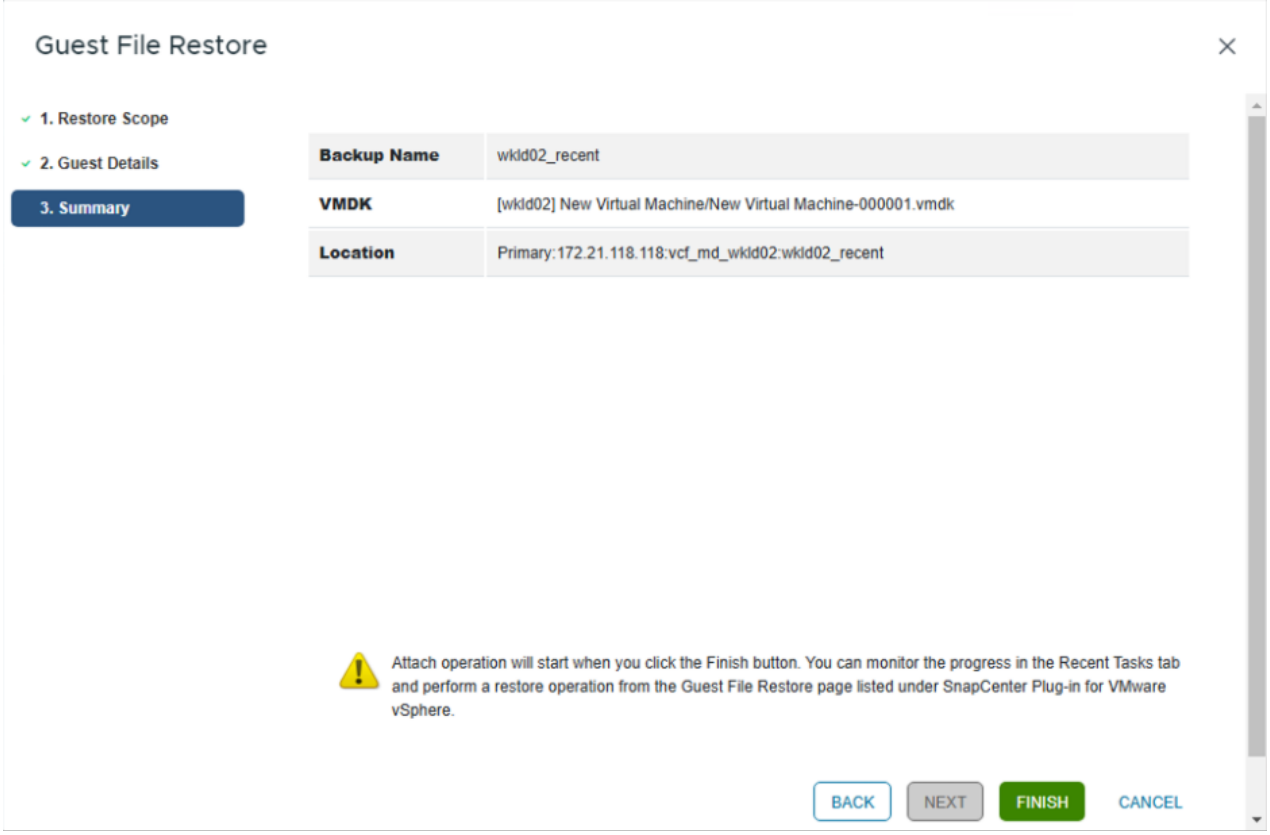


Schritte zum Wiederherstellen von Dateien und Ordnern

1. Wenn Sie für Datei- oder Ordnerwiederherstellungsvorgänge von Gastbenutzern eine virtuelle Festplatte anhängen, müssen vor der Wiederherstellung die Anmeldeinformationen der Ziel-VM für den Anschluss konfiguriert sein. Wählen Sie im SnapCenter Plug-in for VMware vSphere unter Plug-ins die Option „Guest File Restore“ und „Run As Credentials“ aus und geben Sie die Benutzeranmeldeinformationen ein. Als Benutzernamen müssen Sie „Administrator“ eingeben.



2. Klicken Sie im vSphere-Client mit der rechten Maustaste auf die VM und wählen Sie „SnapCenter Plug-in for VMware vSphere“ > „Guest File Restore“. Geben Sie auf der Seite „Wiederherstellungsbereich“ den Sicherungsnamen, die virtuelle VMDK-Festplatte und den Speicherort – primär oder sekundär – an. Klicken Sie zur Bestätigung auf „Zusammenfassung“.



NetApp SnapCenter für VCP Multi-Domain zentralisiert den Datenschutz, reduziert effizient den Zeit- und Speicherplatzbedarf für Backups mithilfe von NetApp Snapshots, unterstützt große VMware-Umgebungen mit robusten Backup- und Replikationsfunktionen und ermöglicht die granulare Wiederherstellung ganzer VMs,

bestimmter VMDKs oder einzelner Dateien.

Videodemo zum Schützen mehrerer VCF-Domänen mit SCV

Schützen Sie mehrere VMware VCF-Domänen mit NetApp SCV

Schützen Sie VCF-Workload-Domänen mit NVMe über TCP-Speicher und SnapCenter -Plug-in für VMware vSphere

Verwenden Sie das SnapCenter Plug-in for VMware vSphere, um VCF-Workloaddomänen mit NVMe zu schützen. Dieses Verfahren umfasst das Einrichten des Plug-ins, das Konfigurieren von NVMe über TCP für optimale Leistung und das Durchführen von Sicherungs-, Wiederherstellungs- oder Klonvorgängen.

NVMe (Non-Volatile Memory Express) über TCP ist ein hochmodernes Netzwerkprotokoll, das die Hochgeschwindigkeitsdatenübertragung zwischen VMware Cloud Foundation ESXi-Servern und NetApp -Speicher, einschließlich All Flash FAS (AFF) und All SAN Array (ASA), ermöglicht.

Einführung

Die Nutzung von NVMe über TCP bietet geringe Latenz und hohen Durchsatz für anspruchsvolle Workloads. Die Integration von NVMe über TCP mit dem NetApp SnapCenter Plug-in for VMware vSphere (SCV) bietet eine leistungsstarke Kombination für effizientes Datenmanagement und verbessert Backup-, Wiederherstellungs- und Klonvorgänge in VMware-Umgebungen.

Vorteile von NVMe gegenüber TCP

- Hohe Leistung: Bietet außergewöhnliche Leistung mit geringer Latenz und hohen Datenübertragungsraten. Dies ist für anspruchsvolle Anwendungen und umfangreiche Datenoperationen von entscheidender Bedeutung.
- Skalierbarkeit: Unterstützt skalierbare Konfigurationen, sodass IT-Administratoren ihre Infrastruktur bei steigendem Datenbedarf nahtlos erweitern können.
- Effizienz: Ermöglicht schnellere Sicherungs- und Wiederherstellungsvorgänge, reduziert Ausfallzeiten und verbessert die allgemeine Systemverfügbarkeit.

Dieses Dokument enthält Schritte zum Bereitstellen und Verwalten von SCV in VMware Cloud Foundation (VCF)-Umgebungen, wobei der Schwerpunkt auf der Nutzung von NVMe über TCP für optimale Leistung liegt.

Publikum

Lösungsarchitekten oder Speicheradministratoren, die Datenschutz und Notfallwiederherstellung für VMware VCF-Workloaddomänen sicherstellen.

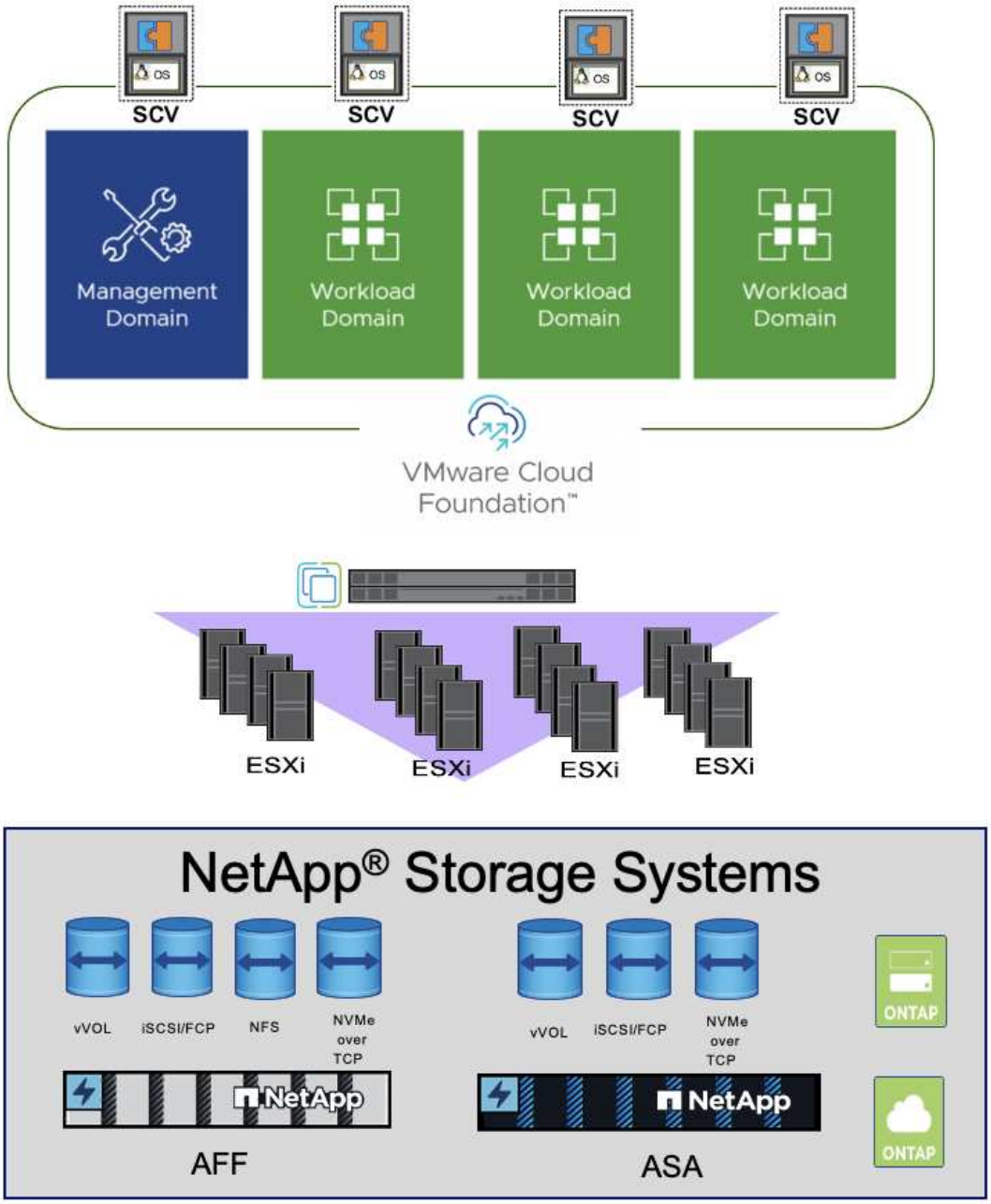
Architekturübersicht

SCV ist ein leistungsstarkes Tool, das schnelle, platzsparende, absturzkonsistente und VM-konsistente Sicherungs- und Wiederherstellungsvorgänge für VMs, Datenspeicher sowie Dateien und Ordner in VMware-Umgebungen ermöglicht. SCV wird als virtuelle Linux-Appliance mithilfe einer OVA-Datei bereitgestellt und nutzt eine Remote-Plug-In-Architektur.

SCV-Bereitstellungsarchitektur

- Bereitstellung einer virtuellen Appliance: SCV wird mithilfe einer OVA-Datei als virtuelle Linux-Appliance bereitgestellt. Diese Bereitstellungsmethode gewährleistet einen optimierten und effizienten Einrichtungsprozess.
- Remote-Plug-in-Architektur: SCV verwendet eine Remote-Plug-in-Architektur, die Skalierbarkeit und Flexibilität bei der Verwaltung mehrerer Instanzen ermöglicht.
- Eins-zu-eins-Beziehung: Jede VCF-Domäne erfordert eine dedizierte SCV-Instanz, um isolierte und effiziente Sicherungs- und Wiederherstellungsvorgänge zu gewährleisten.

Mit ONTAP 9.10.1 und späteren Versionen unterstützen NetApp AFF und ASA NVMe über TCP. Daten, die sich auf AFF oder ASA Primärsystemen befinden und auf ONTAP AFF oder ASA Sekundärsysteme repliziert werden können. SCV arbeitet auch mit SnapCenter Server zusammen, um anwendungsbasierte Sicherungs- und Wiederherstellungsvorgänge in VMware-Umgebungen für anwendungsspezifische SnapCenter -Plug-Ins zu unterstützen. Weitere Informationen finden Sie unter"SnapCenter Plug-in for VMware vSphere Dokumentation" Und"Schützen Sie Workloads mit SnapCenter"



Die 3-2-1-Backup-Regel ist eine Datenschutzstrategie, bei der drei Kopien der Daten erstellt, auf zwei verschiedenen Medientypen gespeichert und eine Kopie extern aufbewahrt wird. BlueXP backup and recovery ist ein Cloud-basiertes Tool für die Datenverwaltung, das eine einzige Kontrollebene für eine breite Palette von Backup- und Wiederherstellungsvorgängen sowohl in lokalen als auch in Cloud-Umgebungen bietet. Teil der BlueXP backup and recovery Suite NetApp BlueXP ist eine Funktion, die sich in SCV (vor Ort) integrieren lässt, um eine Kopie der Daten auf den Objektspeicher in der Cloud zu erweitern. Dadurch wird eine dritte Kopie der Daten außerhalb des Standorts erstellt, die aus den Backups des primären oder sekundären Speichers stammt. Mit BlueXP backup and recovery können Sie ganz einfach Speicherrichtlinien einrichten, die Kopien Ihrer Daten von einem dieser beiden lokalen Standorte übertragen. Weitere Einzelheiten finden Sie unter"3-2-1-Datenschutz für VMware mit SnapCenter -Plug-in und BlueXP backup and recovery für VMs" .

SCV für VCF auf NVMe-Bereitstellungsschritten

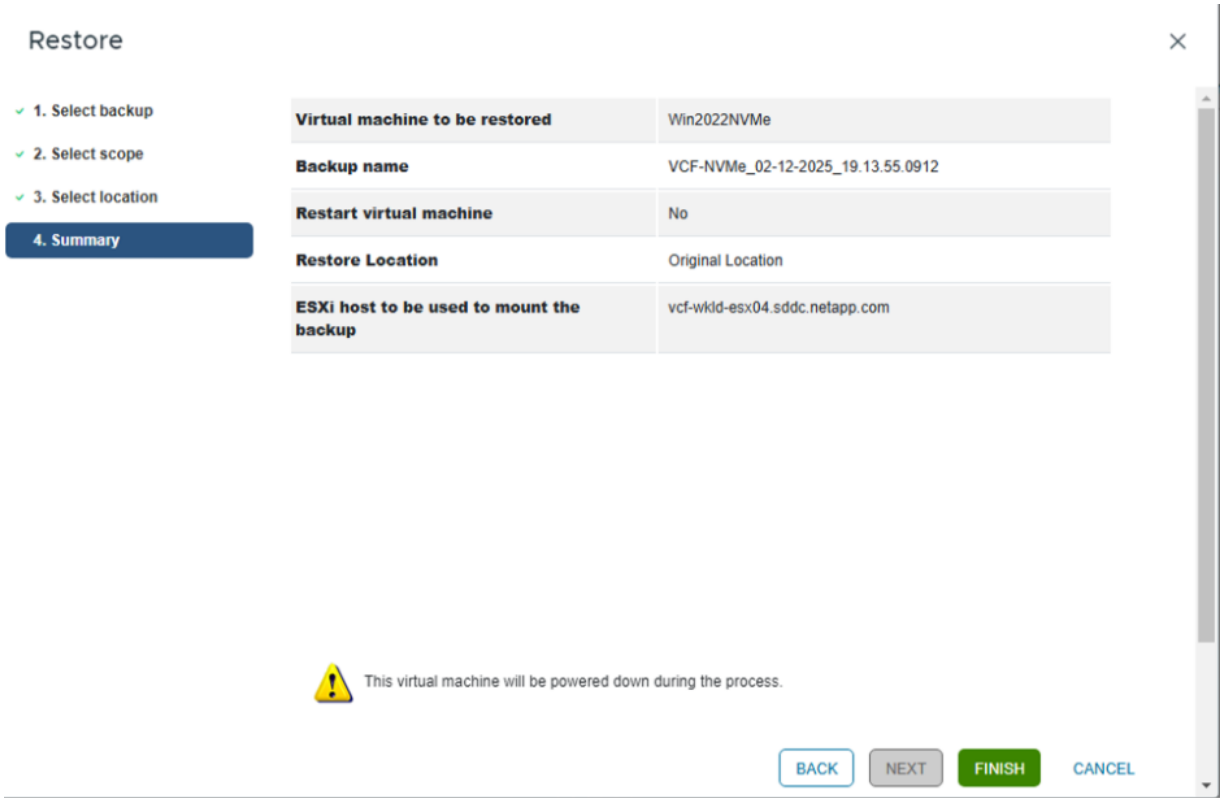
Der"ONTAP tools for VMware vSphere" (OTV) bietet eine leistungsstarke und effiziente Lösung für die Verwaltung von NetApp -Speicher in VMware-Umgebungen. Durch die direkte Integration mit dem vCenter Server vereinfacht OTV die Speicherverwaltung, verbessert den Datenschutz und optimiert die Leistung. Obwohl optional, kann die Bereitstellung von OTV die Verwaltungsfunktionen und die Gesamteffizienz von VMware-Umgebungen erheblich verbessern.

- "Erstellen Sie einen NVMe/TCP-Speicher für VCF-Workloaddomänen"
- "Konfigurieren Sie NetApp SnapCenter für VMware vSphere (SCV)."

Stellen Sie VM, Datenspeicher, virtuelle Festplatte und Dateien oder Ordner wieder her

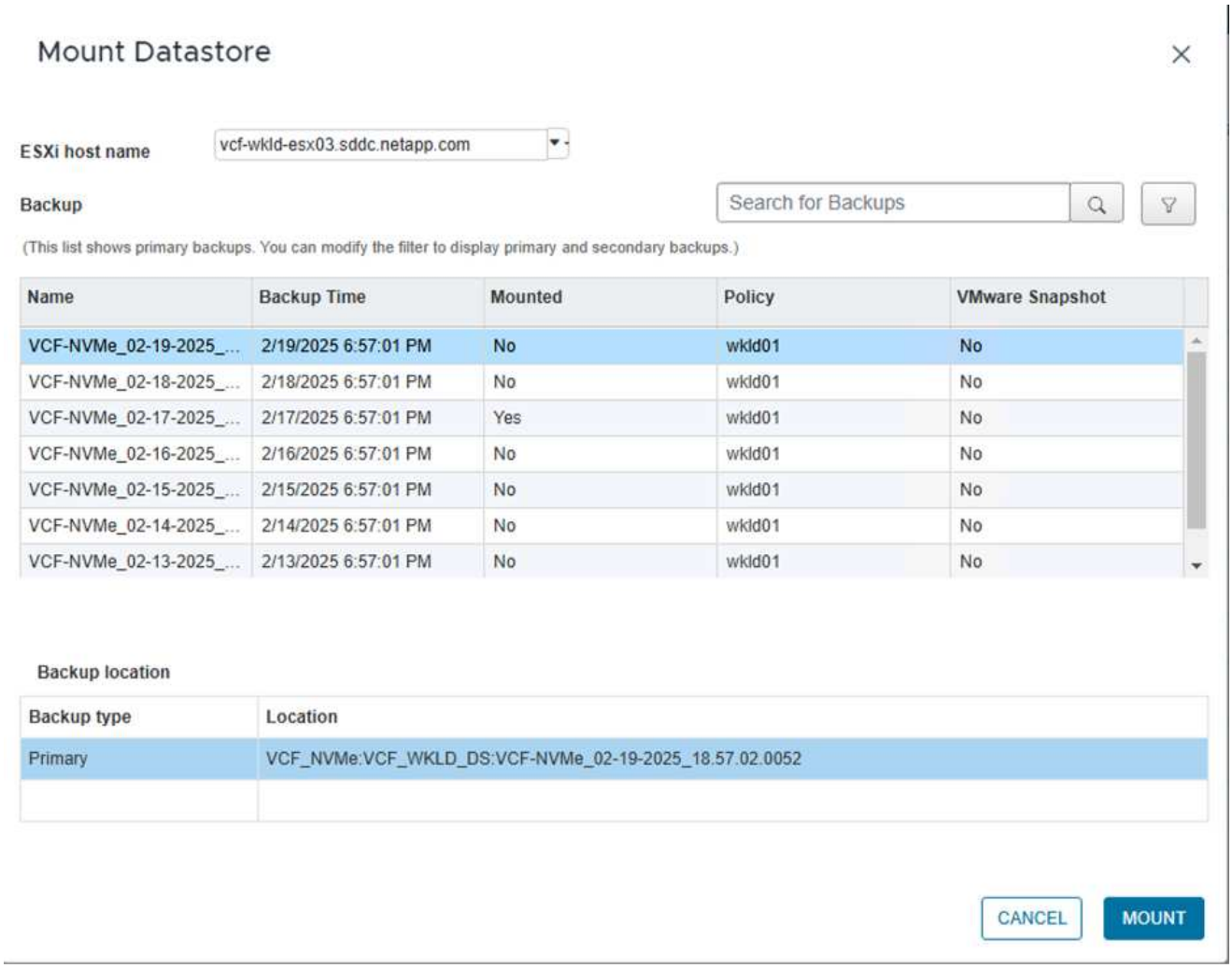
SCV bietet umfassende Sicherungs- und Wiederherstellungsfunktionen für VMware-Umgebungen. Für VMFS-Umgebungen verwendet SCV Klon- und Mountvorgänge in Verbindung mit Storage VMotion, um Wiederherstellungsvorgänge durchzuführen. Dies gewährleistet eine effiziente und nahtlose Wiederherstellung der Daten. Weitere Einzelheiten finden Sie unter"wie die Wiederherstellungsvorgänge durchgeführt werden."

- VM-Wiederherstellung Sie können die VM auf ihrem ursprünglichen Host innerhalb desselben vCenter Servers oder auf einem alternativen ESXi-Host wiederherstellen, der vom selben vCenter Server verwaltet wird.
  a. Klicken Sie mit der rechten Maustaste auf eine VM und wählen Sie in der Dropdownliste „SnapCenter Plug-in for VMware vSphere“ aus. Wählen Sie dann in der sekundären Dropdownliste „Wiederherstellen“ aus, um den Assistenten zu starten.
  b. Wählen Sie im Wiederherstellungsassistenten den Sicherungs-Snapshot aus, den Sie wiederherstellen möchten, und wählen Sie im Feld „Wiederherstellungsbereich“ die Option „Gesamte virtuelle Maschine“ aus. Wählen Sie den Wiederherstellungsort aus und geben Sie dann die Zielinformationen ein, unter denen die Sicherung bereitgestellt werden soll. Wählen Sie auf der Seite „Speicherort auswählen“ den Speicherort für den wiederhergestellten Datenspeicher aus. Überprüfen Sie die Seite „Zusammenfassung“ und klicken Sie auf „Fertig stellen“.

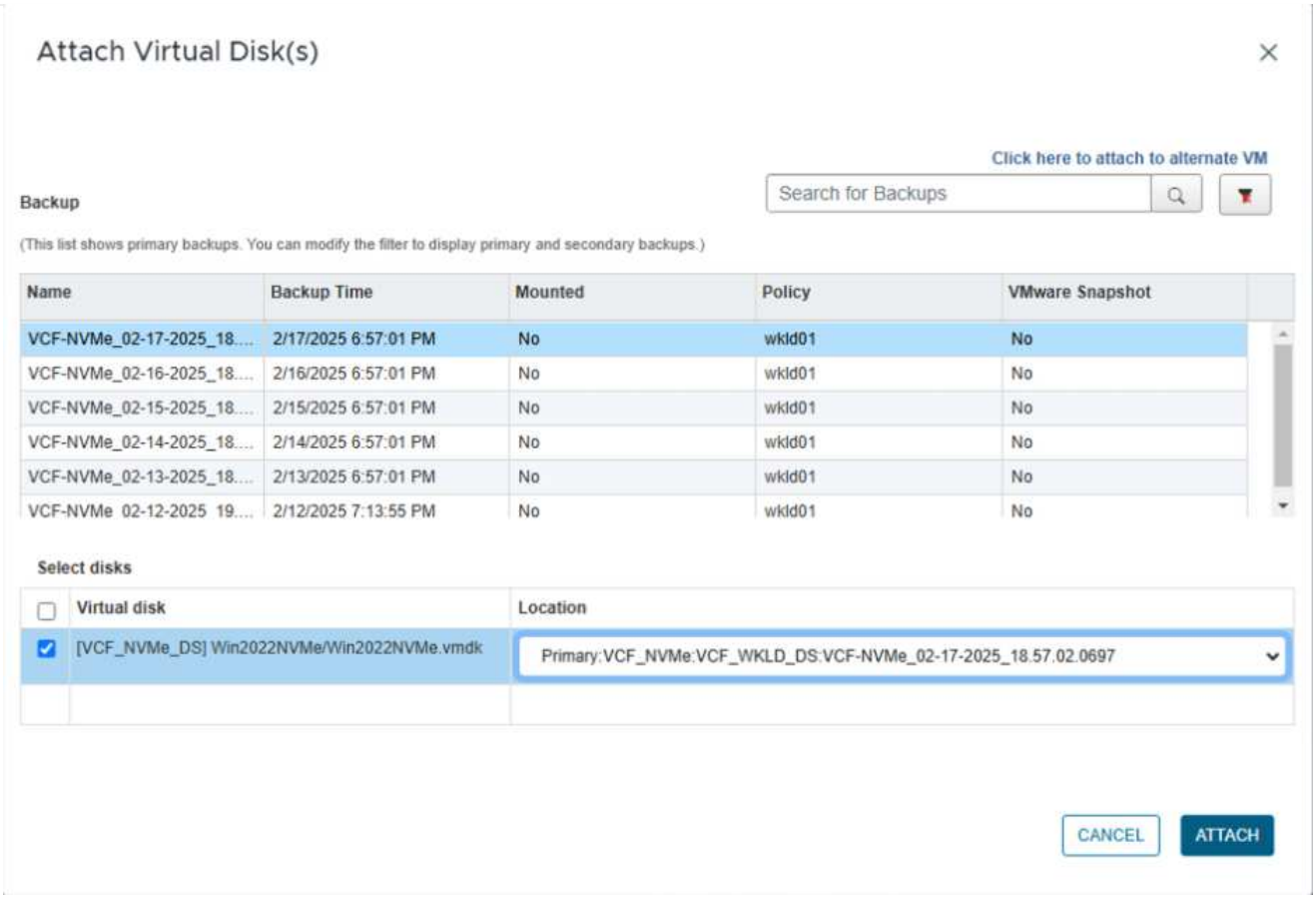


- Mounten Sie einen Datenspeicher. Sie können einen herkömmlichen Datenspeicher aus einer Sicherung mounten, wenn Sie auf Dateien in der Sicherung zugreifen möchten. Sie können das Backup entweder auf demselben ESXi-Host mounten, auf dem das Backup erstellt wurde, oder auf einem alternativen ESXi-Host, der über denselben VM-Typ und dieselben Hostkonfigurationen verfügt. Sie können einen Datenspeicher mehrmals auf einem Host mounten.
  a. Klicken Sie mit der rechten Maustaste auf einen Datenspeicher und wählen Sie „SnapCenter Plug-in for VMware vSphere“ > „Backup mounten“.

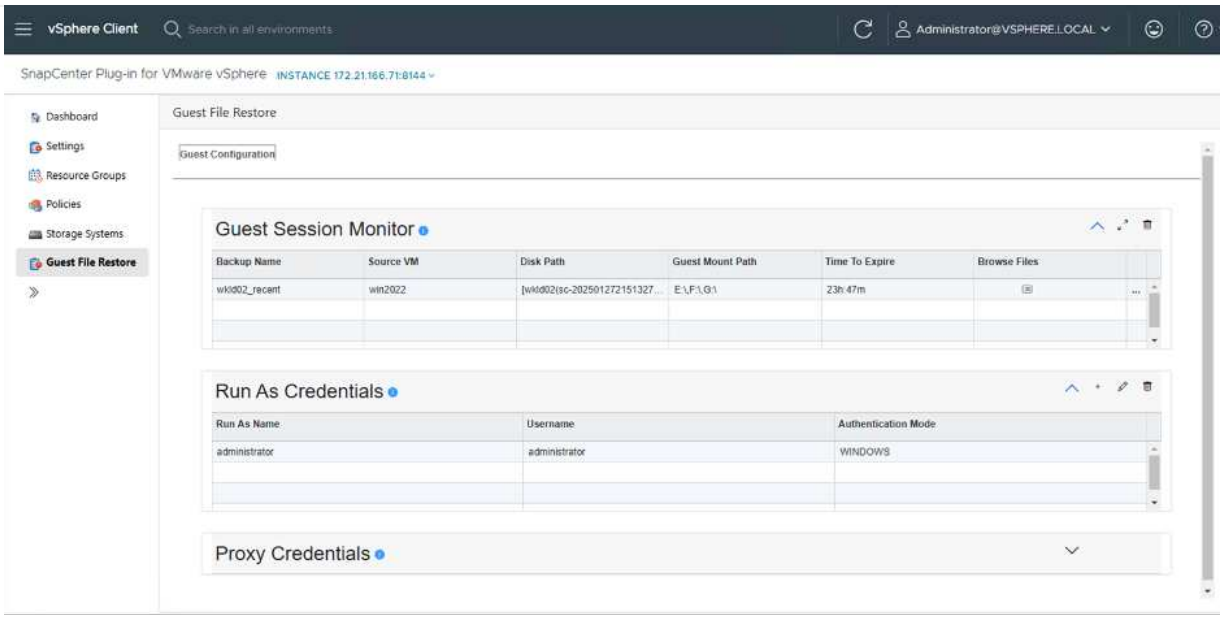
b. Wählen Sie auf der Seite „Datenspeicher bereitstellen“ eine Sicherung und einen Sicherungsspeicherort (primär oder sekundär) aus und klicken Sie dann auf „Befestigen“.



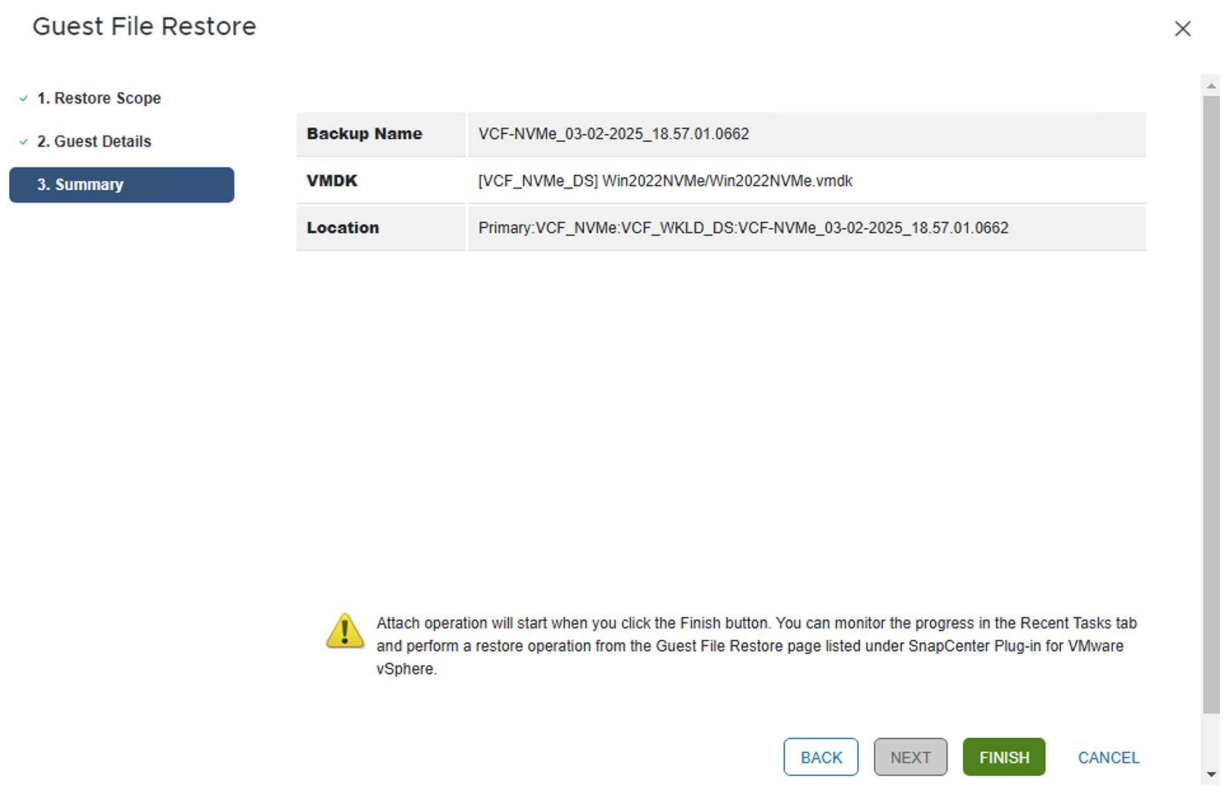
- Anhängen einer virtuellen Festplatte Sie können eine oder mehrere VMDKs aus einer Sicherung an die übergeordnete VM oder an eine alternative VM auf demselben ESXi-Host oder an eine alternative VM auf einem alternativen ESXi-Host anhängen, der vom selben vCenter oder einem anderen vCenter im verknüpften Modus verwaltet wird.
  a. Klicken Sie mit der rechten Maustaste auf eine VM und wählen Sie „SnapCenter Plug-in for VMware vSphere“ > „Virtuelle Festplatte(n) anhängen“.
  b. Wählen Sie im Fenster „Virtuelle Festplatte anhängen“ eine Sicherung aus und wählen Sie eine oder mehrere Festplatten aus, die Sie anhängen möchten, sowie den Speicherort, von dem aus Sie die Verbindung herstellen möchten (primär oder sekundär). Standardmäßig werden die ausgewählten virtuellen Datenträger an die übergeordnete VM angeschlossen. Um die ausgewählten virtuellen Datenträger an eine alternative VM im selben ESXi-Host anzuhängen, wählen Sie „Klicken Sie hier, um eine Verbindung zur alternativen VM herzustellen“ und geben Sie die alternative VM an. Klicken Sie auf Anhängen.



- Schritte zur Wiederherstellung von Dateien und Ordnern Einzelne Dateien und Ordner können in einer Dateiwiederherstellungssitzung des Gastes wiederhergestellt werden, bei der eine Sicherungskopie einer virtuellen Festplatte angehängt und dann die ausgewählten Dateien oder Ordner wiederhergestellt werden. Auch Dateien und Ordner können wiederhergestellt werden. Weitere Details finden Sie unter"SnapCenter Datei- und Ordnerwiederherstellung."
  a. Wenn Sie für Datei- oder Ordnerwiederherstellungsvorgänge von Gastbenutzern eine virtuelle Festplatte anhängen, müssen vor der Wiederherstellung die Anmeldeinformationen der Ziel-VM für den Anschluss konfiguriert sein. Wählen Sie im SnapCenter Plug-in for VMware vSphere unter Plug-ins die Option „Guest File Restore“ und „Run As Credentials“ aus und geben Sie die Benutzeranmeldeinformationen ein. Als Benutzernamen müssen Sie „Administrator“ eingeben.

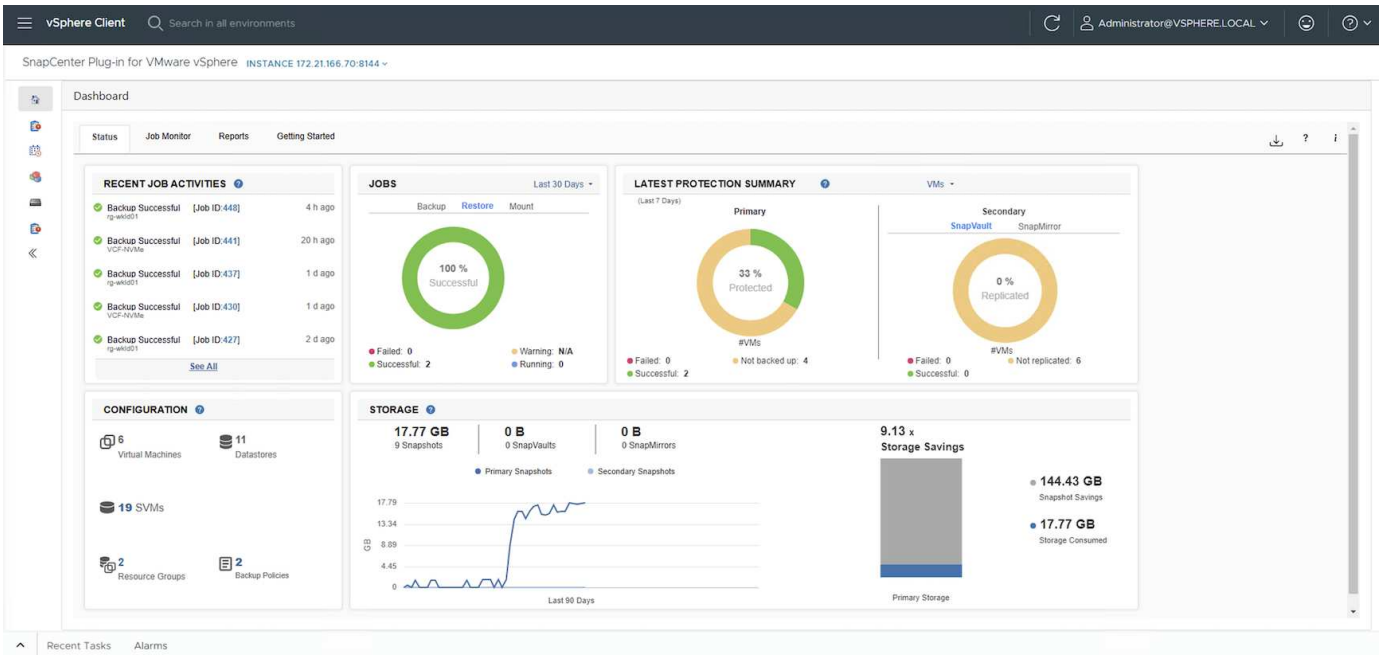


b. Klicken Sie im vSphere-Client mit der rechten Maustaste auf die VM und wählen Sie „SnapCenter Plug-in for VMware vSphere > Guest File Restore“. Geben Sie auf der Seite „Wiederherstellungsbereich“ den Sicherungsnamen, die virtuelle VMDK-Festplatte und den Speicherort – primär oder sekundär – an. Klicken Sie zur Bestätigung auf „Zusammenfassung“.



Überwachen und berichten

SCV bietet robuste Überwachungs- und Berichtsfunktionen, die Administratoren dabei helfen, Sicherungs- und Wiederherstellungsvorgänge effizient zu verwalten. Sie können Statusinformationen anzeigen, Jobs überwachen, Jobprotokolle herunterladen, auf Berichte zugreifen und weitere Details überprüfen"SnapCenter Plug-in für VMware vSphere Monitor und Report."



Durch die Nutzung der Leistung von NVMe über TCP und des NetApp SnapCenter Plug-in for VMware vSphere können Unternehmen einen leistungsstarken Datenschutz und eine Notfallwiederherstellung für VMware Cloud Foundation-Workloaddomänen erreichen. Dieser Ansatz gewährleistet schnelle und zuverlässige Sicherungs- und Wiederherstellungsvorgänge, minimiert Ausfallzeiten und schützt kritische Daten.

Schützen Sie VMware-Datenspeicher mit BlueXP

Erfahren Sie mehr über den Schutz von VMware-Datenspeichern mit BlueXP disaster recovery

Informieren Sie sich über die NetApp -Lösungen für Disaster Recovery mit BlueXP disaster recovery für VMware. Dies ermöglicht robuste Lösungen für die Notfallwiederherstellung durch Blockebenenreplikation von einem primären Standort zu einem Notfallwiederherstellungsstandort.

BlueXP DRaaS ist eine effektive und kostengünstige Methode zum Schutz von Workloads vor Site-Ausfällen und Datenintegritätsproblemen, einschließlich Ransomware-Angriffen. Darüber hinaus verbessert NetApp BlueXP DRaaS diese Strategie, indem es eine verwaltete, Cloud-basierte Disaster-Recovery-Lösung bereitstellt, die eine schnelle Wiederherstellung und minimale Ausfallzeiten während Katastrophen gewährleistet.

Die technischen Details entnehmen Sie bitte den folgenden Lösungen.

- "DR mit BlueXP DRaaS für VMFS-Datenspeicher"
- "DR mit BlueXP DRaaS für NFS-Datenspeicher"

Konfigurieren Sie 3-2-1-Datenschutz für VMware mit dem SnapCenter -Plug-in für VMware vSphere und BlueXP backup and recovery

Konfigurieren Sie eine 3-2-1-Datenschutzstrategie für VMware-Umgebungen mithilfe des

SnapCenter -Plug-ins für VMware vSphere und BlueXP backup and recovery. Dieses Verfahren umfasst das Einrichten von Backups von VMs und Datenspeichern auf primären und sekundären ONTAP Clustern, das Konfigurieren des Plug-ins und von BlueXP sowie das Verwalten der Datenreplikation in die Cloud oder auf externe Speicher für eine zuverlässige Wiederherstellung.

Die 3-2-1-Backup-Strategie ist eine branchenweit anerkannte Methode zum Datenschutz und bietet einen umfassenden Ansatz zum Schutz wertvoller Daten. Diese Strategie ist zuverlässig und stellt sicher, dass auch im Falle eines unerwarteten Notfalls immer noch eine Kopie der Daten verfügbar ist.

Überblick

Die Strategie besteht aus drei Grundregeln:

1. Bewahren Sie mindestens drei Kopien Ihrer Daten auf. Dadurch wird sichergestellt, dass Sie auch dann noch über mindestens zwei verbleibende Kopien verfügen, wenn eine Kopie verloren geht oder beschädigt wird.
2. Speichern Sie zwei Sicherungskopien auf unterschiedlichen Speichermedien oder Geräten. Durch die Diversifizierung der Speichermedien können Sie sich vor geräte- oder medienspezifischen Ausfällen schützen. Wenn ein Gerät beschädigt wird oder ein Medientyp ausfällt, bleibt die andere Sicherungskopie davon unberührt.
3. Stellen Sie abschließend sicher, dass mindestens eine Sicherungskopie außerhalb des Standorts gespeichert ist. Die externe Speicherung dient als Ausfallsicherung gegen lokale Katastrophen wie Brände oder Überschwemmungen, die die Kopien vor Ort unbrauchbar machen könnten.

Dieses Lösungsdokument behandelt eine 3-2-1-Sicherungslösung mit dem SnapCenter Plug-in for VMware vSphere (SCV) zum Erstellen primärer und sekundärer Sicherungen unserer virtuellen Maschinen vor Ort und BlueXP backup and recovery für virtuelle Maschinen zum Sichern einer Kopie unserer Daten im Cloud-Speicher oder StorageGRID.

Anwendungsfälle

Diese Lösung ist für die folgenden Anwendungsfälle geeignet:

- Sicherung und Wiederherstellung von virtuellen Maschinen und Datenspeichern vor Ort mithilfe des SnapCenter Plug-in for VMware vSphere.
- Sicherung und Wiederherstellung von virtuellen Maschinen und Datenspeichern vor Ort, die auf ONTAP Clustern gehostet und mithilfe von BlueXP backup and recovery für virtuelle Maschinen in einem Objektspeicher gesichert werden.

NetApp ONTAP Datenspeicher

ONTAP ist die branchenführende Speicherlösung von NetApp, die einheitlichen Speicher bietet, unabhängig davon, ob Sie über SAN- oder NAS-Protokolle zugreifen. Die 3-2-1-Backup-Strategie stellt sicher, dass lokale Daten auf mehr als einem Medientyp geschützt sind, und NetApp bietet Plattformen von Hochgeschwindigkeits-Flash bis hin zu kostengünstigeren Medien.

FAS	AFF C-Series	AFF A-Series	ASA A-Series
Hybrid flash storage	**Capacity all-flash storage**	**Performance all-flash storage**	**All-flash SAN storage**
Unified (file, block, object)	Unified (file, block, object)	Unified (file, block, object)	Block optimized
Lowest price storage	Balanced price storage	Premium priced storage	Aggressively priced storage
Tier 2 @ 5-10ms latency Backup / Low-cost DR	Refresh of hybrid flash, Tier 1 @ 2-4ms latency Tier 2 workloads VMware datastores	Ideal for Tier 1 business-critical workloads with <1ms latency	Ideal for Tier 1 Block Six Nines Guaranteed

Weitere Informationen zu allen Hardware-Plattformen von NetApp finden Sie unter "NetApp Datenspeicher" .

SnapCenter Plug-in for VMware vSphere

Das SnapCenter -Plugin für VMware vSphere ist ein Datenschutzangebot, das eng in VMware vSphere integriert ist und eine einfache Verwaltung von Backups und Wiederherstellungen für virtuelle Maschinen ermöglicht. Als Teil dieser Lösung bietet SnapMirror eine schnelle und zuverlässige Methode zum Erstellen einer zweiten unveränderlichen Sicherungskopie der Daten virtueller Maschinen auf einem sekundären ONTAP Speichercluster. Mit dieser Architektur können Wiederherstellungsvorgänge für virtuelle Maschinen problemlos von den primären oder sekundären Sicherungsstandorten aus gestartet werden.

SCV wird als virtuelle Linux-Appliance mithilfe einer OVA-Datei bereitgestellt. Das Plug-in verwendet jetzt eine Remote-Plug-in-Architektur. Das Remote-Plug-In wird außerhalb des vCenter-Servers ausgeführt und auf der virtuellen SCV-Appliance gehostet.

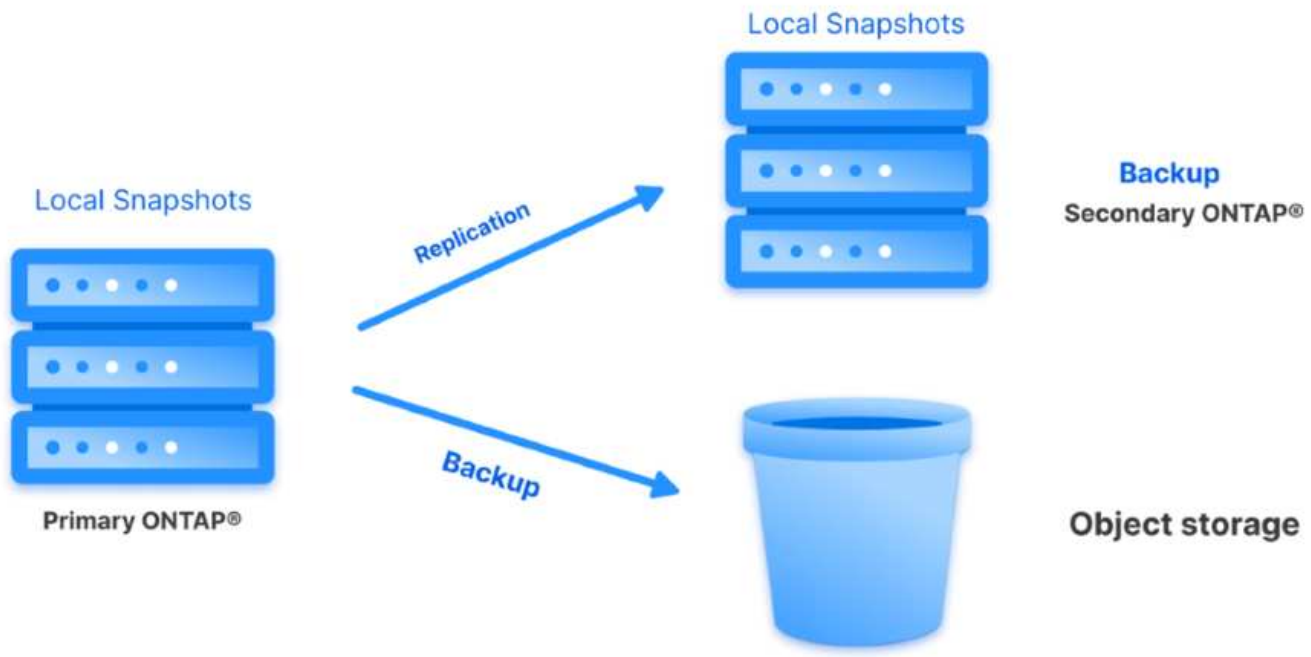
Ausführliche Informationen zu SCV finden Sie unter "SnapCenter Plug-in for VMware vSphere Dokumentation" .

BlueXP backup and recovery für virtuelle Maschinen

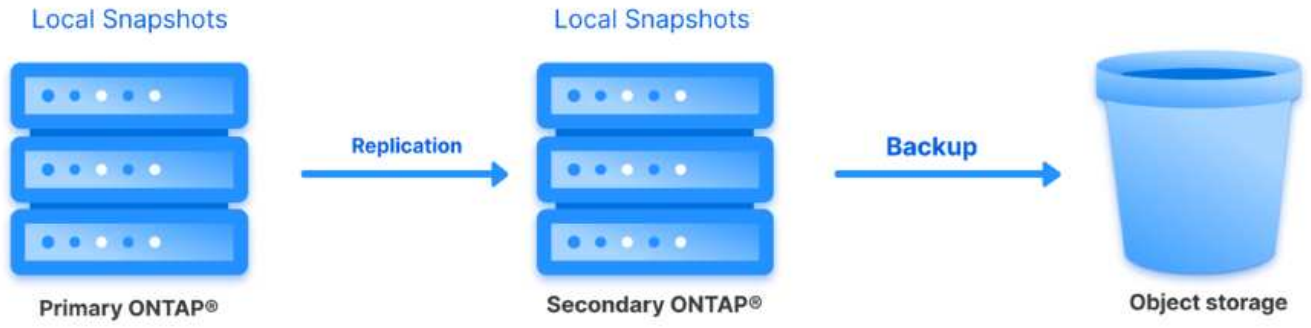
BlueXP backup and recovery ist ein Cloud-basiertes Tool für die Datenverwaltung, das eine einzige Kontrollebene für eine breite Palette von Backup- und Wiederherstellungsvorgängen sowohl in lokalen als auch in Cloud-Umgebungen bietet. Teil der BlueXP backup and recovery Suite von NetApp BlueXP ist eine Funktion, die sich in das SnapCenter -Plugin für VMware vSphere (vor Ort) integrieren lässt, um eine Kopie der Daten auf den Objektspeicher in der Cloud zu erweitern. Dadurch wird eine dritte Kopie der Daten außerhalb des Standorts erstellt, die aus den Backups des primären oder sekundären Speichers stammt. Mit BlueXP backup and recovery können Sie ganz einfach Speicherrichtlinien einrichten, die Kopien Ihrer Daten von einem dieser beiden lokalen Standorte übertragen.

Wenn Sie in BlueXP Backup and Recovery zwischen primären und sekundären Backups als Quelle wählen, wird eine von zwei Topologien implementiert:

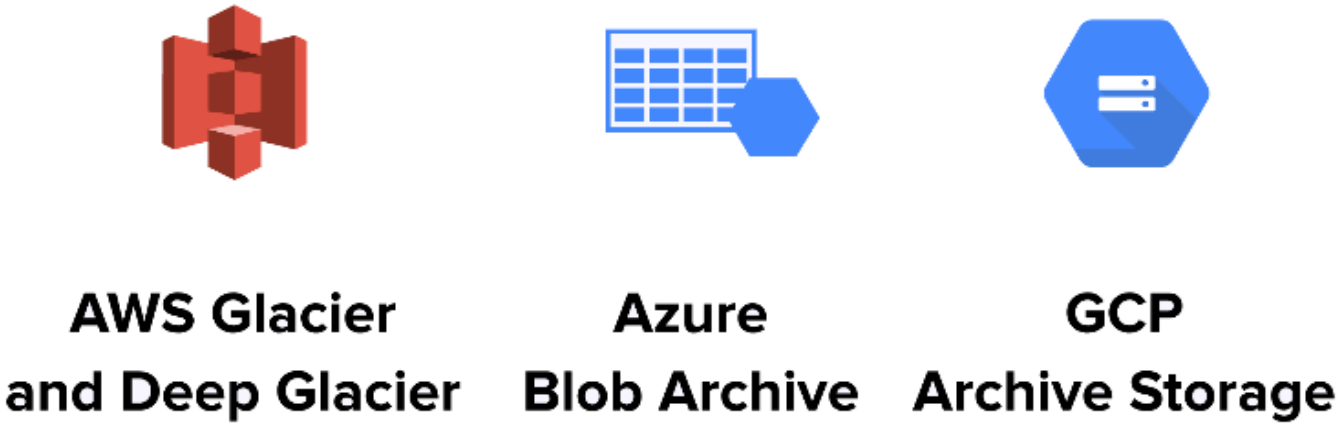
Fan-Out-Topologie – Wenn eine Sicherung vom SnapCenter Plug-in for VMware vSphere initiiert wird, wird sofort ein lokaler Snapshot erstellt. SCV initiiert dann einen SnapMirror Vorgang, der den aktuellsten Snapshot auf den Secondary ONTAP Cluster repliziert. In BlueXP Backup and Recovery gibt eine Richtlinie den primären ONTAP -Cluster als Quelle für eine Snapshot-Kopie der Daten an, die in den Objektspeicher des Cloud-Anbieters Ihrer Wahl übertragen werden sollen.



Kaskadierende Topologie – Das Erstellen der primären und sekundären Datenkopien mit SCV ist identisch mit der oben erwähnten Fan-Out-Topologie. Dieses Mal wird jedoch in BlueXP Backup and Recovery eine Richtlinie erstellt, die angibt, dass die Sicherung im Objektspeicher vom sekundären ONTAP Cluster stammt.



Mit BlueXP backup and recovery können Sicherungskopien von lokalen ONTAP Snapshots in AWS Glacier, Azure Blob und GCP Archive-Speicher erstellt werden.



Darüber hinaus können Sie NetApp StorageGRID als Sicherungsziel für den Objektspeicher verwenden. Weitere Informationen zu StorageGRID finden Sie im "StorageGRID -Landingpage" .

Übersicht über die Lösungsbereitstellung

Diese Liste enthält die grundlegenden Schritte, die zum Konfigurieren dieser Lösung und zum Ausführen von Sicherungs- und Wiederherstellungsvorgängen von SCV und BlueXP backup and recovery erforderlich sind:

1. Konfigurieren Sie die SnapMirror -Beziehung zwischen den ONTAP Clustern, die für primäre und sekundäre Datenkopien verwendet werden sollen.
2. Konfigurieren Sie das SnapCenter Plug-In für VMware vSphere.
   a. Speichersysteme hinzufügen
   b. Erstellen von Sicherungsrichtlinien
   c. Erstellen von Ressourcengruppen
   d. Führen Sie die ersten Sicherungsaufträge aus
3. Konfigurieren Sie BlueXP backup and recovery für virtuelle Maschinen
   a. Arbeitsumgebung hinzufügen
   b. Entdecken Sie SCV- und vCenter-Geräte
   c. Erstellen von Sicherungsrichtlinien
   d. Backups aktivieren
4. Stellen Sie virtuelle Maschinen mithilfe von SCV vom primären und sekundären Speicher wieder her.
5. Stellen Sie virtuelle Maschinen mithilfe von BlueXP Backup und Restore aus dem Objektspeicher wieder her.

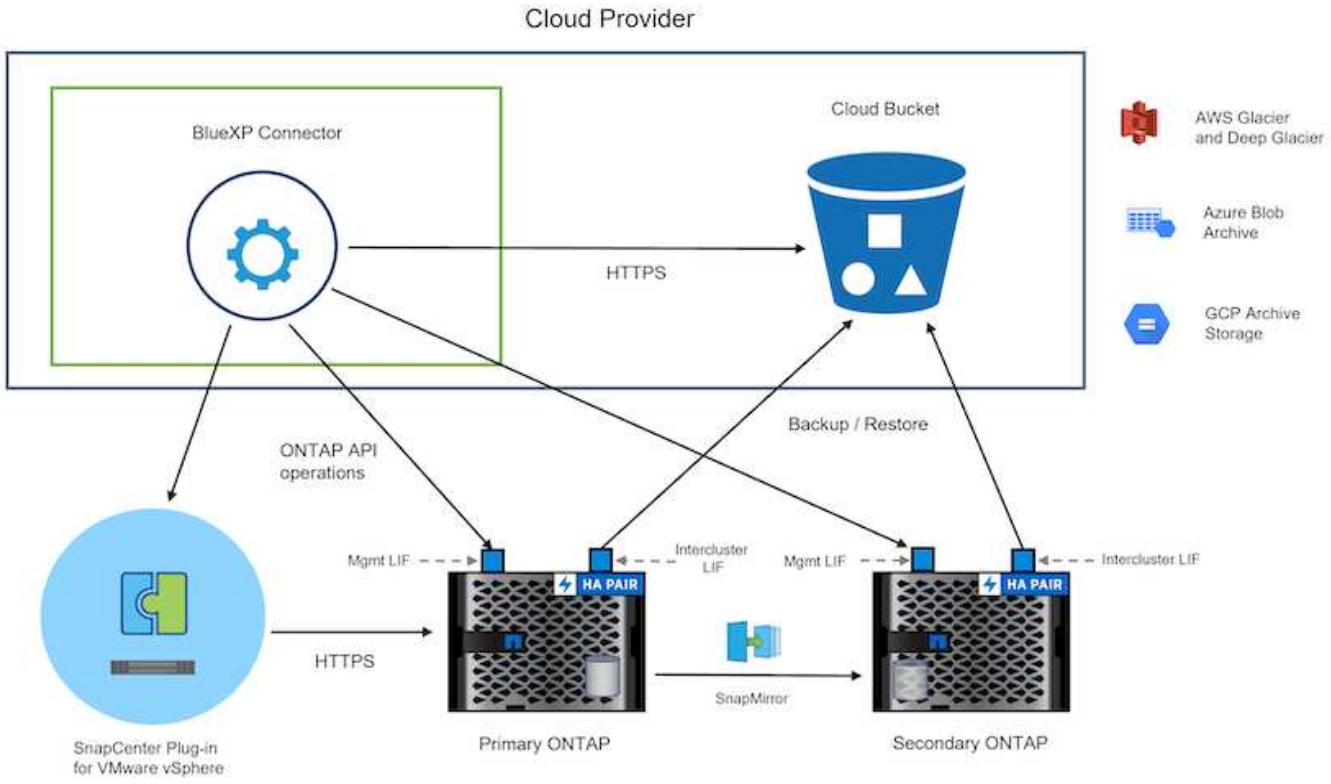
Voraussetzungen

Der Zweck dieser Lösung besteht darin, den Datenschutz von virtuellen Maschinen zu demonstrieren, die in VMware vSphere, VCF VI-Workloaddomänen oder VCF-Verwaltungsdomänen ausgeführt werden. Virtuelle Maschinen in dieser Lösung werden auf NFS-Datenspeichern gehostet, die von NetApp ONTAP bereitgestellt werden. Diese Lösung setzt voraus, dass die folgenden Komponenten konfiguriert und einsatzbereit sind:

1. ONTAP -Speichercluster mit NFS- oder VMFS-Datenspeichern, verbunden mit VMware vSphere. Es werden sowohl NFS- als auch VMFS-Datenspeicher unterstützt. Für diese Lösung wurden NFS-Datenspeicher verwendet.
2. Sekundärer ONTAP Speichercluster mit SnapMirror -Beziehungen, die für Volumes eingerichtet wurden, die für NFS-Datenspeicher verwendet werden.
3. BlueXP Connector für Cloud-Anbieter installiert, der für Objektspeicher-Backups verwendet wird.
4. Zu sichernde virtuelle Maschinen befinden sich auf NFS-Datenspeichern, die sich auf dem primären ONTAP Speichercluster befinden.
5. Netzwerkkonnektivität zwischen dem BlueXP -Connector und den lokalen ONTAP Speichercluster-Verwaltungsschnittstellen.
6. Netzwerkkonnektivität zwischen dem BlueXP Connector und der lokalen SCV-Appliance-VM und zwischen dem BlueXP Connector und vCenter.
7. Netzwerkkonnektivität zwischen den lokalen ONTAP Intercluster-LIFs und dem Objektspeicherdienst.
8. DNS für Management-SVM auf primären und sekundären ONTAP Speicherclustern konfiguriert. Weitere Informationen finden Sie unter "Konfigurieren Sie DNS für die Hostnamenauflösung" .

High-Level-Architektur

Die Prüfung/Validierung dieser Lösung wurde in einem Labor durchgeführt, das möglicherweise nicht der endgültigen Bereitstellungsumgebung entspricht.



Lösungsbereitstellung

In dieser Lösung bieten wir detaillierte Anweisungen zum Bereitstellen und Validieren einer Lösung, die das SnapCenter Plug-in for VMware vSphere zusammen mit BlueXP backup and recovery verwendet, um die Sicherung und Wiederherstellung von virtuellen Windows- und Linux-Maschinen innerhalb eines VMware vSphere-Clusters in einem lokalen Rechenzentrum durchzuführen. Die virtuellen Maschinen in diesem Setup werden auf NFS-Datenspeichern gespeichert, die von einem ONTAP A300-Speichercluster gehostet werden. Darüber hinaus dient ein separater ONTAP A300-Speichercluster als sekundäres Ziel für mit SnapMirror replizierte Volumes. Darüber hinaus wurden auf Amazon Web Services und Azure Blob gehostete Objektspeicher als Ziele für eine dritte Kopie der Daten verwendet.

Wir werden die Erstellung von SnapMirror -Beziehungen für sekundäre Kopien unserer von SCV verwalteten Backups und die Konfiguration von Backup-Jobs in SCV- und BlueXP backup and recovery durchgehen.

Ausführliche Informationen zum SnapCenter Plug-in for VMware vSphere finden Sie im "SnapCenter Plug-in for VMware vSphere Dokumentation" .

Ausführliche Informationen zur BlueXP backup and recovery finden Sie im "BlueXP backup and recovery" .

Herstellen von SnapMirror -Beziehungen zwischen ONTAP Clustern

Das SnapCenter Plug-in for VMware vSphere verwendet die ONTAP SnapMirror -Technologie, um den Transport sekundärer SnapMirror und/oder SnapVault -Kopien zu einem sekundären ONTAP Cluster zu verwalten.

SCV-Sicherungsrichtlinien bieten die Möglichkeit, SnapMirror oder SnapVault -Beziehungen zu verwenden. Der Hauptunterschied besteht darin, dass bei Verwendung der SnapMirror -Option der in der Richtlinie für Backups konfigurierte Aufbewahrungsplan am primären und sekundären Standort derselbe ist. SnapVault ist für die Archivierung konzipiert und bei Verwendung dieser Option kann mit der SnapMirror -Beziehung ein separater Aufbewahrungsplan für die Snapshot-Kopien auf dem sekundären ONTAP Speichercluster erstellt

werden.

Das Einrichten von SnapMirror -Beziehungen kann in BlueXP erfolgen, wo viele Schritte automatisiert sind, oder mithilfe von System Manager und der ONTAP CLI. Alle diese Methoden werden im Folgenden erläutert.

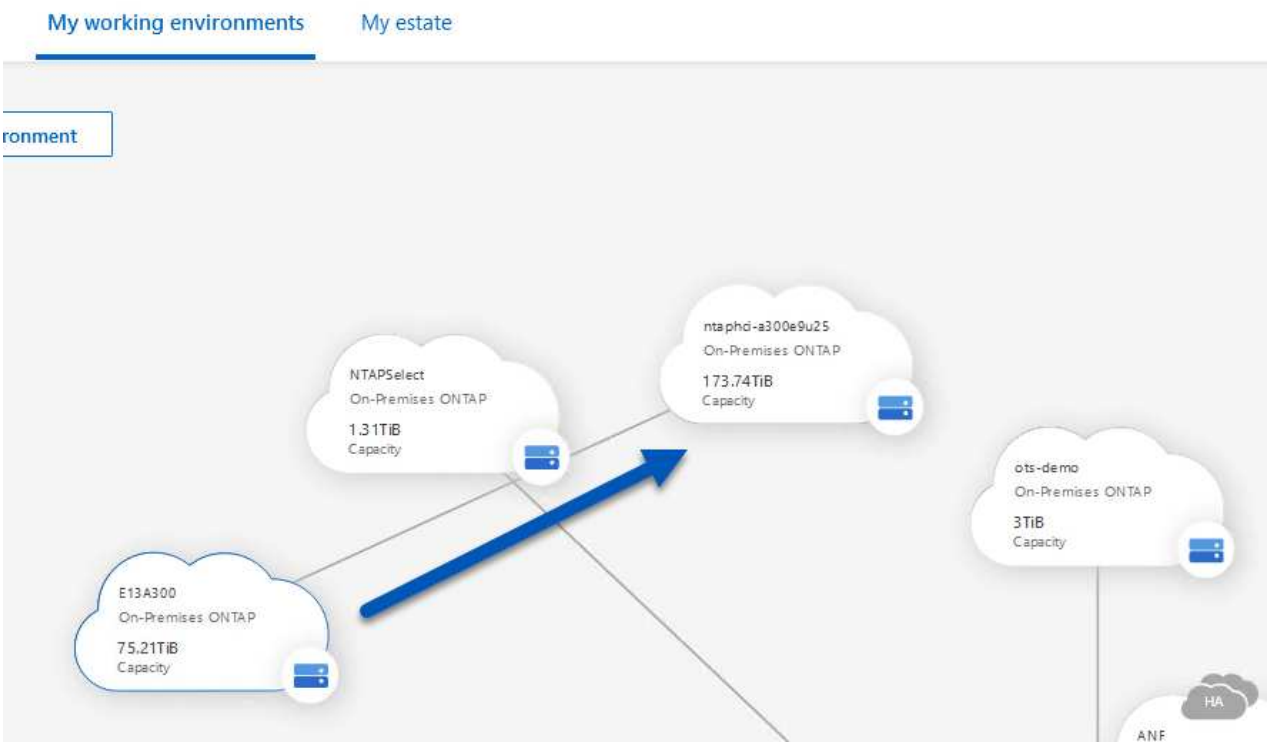
Bauen Sie SnapMirror -Beziehungen mit BlueXP auf

Die folgenden Schritte müssen über die BlueXP Webkonsole ausgeführt werden:

Replikations-Setup für primäre und sekundäre ONTAP Speichersysteme

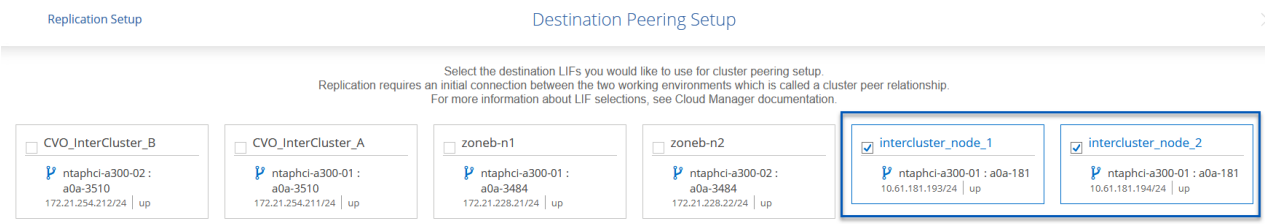
Melden Sie sich zunächst bei der BlueXP Webkonsole an und navigieren Sie zum Canvas.

1. Ziehen Sie das Quell ONTAP -Speichersystem (primär) per Drag & Drop auf das Ziel ONTAP -Speichersystem (sekundär).

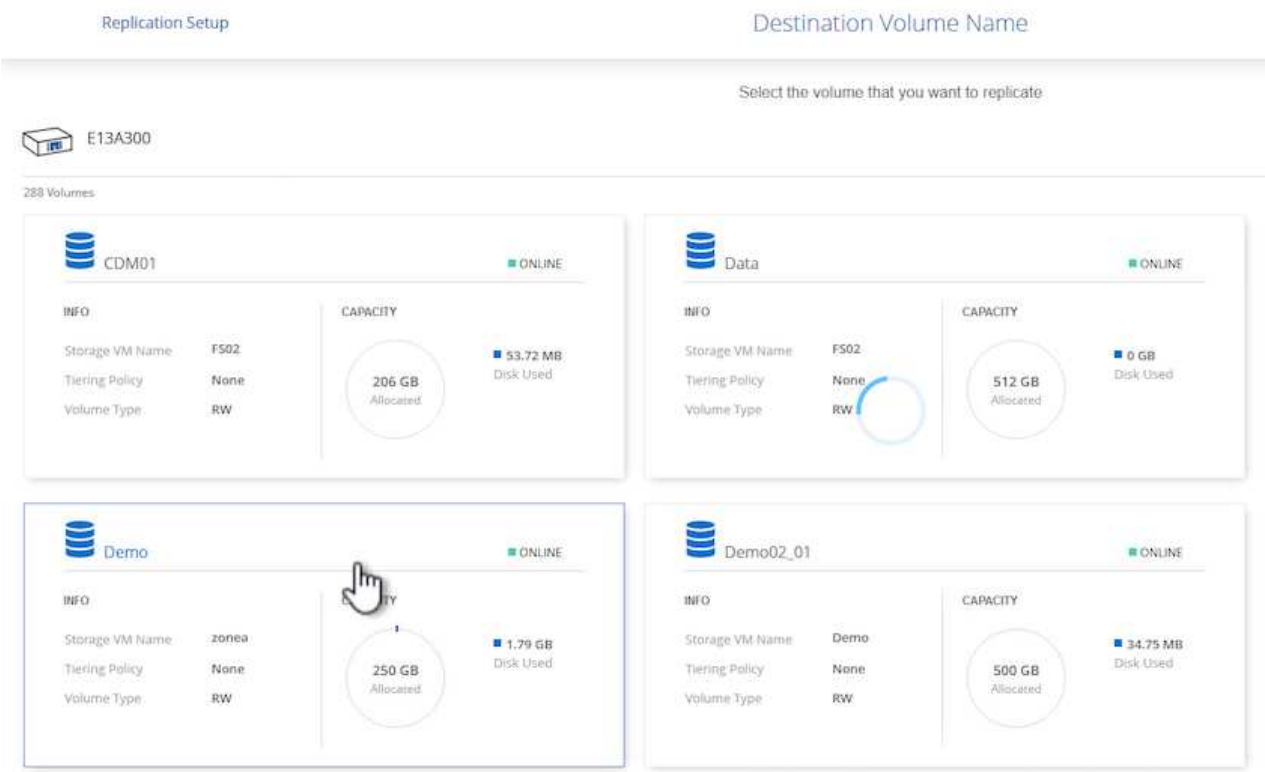


2. Wählen Sie im angezeigten Menü **Replikation** aus.

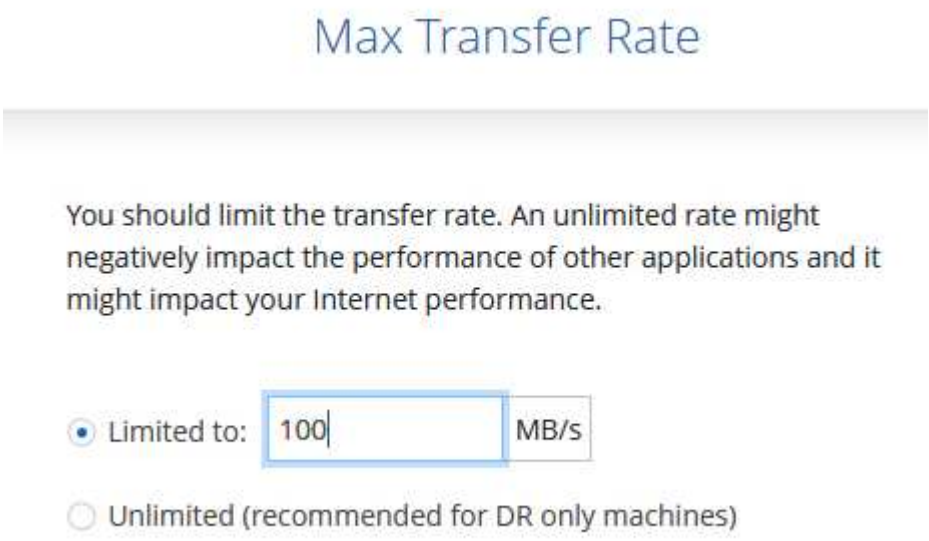
3. Wählen Sie auf der Seite **Destination Peering Setup** die Ziel-Intercluster-LIFs aus, die für die Verbindung zwischen Speichersystemen verwendet werden sollen.



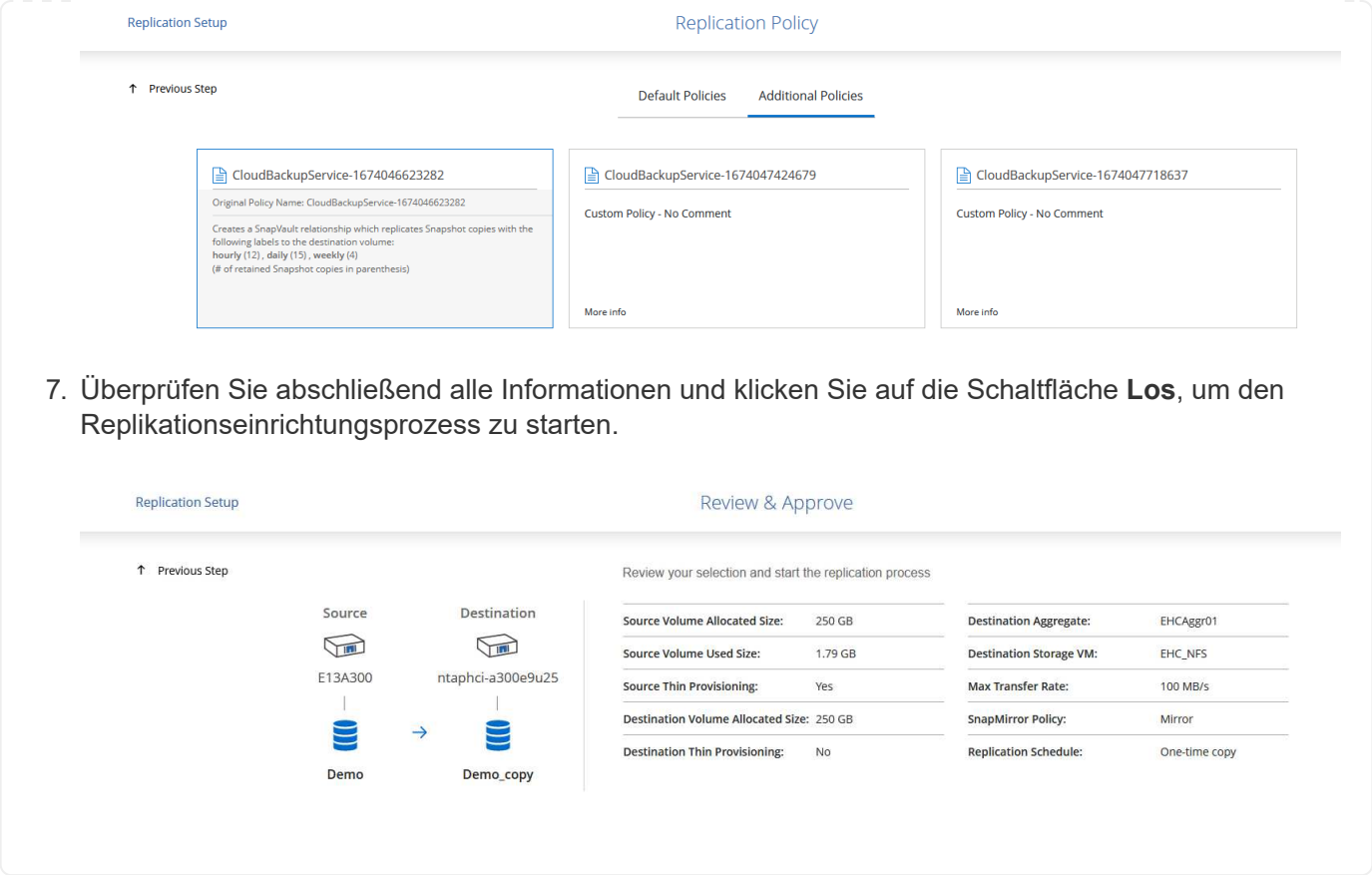
4. Wählen Sie auf der Seite **Zielvolumename** zuerst das Quellvolume aus, geben Sie dann den Zielvolumenamen ein und wählen Sie die Ziel-SVM und das Zielaggregat aus. Klicken Sie auf **Weiter**, um fortzufahren.



5. Wählen Sie die maximale Übertragungsrate für die Replikation.



6. Wählen Sie die Richtlinie aus, die den Aufbewahrungszeitplan für sekundäre Sicherungen bestimmt. Diese Richtlinie kann im Voraus erstellt werden (siehe den manuellen Prozess unten im Schritt **Erstellen einer Snapshot-Aufbewahrungsrichtlinie**) oder bei Bedarf nachträglich geändert werden.



7. Überprüfen Sie abschließend alle Informationen und klicken Sie auf die Schaltfläche **Los**, um den Replikationseinrichtungsprozess zu starten.

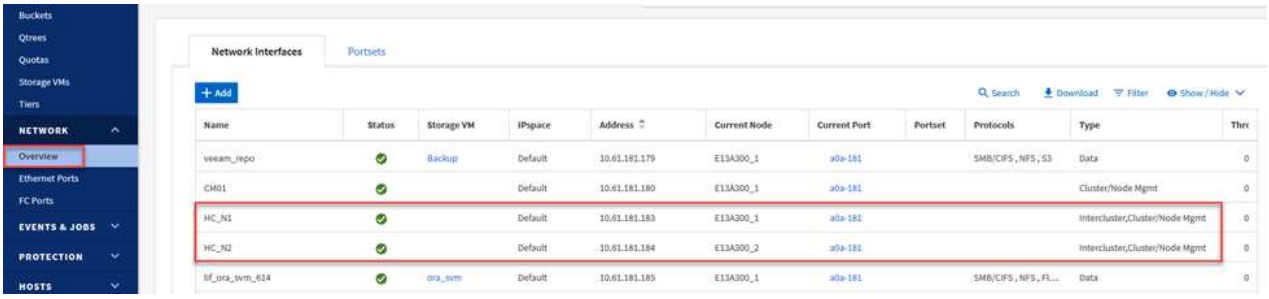
Stellen Sie SnapMirror -Beziehungen mit System Manager und ONTAP CLI her

Alle erforderlichen Schritte zum Herstellen von SnapMirror -Beziehungen können mit System Manager oder der ONTAP CLI durchgeführt werden. Der folgende Abschnitt enthält detaillierte Informationen zu beiden Methoden:

Notieren Sie die logischen Quell- und Zielschnittstellen zwischen Clustern.

Für die Quell- und Ziel ONTAP Cluster können Sie die LIF-Informationen zwischen den Clustern vom System Manager oder von der CLI abrufen.

1. Navigieren Sie im ONTAP System Manager zur Seite „Netzwerkübersicht“ und rufen Sie die IP-Adressen vom Typ „Intercluster“ ab, die für die Kommunikation mit dem AWS VPC konfiguriert sind, auf dem FSx installiert ist.



2. Um die Intercluster-IP-Adressen mithilfe der CLI abzurufen, führen Sie den folgenden Befehl aus:

```
ONTAP-Dest::> network interface show -role intercluster
```

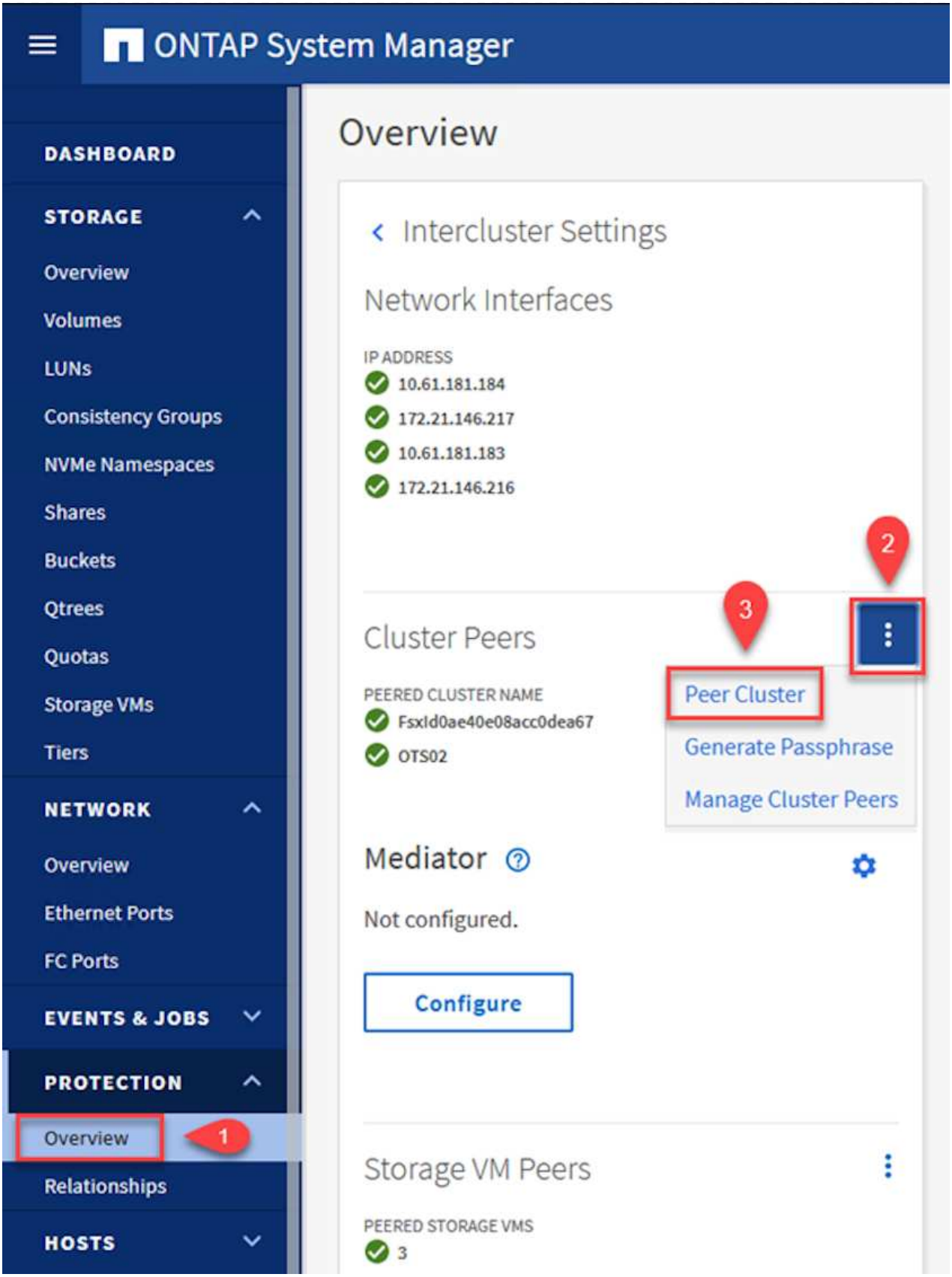
Cluster-Peering zwischen ONTAP -Clustern einrichten

Um Cluster-Peering zwischen ONTAP Clustern herzustellen, muss eine eindeutige Passphrase, die im initiierenden ONTAP Cluster eingegeben wird, im anderen Peer-Cluster bestätigt werden.

1. Richten Sie Peering auf dem Ziel ONTAP -Cluster ein, indem Sie `cluster peer create` Befehl. Geben Sie bei entsprechender Aufforderung eine eindeutige Passphrase ein, die später im Quellcluster verwendet wird, um den Erstellungsprozess abzuschließen.

   ```
   ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
   source_intercluster_1, source_intercluster_2
   Enter the passphrase:
   Confirm the passphrase:
   ```

2. Im Quellcluster können Sie die Cluster-Peer-Beziehung entweder mit ONTAP System Manager oder der CLI herstellen. Navigieren Sie im ONTAP System Manager zu „Schutz > Übersicht“ und wählen Sie „Peer-Cluster“ aus.

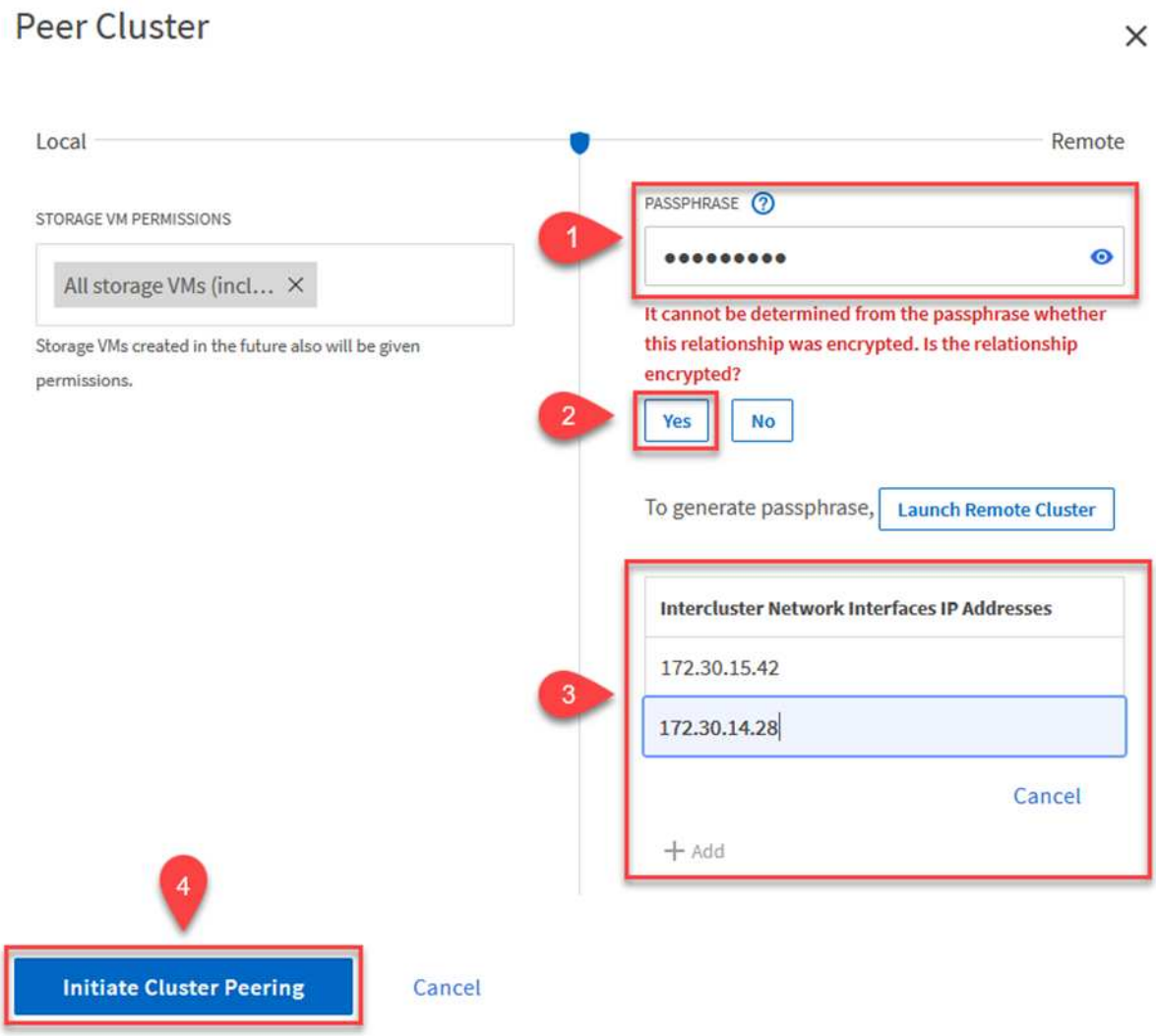


3. Geben Sie im Dialogfeld „Peer-Cluster“ die erforderlichen Informationen ein:
   a. Geben Sie die Passphrase ein, die zum Herstellen der Peer-Cluster-Beziehung auf dem Ziel ONTAP Cluster verwendet wurde.

b. Wählen `Yes` um eine verschlüsselte Beziehung aufzubauen.

c. Geben Sie die Intercluster-LIF-IP-Adresse(n) des Ziel ONTAP Clusters ein.

d. Klicken Sie auf „Cluster-Peering starten“, um den Vorgang abzuschließen.



4. Überprüfen Sie den Status der Cluster-Peer-Beziehung vom Ziel ONTAP -Cluster mit dem folgenden Befehl:

```
ONTAP-Dest::> cluster peer show
```

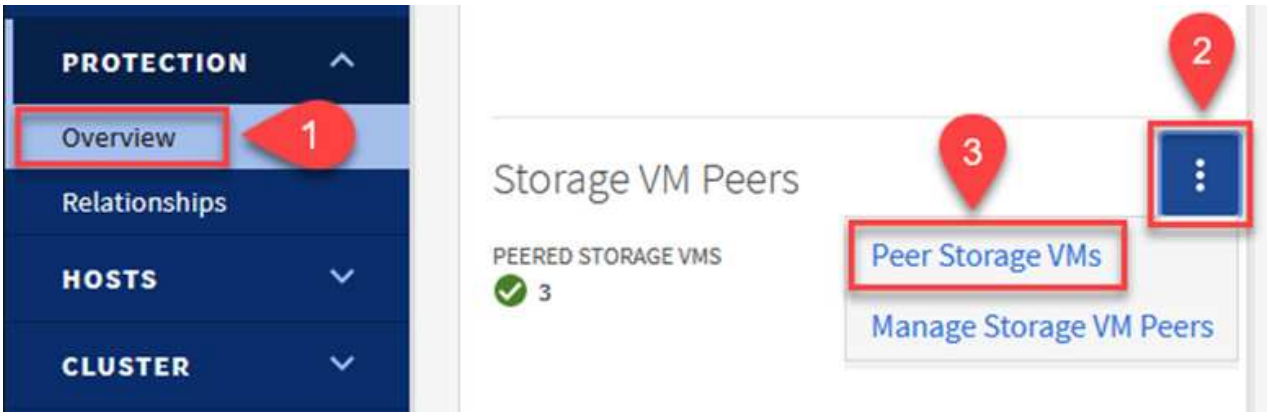
Herstellen einer SVM-Peering-Beziehung

Der nächste Schritt besteht darin, eine SVM-Beziehung zwischen den virtuellen Ziel- und Quellspeichermaschinen einzurichten, die die Volumes enthalten, die in SnapMirror -Beziehungen enthalten sein werden.

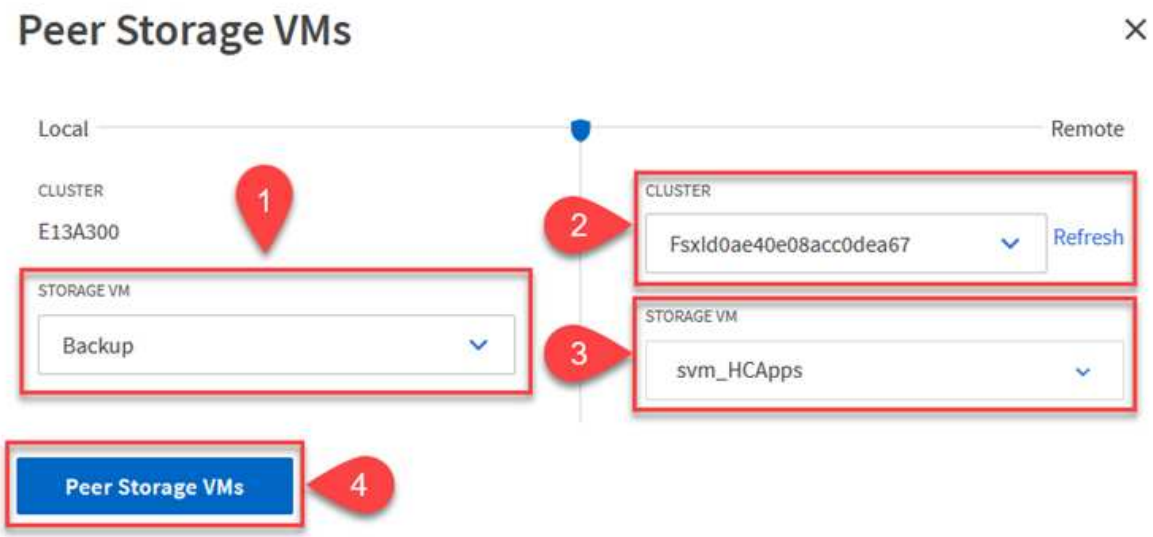
1. Verwenden Sie vom Ziel ONTAP Cluster aus den folgenden Befehl aus der CLI, um die SVM-Peer-Beziehung zu erstellen:

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Akzeptieren Sie vom Quell ONTAP Cluster aus die Peering-Beziehung entweder mit dem ONTAP System Manager oder der CLI.
3. Gehen Sie im ONTAP System Manager zu „Schutz > Übersicht“ und wählen Sie unter „Storage VM Peers“ die Option „Peer Storage VMs“ aus.



4. Füllen Sie im Dialogfeld der Peer Storage-VM die erforderlichen Felder aus:
   - Die Quellspeicher-VM
   - Der Zielcluster
   - Die Zielspeicher-VM



5. Klicken Sie auf „Peer-Storage-VMs“, um den SVM-Peering-Prozess abzuschließen.

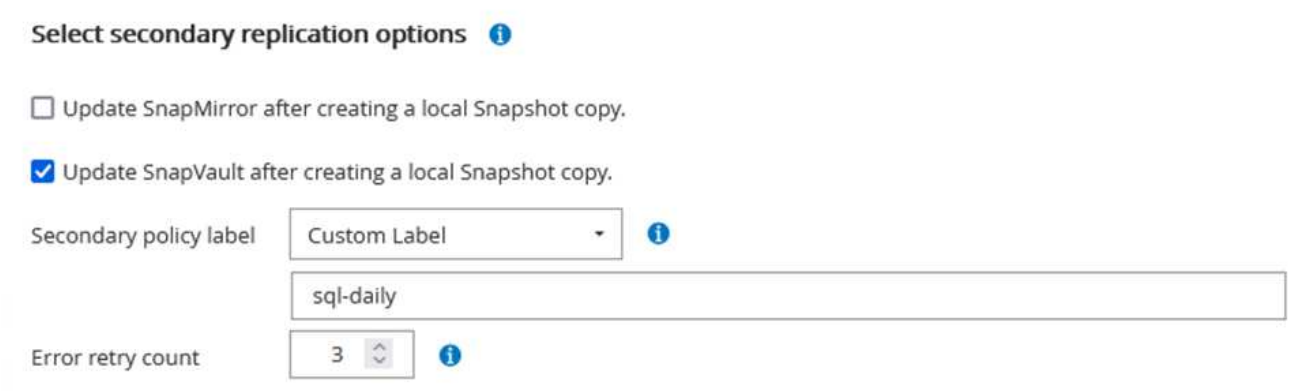
Erstellen einer Snapshot-Aufbewahrungsrichtlinie

SnapCenter verwaltet Aufbewahrungspläne für Backups, die als Snapshot-Kopien auf dem primären Speichersystem vorhanden sind. Dies wird beim Erstellen einer Richtlinie in SnapCenter festgelegt. SnapCenter verwaltet keine Aufbewahrungsrichtlinien für Backups, die auf sekundären Speichersystemen aufbewahrt werden. Diese Richtlinien werden separat über eine SnapMirror -Richtlinie verwaltet, die auf dem sekundären FSx-Cluster erstellt und den Zielvolumes zugeordnet wird, die in einer SnapMirror -Beziehung mit dem Quellvolume stehen.

Beim Erstellen einer SnapCenter -Richtlinie haben Sie die Möglichkeit, eine sekundäre Richtlinienbezeichnung anzugeben, die der SnapMirror Bezeichnung jedes Snapshots hinzugefügt wird, der beim Erstellen einer SnapCenter Sicherung generiert wird.

> Auf dem sekundären Speicher werden diese Bezeichnungen mit den Richtlinienregeln des Zielvolumes abgeglichen, um die Aufbewahrung von Snapshots zu erzwingen.

Das folgende Beispiel zeigt ein SnapMirror -Label, das auf allen Snapshots vorhanden ist, die im Rahmen einer Richtlinie für tägliche Sicherungen unserer SQL Server-Datenbank und Protokollvolumes generiert werden.



Weitere Informationen zum Erstellen von SnapCenter -Richtlinien für eine SQL Server-Datenbank finden Sie im "SnapCenter -Dokumentation" .

Sie müssen zunächst eine SnapMirror -Richtlinie mit Regeln erstellen, die die Anzahl der aufzubewahrenden Snapshot-Kopien vorgeben.

1. Erstellen Sie die SnapMirror Richtlinie auf dem FSx-Cluster.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Fügen Sie der Richtlinie Regeln mit SnapMirror -Beschriftungen hinzu, die den in den SnapCenter -Richtlinien angegebenen sekundären Richtlinienbezeichnungen entsprechen.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Das folgende Skript bietet ein Beispiel für eine Regel, die einer Richtlinie hinzugefügt werden könnte:

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Erstellen Sie zusätzliche Regeln für jedes SnapMirror Label und die Anzahl der aufzubewahrenden Snapshots (Aufbewahrungszeitraum).

Zielvolumes erstellen

Um ein Zielvolume auf ONTAP zu erstellen, das Snapshot-Kopien von unseren Quellvolumes empfängt, führen Sie den folgenden Befehl auf dem Ziel ONTAP Cluster aus:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

Erstellen Sie die SnapMirror -Beziehungen zwischen Quell- und Zielvolumes

Um eine SnapMirror -Beziehung zwischen einem Quell- und einem Zielvolume zu erstellen, führen Sie den folgenden Befehl auf dem Ziel- ONTAP Cluster aus:

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

Initialisieren Sie die SnapMirror -Beziehungen

Initialisieren Sie die SnapMirror -Beziehung. Dieser Vorgang initiiert einen neuen Snapshot, der vom Quellvolume generiert wird, und kopiert ihn auf das Zielvolume.

Um ein Volume zu erstellen, führen Sie den folgenden Befehl auf dem Ziel ONTAP -Cluster aus:

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Konfigurieren des SnapCenter Plug-in for VMware vSphere

Nach der Installation kann über die Verwaltungsschnittstelle der vCenter Server Appliance auf das SnapCenter Plug-in for VMware vSphere zugegriffen werden. SCV verwaltet Backups für die auf den ESXi-Hosts bereitgestellten NFS-Datenspeicher, die die Windows- und Linux-VMs enthalten.

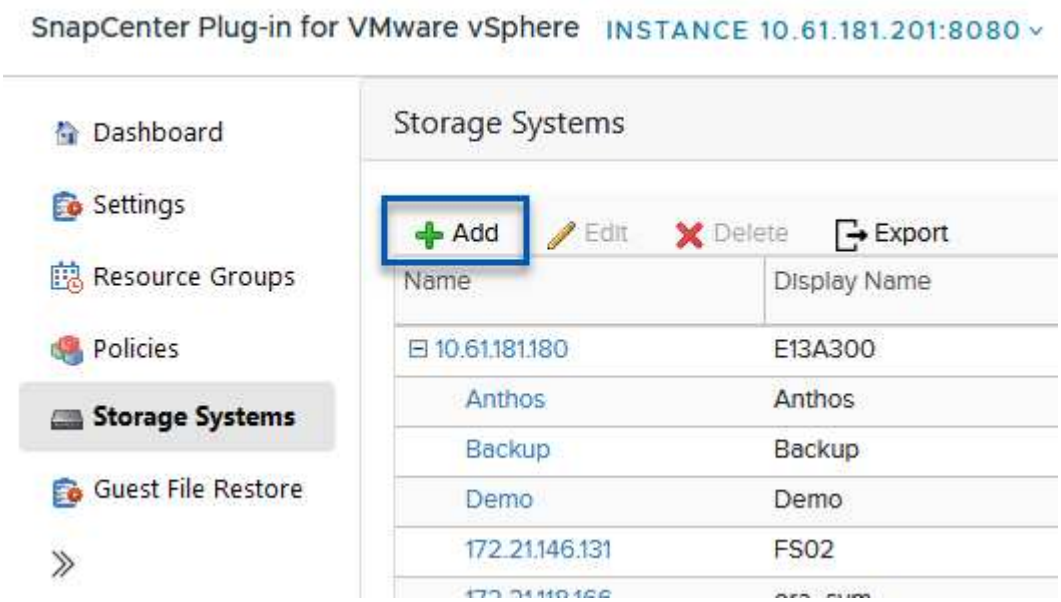
Überprüfen Sie die "Datenschutz-Workflow" Weitere Informationen zu den Schritten zum Konfigurieren von Sicherungen finden Sie im Abschnitt „Sicherungskonfiguration“ der SCV-Dokumentation.

Um Sicherungen Ihrer virtuellen Maschinen und Datenspeicher zu konfigurieren, müssen die folgenden Schritte über die Plug-In-Schnittstelle ausgeführt werden.

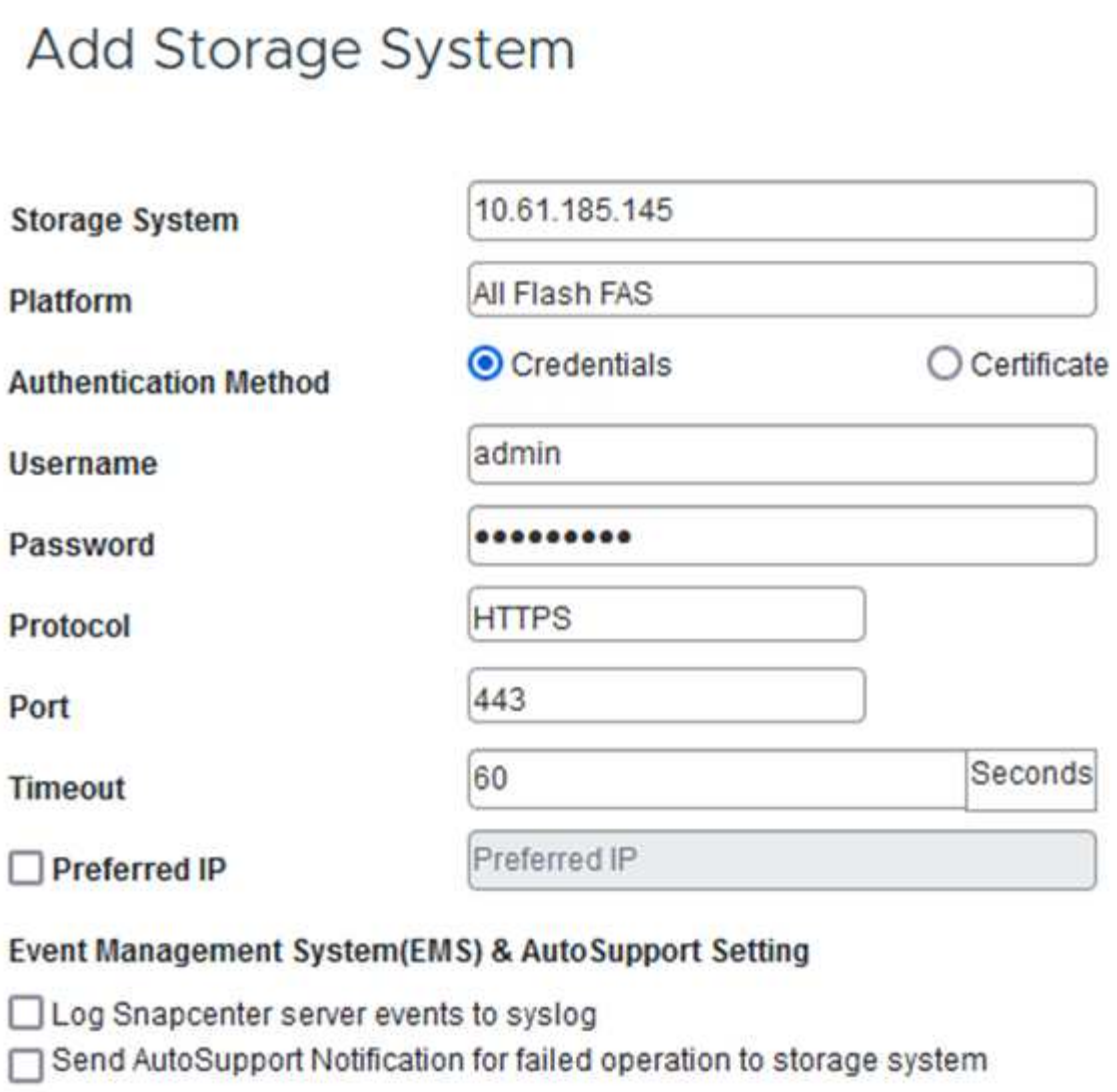
Discovery ONTAP -Speichersysteme

Entdecken Sie die ONTAP Speichercluster, die sowohl für primäre als auch für sekundäre Backups verwendet werden sollen.

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Speichersysteme** und klicken Sie auf die Schaltfläche **Hinzufügen**.



2. Geben Sie die Anmeldeinformationen und den Plattformtyp für das primäre ONTAP Speichersystem ein und klicken Sie auf **Hinzufügen**.



3. Wiederholen Sie diesen Vorgang für das sekundäre ONTAP Speichersystem.

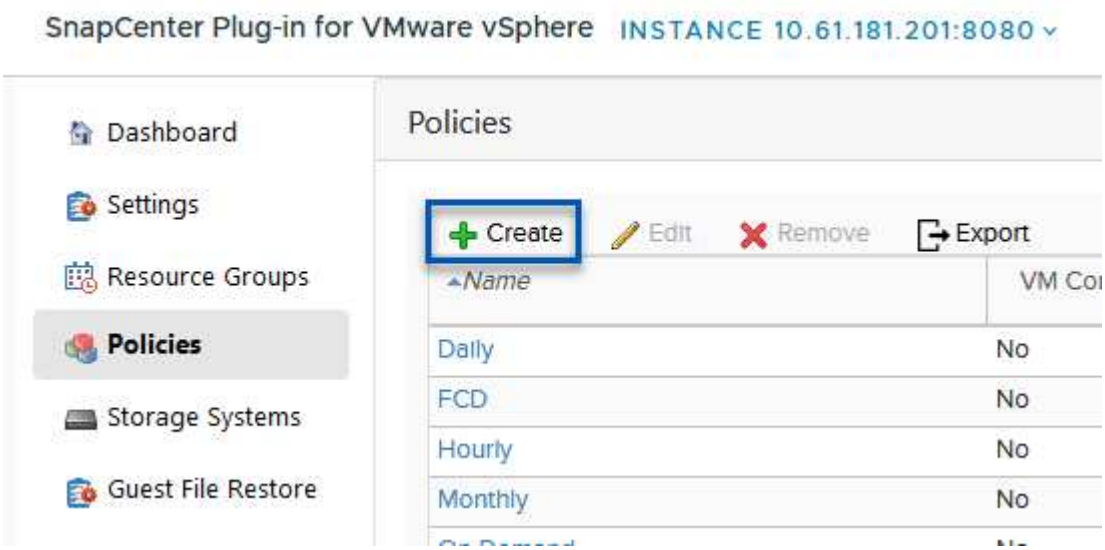
Erstellen von SCV-Sicherungsrichtlinien

Richtlinien legen die Aufbewahrungsdauer, Häufigkeit und Replikationsoptionen für die von SCV verwalteten Backups fest.

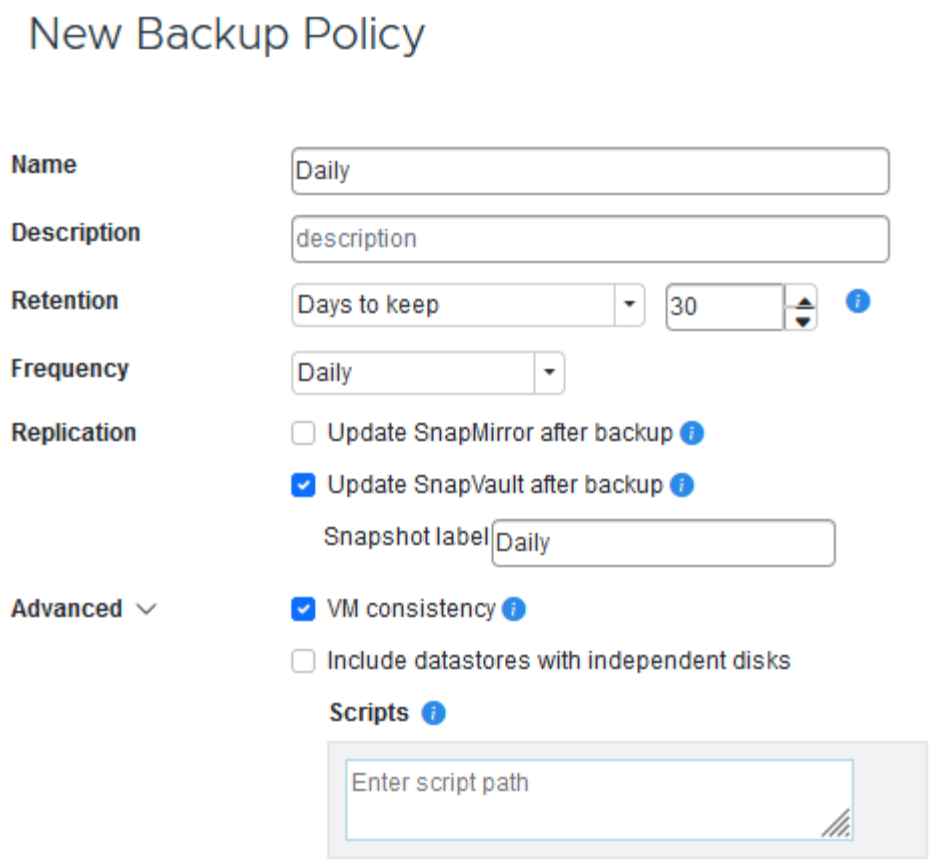
Überprüfen Sie die "Erstellen Sie Sicherungsrichtlinien für VMs und Datenspeicher" Weitere Informationen finden Sie im Abschnitt der Dokumentation.

Führen Sie zum Erstellen von Sicherungsrichtlinien die folgenden Schritte aus:

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Richtlinien** und klicken Sie auf die Schaltfläche **Erstellen**.



2. Geben Sie einen Namen für die Richtlinie, den Aufbewahrungszeitraum, die Häufigkeit und Replikationsoptionen sowie die Snapshot-Bezeichnung an.



Beim Erstellen einer Richtlinie im SnapCenter -Plug-in werden Optionen für SnapMirror und SnapVault angezeigt. Wenn Sie SnapMirror wählen, ist der in der Richtlinie angegebene Aufbewahrungszeitplan für die primären und sekundären Snapshots derselbe. Wenn Sie SnapVault wählen, basiert der Aufbewahrungszeitplan für den sekundären Snapshot auf einem separaten Zeitplan, der mit der SnapMirror -Beziehung implementiert wird. Dies ist nützlich, wenn Sie längere Aufbewahrungszeiträume für sekundäre Sicherungen wünschen.

Snapshot-Labels sind insofern nützlich, als dass sie zum Erlassen von Richtlinien mit einer bestimmten Aufbewahrungsdauer für die auf den sekundären ONTAP Cluster replizierten SnapVault -Kopien verwendet werden können. Wenn SCV mit BlueXP Backup and Restore verwendet wird, muss das Feld „Snapshot-Bezeichnung“ entweder leer sein oder mit der in der BlueXP -Sicherungsrichtlinie angegebenen Bezeichnung übereinstimmen.

3. Wiederholen Sie den Vorgang für jede erforderliche Richtlinie. Beispielsweise separate Richtlinien für tägliche, wöchentliche und monatliche Backups.

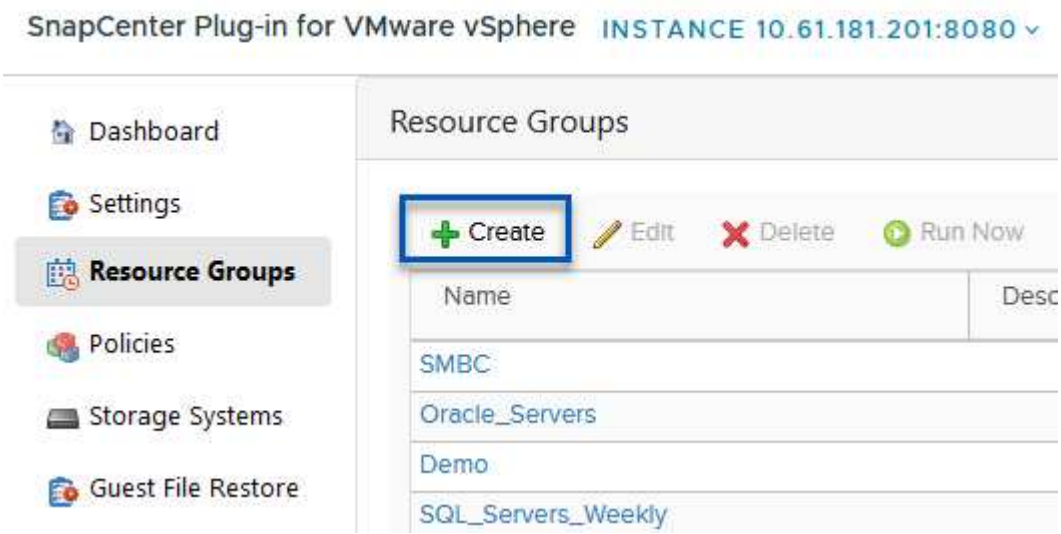
Erstellen von Ressourcengruppen

Ressourcengruppen enthalten die Datenspeicher und virtuellen Maschinen, die in einen Sicherungsauftrag einbezogen werden sollen, zusammen mit der zugehörigen Richtlinie und dem Sicherungszeitplan.

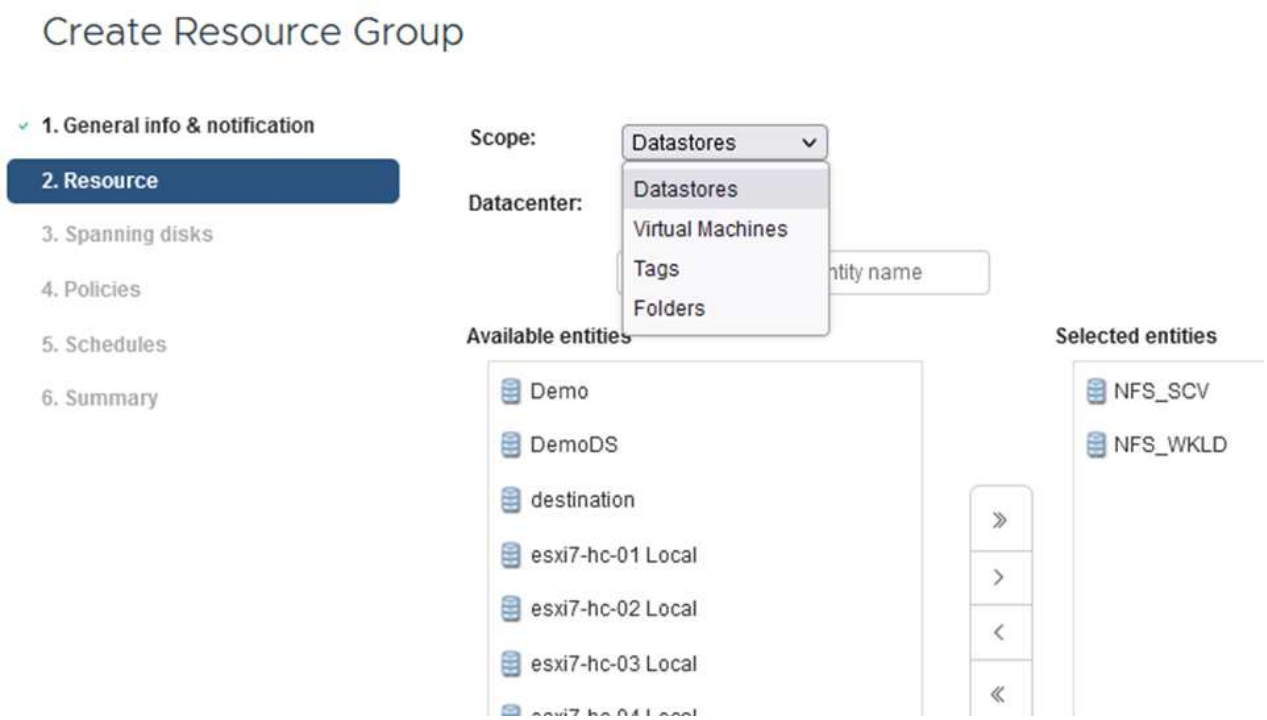
Überprüfen Sie die "Erstellen von Ressourcengruppen" Weitere Informationen finden Sie im Abschnitt der Dokumentation.

Führen Sie zum Erstellen von Ressourcengruppen die folgenden Schritte aus.

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Ressourcengruppen** und klicken Sie auf die Schaltfläche **Erstellen**.

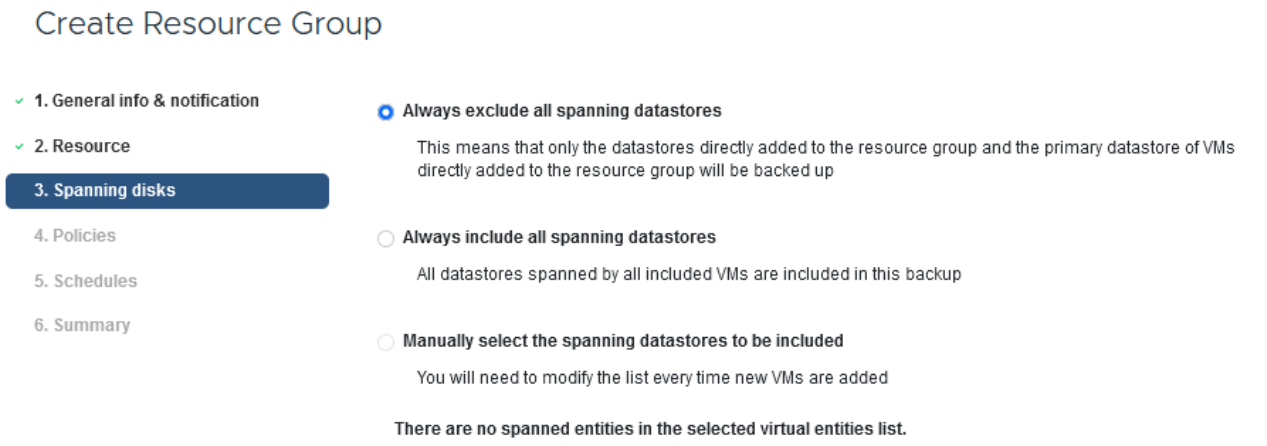


2. Geben Sie im Assistenten „Ressourcengruppe erstellen“ einen Namen und eine Beschreibung für die Gruppe sowie die zum Empfangen von Benachrichtigungen erforderlichen Informationen ein. Klicken Sie auf **Weiter**
3. Wählen Sie auf der nächsten Seite die Datenspeicher und virtuellen Maschinen aus, die in den Sicherungsauftrag einbezogen werden sollen, und klicken Sie dann auf **Weiter**.



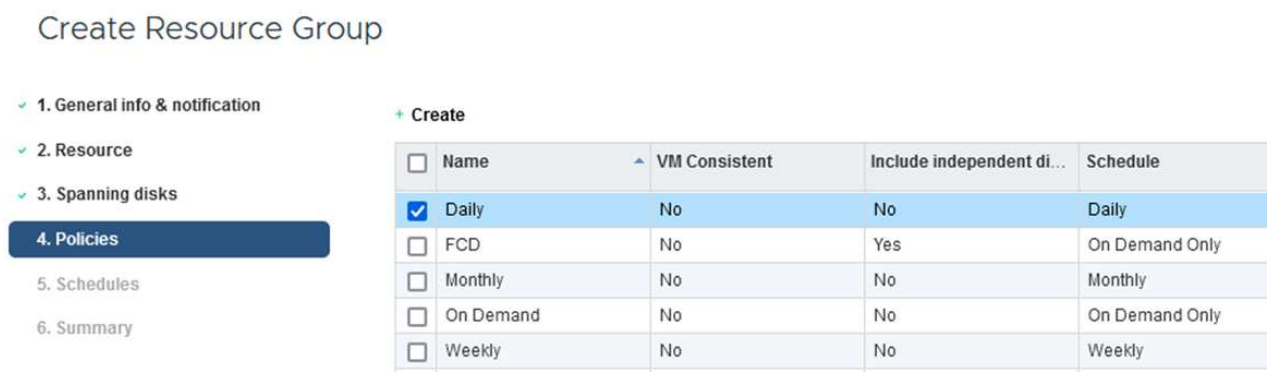
Sie haben die Möglichkeit, bestimmte VMs oder ganze Datenspeicher auszuwählen. Unabhängig davon, welche Option Sie auswählen, wird das gesamte Volume (und der Datenspeicher) gesichert, da die Sicherung das Ergebnis der Erstellung eines Snapshots des zugrunde liegenden Volumes ist. In den meisten Fällen ist es am einfachsten, den gesamten Datenspeicher auszuwählen. Wenn Sie jedoch die Liste der verfügbaren VMs beim Wiederherstellen einschränken möchten, können Sie nur eine Teilmenge der VMs für die Sicherung auswählen.

4. Wählen Sie Optionen zum Überspannen von Datenspeichern für VMs mit VMDKs, die sich auf mehreren Datenspeichern befinden, und klicken Sie dann auf **Weiter**.



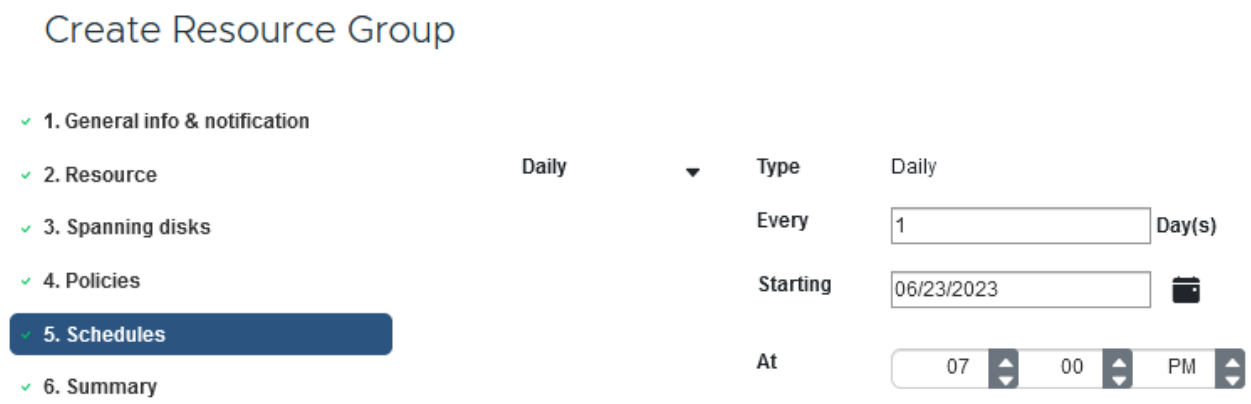
BlueXP backup and recovery unterstützt derzeit nicht das Sichern von VMs mit VMDKs, die sich über mehrere Datenspeicher erstrecken.

5. Wählen Sie auf der nächsten Seite die Richtlinien aus, die der Ressourcengruppe zugeordnet werden sollen, und klicken Sie auf **Weiter**.



> Beim Sichern von SCV-verwalteten Snapshots in einem Objektspeicher mithilfe von BlueXP backup and recovery kann jede Ressourcengruppe nur einer einzigen Richtlinie zugeordnet werden.

6. Wählen Sie einen Zeitplan aus, der bestimmt, zu welchen Zeiten die Sicherungen ausgeführt werden. Klicken Sie auf **Weiter**.

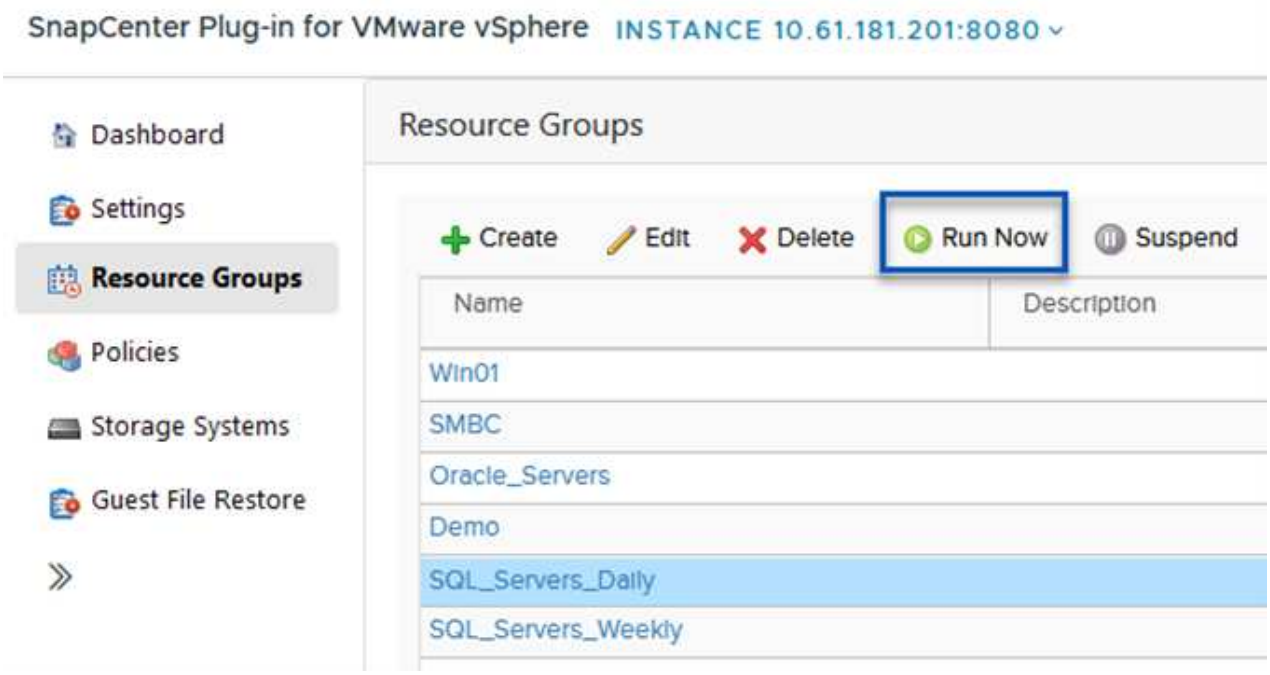


7. Überprüfen Sie abschließend die Übersichtsseite und klicken Sie dann auf **Fertig**, um die Erstellung der Ressourcengruppe abzuschließen.

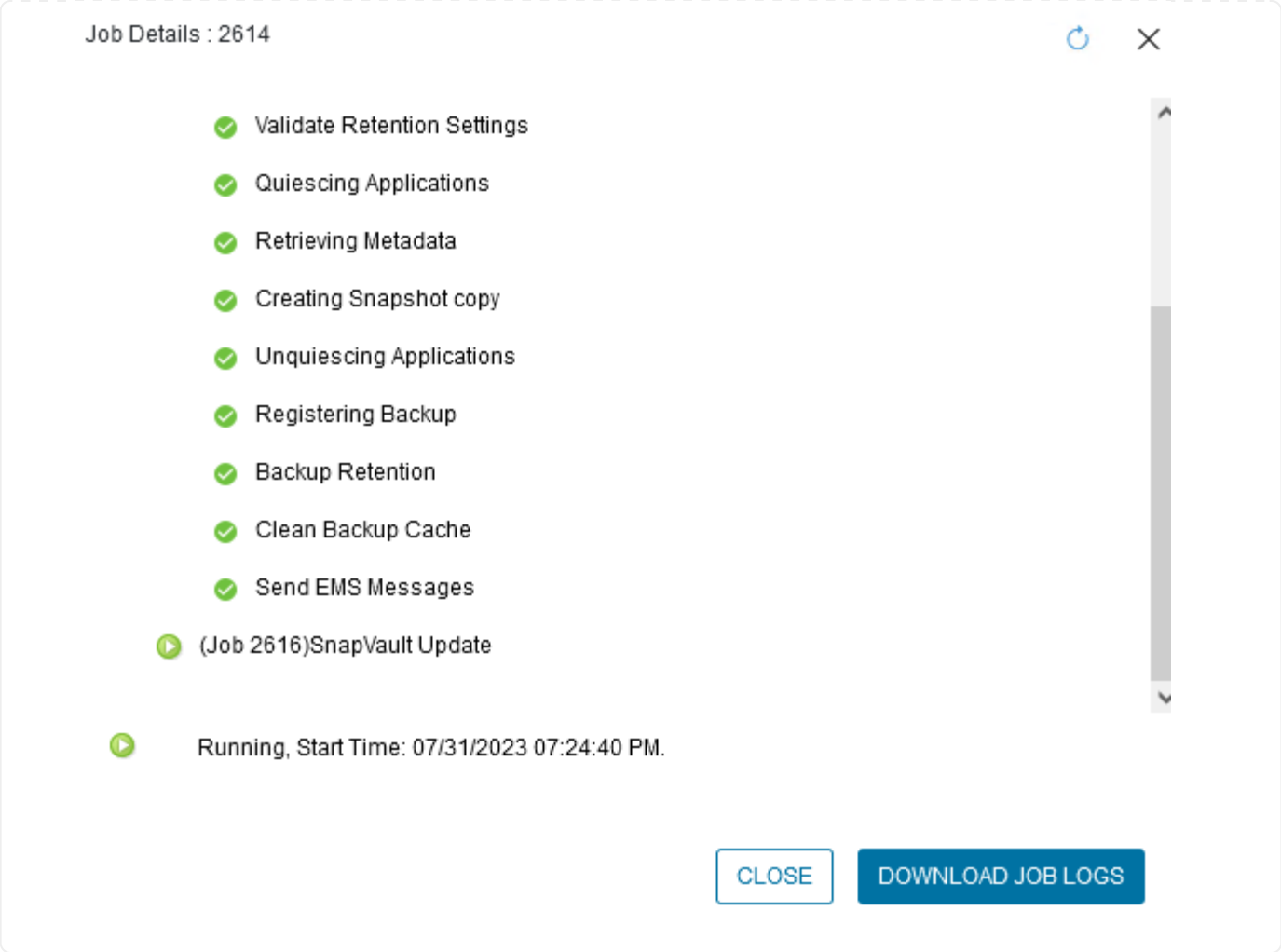
Ausführen eines Sicherungsauftrags

Führen Sie in diesem letzten Schritt einen Sicherungsauftrag aus und überwachen Sie seinen Fortschritt. Mindestens ein Sicherungsauftrag muss in SCV erfolgreich abgeschlossen werden, bevor Ressourcen von BlueXP backup and recovery erkannt werden können.

1. Navigieren Sie im SnapCenter Plug-in for VMware vSphere im linken Menü zu **Ressourcengruppen**.
2. Um einen Sicherungsauftrag zu starten, wählen Sie die gewünschte Ressourcengruppe aus und klicken Sie auf die Schaltfläche **Jetzt ausführen**.



3. Um den Sicherungsauftrag zu überwachen, navigieren Sie im linken Menü zu **Dashboard**. Klicken Sie unter **Letzte Jobaktivitäten** auf die Job-ID-Nummer, um den Jobfortschritt zu überwachen.



Konfigurieren Sie Backups im Objektspeicher in BlueXP backup and recovery

Damit BlueXP die Dateninfrastruktur effektiv verwalten kann, ist die vorherige Installation eines Connectors erforderlich. Der Connector führt die Aktionen aus, die zum Erkennen von Ressourcen und Verwalten von Datenvorgängen erforderlich sind.

Weitere Informationen zum BlueXP Connector finden Sie unter "Erfahren Sie mehr über Konnektoren" in der BlueXP Dokumentation.

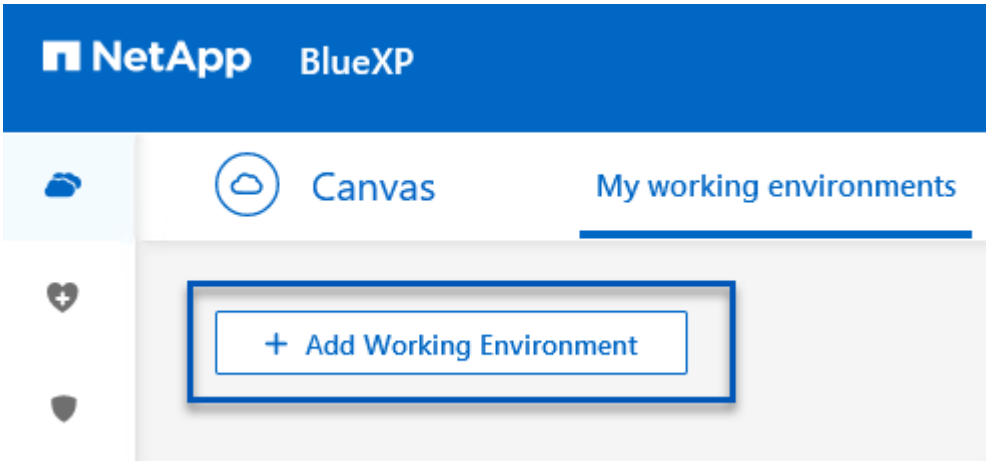
Sobald der Connector für den verwendeten Cloud-Anbieter installiert ist, kann im Canvas eine grafische Darstellung des Objektspeichers angezeigt werden.

Führen Sie die folgenden Schritte aus, um BlueXP backup and recovery für die Sicherung von Daten zu konfigurieren, die vor Ort von SCV verwaltet werden:

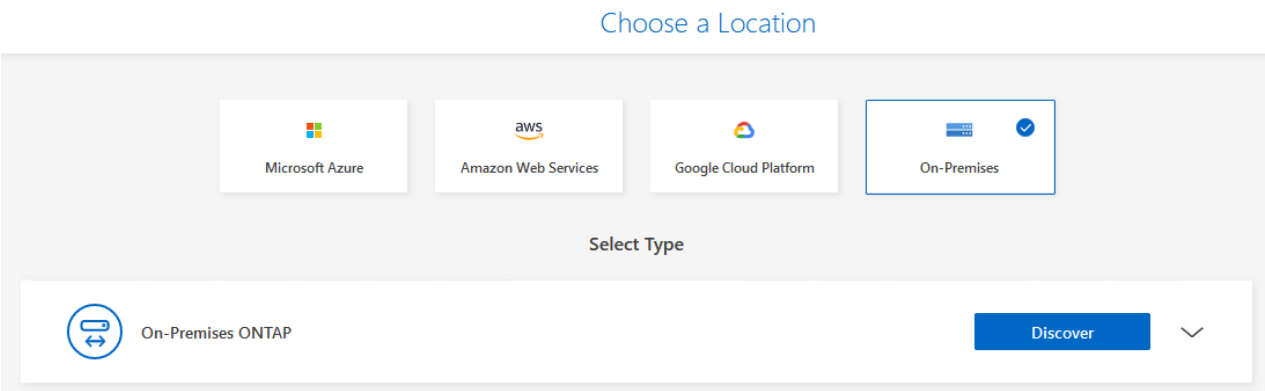
Arbeitsumgebungen zum Canvas hinzufügen

Der erste Schritt besteht darin, die lokalen ONTAP Speichersysteme zu BlueXP hinzuzufügen

1. Wählen Sie im Canvas „Arbeitsumgebung hinzufügen“ aus, um zu beginnen.



2. Wählen Sie aus der Standortauswahl **On-Premises** aus und klicken Sie dann auf die Schaltfläche **Discover**.



3. Geben Sie die Anmeldeinformationen für das ONTAP Speichersystem ein und klicken Sie auf die Schaltfläche **Erkennen**, um die Arbeitsumgebung hinzuzufügen.

ONTAP Cluster IP

10.61.181.180

User Name

admin

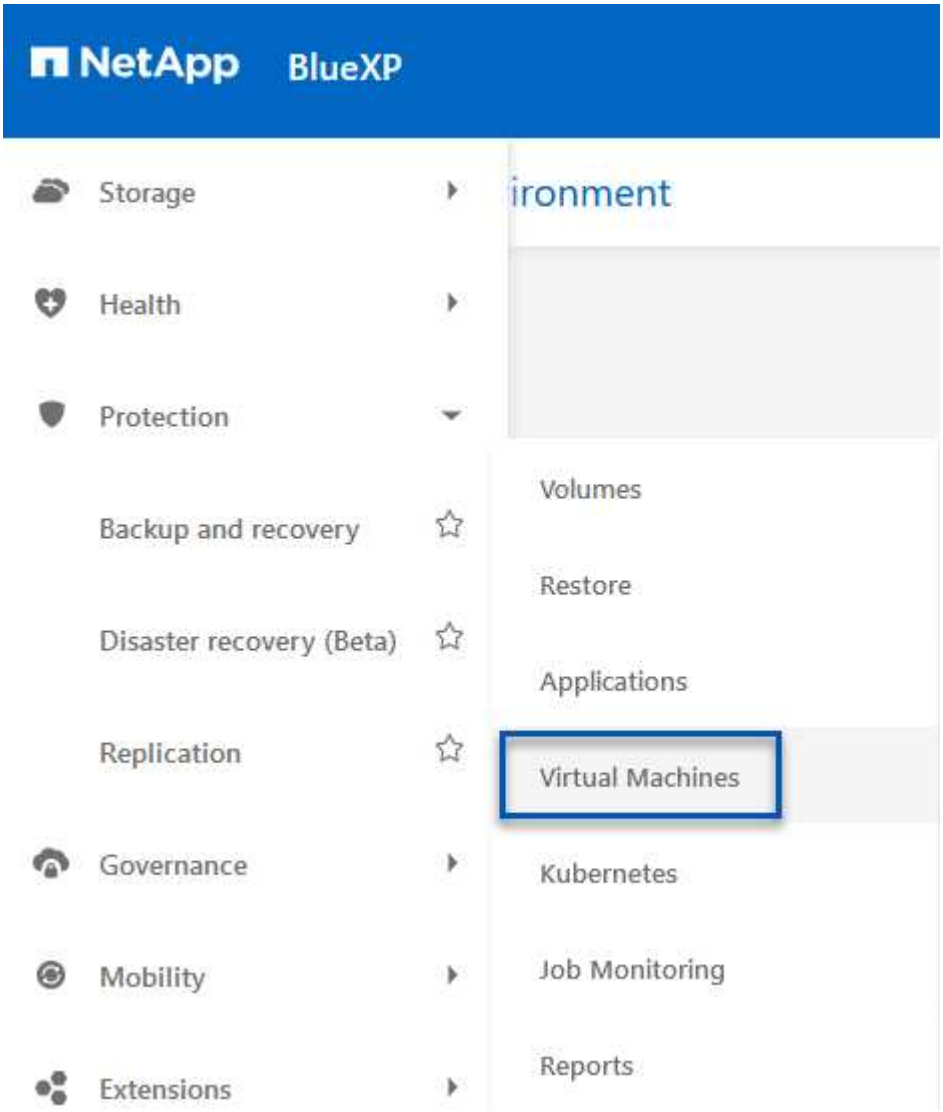
Password

••••••••••

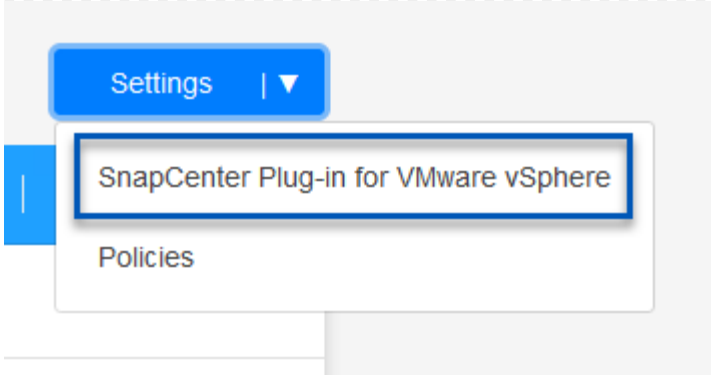
Entdecken Sie lokale SCV-Geräte und vCenter

Um den lokalen Datenspeicher und die virtuellen Maschinenressourcen zu ermitteln, fügen Sie Informationen für den SCV-Datenbroker und Anmeldeinformationen für die vCenter-Verwaltungs-Appliance hinzu.

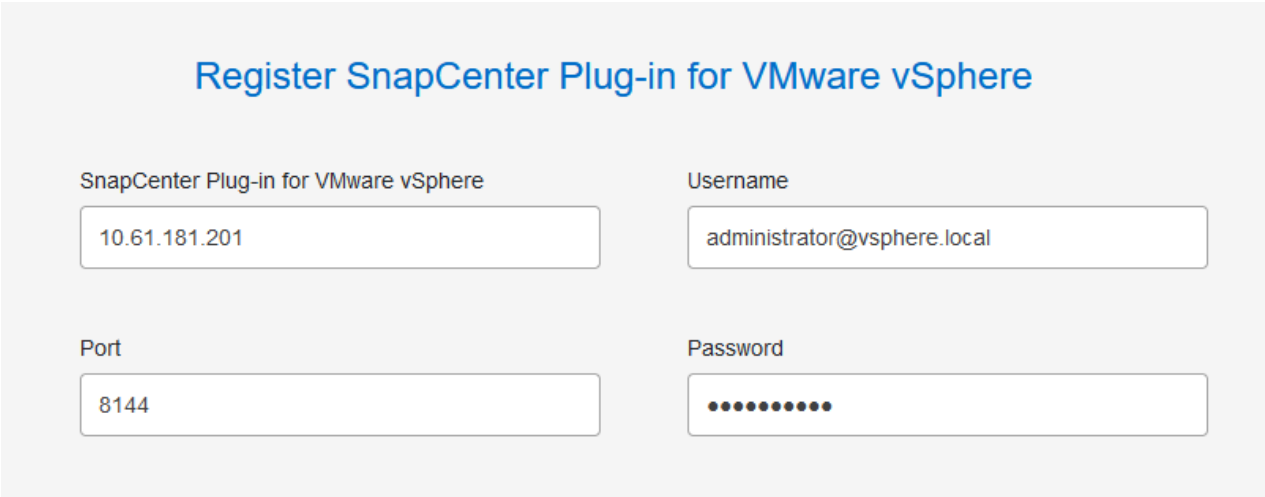
1. Wählen Sie im linken Menü von BlueXP „Schutz > Sicherung und Wiederherstellung > Virtuelle Maschinen“ aus.



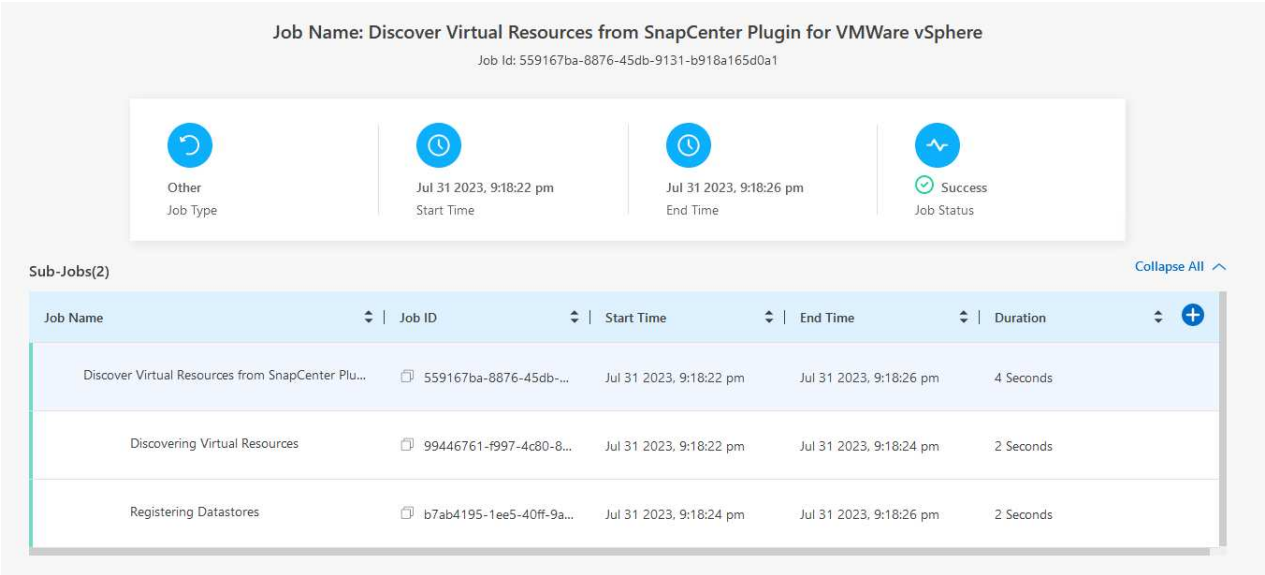
2. Rufen Sie vom Hauptbildschirm der virtuellen Maschinen aus das Dropdown-Menü **Einstellungen** auf und wählen Sie * SnapCenter Plug-in for VMware vSphere* aus.



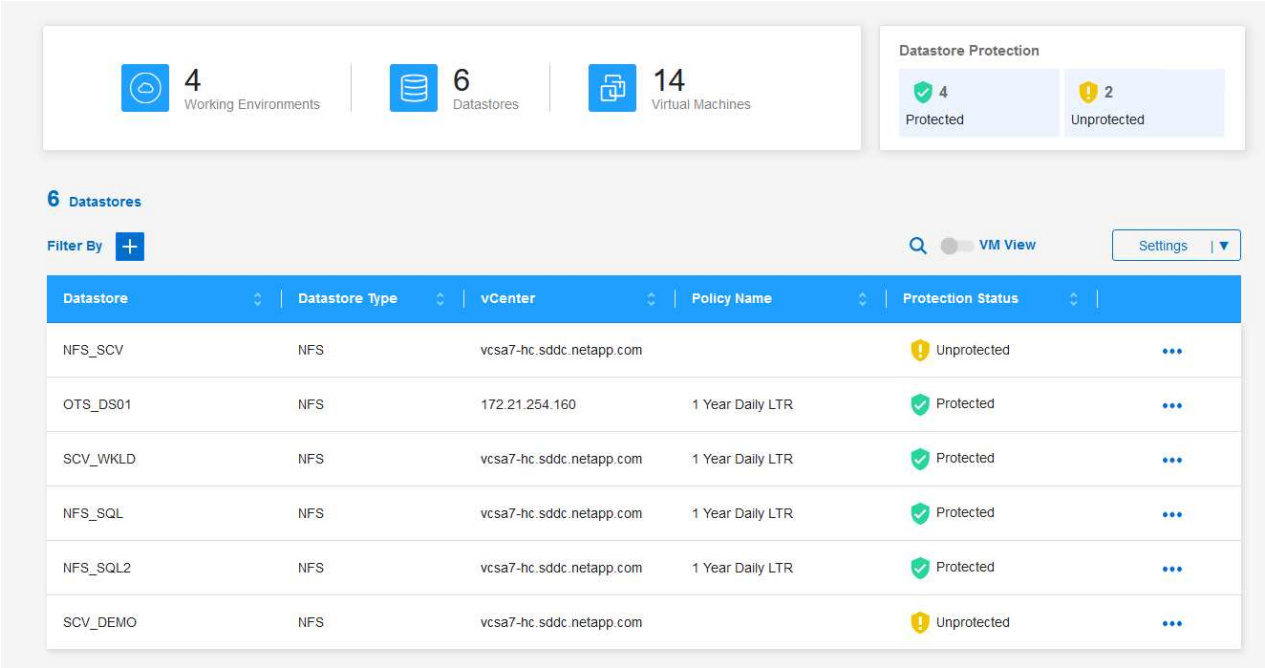
3. Klicken Sie auf die Schaltfläche **Registrieren** und geben Sie dann die IP-Adresse und Portnummer für das SnapCenter Plug-in-Gerät sowie den Benutzernamen und das Kennwort für das vCenter-Verwaltungsgerät ein. Klicken Sie auf die Schaltfläche **Registrieren**, um den Erkennungsprozess zu starten.



4. Der Fortschritt von Jobs kann auf der Registerkarte „Jobüberwachung“ überwacht werden.



5. Sobald die Erkennung abgeschlossen ist, können Sie die Datenspeicher und virtuellen Maschinen auf allen erkannten SCV-Geräten anzeigen.

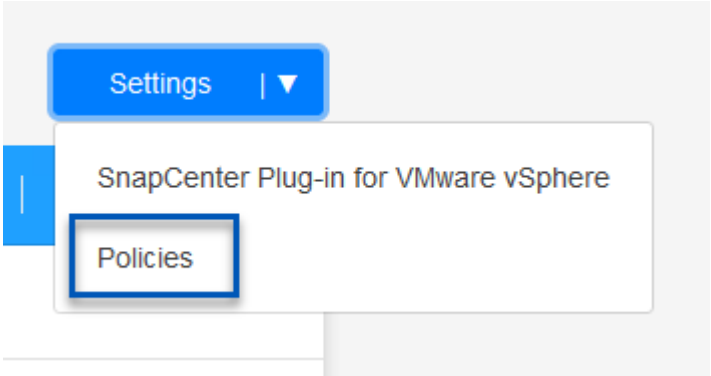

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV
NFS
vcsa7-hc.sddc.netapp.com
Unprotected
OTS_DS01
NFS
172.21.254.160
1 Year Daily LTR
Protected
SCV_WKLD
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL2
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
SCV_DEMO
NFS
vcsa7-hc.sddc.netapp.com
Unprotected

Erstellen Sie BlueXP -Sicherungsrichtlinien

Erstellen Sie in BlueXP backup and recovery für virtuelle Maschinen Richtlinien, um den Aufbewahrungszeitraum, die Sicherungsquelle und die Archivierungsrichtlinie festzulegen.

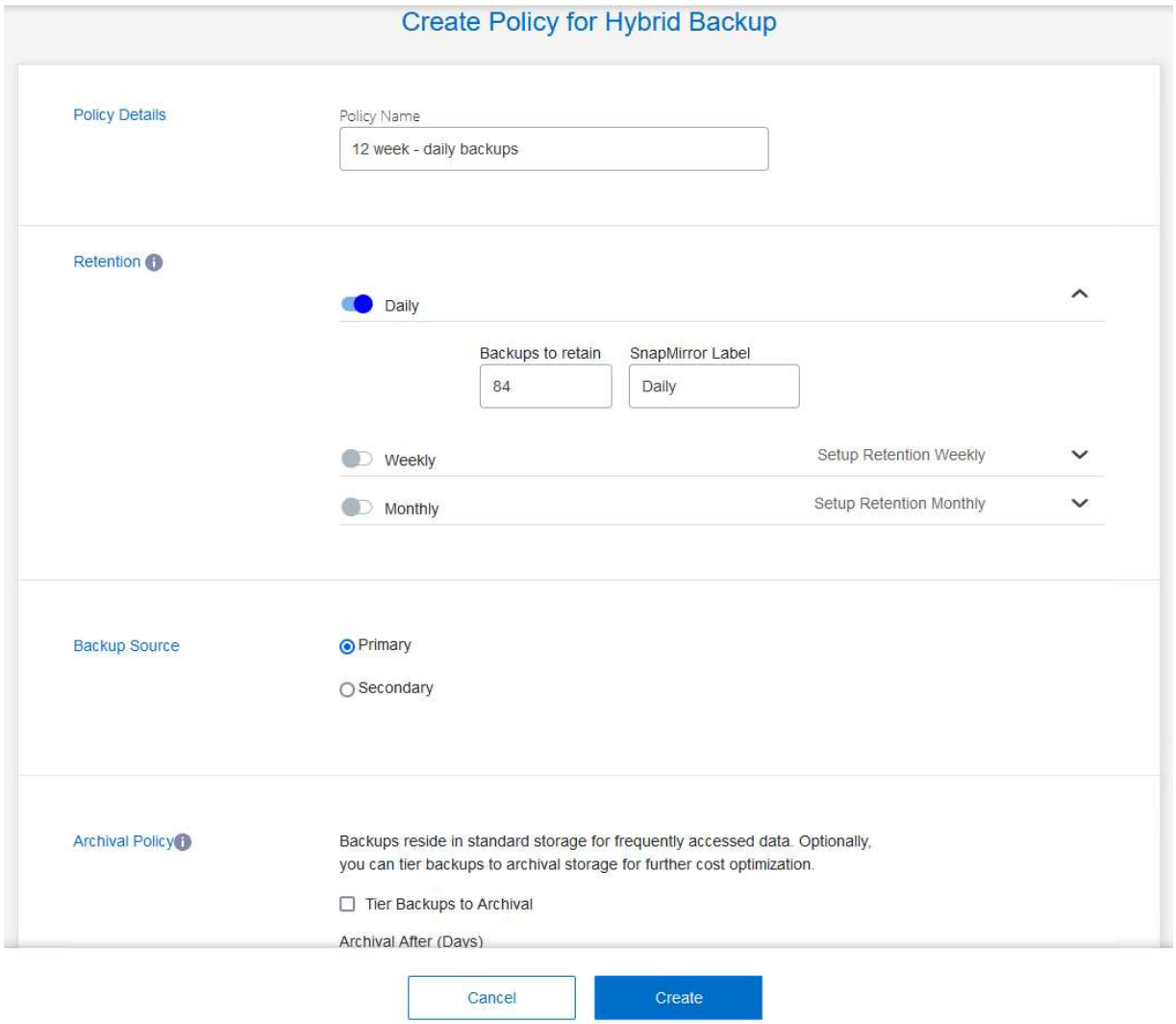
Weitere Informationen zum Erstellen von Richtlinien finden Sie unter "Erstellen einer Richtlinie zum Sichern von Datenspeichern" .

1. Rufen Sie auf der Hauptseite von BlueXP backup and recovery für virtuelle Maschinen das Dropdown-Menü **Einstellungen** auf und wählen Sie **Richtlinien** aus.



2. Klicken Sie auf **Richtlinie erstellen**, um auf das Fenster **Richtlinie für Hybrid-Backup erstellen** zuzugreifen.

   a. Fügen Sie einen Namen für die Richtlinie hinzu
   b. Wählen Sie die gewünschte Aufbewahrungsdauer
   c. Wählen Sie aus, ob die Backups vom primären oder sekundären lokalen ONTAP Speichersystem stammen sollen
   d. Geben Sie optional an, nach welchem Zeitraum die Sicherungen in den Archivspeicher verschoben werden, um zusätzliche Kosten zu sparen.



Das hier eingegebene SnapMirror -Label wird verwendet, um zu identifizieren, auf welche Backups die Richtlinie angewendet werden soll. Der Bezeichnungsname muss mit dem Bezeichnungsnamen in der entsprechenden lokalen SCV-Richtlinie übereinstimmen.

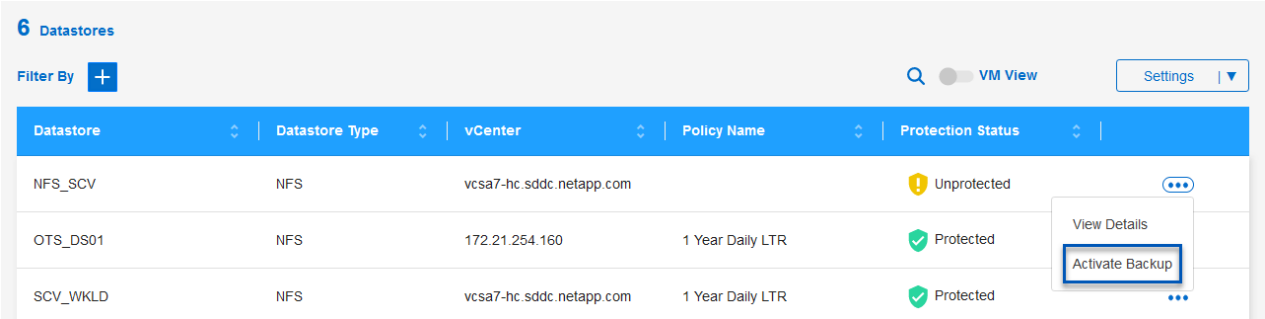
3. Klicken Sie auf **Erstellen**, um die Richtlinienerstellung abzuschließen.

Datenspeicher auf Amazon Web Services sichern

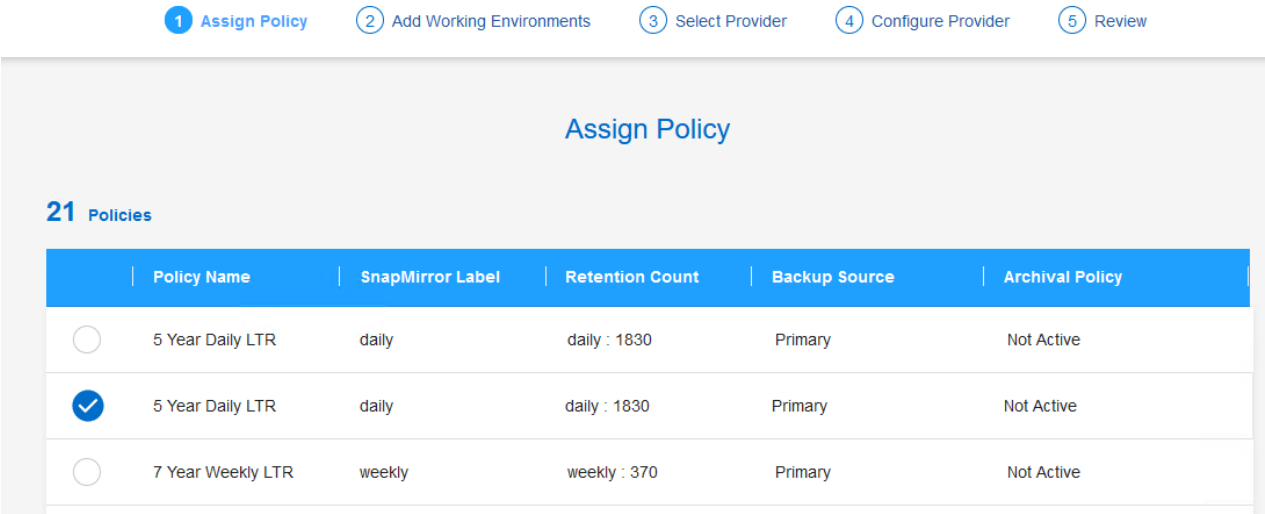
Der letzte Schritt besteht darin, den Datenschutz für die einzelnen Datenspeicher und virtuellen Maschinen zu aktivieren. Die folgenden Schritte beschreiben, wie Sie Backups in AWS aktivieren.

Weitere Informationen finden Sie unter "Sichern Sie Datenspeicher auf Amazon Web Services" .

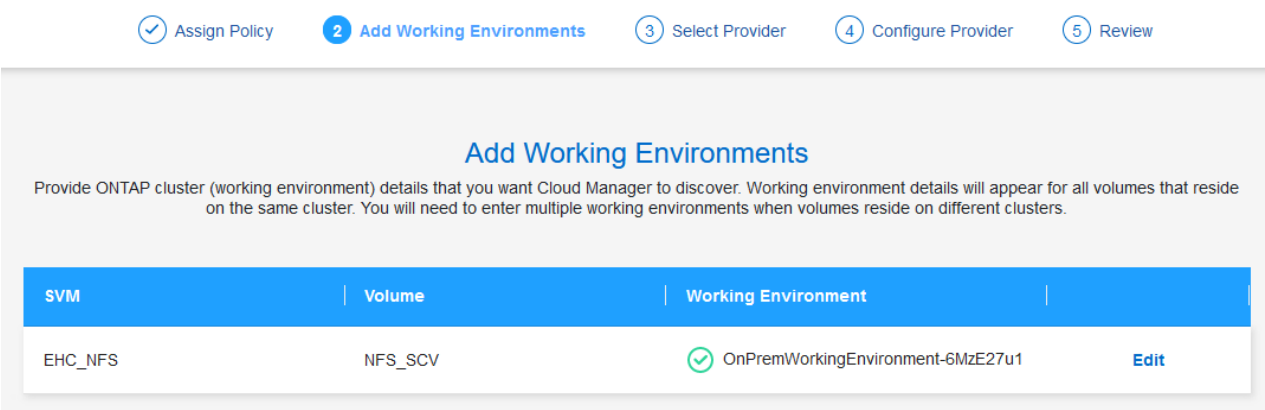
1. Rufen Sie auf der Hauptseite von BlueXP backup and recovery für virtuelle Maschinen das Dropdown-Menü „Einstellungen“ für den zu sichernden Datenspeicher auf und wählen Sie „Sicherung aktivieren“ aus.



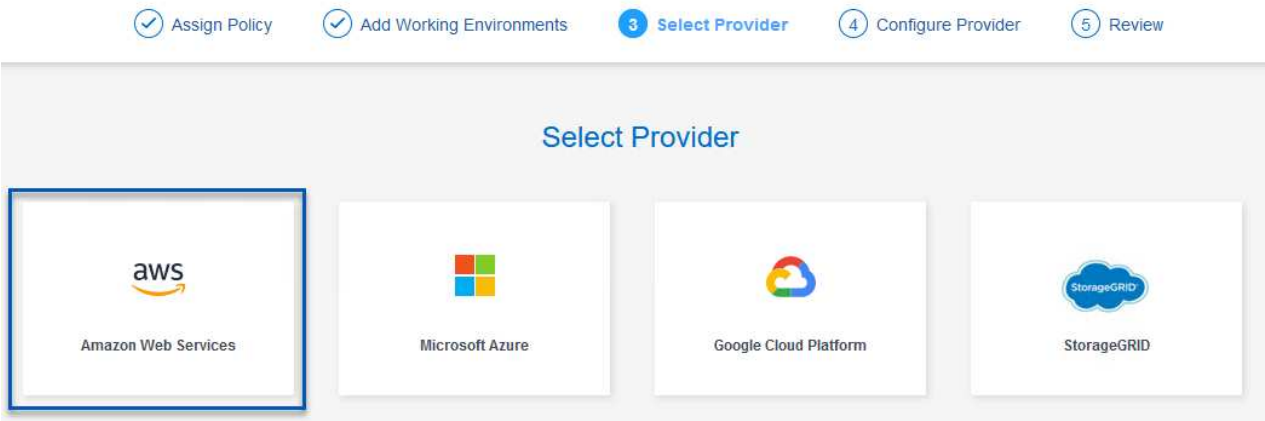
2. Weisen Sie die für den Datenschutzvorgang zu verwendende Richtlinie zu und klicken Sie auf **Weiter**.



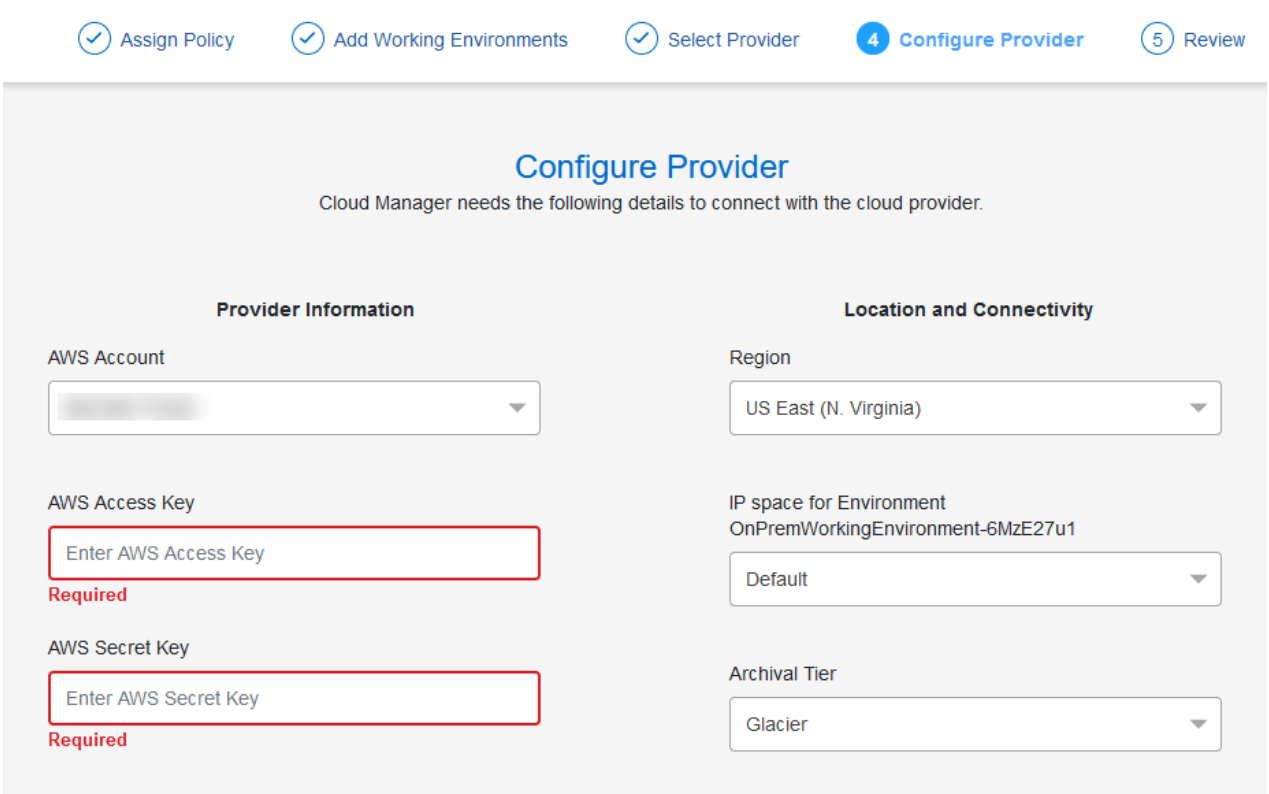
3. Auf der Seite **Arbeitsumgebungen hinzufügen** sollten der Datenspeicher und die Arbeitsumgebung mit einem Häkchen angezeigt werden, wenn die Arbeitsumgebung zuvor erkannt wurde. Wenn die Arbeitsumgebung noch nicht erkannt wurde, können Sie sie hier hinzufügen. Klicken Sie auf **Weiter**, um fortzufahren.



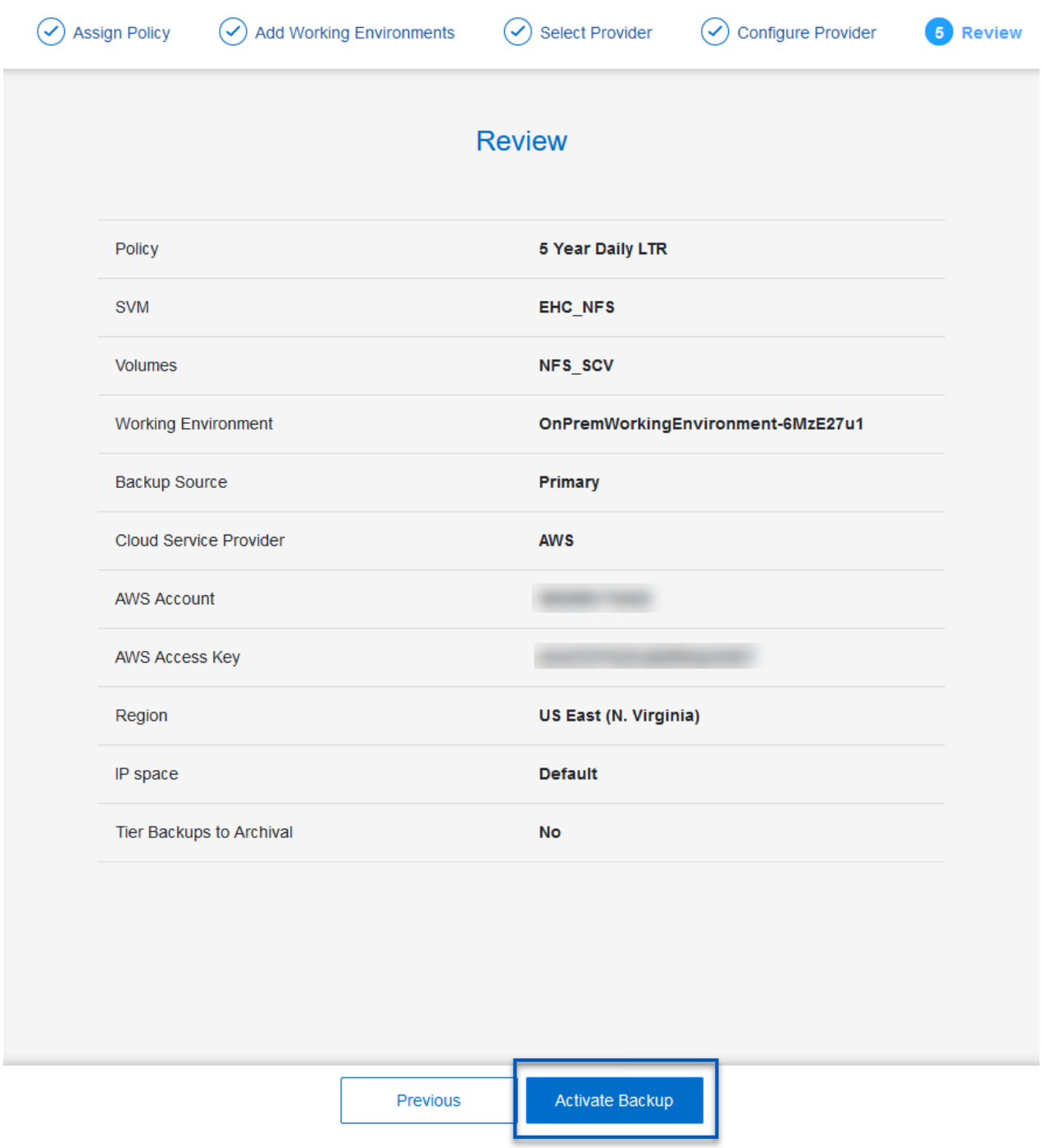
4. Klicken Sie auf der Seite **Anbieter auswählen** auf AWS und dann auf die Schaltfläche **Weiter**, um fortzufahren.



5. Füllen Sie die anbieterspezifischen Anmeldeinformationen für AWS aus, einschließlich des AWS-Zugriffsschlüssels und des geheimen Schlüssels, der Region und der zu verwendenden Archivierungsebene. Wählen Sie außerdem den ONTAP -IP-Bereich für das lokale ONTAP Speichersystem aus. Klicken Sie auf **Weiter**.



6. Überprüfen Sie abschließend die Details des Sicherungsauftrags und klicken Sie auf die Schaltfläche **Sicherung aktivieren**, um den Datenschutz des Datenspeichers zu starten.



Zu diesem Zeitpunkt beginnt die Datenübertragung möglicherweise nicht sofort. BlueXP backup and recovery sucht stündlich nach ausstehenden Snapshots und überträgt diese dann in den Objektspeicher.

Wiederherstellung virtueller Maschinen im Falle eines Datenverlusts

Die Gewährleistung der Sicherheit Ihrer Daten ist nur ein Aspekt eines umfassenden Datenschutzes. Ebenso wichtig ist die Möglichkeit, Daten im Falle eines Datenverlusts oder eines Ransomware-Angriffs umgehend von jedem beliebigen Ort aus wiederherzustellen. Diese Fähigkeit ist für die Aufrechterhaltung eines reibungslosen Geschäftsbetriebs und das Erreichen der Wiederherstellungspunktziele von entscheidender Bedeutung.

NetApp bietet eine äußerst anpassungsfähige 3-2-1-Strategie, die eine individuelle Kontrolle über Aufbewahrungspläne an den primären, sekundären und Objektspeicherstandorten ermöglicht. Diese Strategie bietet die Flexibilität, Datenschutzansätze an spezifische Anforderungen anzupassen.

Dieser Abschnitt bietet einen Überblick über den Datenwiederherstellungsprozess sowohl vom SnapCenter Plug-in for VMware vSphere als auch von BlueXP backup and recovery für virtuelle Maschinen.

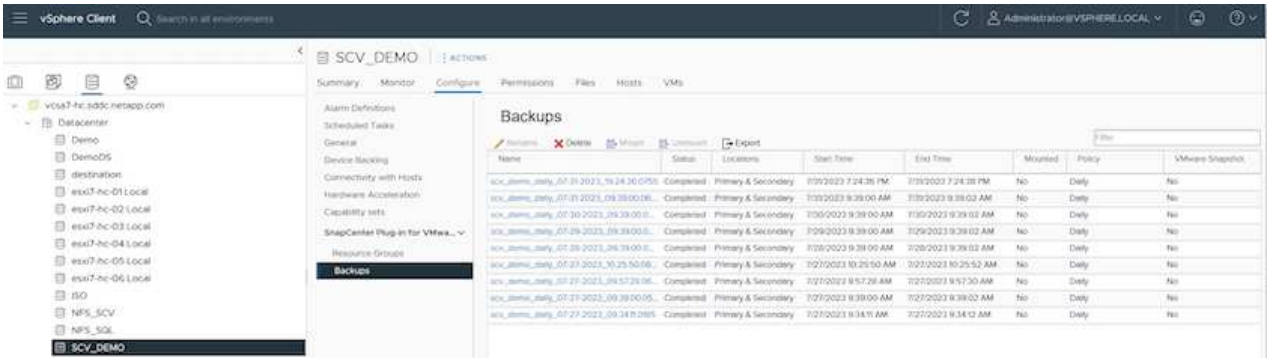
Wiederherstellen virtueller Maschinen vom SnapCenter Plug-in for VMware vSphere

Für diese Lösung wurden virtuelle Maschinen an ursprünglichen und alternativen Standorten wiederhergestellt. Diese Lösung deckt nicht alle Aspekte der Datenwiederherstellungsfunktionen von SCV ab. Ausführliche Informationen zu allen Angeboten von SCV finden Sie im "Wiederherstellen von VMs aus Backups" in der Produktdokumentation.

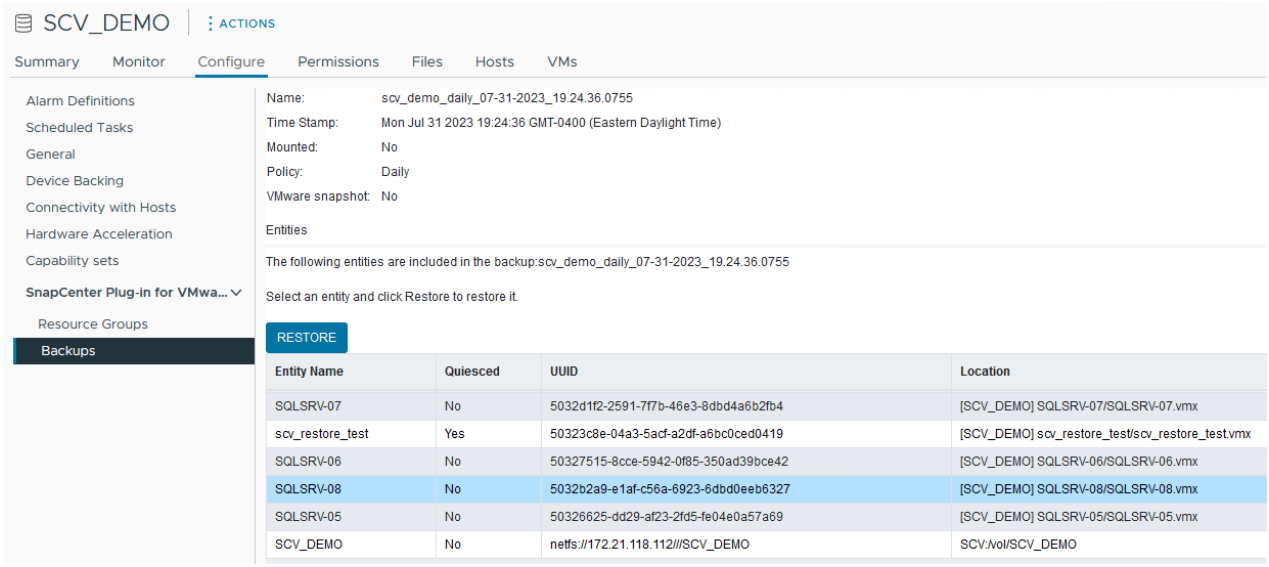
Wiederherstellen virtueller Maschinen aus SCV

Führen Sie die folgenden Schritte aus, um eine virtuelle Maschine vom primären oder sekundären Speicher wiederherzustellen.

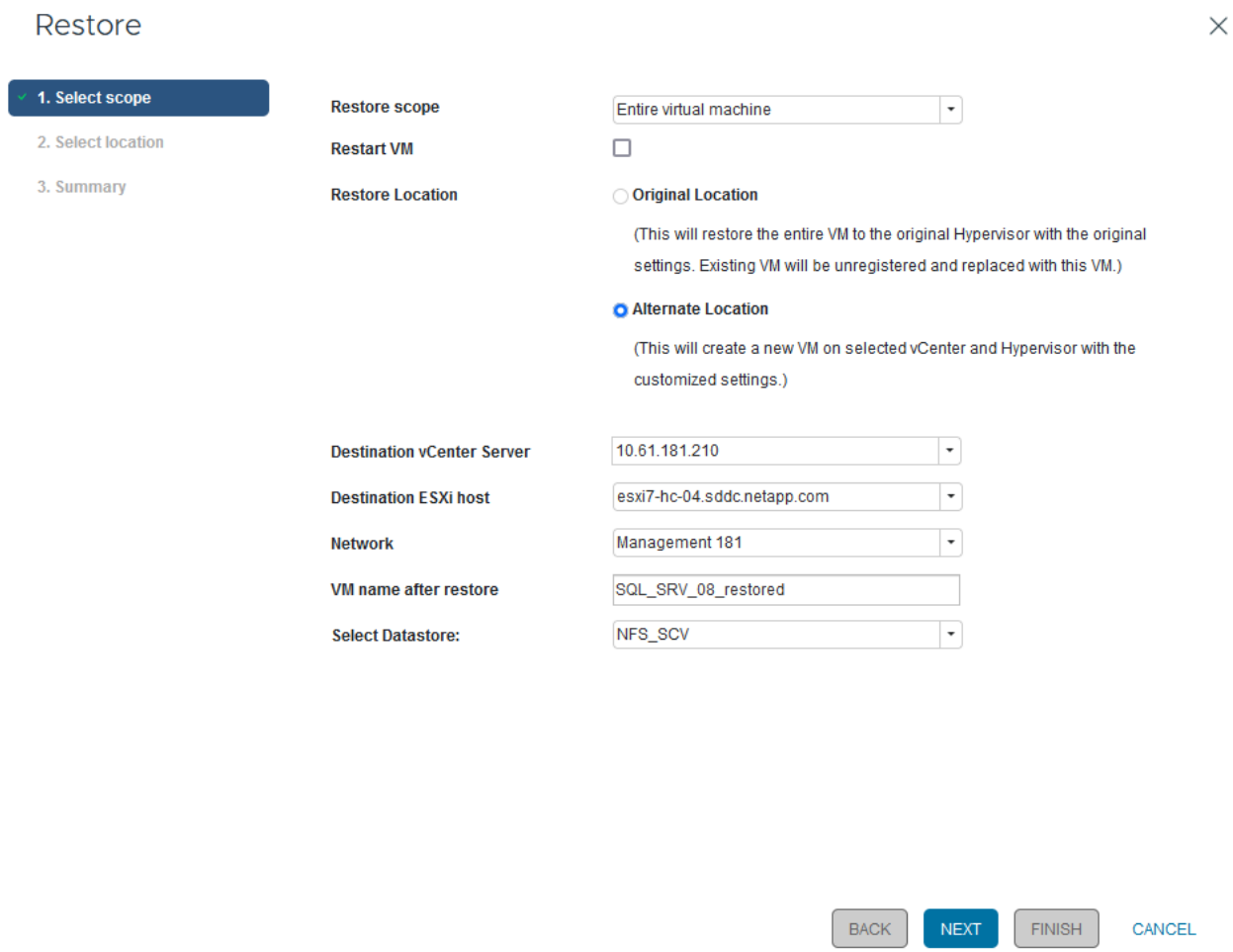
1. Navigieren Sie im vCenter-Client zu **Inventar > Speicher** und klicken Sie auf den Datenspeicher, der die virtuellen Maschinen enthält, die Sie wiederherstellen möchten.
2. Klicken Sie auf der Registerkarte **Konfigurieren** auf **Backups**, um auf die Liste der verfügbaren Backups zuzugreifen.



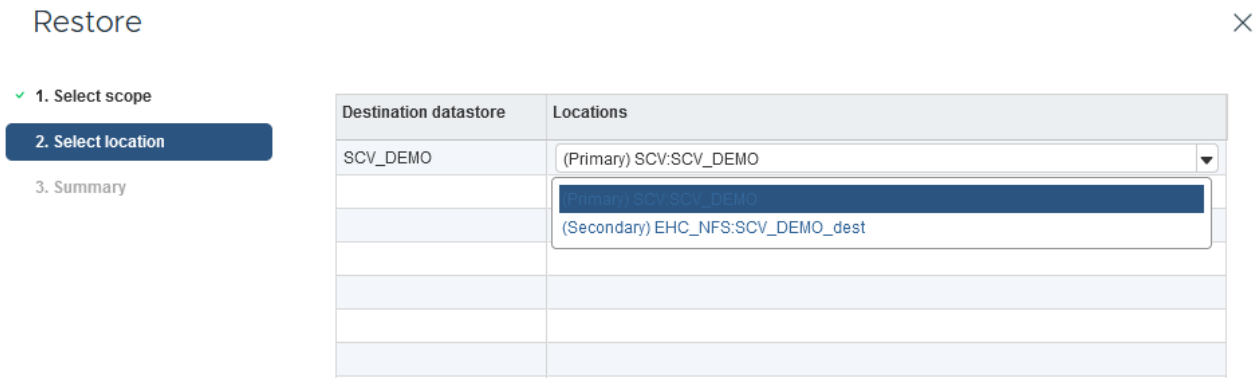
3. Klicken Sie auf eine Sicherung, um auf die Liste der VMs zuzugreifen, und wählen Sie dann eine VM zur Wiederherstellung aus. Klicken Sie auf **Wiederherstellen**.



4. Wählen Sie im Wiederherstellungsassistenten aus, ob die gesamte virtuelle Maschine oder ein bestimmtes VMDK wiederhergestellt werden soll. Wählen Sie die Installation am ursprünglichen oder alternativen Speicherort aus, geben Sie den VM-Namen nach der Wiederherstellung und den Zieldatenspeicher an. Klicken Sie auf **Weiter**.



5. Wählen Sie, ob Sie vom primären oder sekundären Speicherort sichern möchten.



6. Überprüfen Sie abschließend eine Zusammenfassung des Sicherungsauftrags und klicken Sie auf „Fertig stellen“, um den Wiederherstellungsvorgang zu starten.

Wiederherstellen virtueller Maschinen aus BlueXP backup and recovery für virtuelle Maschinen

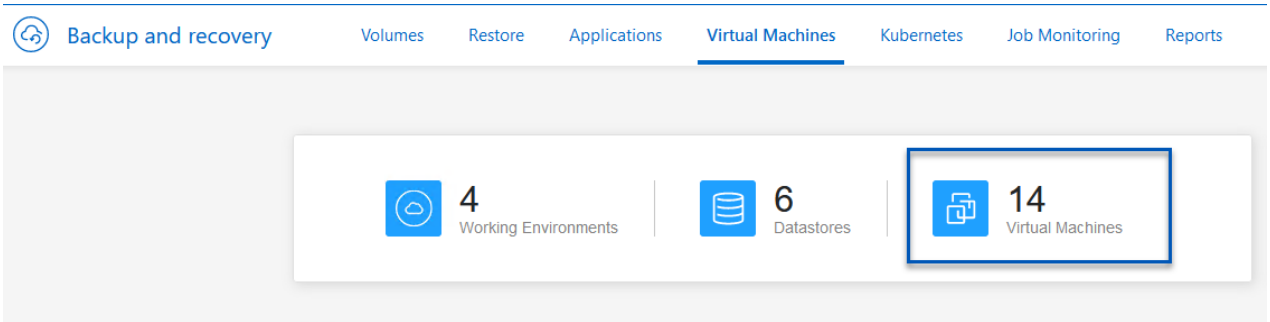
BlueXP backup and recovery für virtuelle Maschinen ermöglicht die Wiederherstellung virtueller Maschinen an ihrem ursprünglichen Speicherort. Der Zugriff auf die Wiederherstellungsfunktionen erfolgt über die BlueXP Webkonsole.

Weitere Informationen finden Sie unter "Wiederherstellen von Daten virtueller Maschinen aus der Cloud" .

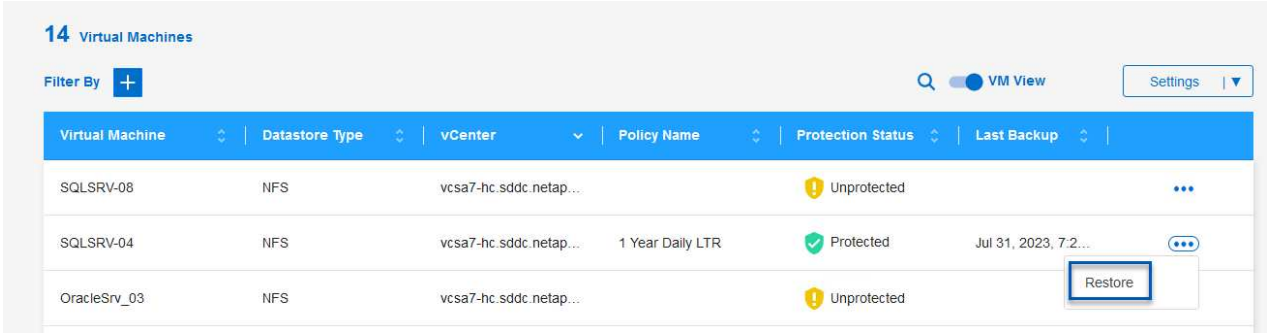
Wiederherstellen virtueller Maschinen aus BlueXP backup and recovery

Führen Sie die folgenden Schritte aus, um eine virtuelle Maschine aus BlueXP backup and recovery wiederherzustellen.

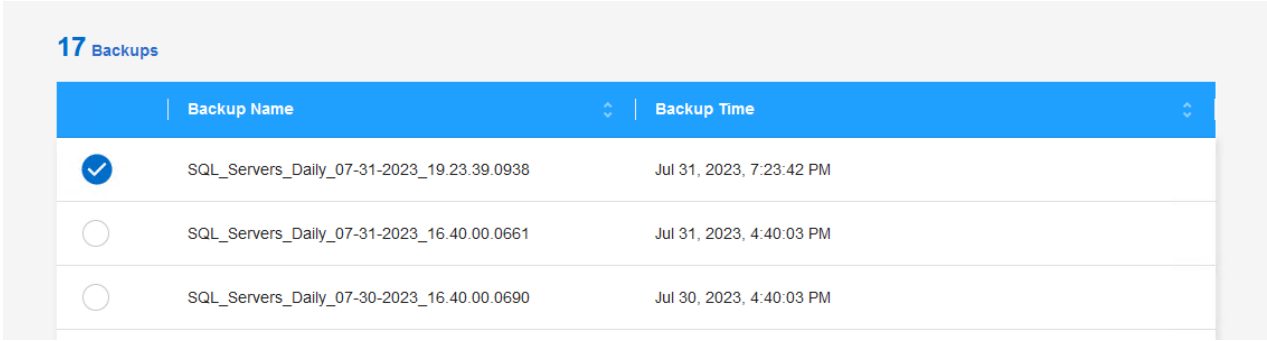
1. Navigieren Sie zu **Schutz > Sicherung und Wiederherstellung > Virtuelle Maschinen** und klicken Sie auf Virtuelle Maschinen, um die Liste der für die Wiederherstellung verfügbaren virtuellen Maschinen anzuzeigen.



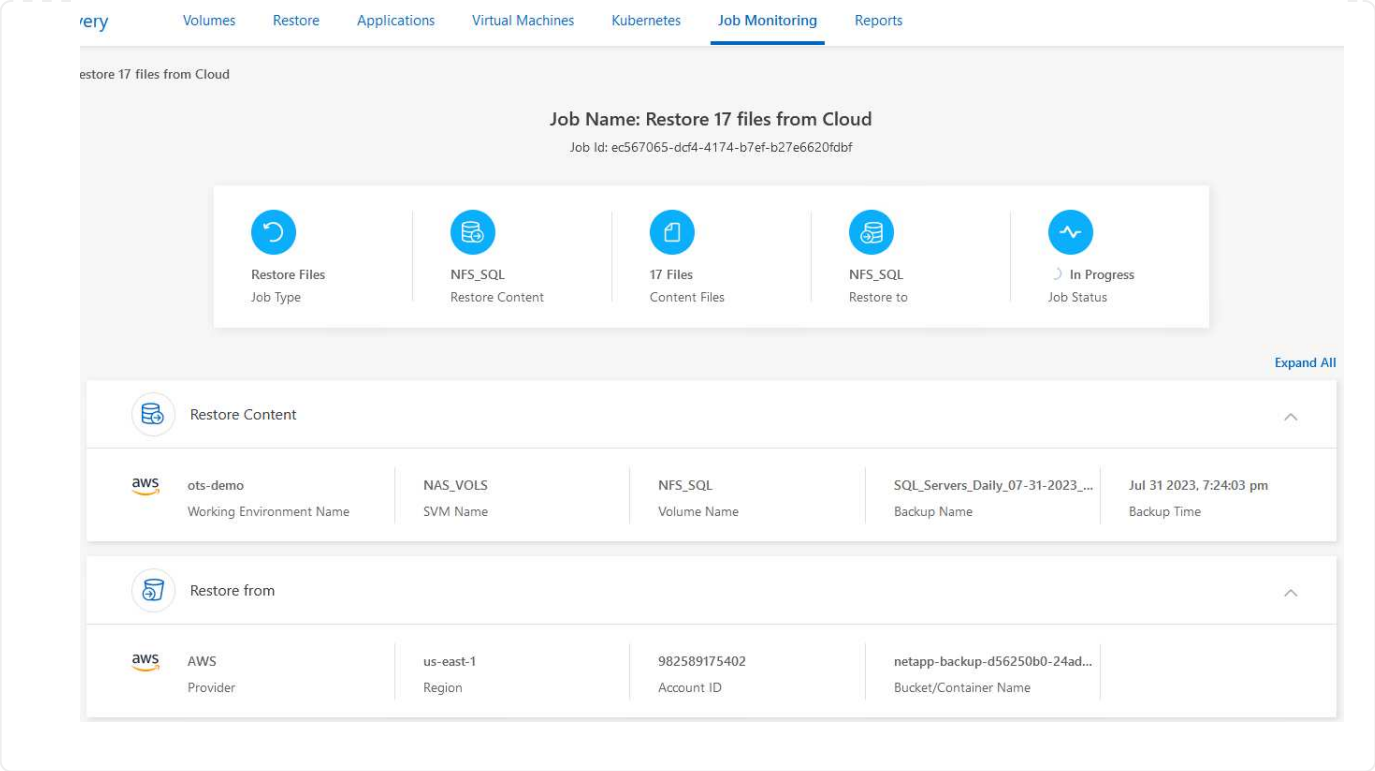
2. Rufen Sie das Dropdown-Menü „Einstellungen“ für die wiederherzustellende VM auf und wählen Sie



3. Wählen Sie das Backup aus, aus dem die Wiederherstellung erfolgen soll, und klicken Sie auf **Weiter**.



4. Überprüfen Sie eine Zusammenfassung des Sicherungsauftrags und klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.
5. Überwachen Sie den Fortschritt des Wiederherstellungsauftrags auf der Registerkarte **Auftragsüberwachung**.



Abschluss

Die 3-2-1-Sicherungsstrategie bietet in Kombination mit dem SnapCenter Plug-in for VMware vSphere und BlueXP backup and recovery für virtuelle Maschinen eine robuste, zuverlässige und kostengünstige Lösung für den Datenschutz. Diese Strategie gewährleistet nicht nur Datenredundanz und -zugänglichkeit, sondern bietet auch die Flexibilität, Daten von jedem Standort und sowohl von lokalen ONTAP Speichersystemen als auch von Cloud-basiertem Objektspeicher wiederherzustellen.

Der in dieser Dokumentation vorgestellte Anwendungsfall konzentriert sich auf bewährte Datenschutztechnologien, die die Integration zwischen NetApp, VMware und den führenden Cloud-Anbietern hervorheben. Das SnapCenter Plug-in for VMware vSphere bietet eine nahtlose Integration mit VMware vSphere und ermöglicht so eine effiziente und zentralisierte Verwaltung von Datenschutzvorgängen. Diese Integration optimiert die Sicherungs- und Wiederherstellungsprozesse für virtuelle Maschinen und ermöglicht eine einfache Planung, Überwachung und flexible Wiederherstellungsvorgänge innerhalb des VMware-Ökosystems. BlueXP backup and recovery für virtuelle Maschinen bietet die Eins (1) in 3-2-1, indem es sichere, Air-Gap-Backups von Daten virtueller Maschinen auf Cloud-basiertem Objektspeicher bereitstellt. Die intuitive Benutzeroberfläche und der logische Arbeitsablauf bieten eine sichere Plattform für die langfristige Archivierung kritischer Daten.

Weitere Informationen

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

- "SnapCenter Plug-in for VMware vSphere Dokumentation"
- "BlueXP -Dokumentation"

Einrichten der Notfallwiederherstellung für VMFS-Datenspeicher mit BlueXP disaster recovery

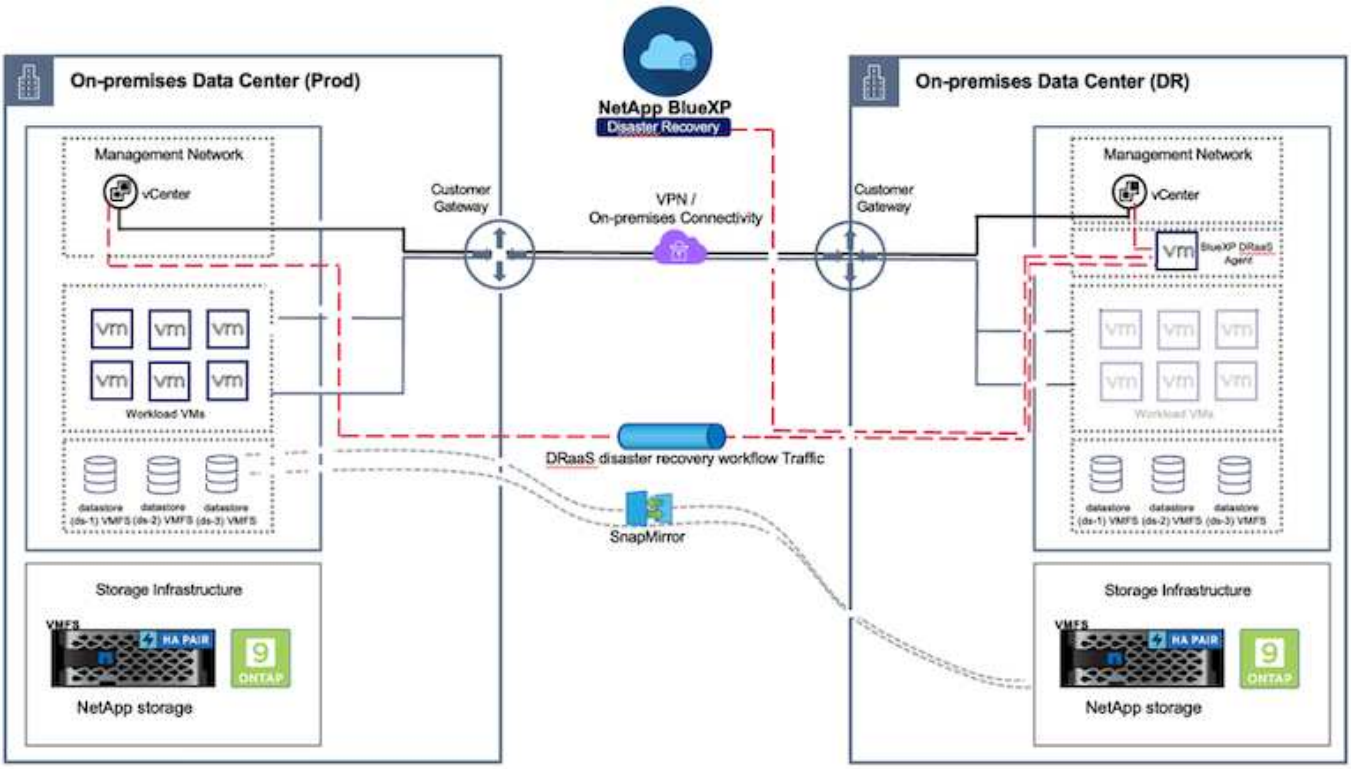
In diesem Anwendungsfall beschreiben wir das Verfahren zum Einrichten der Notfallwiederherstellung mit BlueXP disaster recovery für lokale VMware-VMs unter Verwendung von VMware Virtual Machine File System (VMFS)-Datenspeichern. Dieses Verfahren umfasst das Einrichten des BlueXP -Kontos und -Connectors, das Einrichten der SnapMirror Replikation zwischen ONTAP Systemen, die Integration mit VMware vCenter und die Automatisierung von Failover- und Failback-Vorgängen.

Die Notfallwiederherstellung mithilfe der Blockebenenreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware-Angriffen zu schützen. Mit der NetApp SnapMirror Replikation können VMware-Workloads, die auf lokalen ONTAP -Systemen mit VMFS-Datenspeicher ausgeführt werden, auf ein anderes ONTAP Speichersystem in einem dafür vorgesehenen Wiederherstellungs-Rechenzentrum repliziert werden, in dem sich VMware befindet.

Einführung

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zum Einrichten der Notfallwiederherstellung für lokale VMware-VMs an einem anderen bestimmten Standort beschrieben. Als Teil dieser Einrichtung werden das BlueXP -Konto, der BlueXP Connector und die ONTAP Arrays im BlueXP Arbeitsbereich hinzugefügt, die für die Kommunikation von VMware vCenter mit dem ONTAP Speicher erforderlich sind. Darüber hinaus wird in diesem Dokument detailliert beschrieben, wie die Replikation zwischen Standorten konfiguriert wird und wie ein Wiederherstellungsplan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Site-Failovers und zum Failback, wenn die primäre Site wiederhergestellt und online gestellt wurde.

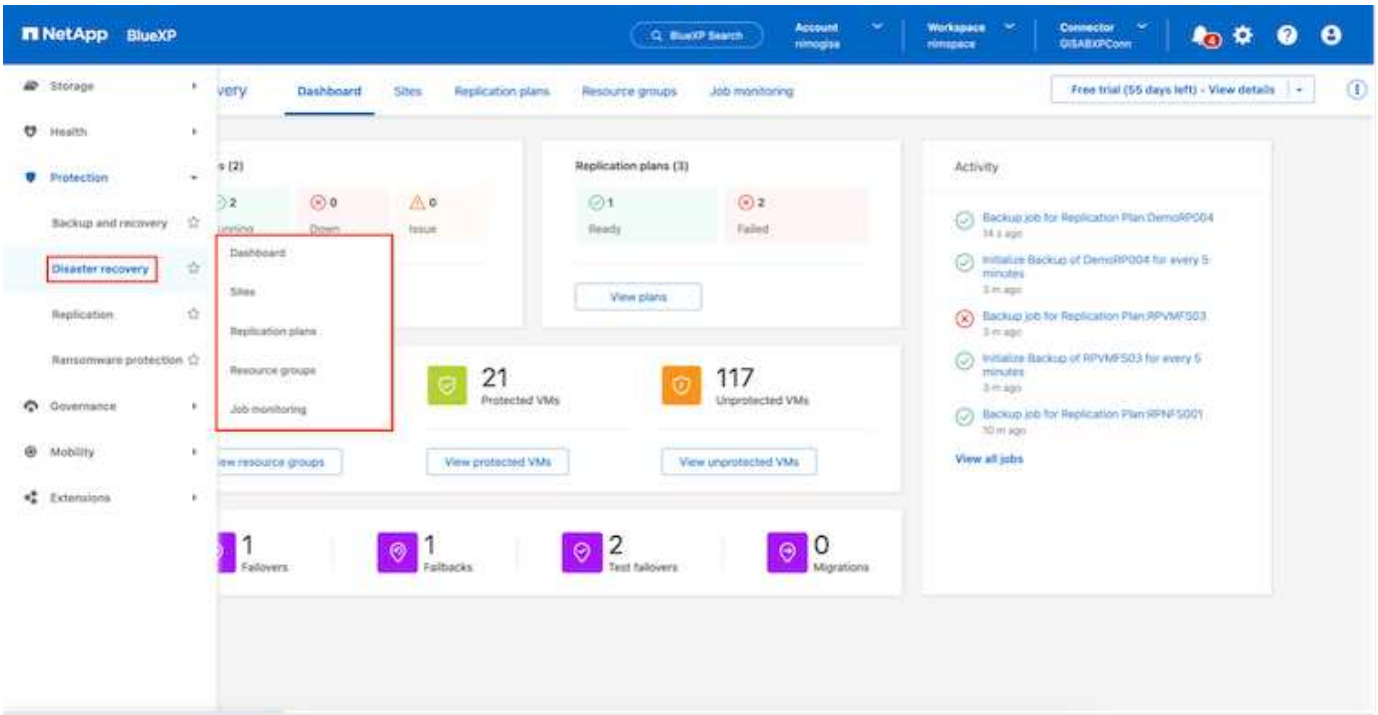
Mithilfe des BlueXP disaster recovery -Dienstes, der in die NetApp BlueXP Konsole integriert ist, können Kunden ihre lokalen VMware vCenter zusammen mit ONTAP Speicher ermitteln, Ressourcengruppierungen erstellen, einen Disaster-Recovery-Plan erstellen, ihn mit Ressourcengruppen verknüpfen und Failover und Failback testen oder ausführen. SnapMirror bietet Blockreplikation auf Speicherebene, um die beiden Sites mit inkrementellen Änderungen auf dem neuesten Stand zu halten, was zu einem RPO von bis zu 5 Minuten führt. Darüber hinaus ist es möglich, DR-Verfahren als reguläre Übung zu simulieren, ohne die Produktion und die replizierten Datenspeicher zu beeinträchtigen oder zusätzliche Speicherkosten zu verursachen. Die BlueXP disaster recovery nutzt die FlexClone -Technologie von ONTAP, um eine platzsparende Kopie des VMFS-Datenspeichers aus dem letzten replizierten Snapshot auf der DR-Site zu erstellen. Sobald der DR-Test abgeschlossen ist, können Kunden die Testumgebung einfach löschen, wiederum ohne Auswirkungen auf die tatsächlich replizierten Produktionsressourcen. Wenn ein tatsächlicher Failover (geplant oder ungeplant) erforderlich ist, orchestriert der BlueXP disaster recovery mit wenigen Klicks alle erforderlichen Schritte, um die geschützten virtuellen Maschinen automatisch am vorgesehenen Notfallwiederherstellungsstandort hochzufahren. Der Dienst kehrt außerdem die SnapMirror -Beziehung zum primären Standort um und repliziert bei Bedarf alle Änderungen vom sekundären zum primären Standort für einen Failback-Vorgang. All dies kann im Vergleich zu anderen bekannten Alternativen zu einem Bruchteil der Kosten erreicht werden.



Erste Schritte

Um mit der BlueXP disaster recovery zu beginnen, verwenden Sie die BlueXP -Konsole und greifen Sie dann auf den Dienst zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste von BlueXP „Schutz“ > „Notfallwiederherstellung“ aus.
3. Das BlueXP disaster recovery wird angezeigt.

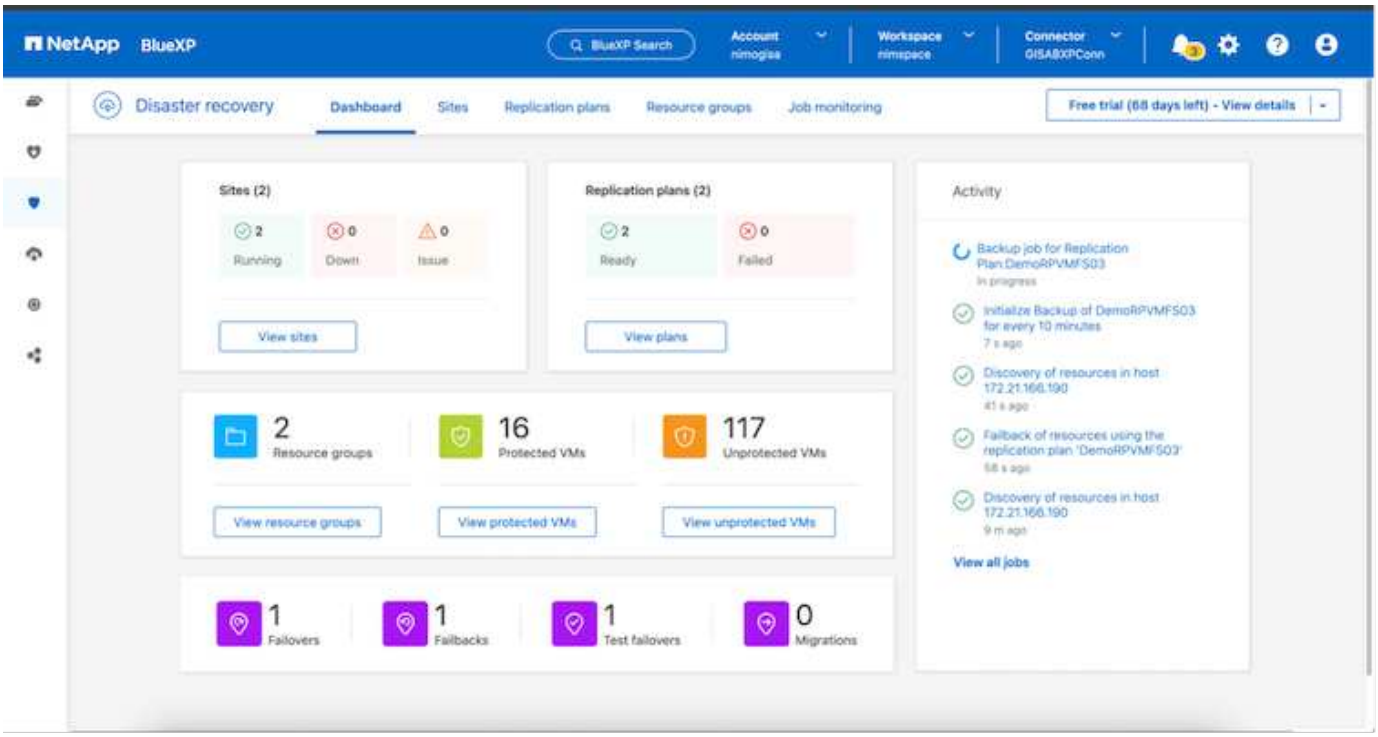


Stellen Sie vor der Konfiguration des Notfallwiederherstellungsplans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- BlueXP Connector wird in NetApp BlueXP eingerichtet. Der Connector sollte in AWS VPC bereitgestellt werden.
- Die BlueXP Connector-Instanz verfügt über eine Verbindung zum Quell- und Ziel-vCenter und den Speichersystemen.
- In BlueXP werden lokale NetApp -Speichersysteme hinzugefügt, die VMFS-Datenspeicher für VMware hosten.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen VMFS-basierten Datenspeichervolumes konfiguriert.

Sobald die Verbindung zwischen Quell- und Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte etwa 3 bis 5 Minuten dauern.

NetApp empfiehlt, den BlueXP Connector am Disaster-Recovery-Standort oder an einem dritten Standort bereitzustellen, damit der BlueXP Connector bei tatsächlichen Ausfällen oder Naturkatastrophen über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.

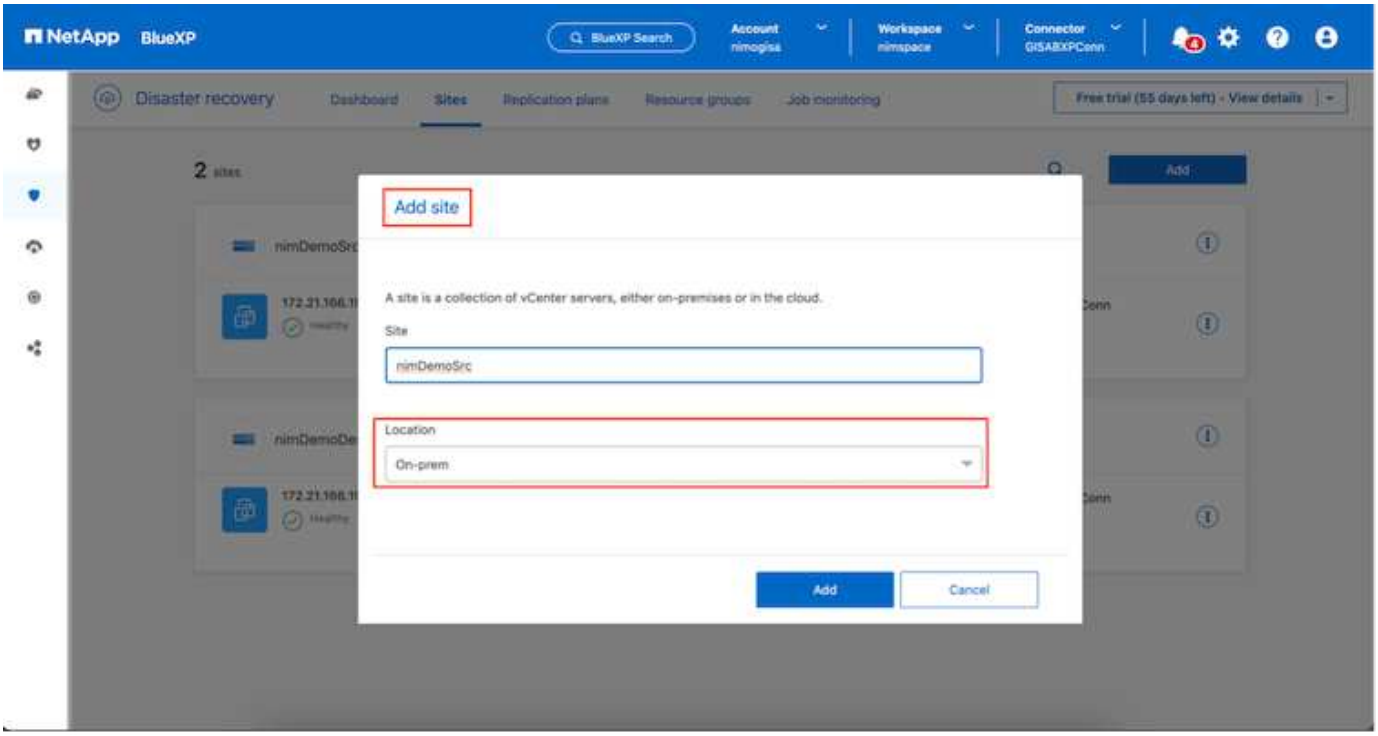


Die Unterstützung für lokale VMFS-Datenspeicher befindet sich beim Schreiben dieses Dokuments in der Technologievorschau. Die Funktion wird sowohl mit FC- als auch mit ISCSI-Protokoll-basierten VMFS-Datenspeichern unterstützt.

BlueXP disaster recovery

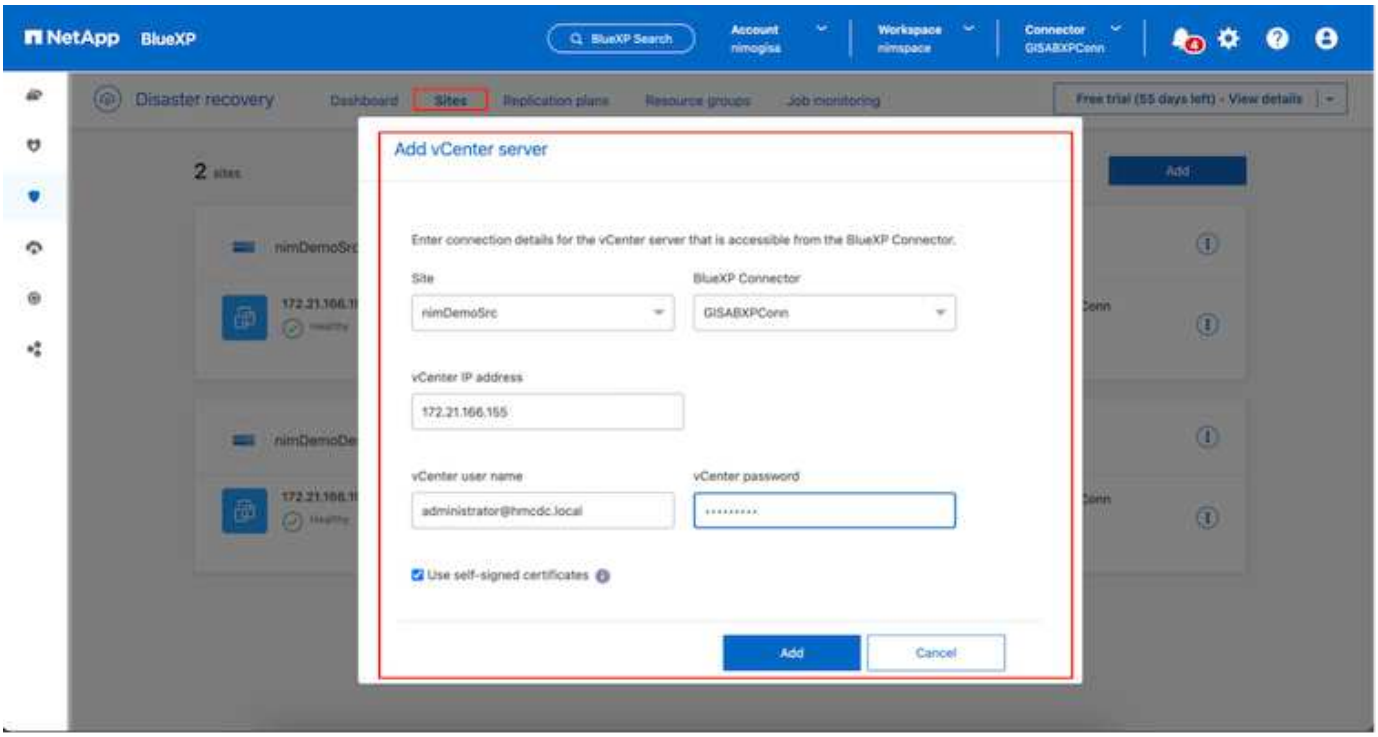
Der erste Schritt bei der Vorbereitung der Notfallwiederherstellung besteht darin, die lokalen vCenter- und Speicherressourcen zu ermitteln und zur BlueXP disaster recovery hinzuzufügen.

Stellen Sie sicher, dass die ONTAP Speichersysteme der Arbeitsumgebung innerhalb des Canvas hinzugefügt werden. Öffnen Sie die BlueXP -Konsole und wählen Sie in der linken Navigation **Schutz > Notfallwiederherstellung**. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü. Wählen Sie **Sites > Hinzufügen > vCenter hinzufügen**.

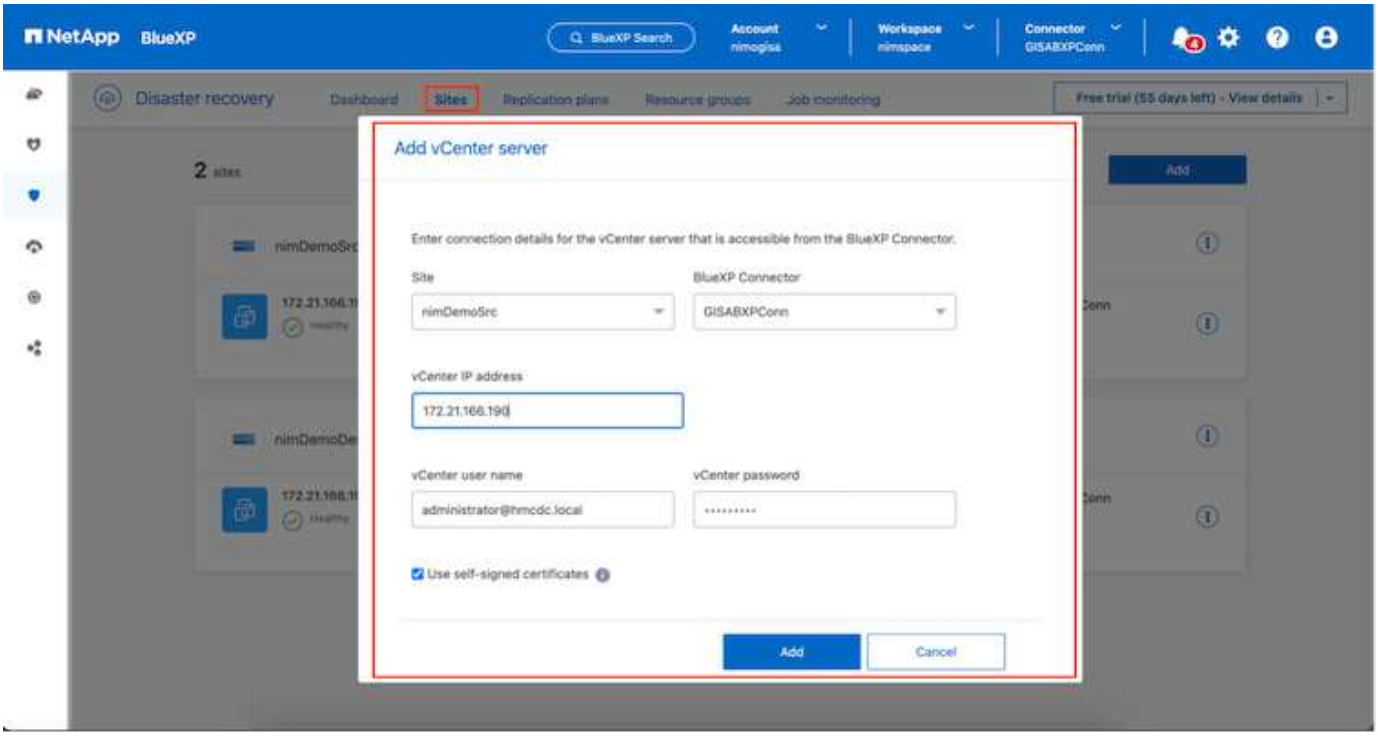


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle**. Lokales vCenter.



- **Ziel**. VMC SDDC vCenter.



Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort

SnapMirror nutzt ONTAP -Snapshots, um die Datenübertragung von einem Ort zum anderen zu verwalten. Zunächst wird eine vollständige Kopie basierend auf einem Snapshot des Quellvolumes auf das Ziel kopiert, um eine Basissynchronisierung durchzuführen. Wenn an der Quelle Datenänderungen auftreten, wird ein neuer Snapshot erstellt und mit dem Basis-Snapshot verglichen. Die Blöcke, bei denen Änderungen festgestellt wurden, werden dann zum Ziel repliziert, wobei der neuere Snapshot zur aktuellen Basislinie oder zum neuesten gemeinsamen Snapshot wird. Dadurch kann der Vorgang wiederholt und inkrementelle Updates an das Ziel gesendet werden.

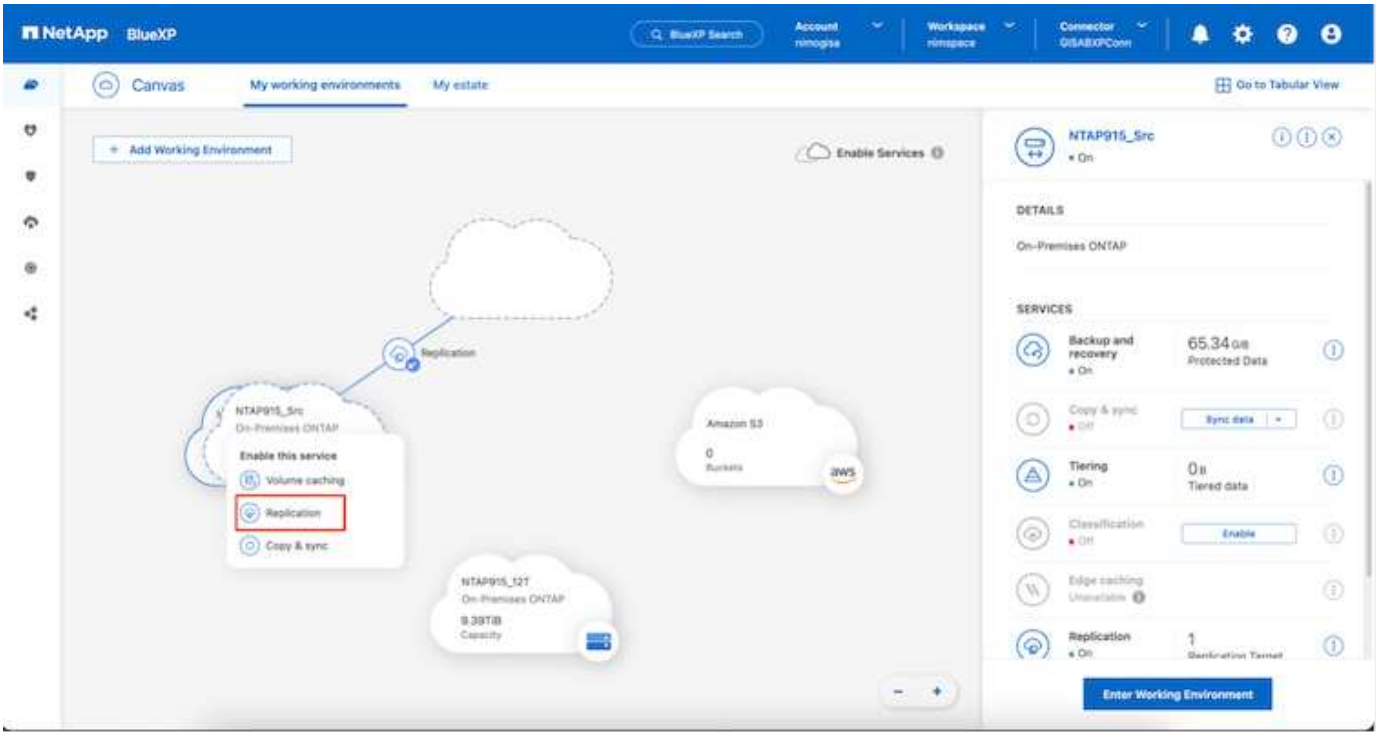
Wenn eine SnapMirror -Beziehung hergestellt wurde, befindet sich das Zielvolume in einem schreibgeschützten Online-Zustand und ist daher weiterhin zugänglich. SnapMirror arbeitet mit physischen Speicherblöcken und nicht auf Datei- oder anderer logischer Ebene. Dies bedeutet, dass das Zielvolume eine identische Replik des Quellvolumes ist, einschließlich Snapshots, Volumeeinstellungen usw. Wenn ONTAP Speicherplatzeffizienzfunktionen wie Datenkomprimierung und Datendeduplizierung vom Quellvolume verwendet werden, behält das replizierte Volume diese Optimierungen bei.

Durch das Aufheben der SnapMirror Beziehung wird das Zielvolume beschreibbar und wird normalerweise zum Durchführen eines Failovers verwendet, wenn SnapMirror zum Synchronisieren von Daten mit einer DR-Umgebung verwendet wird. SnapMirror ist so ausgereift, dass die am Failover-Standort geänderten Daten effizient mit dem primären System resynchronisiert werden können, falls dieses später wieder online geht. Anschließend kann die ursprüngliche SnapMirror Beziehung wiederhergestellt werden.

So richten Sie es für VMware Disaster Recovery ein

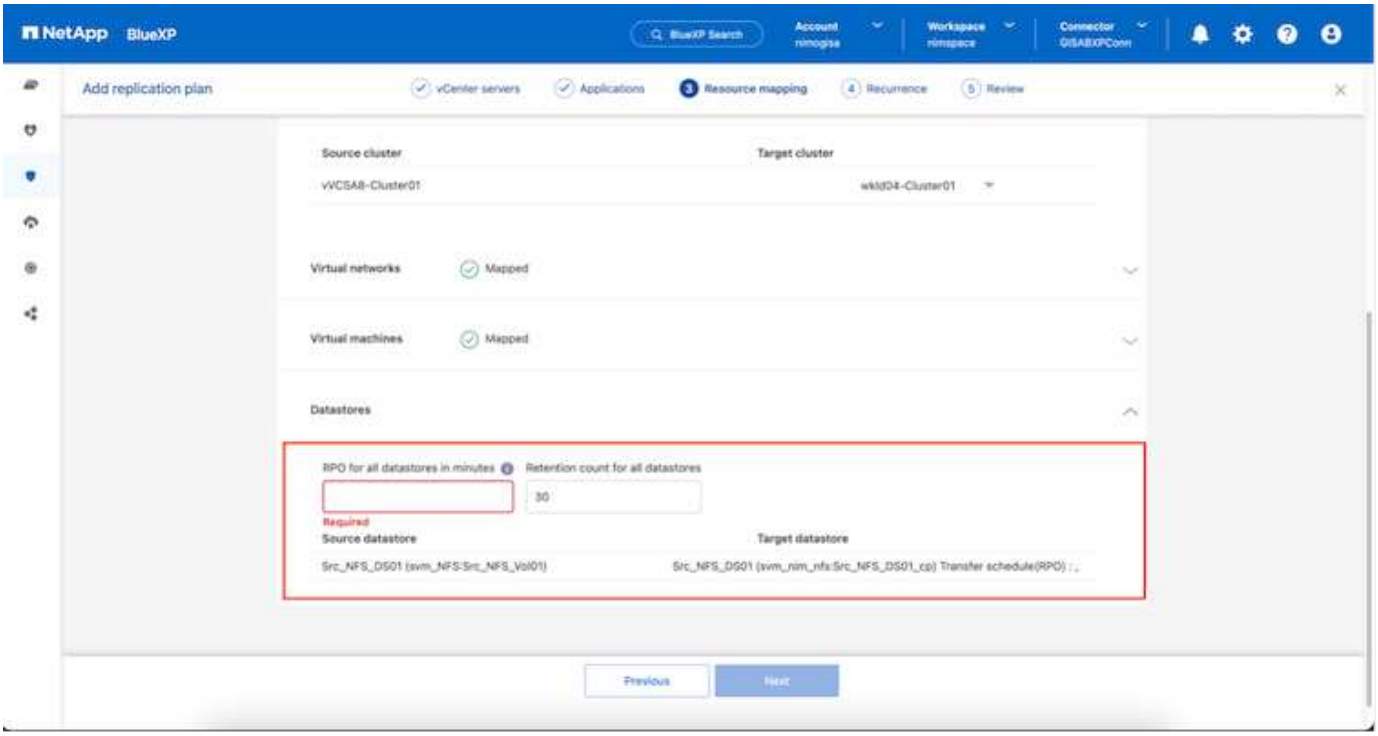
Der Vorgang zum Erstellen der SnapMirror Replikation bleibt für jede Anwendung derselbe. Der Vorgang kann manuell oder automatisiert erfolgen. Am einfachsten ist es, BlueXP zu nutzen, um die SnapMirror -Replikation zu konfigurieren. Dazu ziehen Sie das Quell ONTAP -System in der Umgebung einfach per Drag & Drop auf

das Ziel, um den Assistenten zu starten, der Sie durch den Rest des Prozesses führt.



BlueXP DRaaS kann dies auch automatisieren, sofern die folgenden beiden Kriterien erfüllt sind:

- Quell- und Zielcluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.

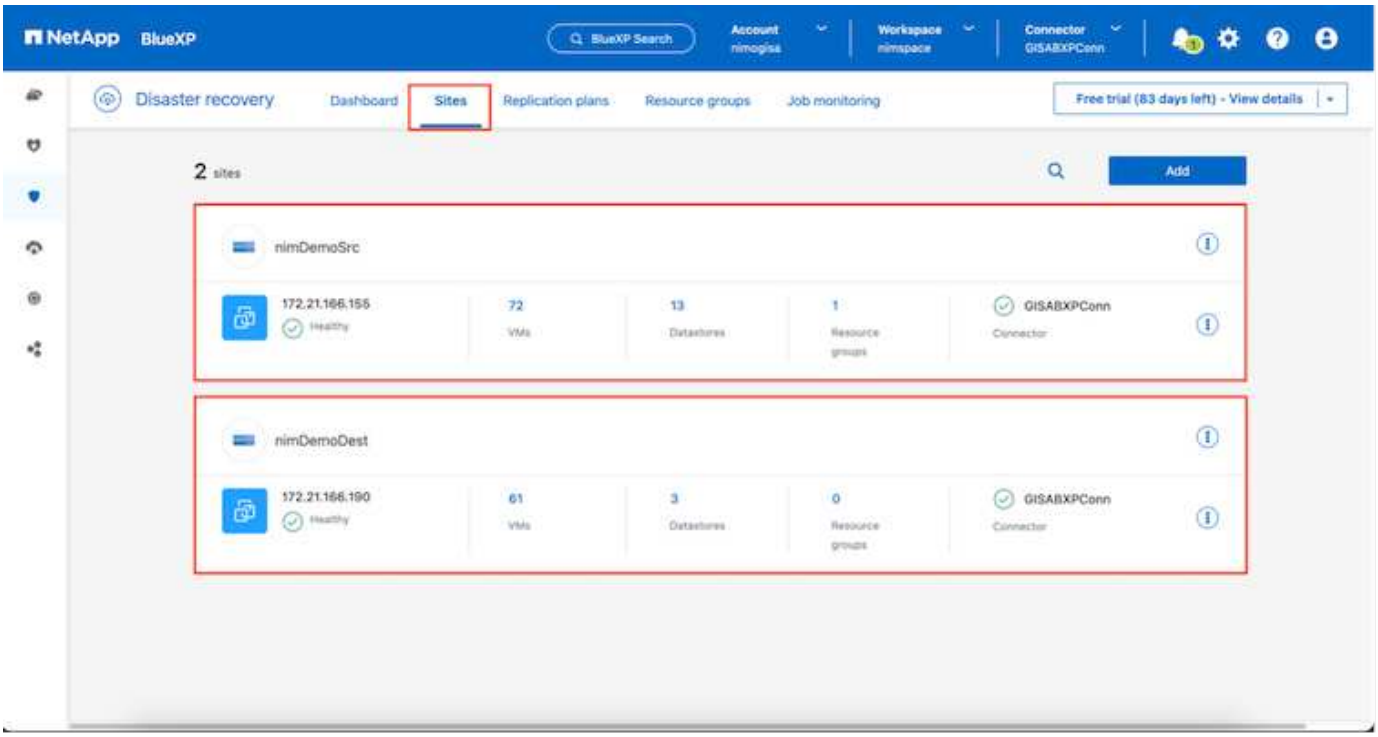


Wenn die SnapMirror -Beziehung für das Volume bereits über die CLI konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.

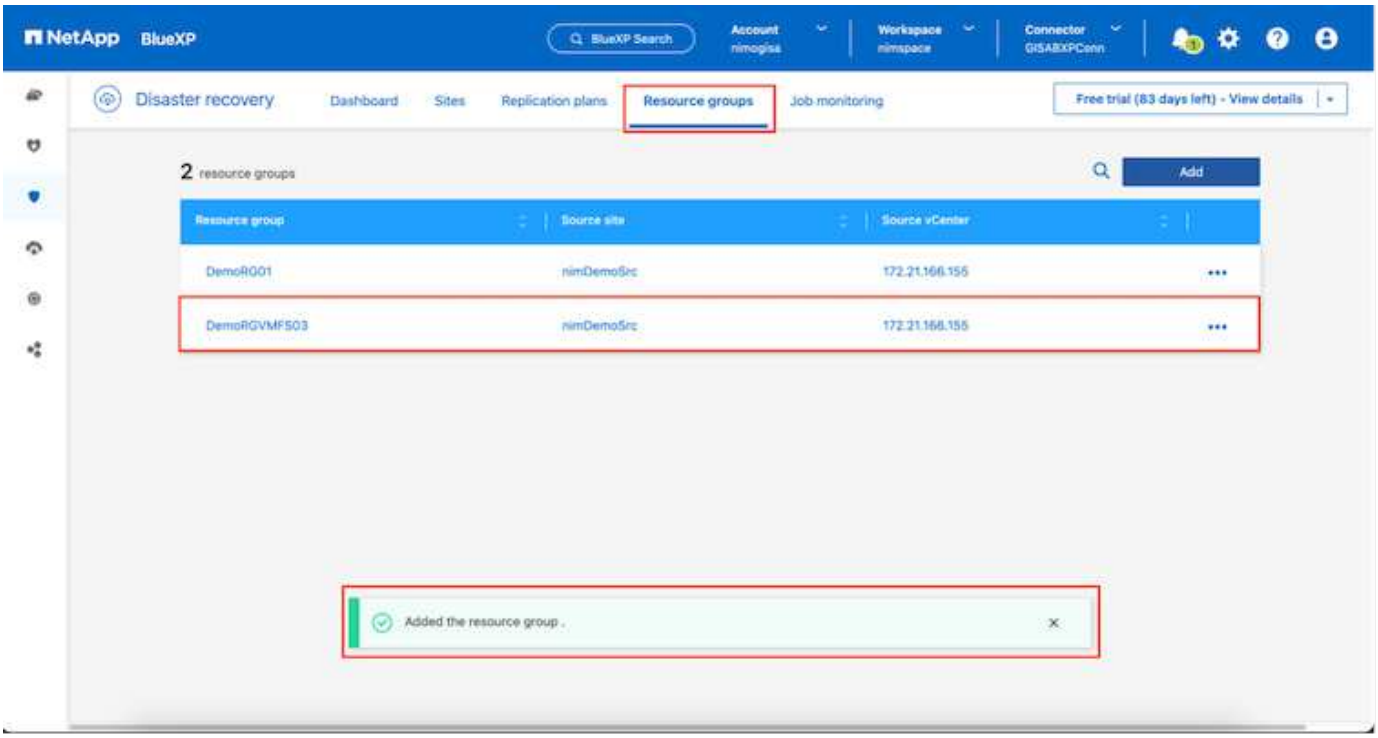
Abgesehen von den oben genannten Ansätzen kann die SnapMirror Replikation auch über ONTAP CLI oder System Manager erstellt werden. Unabhängig vom Ansatz, der zum Synchronisieren der Daten mit SnapMirror verwendet wird, orchestriert BlueXP DRaaS den Workflow für nahtlose und effiziente Disaster-Recovery-Vorgänge.

Was kann BlueXP disaster recovery für Sie tun?

Nachdem die Quell- und Zielsites hinzugefügt wurden, führt die BlueXP disaster recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Die BlueXP disaster recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.

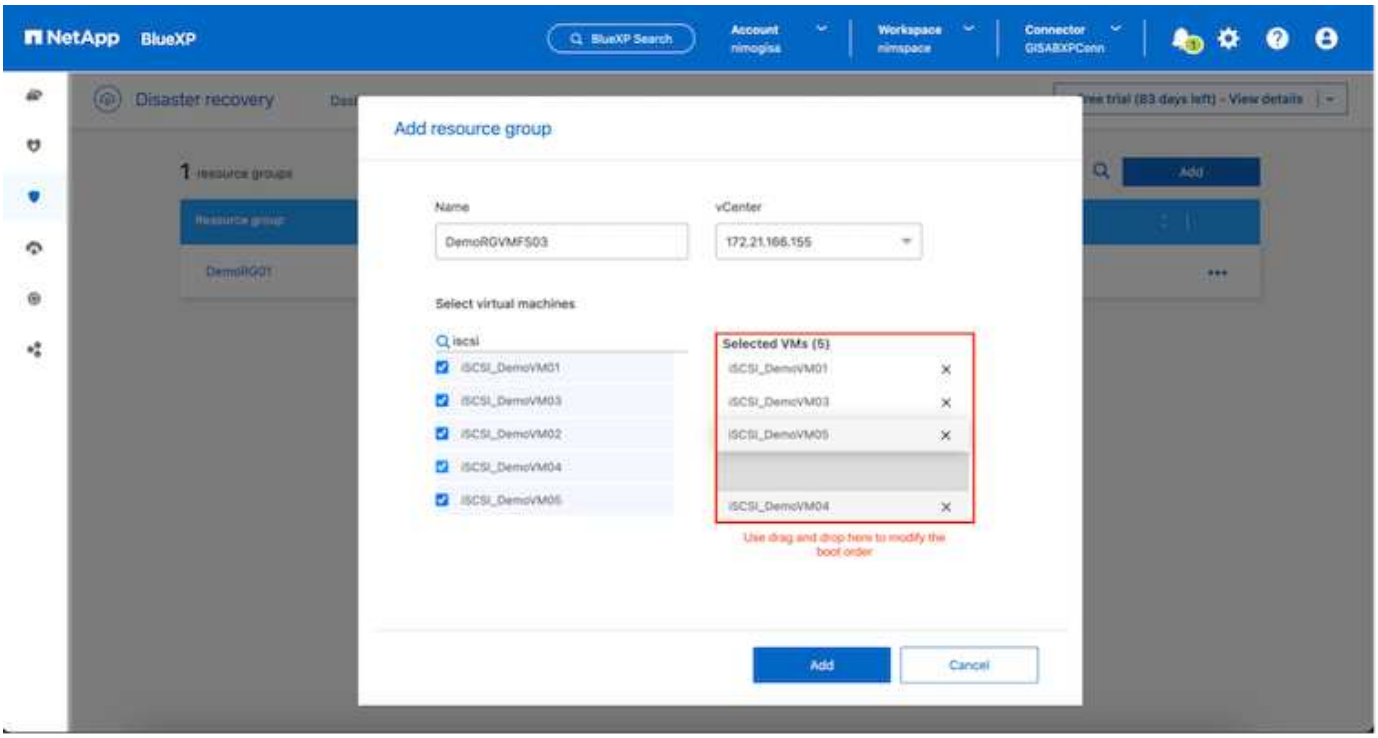


Nachdem die Sites hinzugefügt wurden, können VMs in Ressourcengruppen gruppiert werden. Mit den BlueXP disaster recovery können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen und Startverzögerungen enthalten, die bei der Wiederherstellung ausgeführt werden können. Um mit der Erstellung von Ressourcengruppen zu beginnen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.



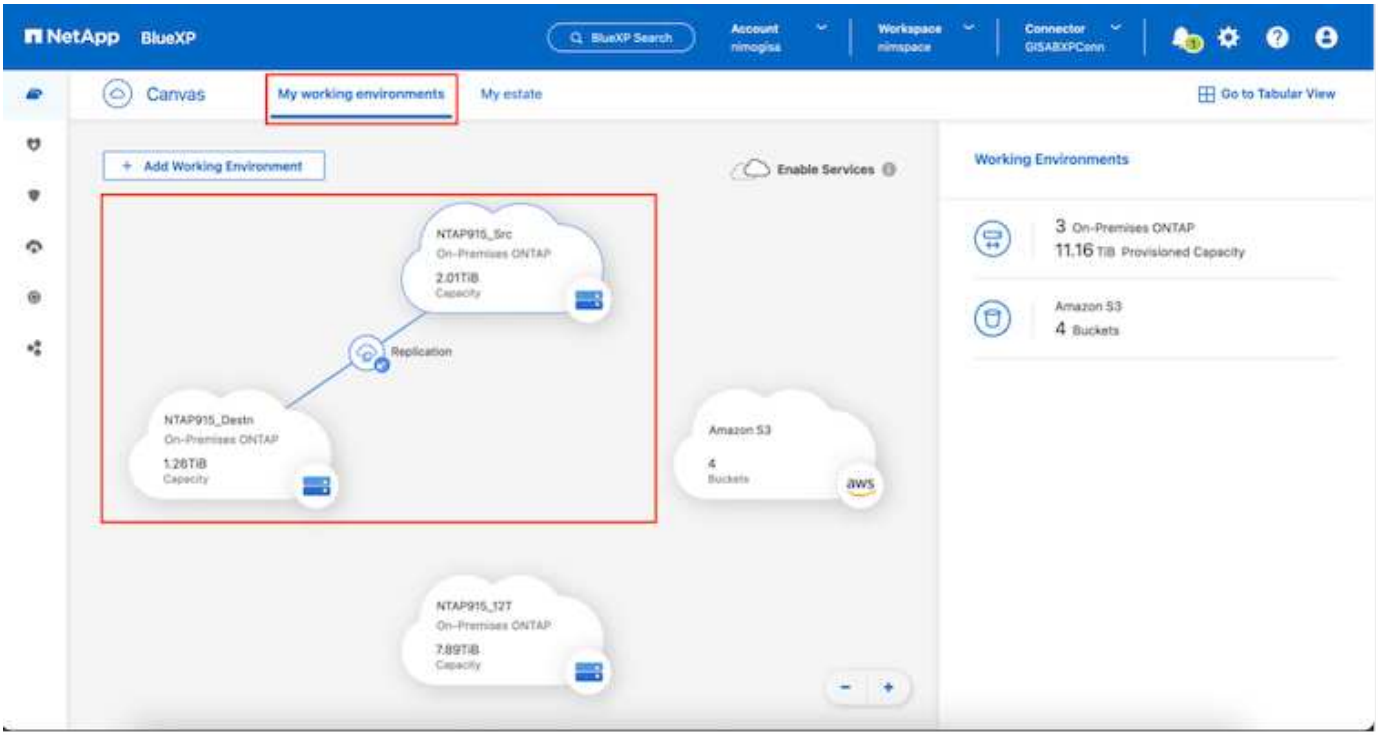
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

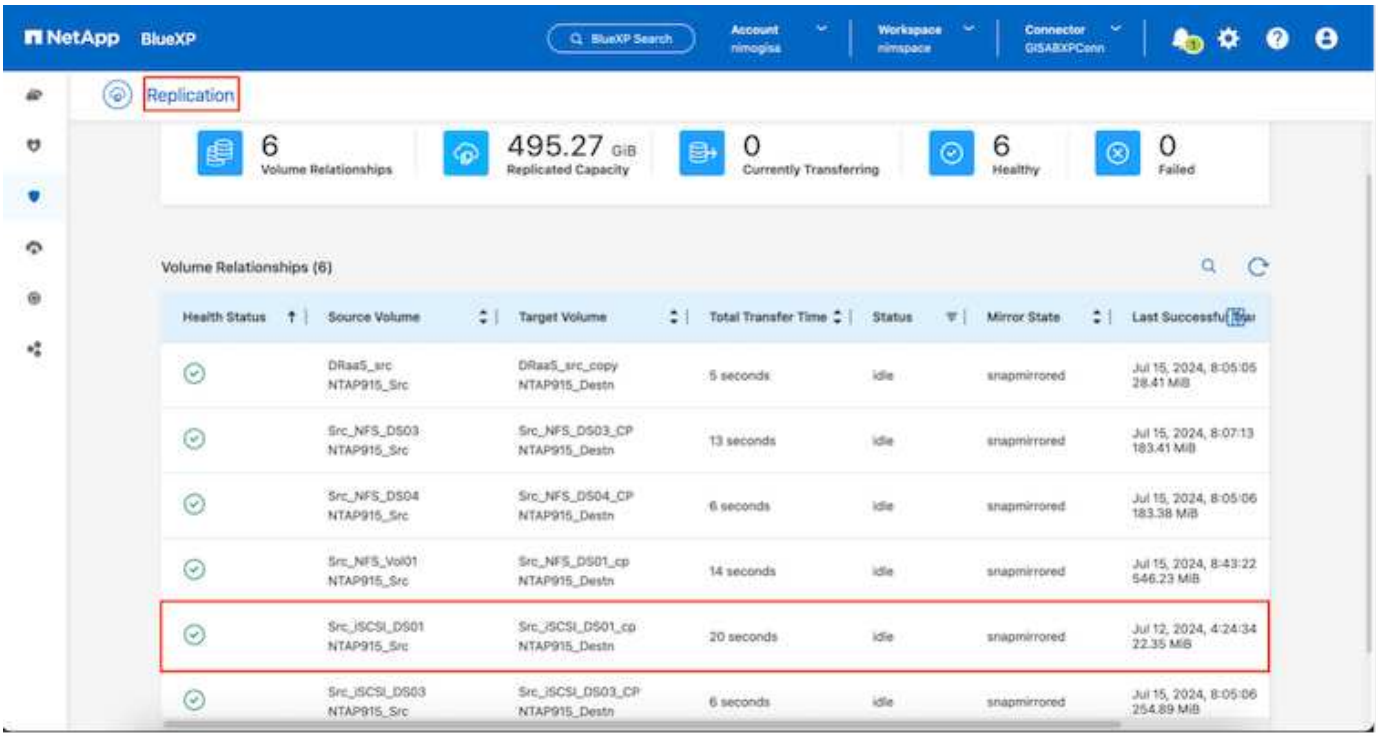
Die Startreihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen Drag-and-Drop-Mechanismus definiert oder geändert werden.



Sobald die Ressourcengruppen erstellt sind, besteht der nächste Schritt darin, den Ausführungsentwurf oder einen Plan zur Wiederherstellung virtueller Maschinen und Anwendungen im Katastrophenfall zu erstellen. Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des

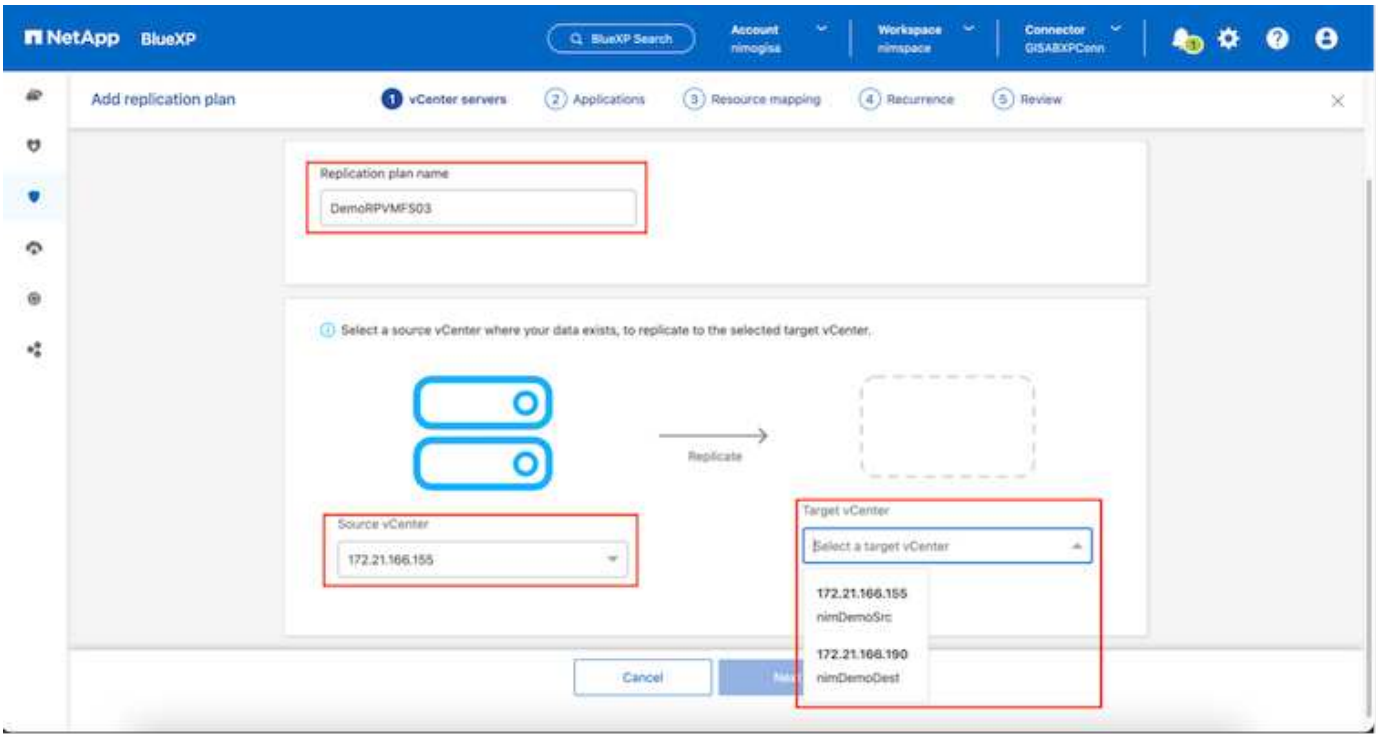
Replikationsplans angegeben wurden.



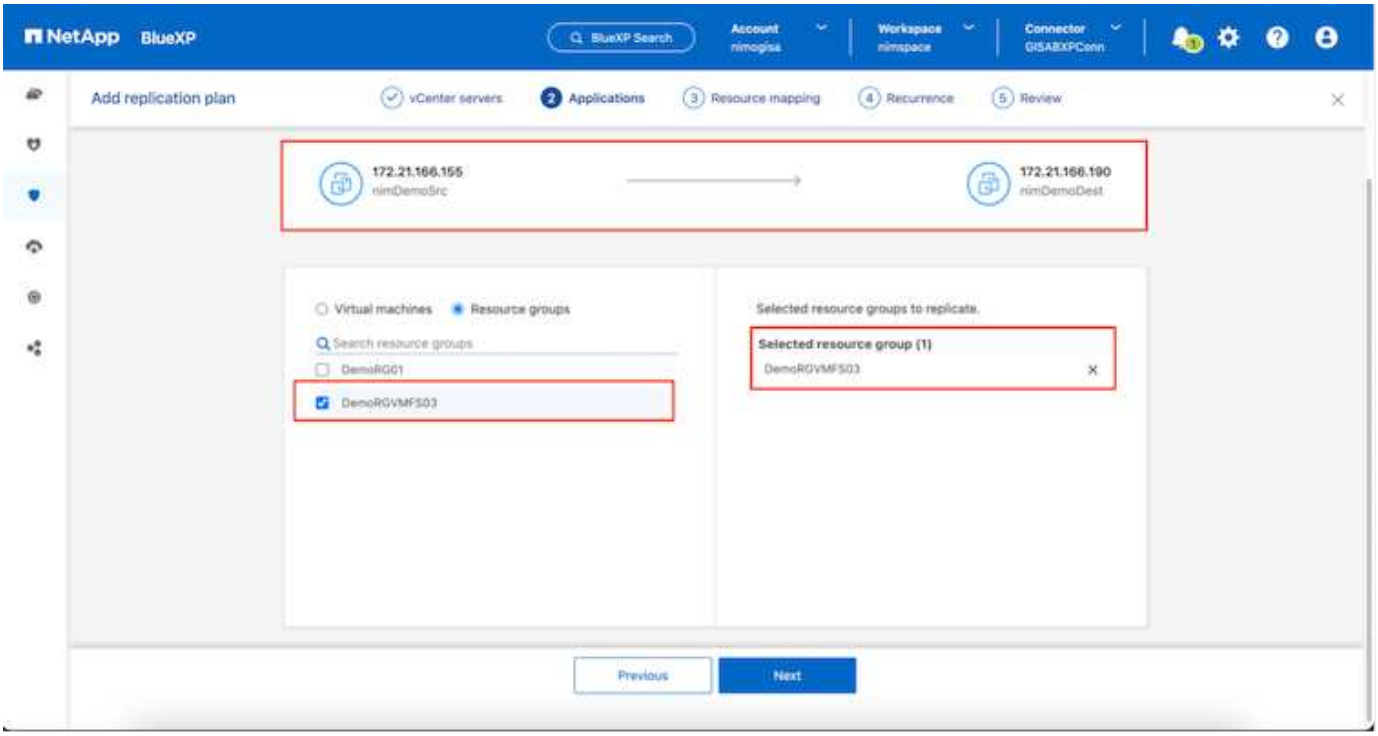


Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

Wählen Sie zuerst das Quell-vCenter und dann das Ziel-vCenter aus.



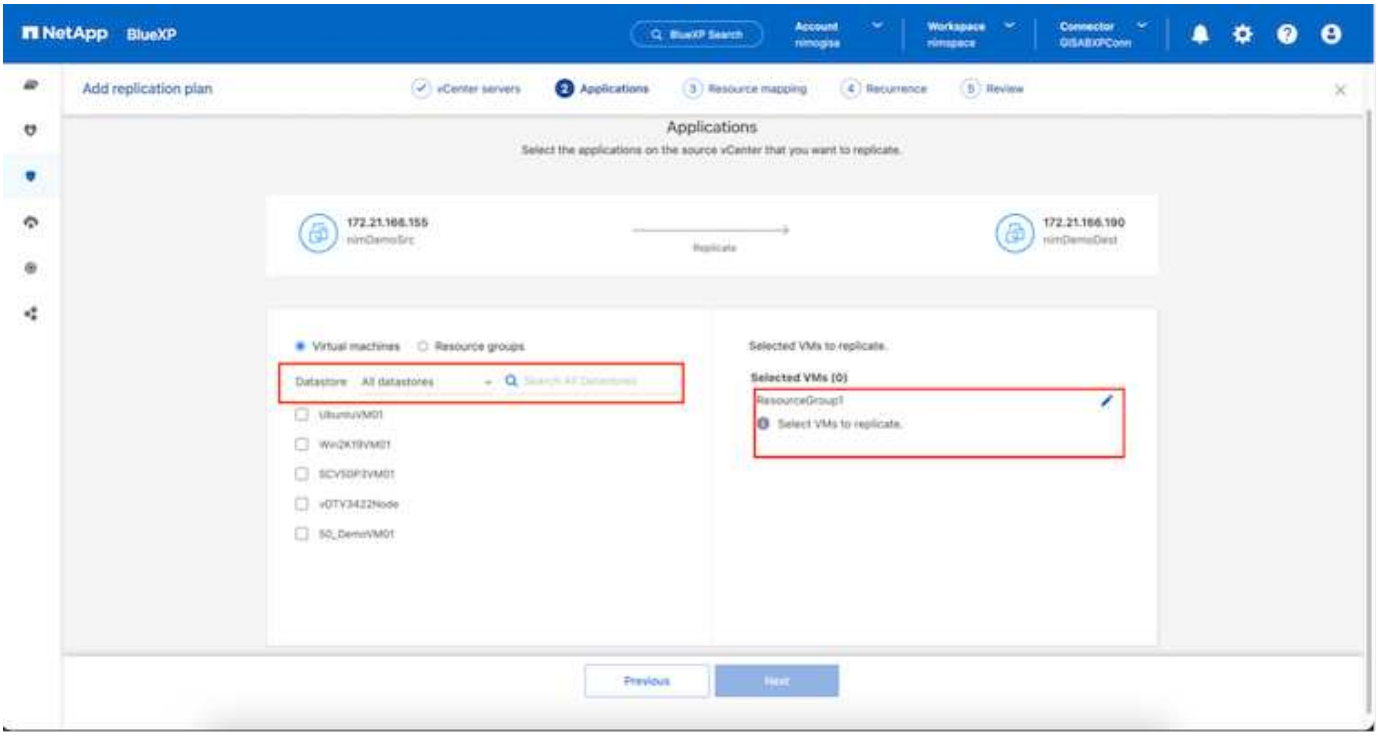
Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.



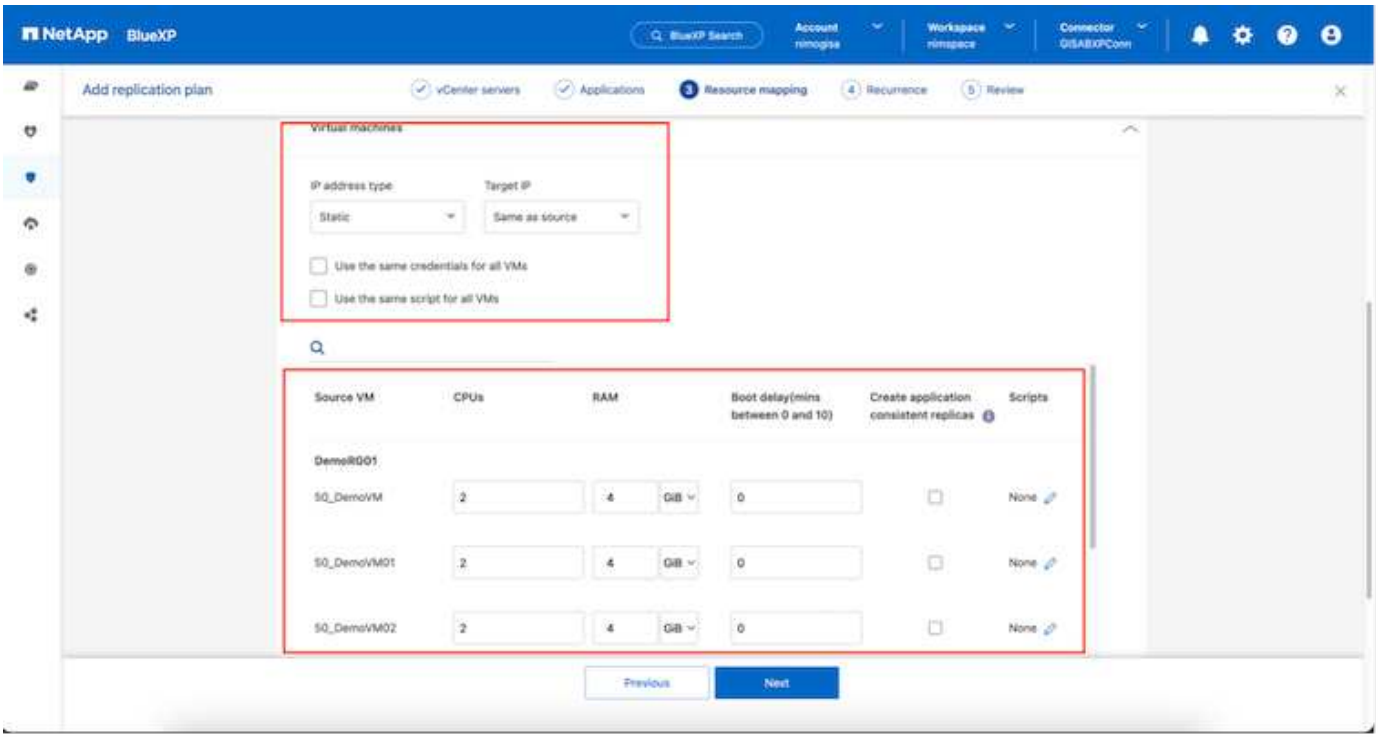
Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

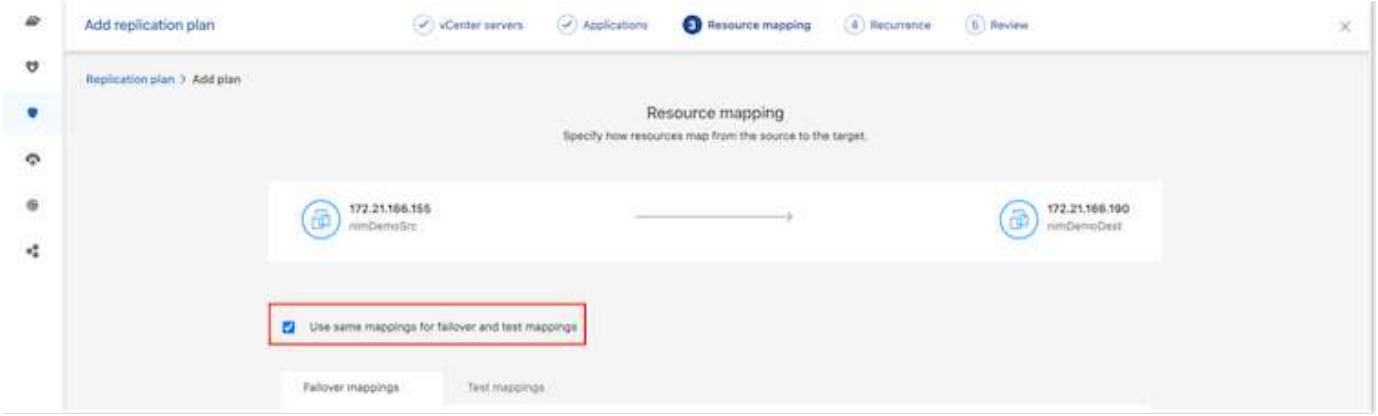
Der folgende Screenshot zeigt die Option zum Filtern virtueller Maschinen oder bestimmter Datenspeicher basierend auf organisatorischen Anforderungen, wenn nicht zuvor Ressourcengruppen erstellt wurden.



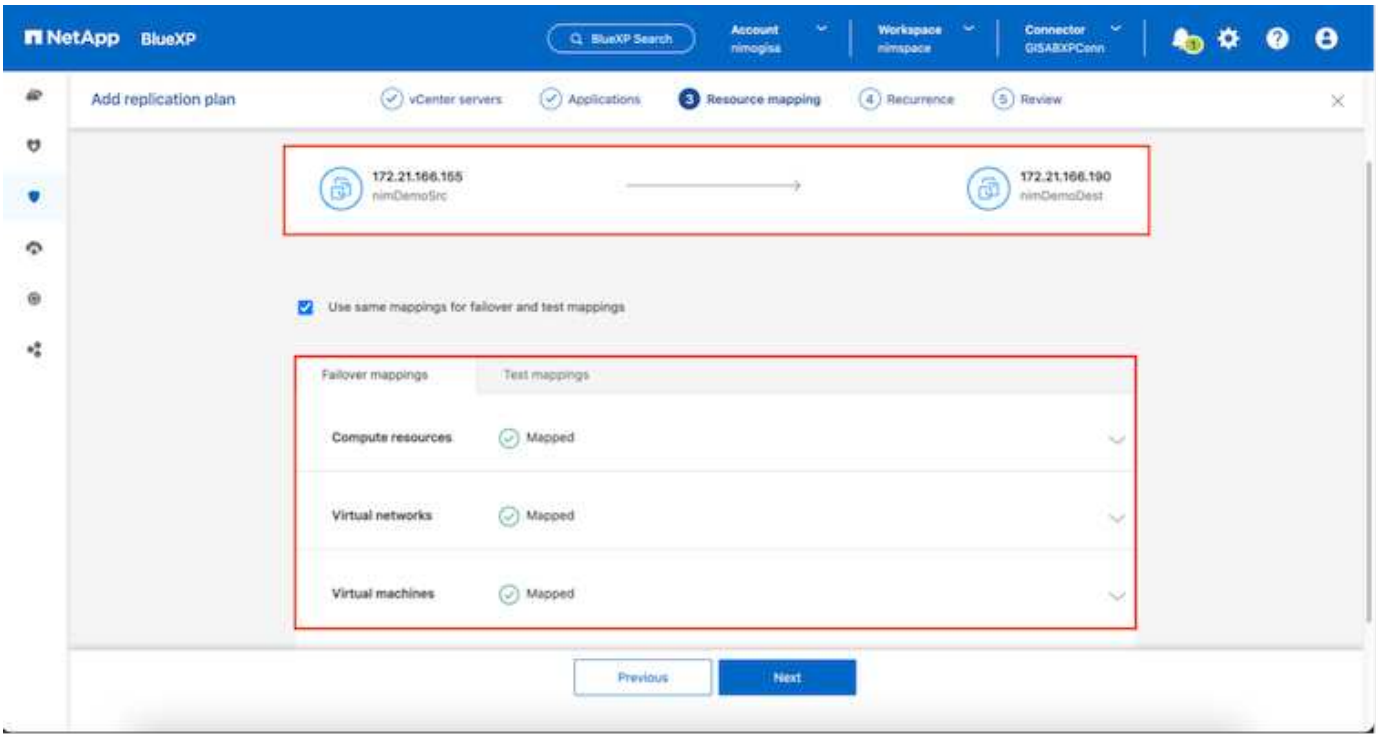
Sobald die Ressourcengruppen ausgewählt sind, erstellen Sie die Failover-Zuordnungen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen und virtuelle Netzwerke. IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Anwendungskonsistenz und so weiter. Ausführliche Informationen finden Sie unter"Erstellen eines Replikationsplans" .



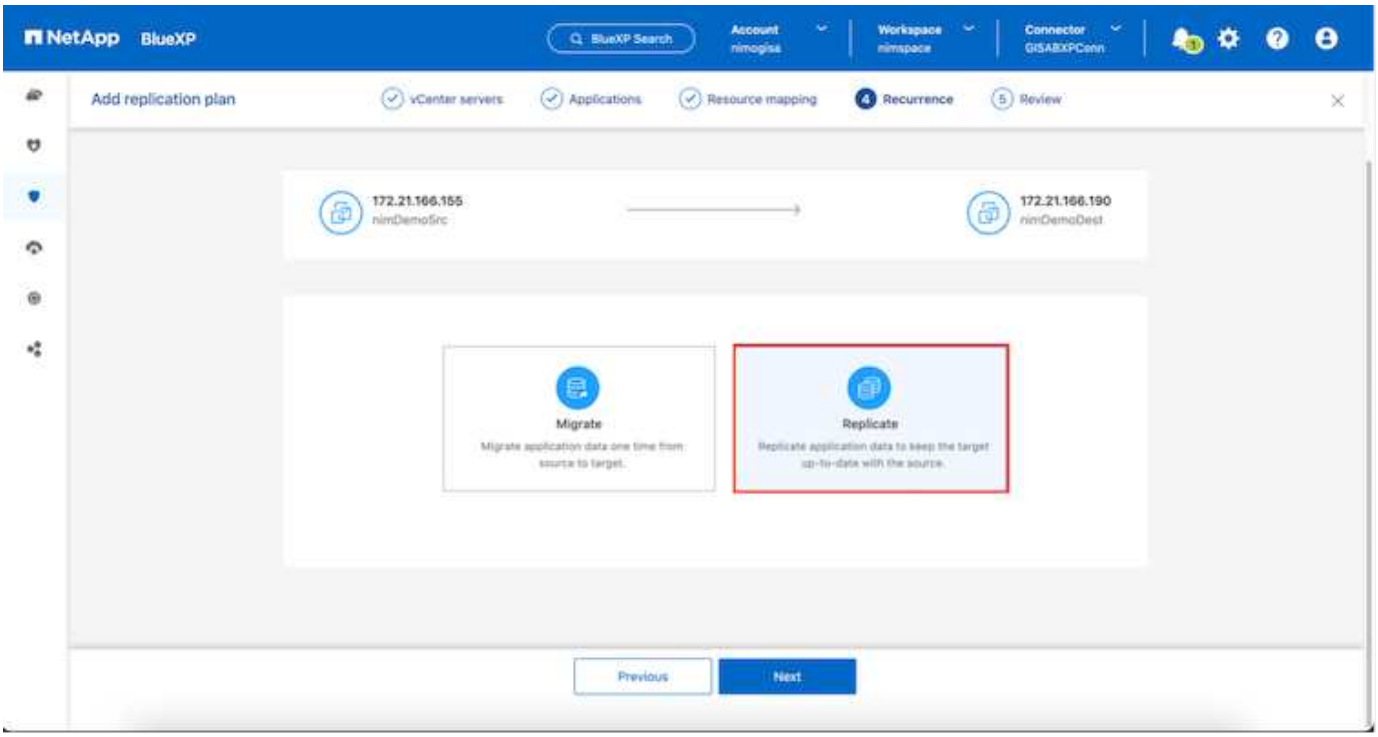
Standardmäßig werden für Test- und Failovervorgänge dieselben Zuordnungsparameter verwendet. Um verschiedene Zuordnungen für die Testumgebung anzuwenden, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:



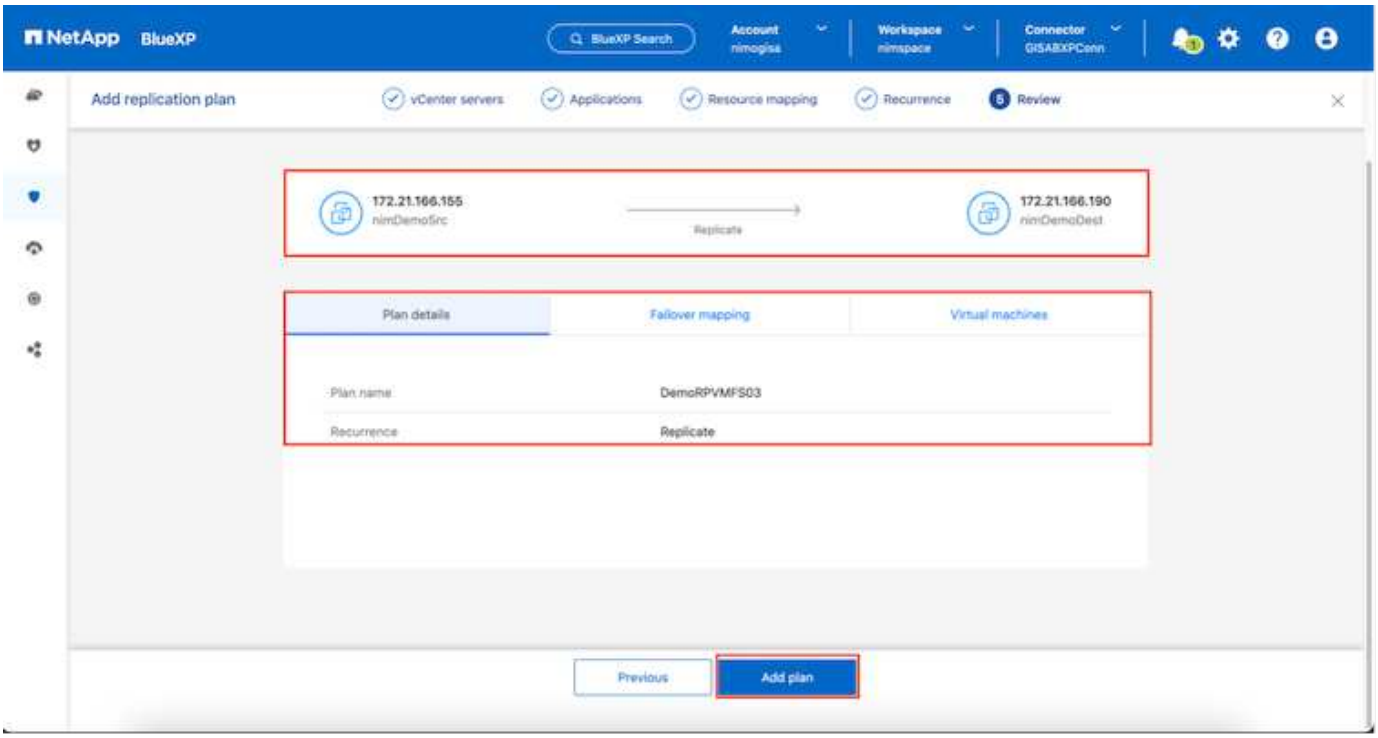
Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.

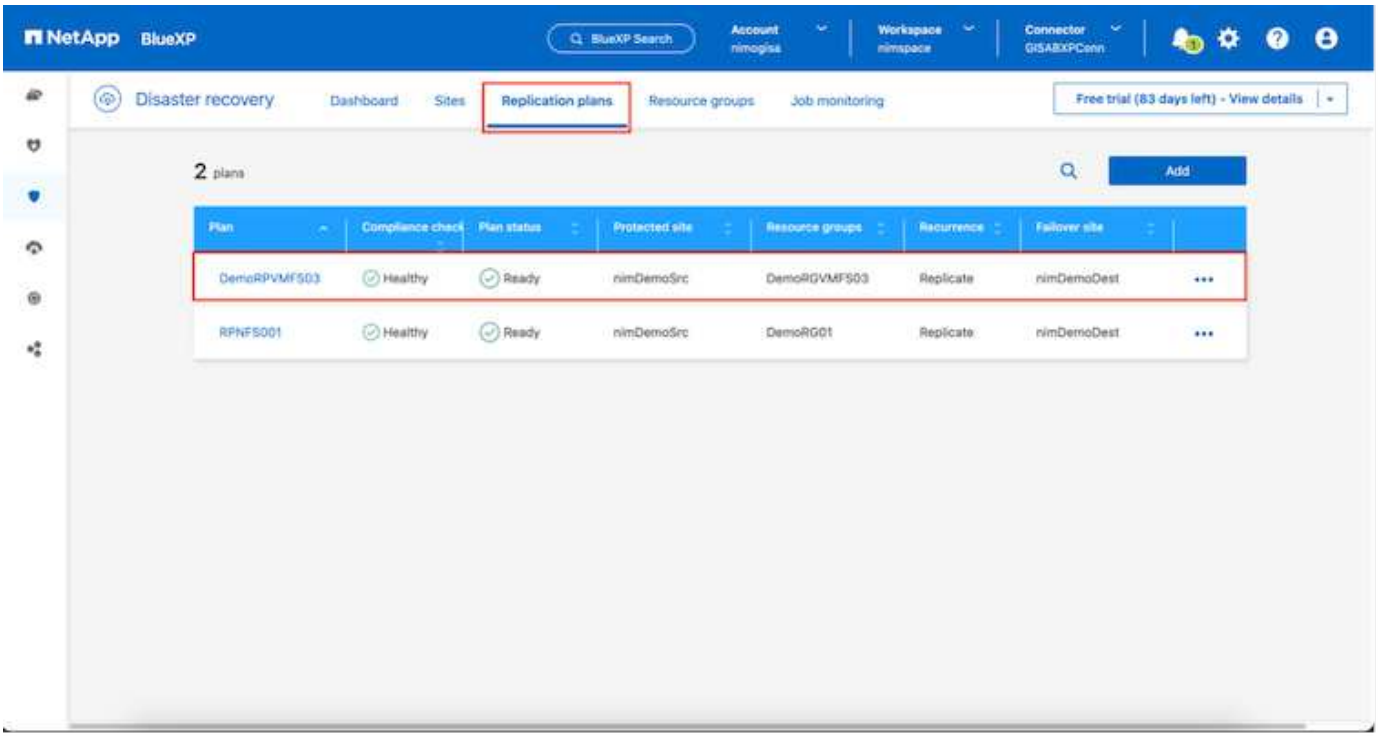


Wählen Sie den Wiederholungstyp aus. Einfach ausgedrückt: Wählen Sie „Migrieren“ (einmalige Migration mit Failover) oder die Option „Wiederkehrende kontinuierliche Replikation“. In dieser exemplarischen Vorgehensweise ist die Option „Replizieren“ ausgewählt.

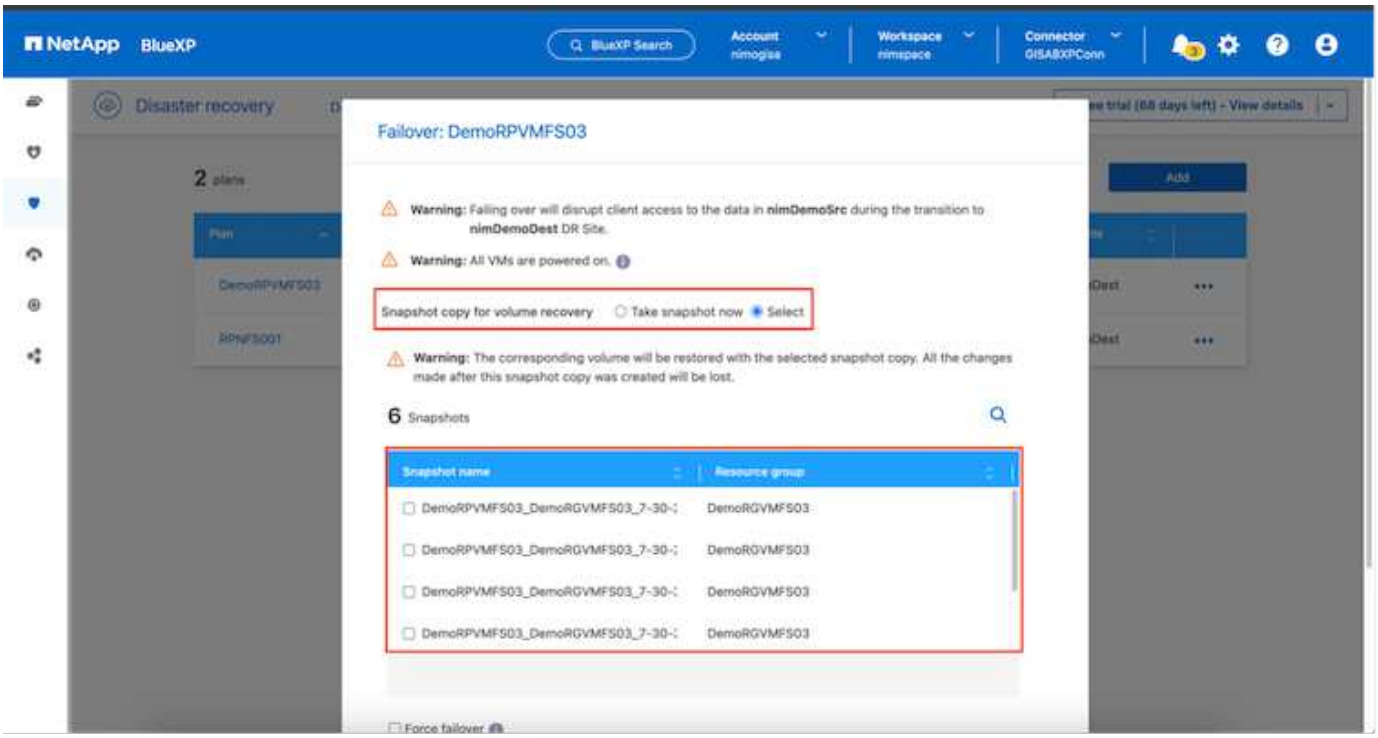


Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf „Plan hinzufügen“.

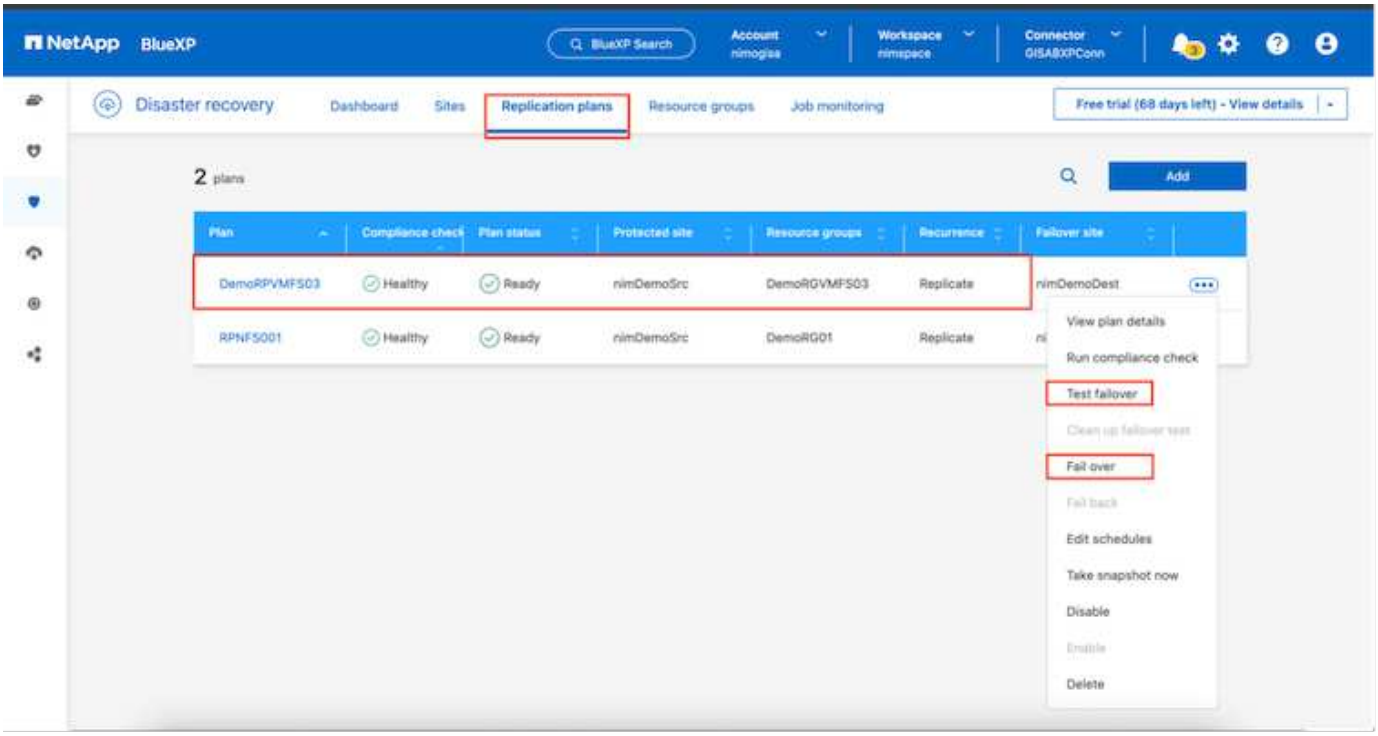




Sobald der Replikationsplan erstellt ist, kann je nach Bedarf ein Failover durchgeführt werden, indem die Failover-Option, die Test-Failover-Option oder die Migrationsoption ausgewählt wird. BlueXP disaster recovery stellt sicher, dass der Replikationsprozess planmäßig alle 30 Minuten ausgeführt wird. Während der Failover- und Test-Failover-Optionen können Sie die aktuellste SnapMirror -Snapshot-Kopie verwenden oder eine bestimmte Snapshot-Kopie aus einer Point-in-Time-Snapshot-Kopie auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann sehr hilfreich sein, wenn es zu einem Korruptionsereignis wie Ransomware kommt, bei dem die aktuellsten Replikate bereits kompromittiert oder verschlüsselt sind. BlueXP disaster recovery zeigt alle verfügbaren Wiederherstellungspunkte an.



Um ein Failover oder ein Test-Failover mit der im Replikationsplan angegebenen Konfiguration auszulösen, klicken Sie auf **Failover** oder **Test-Failover**.

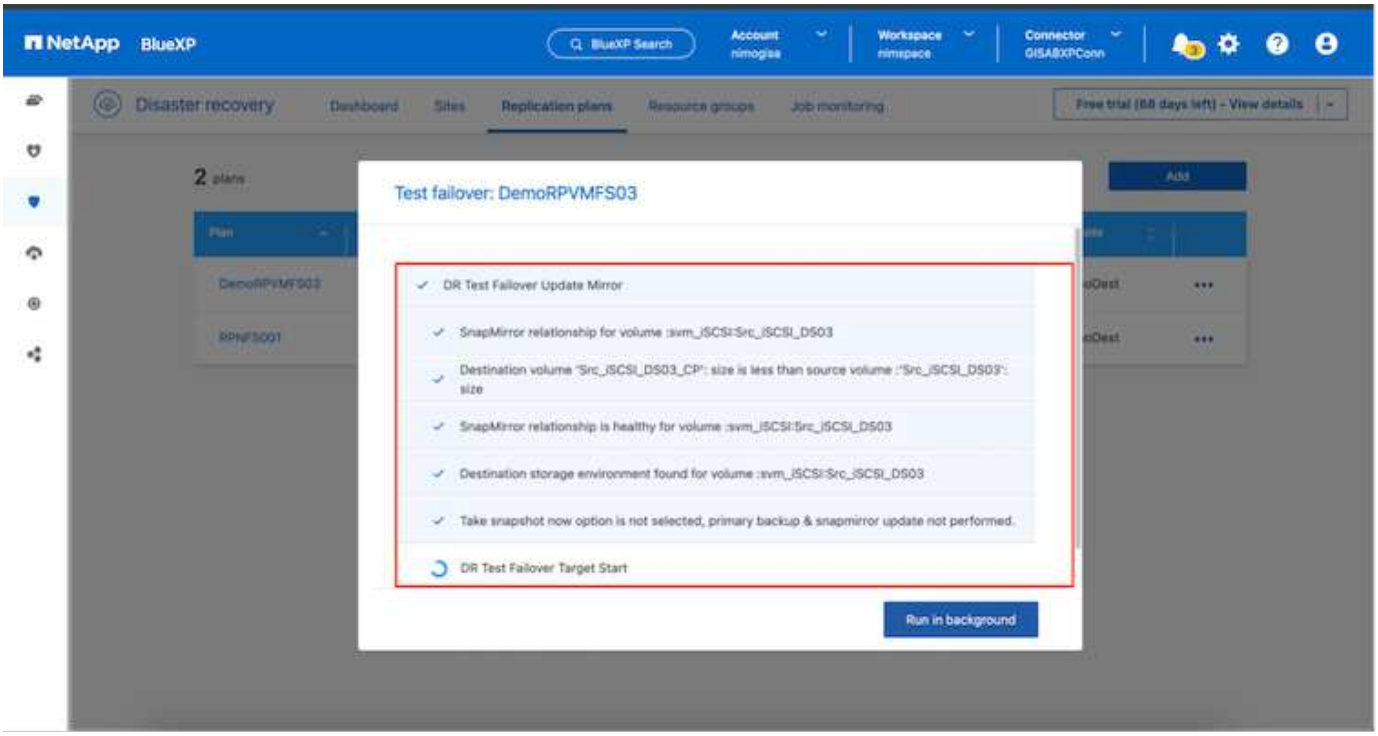


Was passiert während eines Failovers oder Test-Failover-Vorgangs?

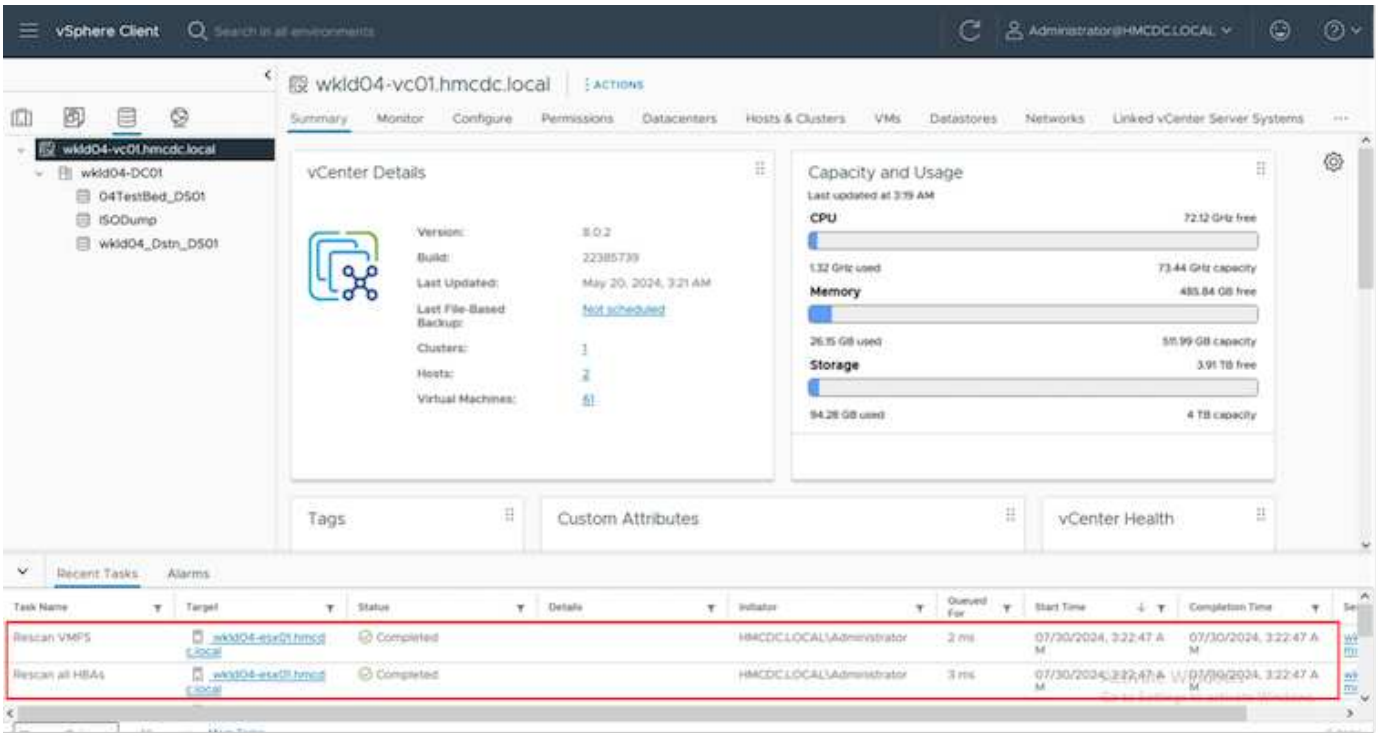
Während eines Test-Failover-Vorgangs erstellt die BlueXP disaster recovery mithilfe der neuesten Snapshot-Kopie oder eines ausgewählten Snapshots des Ziel-Volumes ein FlexClone -Volume auf dem Ziel ONTAP -Speichersystem.

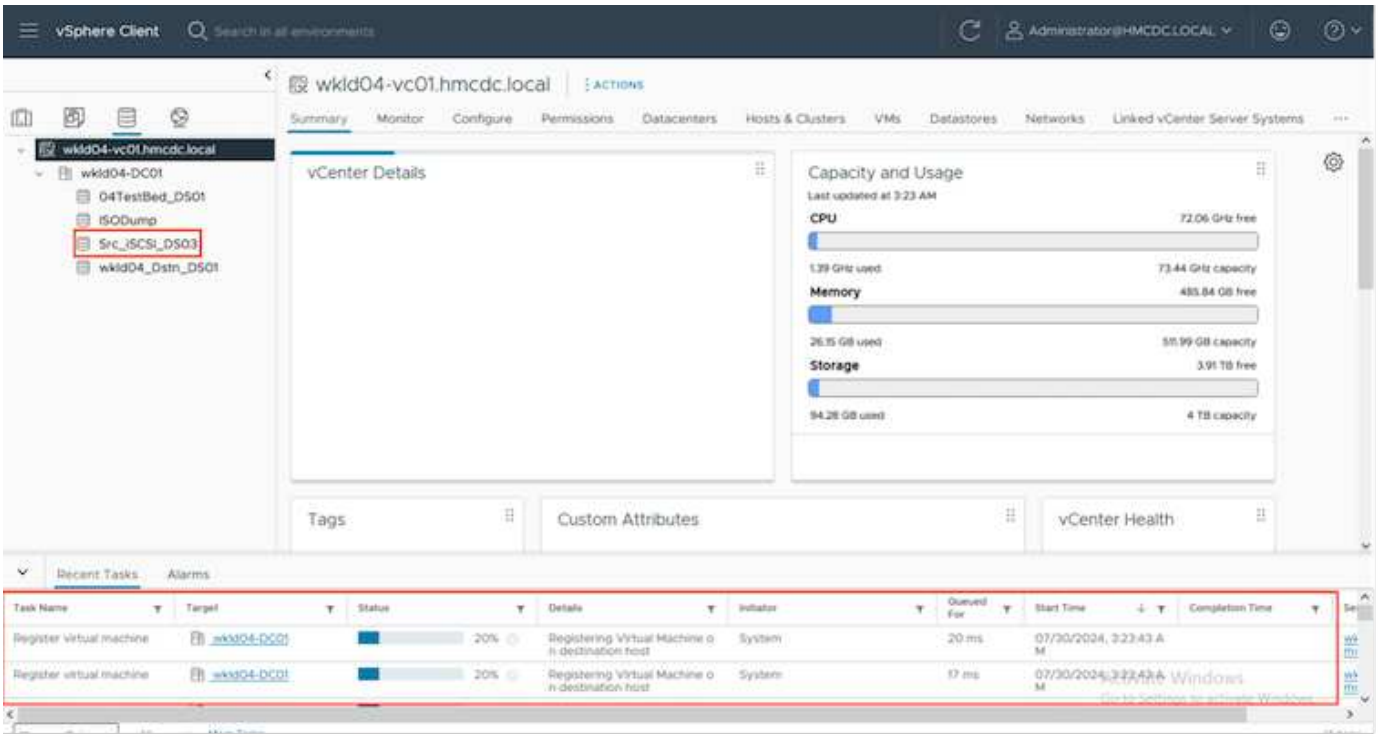
Ein Test-Failover-Vorgang erstellt ein geklontes Volume auf dem Ziel ONTAP -Speichersystem.

Das Ausführen eines Testwiederherstellungsvorgangs hat keine Auswirkungen auf die SnapMirror Replikation.



Während des Vorgangs ordnet BlueXP disaster recovery das ursprüngliche Zielvolume nicht zu. Stattdessen wird aus dem ausgewählten Snapshot ein neues FlexClone Volume erstellt und ein temporärer Datenspeicher, der das FlexClone Volume unterstützt, wird den ESXi-Hosts zugeordnet.

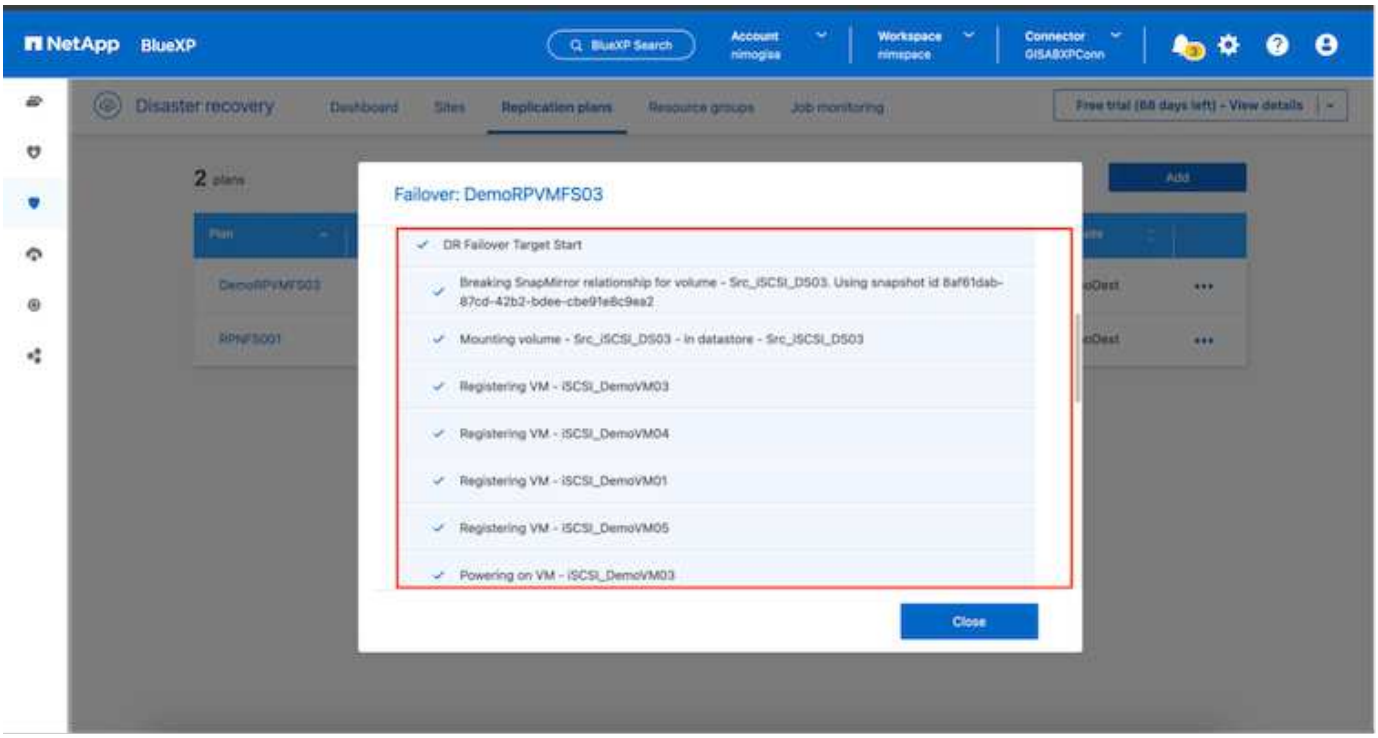




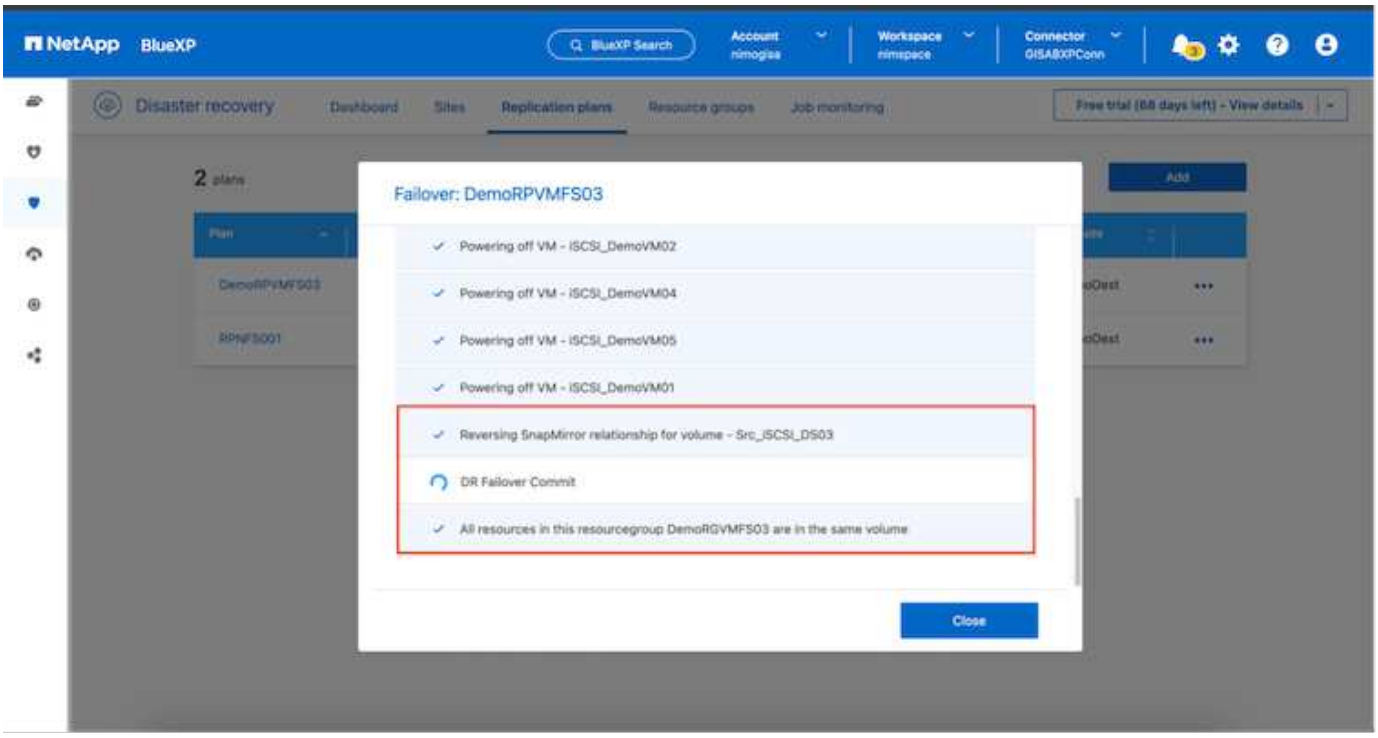
Wenn der Test-Failover-Vorgang abgeschlossen ist, kann der Bereinigungsvorgang mit **"Failover-Test bereinigen"** ausgelöst werden. Während dieses Vorgangs zerstört die BlueXP disaster recovery das FlexClone -Volume, das bei diesem Vorgang verwendet wurde.

Im Falle eines echten Katastrophenfalls führt die BlueXP disaster recovery die folgenden Schritte aus:

1. Bricht die SnapMirror -Beziehung zwischen den Sites ab.
2. Mountet das VMFS-Datenspeichervolume nach der Neusignierung zur sofortigen Verwendung.
3. Registrieren der VMs
4. VMs einschalten



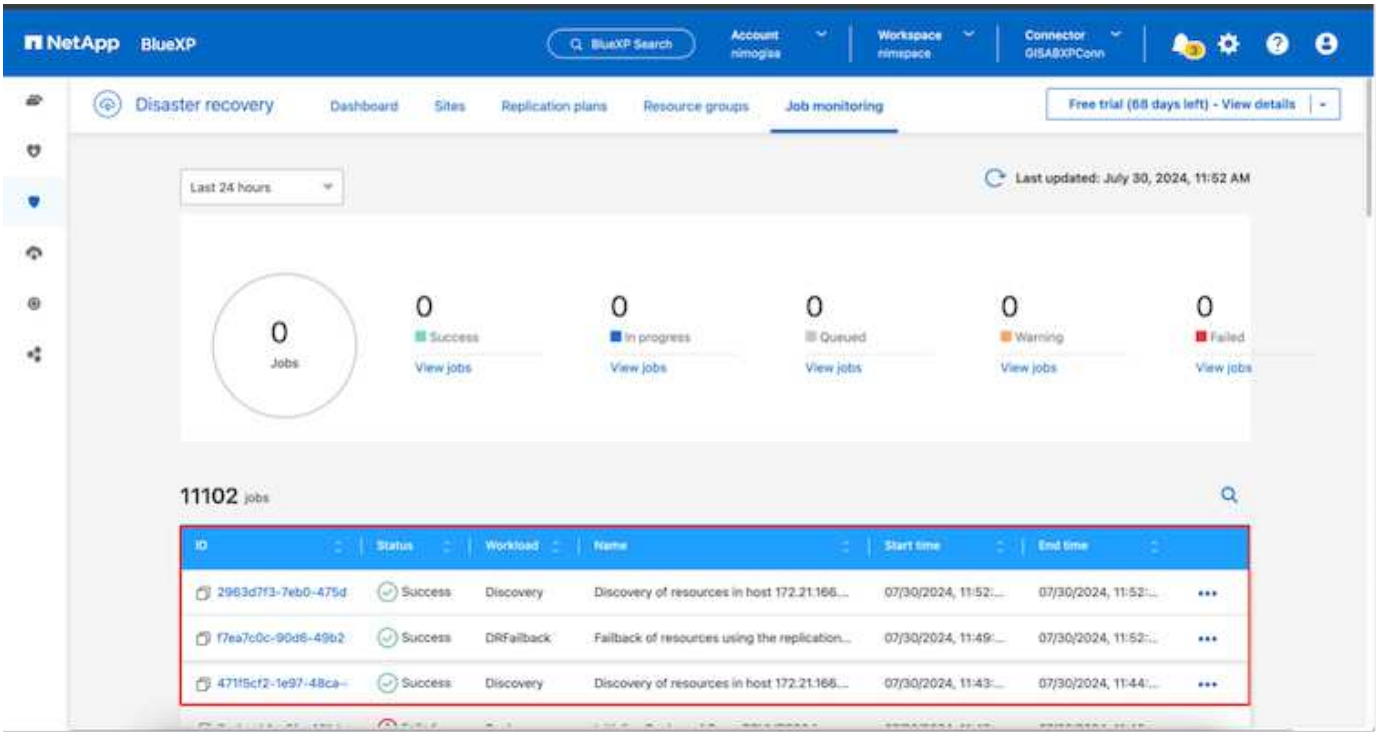
Sobald die primäre Site betriebsbereit ist, ermöglicht die BlueXP disaster recovery die umgekehrte Neusynchronisierung für SnapMirror und ermöglicht ein Failback, das ebenfalls per Mausklick ausgeführt werden kann.



Und wenn die Migrationsoption gewählt wird, wird dies als geplantes Failover-Ereignis betrachtet. In diesem Fall wird ein zusätzlicher Schritt ausgelöst, der darin besteht, die virtuellen Maschinen am Quellstandort herunterzufahren. Die restlichen Schritte bleiben dieselben wie beim Failover-Ereignis.

Von BlueXP oder der ONTAP CLI aus können Sie den Replikationszustand für die entsprechenden Datenspeichervolumes überwachen und den Status eines Failovers oder Testfailovers über die

Jobüberwachung verfolgen.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Prozess zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen oder die"Lösungssimulator" .

Einrichten der Notfallwiederherstellung für NFS-Datenspeicher mit BlueXP disaster recovery

In diesem Anwendungsfall beschreiben wir das Verfahren zum Einrichten der Notfallwiederherstellung mit BlueXP disaster recovery für lokale VMware-VMs unter Verwendung von NFS-Datenspeichern. Dieses Verfahren umfasst das Einrichten des BlueXP -Kontos und -Connectors, das Hinzufügen von ONTAP Arrays, um die Kommunikation zwischen VMware vCenter und ONTAP Speicher zu ermöglichen, das Konfigurieren der Replikation zwischen Standorten sowie das Erstellen und Testen von Wiederherstellungsplänen.

Die Implementierung einer Notfallwiederherstellung durch Blockreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Methode zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen, wie beispielsweise Ransomware-Angriffen. Mithilfe der NetApp SnapMirror Replikation können VMware-Workloads, die auf lokalen ONTAP -Systemen mit NFS-Datenspeicher ausgeführt werden, auf ein anderes ONTAP Speichersystem repliziert werden, das sich in einem dafür vorgesehenen Wiederherstellungs-Rechenzentrum befindet, in dem auch VMware bereitgestellt wird.

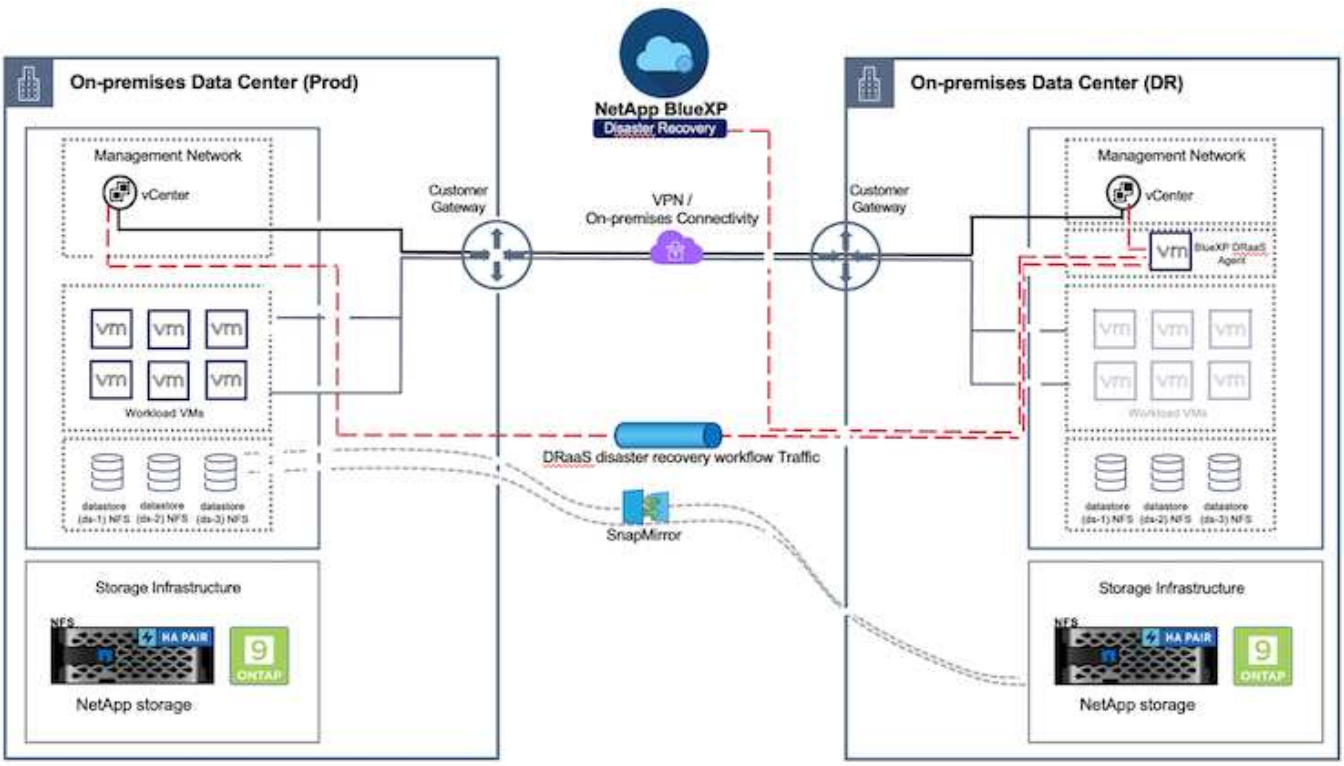
Einführung

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zum Einrichten der

Notfallwiederherstellung für lokale VMware-VMs an einem anderen bestimmten Standort beschrieben. Als Teil dieser Einrichtung werden das BlueXP -Konto, der BlueXP Connector und die ONTAP Arrays im BlueXP Arbeitsbereich hinzugefügt, die für die Kommunikation von VMware vCenter mit dem ONTAP Speicher erforderlich sind. Darüber hinaus wird in diesem Dokument detailliert beschrieben, wie die Replikation zwischen Standorten konfiguriert wird und wie ein Wiederherstellungsplan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Site-Failovers und zum Failback, wenn die primäre Site wiederhergestellt und online gestellt wurde.

Mithilfe des in die NetApp BlueXP Konsole integrierten BlueXP disaster recovery -Dienstes können Unternehmen ihre lokalen VMware vCenter- und ONTAP -Speicher problemlos ermitteln. Organisationen können dann Ressourcengruppierungen erstellen, einen Notfallwiederherstellungsplan erstellen, ihn mit Ressourcengruppen verknüpfen und Failover und Failback testen oder ausführen. SnapMirror bietet Blockreplikation auf Speicherebene, um die beiden Sites mit inkrementellen Änderungen auf dem neuesten Stand zu halten, was zu einem Recovery Point Objective (RPO) von bis zu 5 Minuten führt. Darüber hinaus ist es möglich, Disaster-Recovery-Verfahren zu simulieren, ohne die Produktion zu beeinträchtigen oder zusätzliche Speicherkosten zu verursachen.

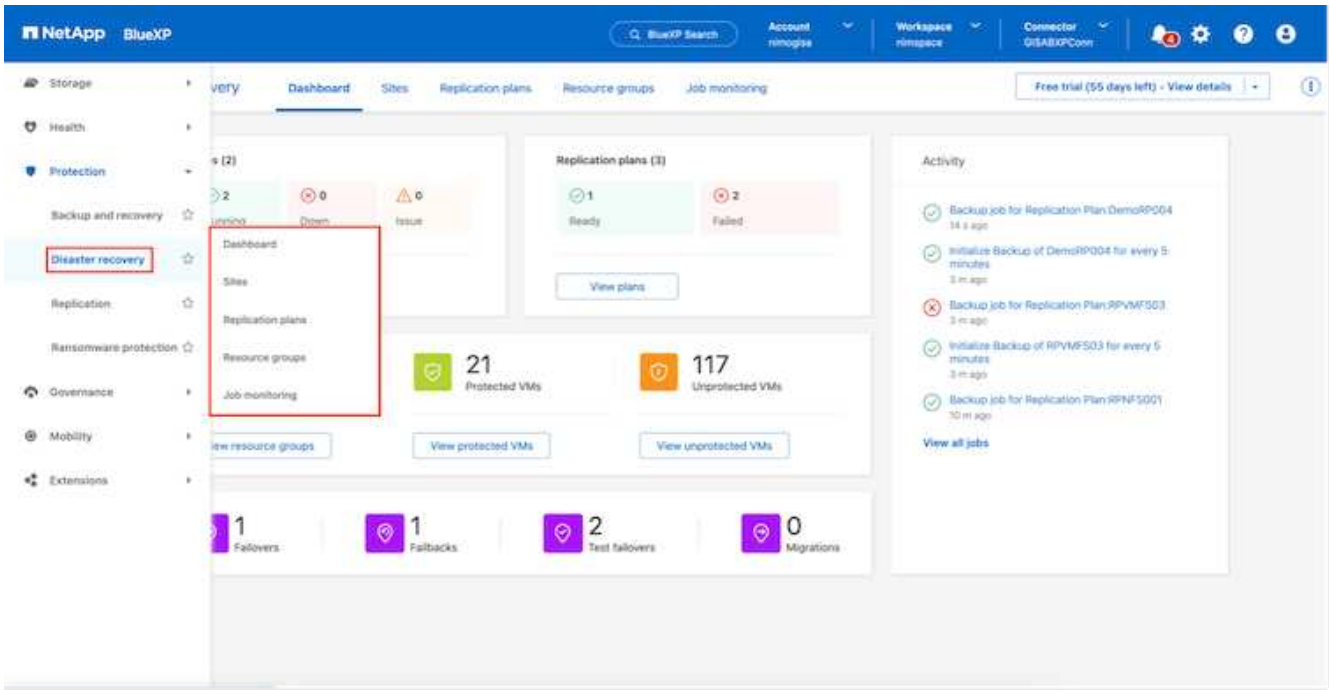
BlueXP disaster recovery nutzt die FlexClone -Technologie von ONTAP, um eine platzsparende Kopie des NFS-Datenspeichers vom letzten replizierten Snapshot auf der Disaster Recovery-Site zu erstellen. Nach Abschluss des Disaster-Recovery-Tests können Kunden die Testumgebung problemlos löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Im Falle eines tatsächlichen Failovers orchestriert der BlueXP disaster recovery -Dienst alle notwendigen Schritte, um die geschützten virtuellen Maschinen mit nur wenigen Klicks automatisch am vorgesehenen Disaster-Recovery-Standort hochzufahren. Der Dienst kehrt außerdem die SnapMirror -Beziehung zum primären Standort um und repliziert bei Bedarf alle Änderungen vom sekundären zum primären Standort für einen Failback-Vorgang. Alle diese Funktionen sind im Vergleich zu anderen bekannten Alternativen zu einem Bruchteil der Kosten erhältlich.



Erste Schritte

Um mit der BlueXP disaster recovery zu beginnen, verwenden Sie die BlueXP -Konsole und greifen Sie dann auf den Dienst zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste von BlueXP „Schutz“ > „Notfallwiederherstellung“ aus.
3. Das BlueXP disaster recovery wird angezeigt.

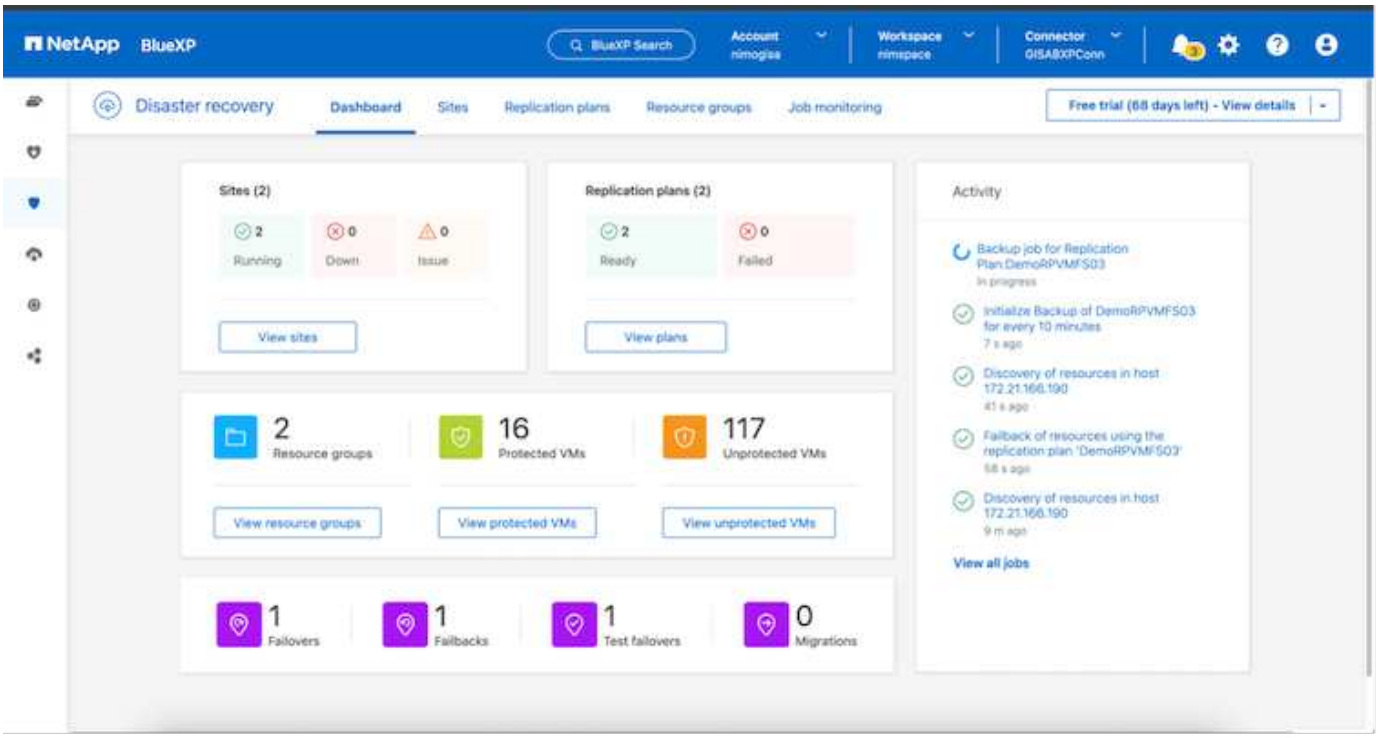


Stellen Sie vor der Konfiguration des Notfallwiederherstellungsplans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- BlueXP Connector wird in NetApp BlueXP eingerichtet.
- Die BlueXP Connector-Instanz verfügt über eine Verbindung zum Quell- und Ziel-vCenter und den Speichersystemen.
- NetApp Data ONTAP Cluster zur Bereitstellung von NFS-Datenspeichern.
- In BlueXP werden lokale NetApp -Speichersysteme hinzugefügt, die NFS-Datenspeicher für VMware hosten.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen NFS-basierten Datenspeichervolumes konfiguriert.
- Stellen Sie sicher, dass die Umgebung über unterstützte Versionen von vCenter Server und ESXi-Servern verfügt.

Sobald die Verbindung zwischen Quell- und Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte einige Klicks dauern und etwa 3 bis 5 Minuten dauern.

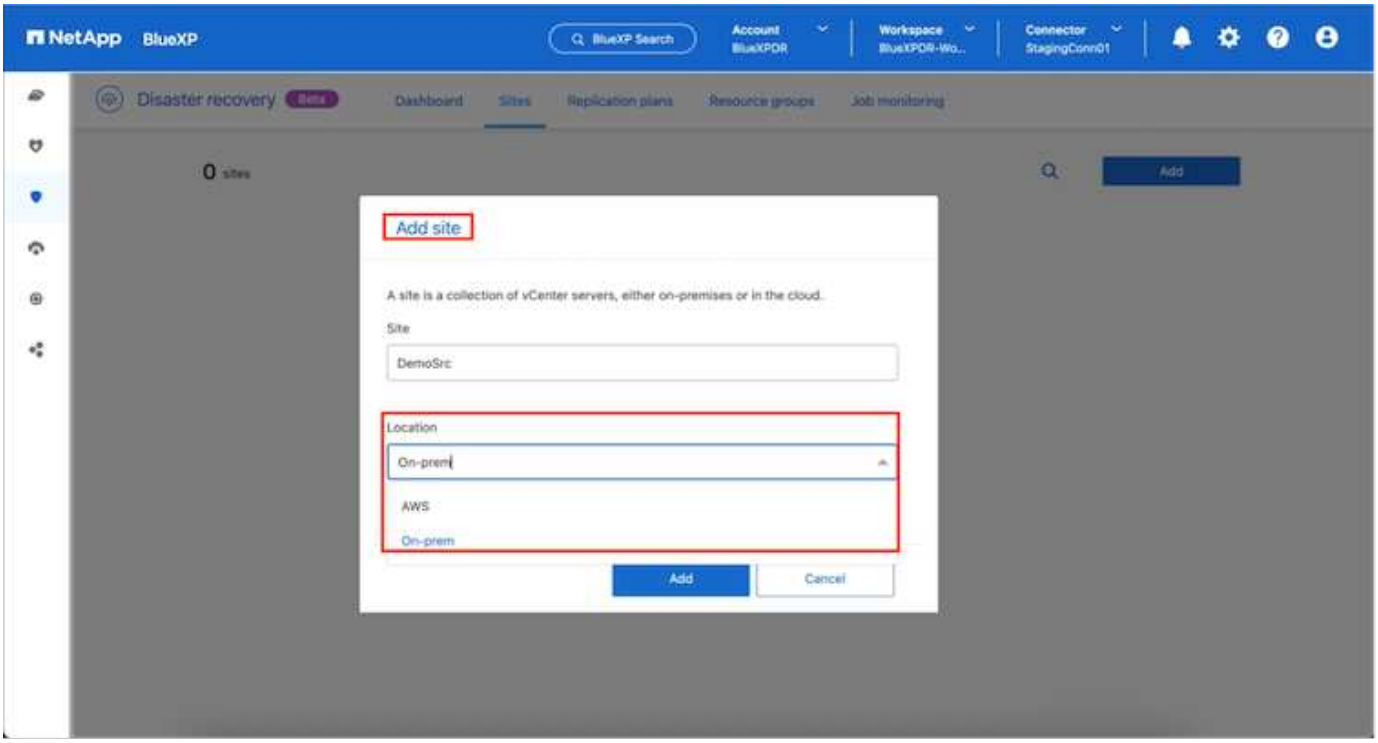
> NetApp empfiehlt, den BlueXP Connector am Zielstandort oder an einem dritten Standort bereitzustellen, damit der BlueXP Connector über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.



BlueXP disaster recovery

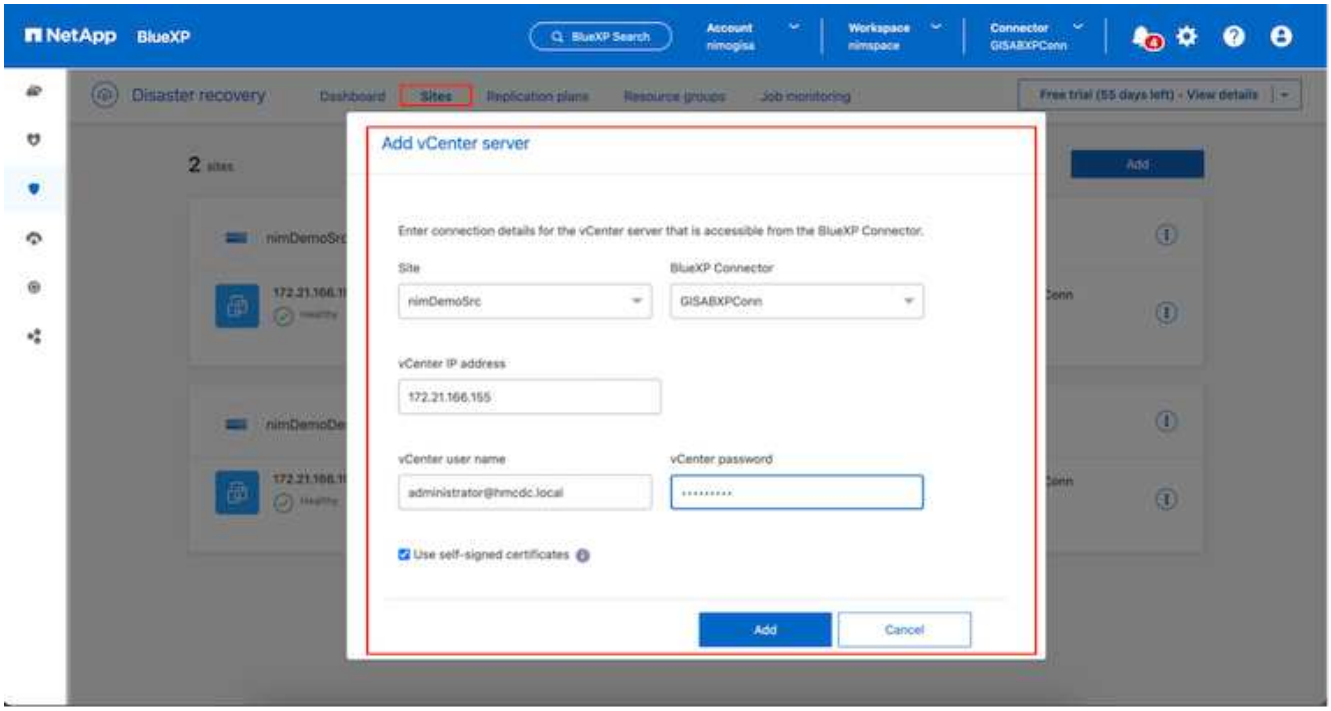
Der erste Schritt bei der Vorbereitung der Notfallwiederherstellung besteht darin, die lokalen vCenter- und Speicherressourcen zu ermitteln und zur BlueXP disaster recovery hinzuzufügen.

Öffnen Sie die BlueXP -Konsole und wählen Sie in der linken Navigation **Schutz > Notfallwiederherstellung**. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü. Wählen Sie **Sites > Hinzufügen > vCenter hinzufügen**.

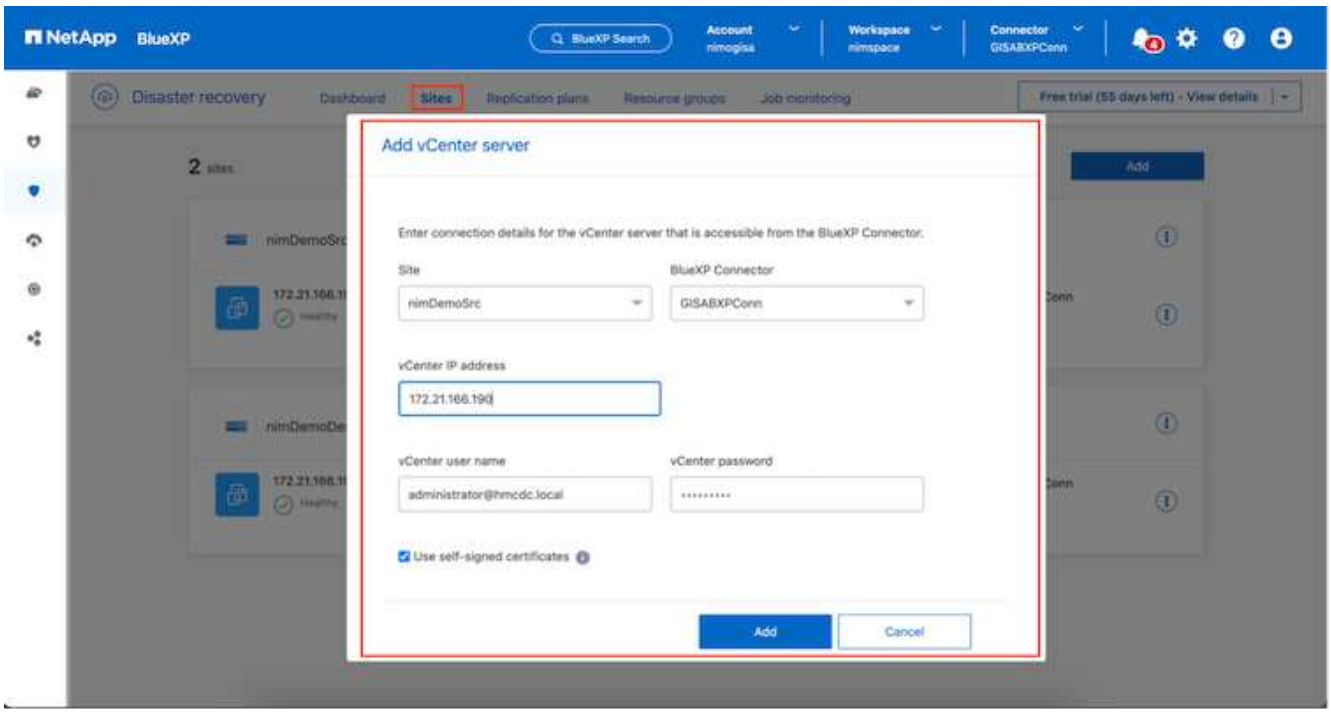


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle**. Lokales vCenter.



- **Ziel**. VMC SDDC vCenter.



Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array

SnapMirror bietet Datenreplikation in einer NetApp Umgebung. Die SnapMirror -Replikation basiert auf der NetApp Snapshot-Technologie und ist äußerst effizient, da sie nur die Blöcke repliziert, die seit dem letzten Update geändert oder hinzugefügt wurden. SnapMirror lässt sich einfach mithilfe des NetApp OnCommand

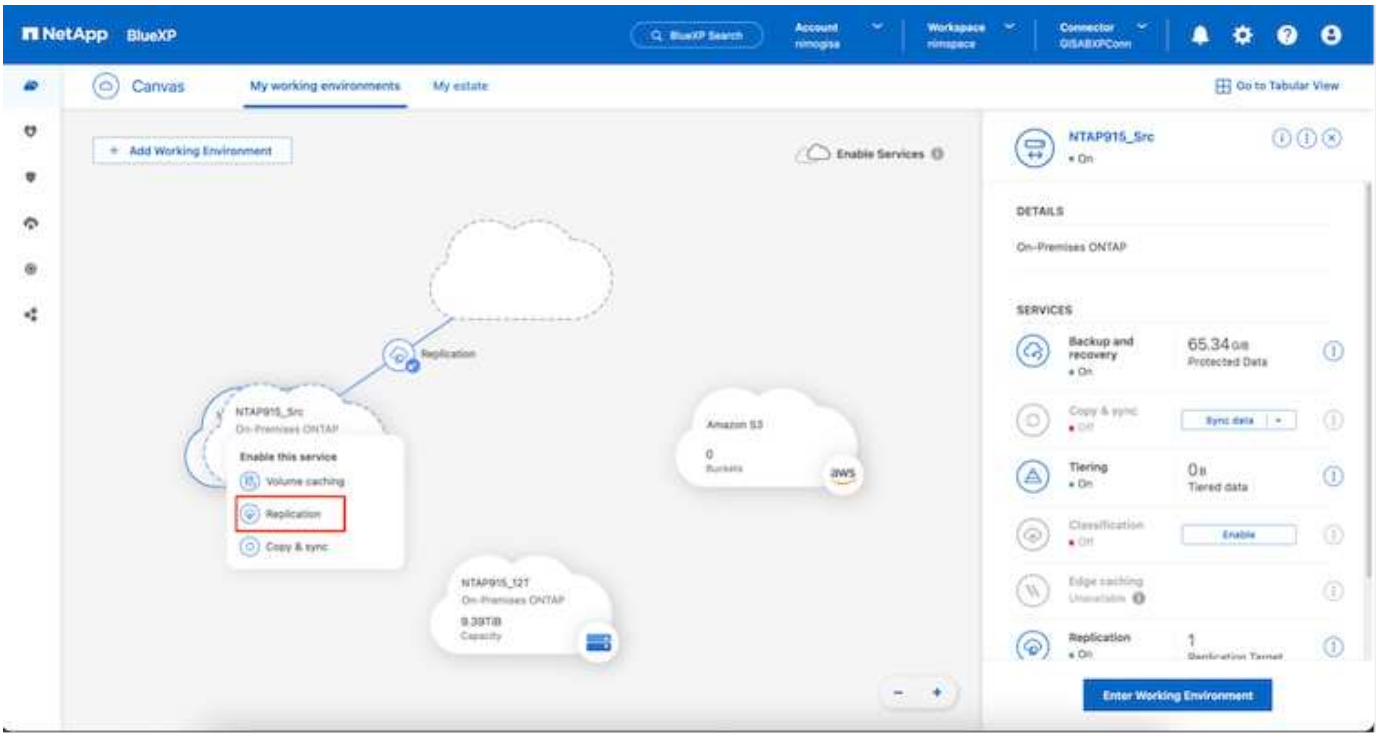
System Manager oder der ONTAP CLI konfigurieren. BlueXP DRaaS erstellt auch die SnapMirror -Beziehung, sofern Cluster- und SVM-Peering zuvor konfiguriert wurden.

In Fällen, in denen der primäre Speicher nicht vollständig verloren geht, bietet SnapMirror eine effiziente Möglichkeit zur Neusynchronisierung der primären und DR-Sites. SnapMirror kann die beiden Sites neu synchronisieren und nur geänderte oder neue Daten von der DR-Site zurück zur primären Site übertragen, indem einfach die SnapMirror Beziehungen umgekehrt werden. Dies bedeutet, dass Replikationspläne in BlueXP DRaaS nach einem Failover in beide Richtungen neu synchronisiert werden können, ohne das gesamte Volume erneut zu kopieren. Wenn eine Beziehung in umgekehrter Richtung erneut synchronisiert wird, werden nur neue Daten an das Ziel zurückgesendet, die seit der letzten erfolgreichen Synchronisierung der Snapshot-Kopie geschrieben wurden.

> Wenn die SnapMirror -Beziehung für das Volume bereits über CLI oder System Manager konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.

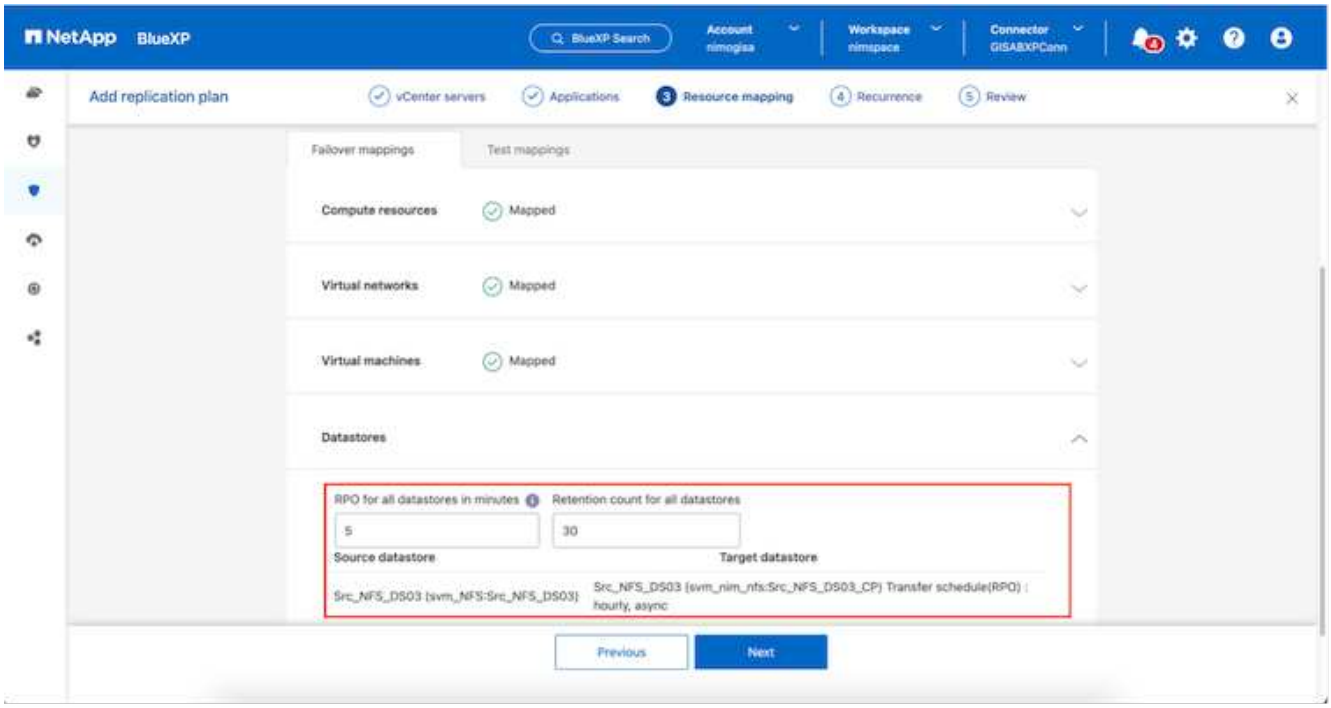
So richten Sie es für VMware Disaster Recovery ein

Der Vorgang zum Erstellen der SnapMirror Replikation bleibt für jede Anwendung derselbe. Der Vorgang kann manuell oder automatisiert erfolgen. Am einfachsten ist es, BlueXP zu nutzen, um die SnapMirror -Replikation zu konfigurieren. Dazu ziehen Sie das Quell ONTAP -System in der Umgebung einfach per Drag & Drop auf das Ziel, um den Assistenten zu starten, der Sie durch den Rest des Prozesses führt.



BlueXP DRaaS kann dies auch automatisieren, sofern die folgenden beiden Kriterien erfüllt sind:

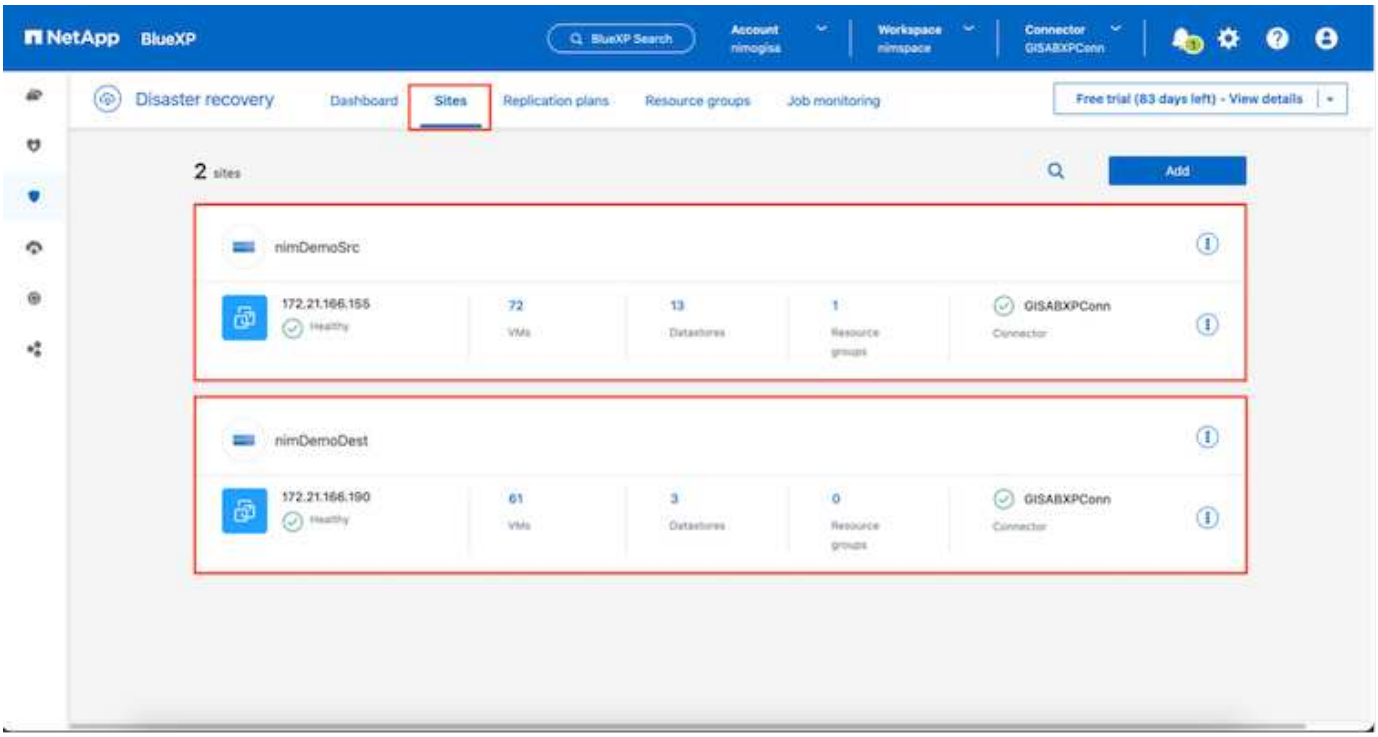
- Quell- und Zielcluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



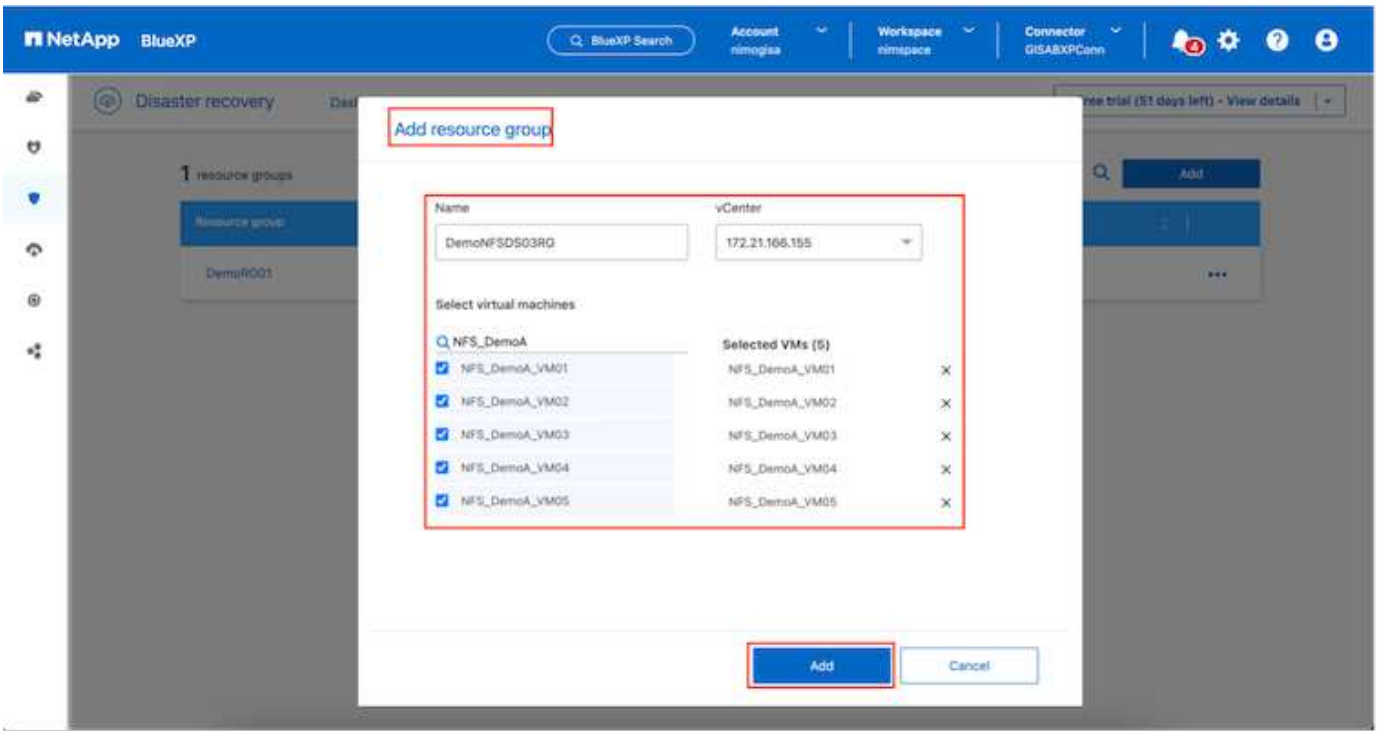
Wenn die SnapMirror -Beziehung für das Volume bereits über die CLI konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.

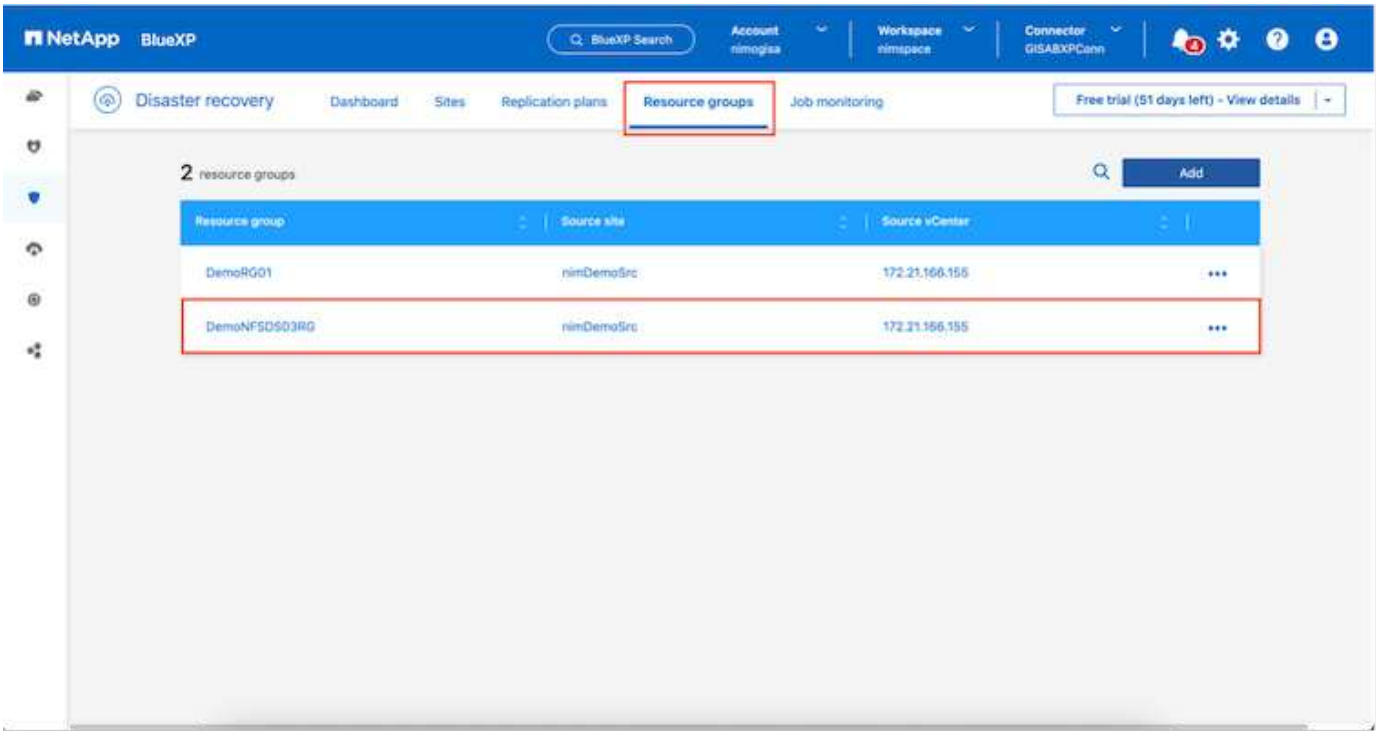
Was kann BlueXP disaster recovery für Sie tun?

Nachdem die Quell- und Zielsites hinzugefügt wurden, führt die BlueXP disaster recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Die BlueXP disaster recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.



Nachdem die Sites hinzugefügt wurden, können VMs in Ressourcengruppen gruppiert werden. Mit den BlueXP disaster recovery können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen und Startverzögerungen enthalten, die bei der Wiederherstellung ausgeführt werden können. Um mit der Erstellung von Ressourcengruppen zu beginnen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.

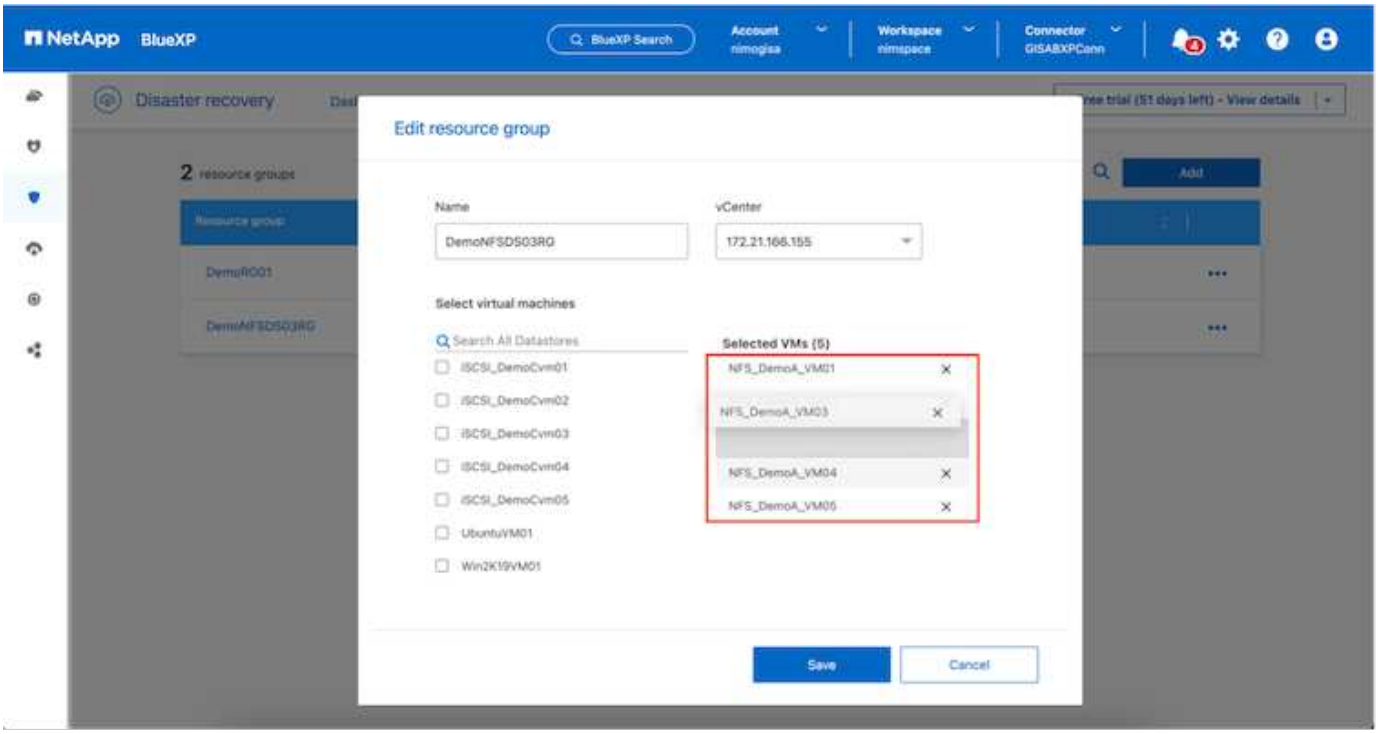




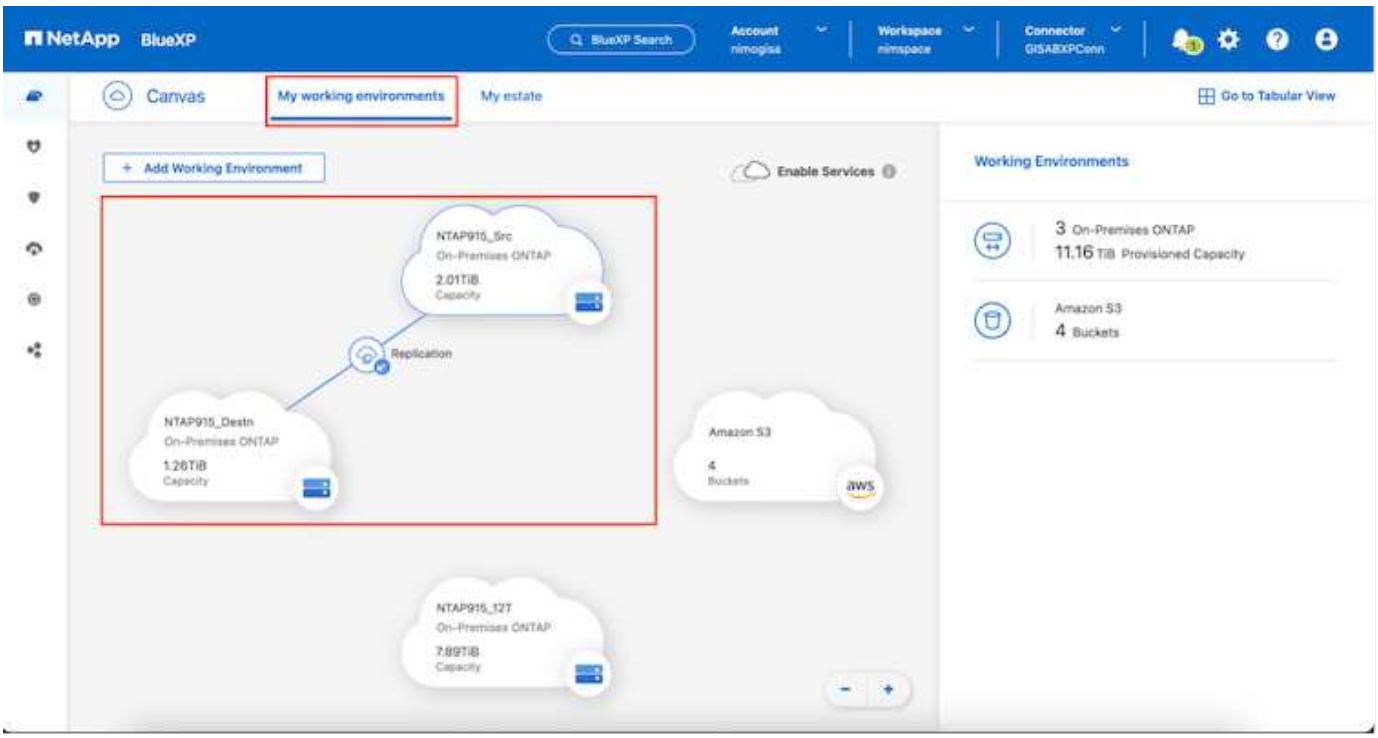
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

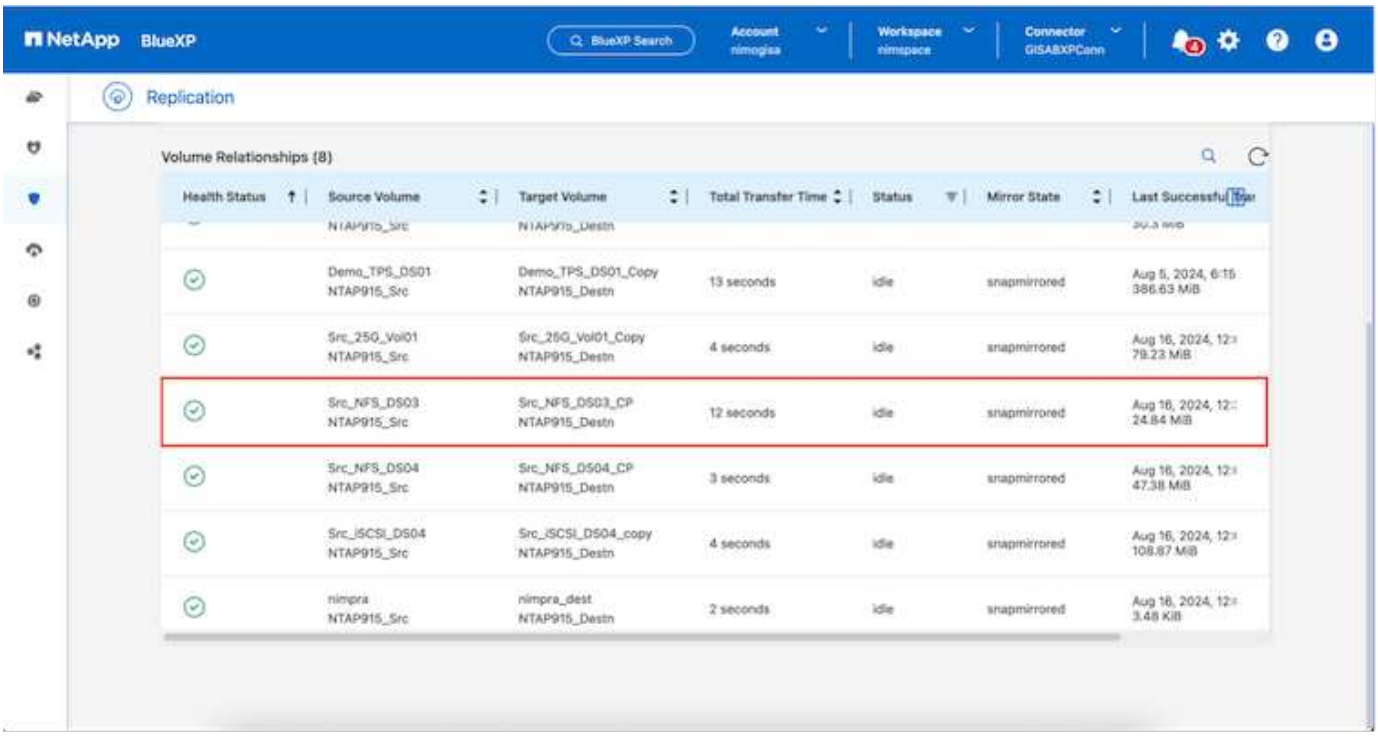
Die Startreihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen

Drag-and-Drop-Mechanismus definiert oder geändert werden.



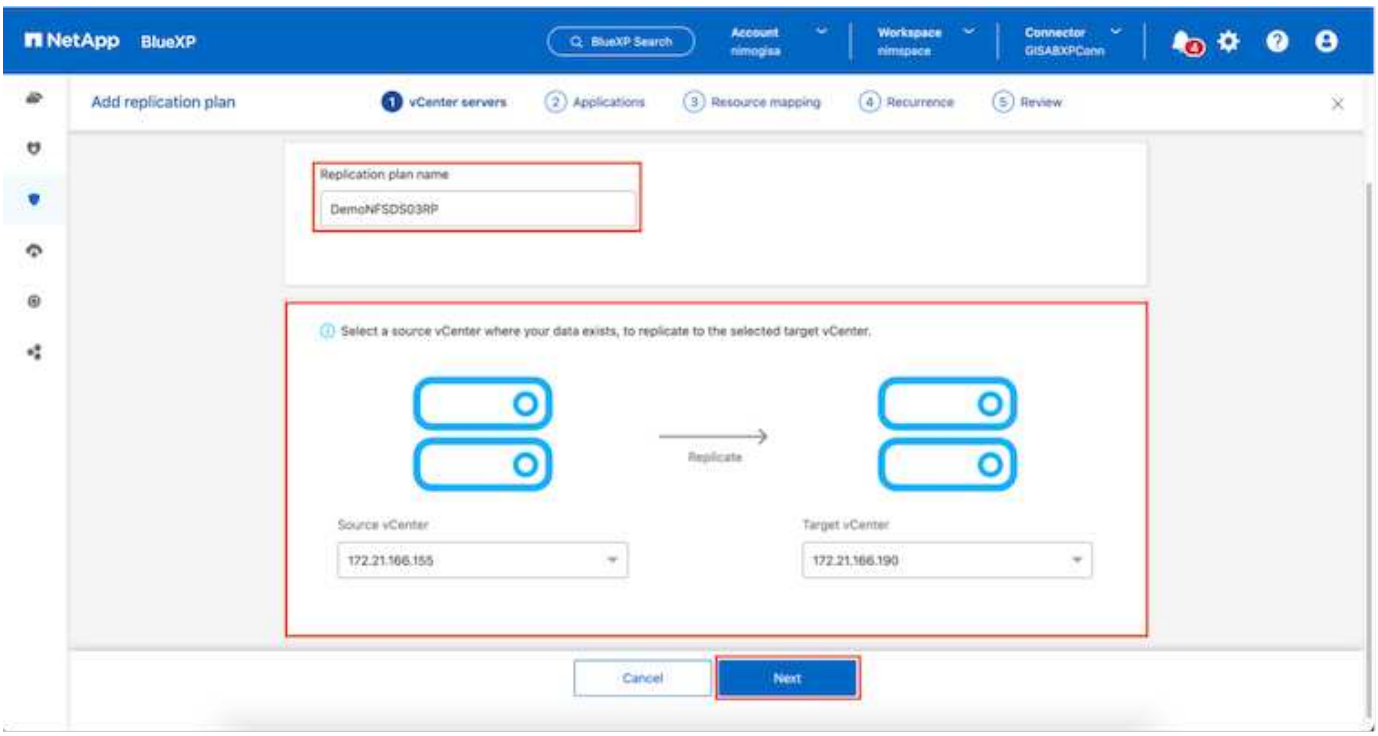
Sobald die Ressourcengruppen erstellt sind, besteht der nächste Schritt darin, den Ausführungsentwurf oder einen Plan zur Wiederherstellung virtueller Maschinen und Anwendungen im Katastrophenfall zu erstellen. Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des Replikationsplans angegeben wurden.





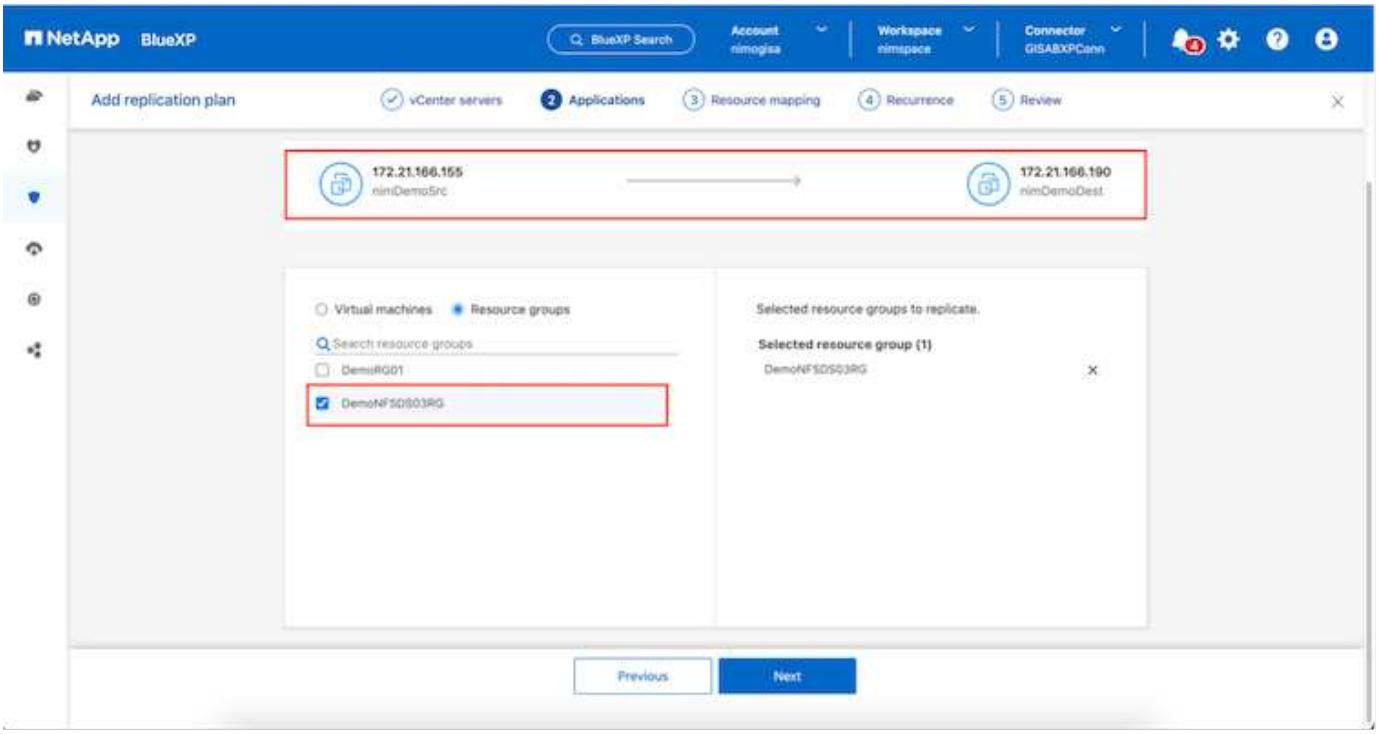
Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

Wählen Sie zuerst das Quell-vCenter und dann das Ziel-vCenter aus.



Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend

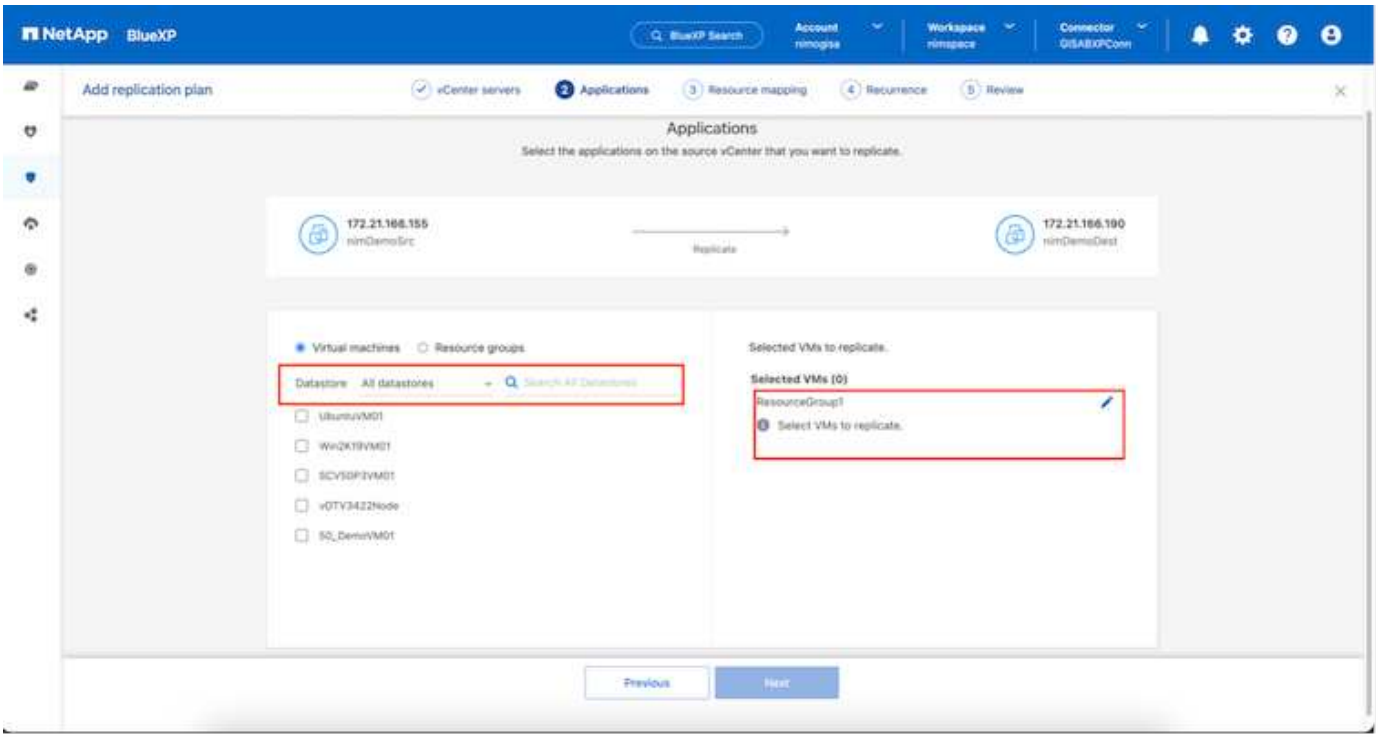
auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.



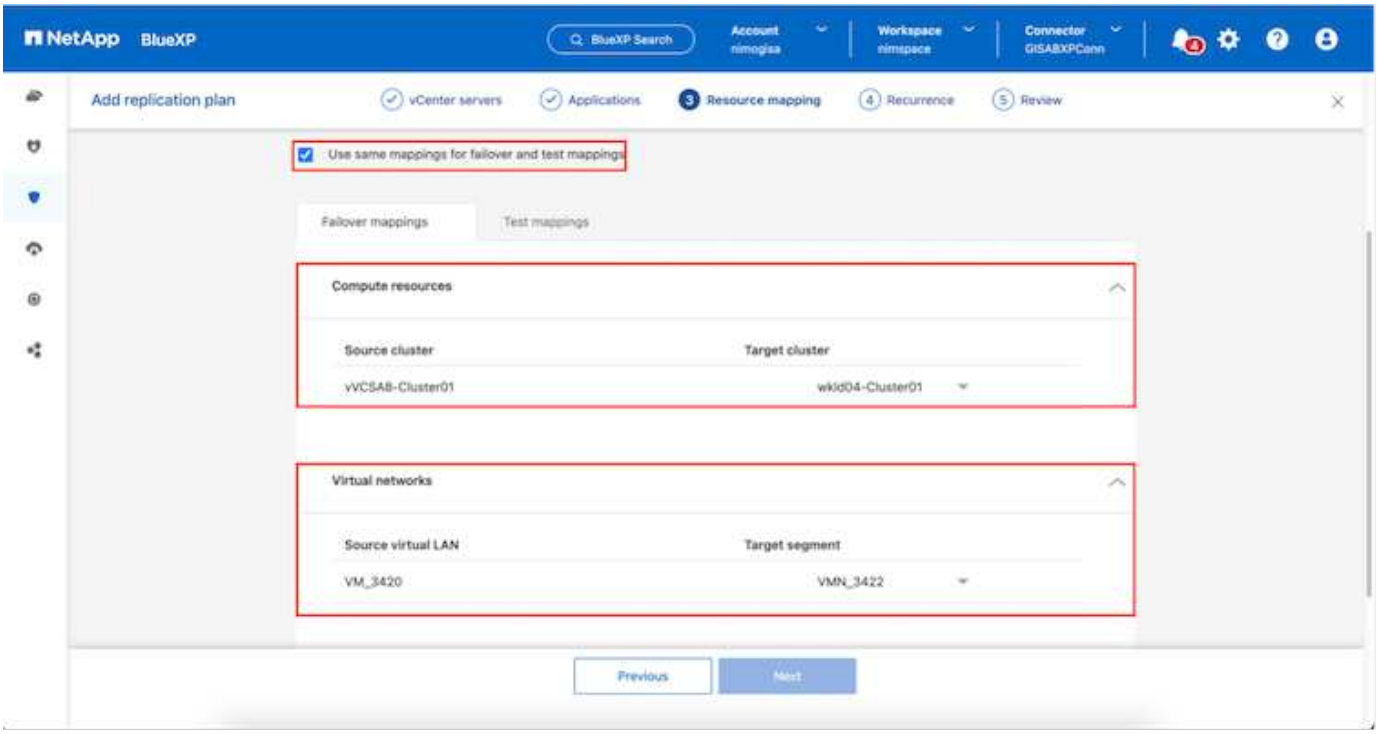
Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

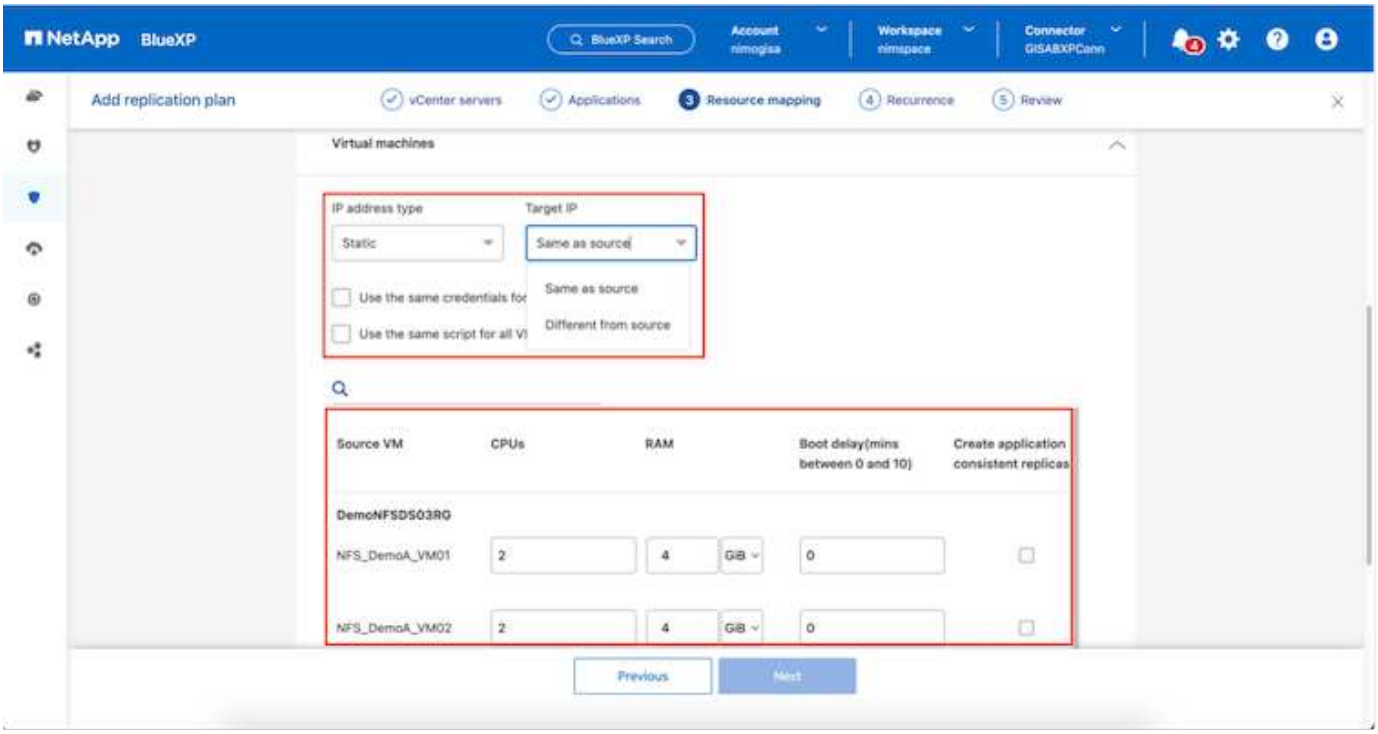
Der folgende Screenshot zeigt die Option zum Filtern virtueller Maschinen oder bestimmter Datenspeicher basierend auf organisatorischen Anforderungen, wenn nicht zuvor Ressourcengruppen erstellt wurden.



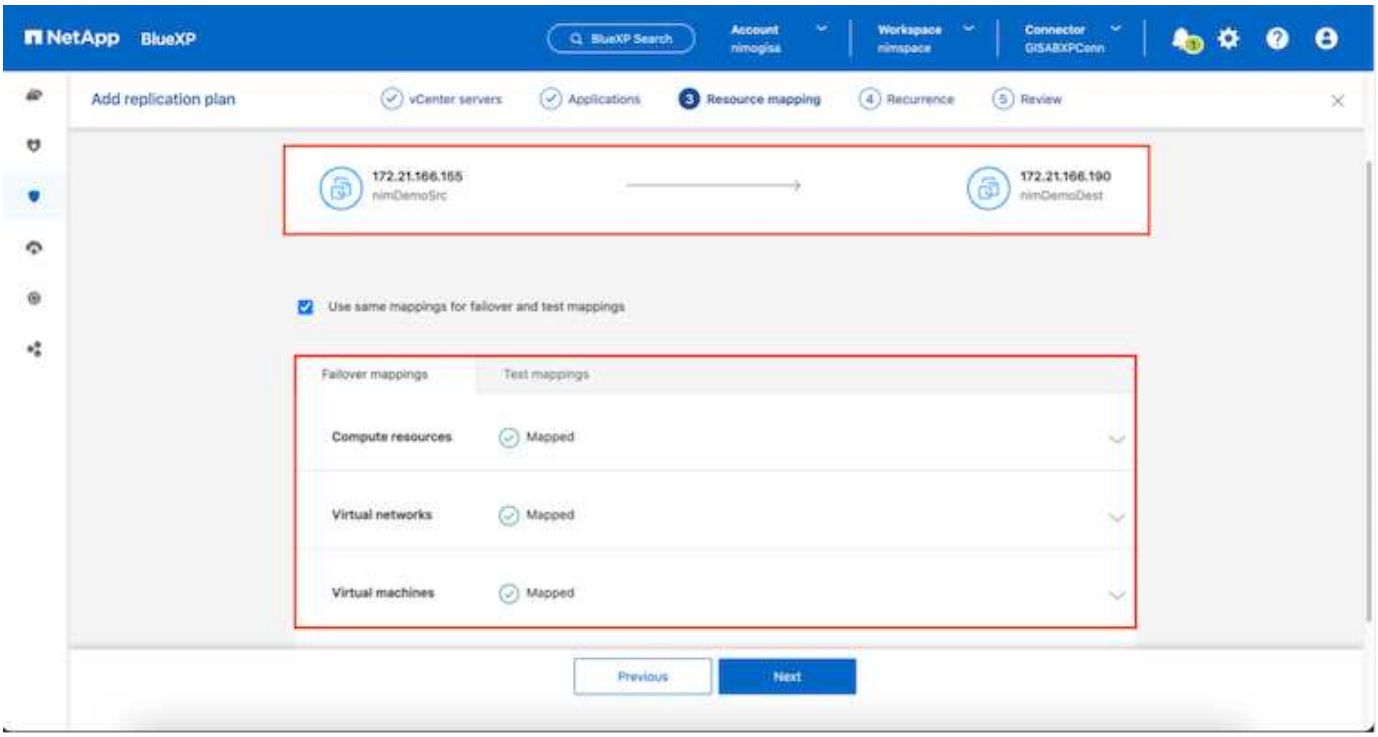
Sobald die Ressourcengruppen ausgewählt sind, erstellen Sie die Failover-Zuordnungen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen und virtuelle Netzwerke. IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Anwendungskonsistenz und so weiter. Ausführliche Informationen finden Sie unter"Erstellen eines Replikationsplans" .



Standardmäßig werden für Test- und Failovervorgänge dieselben Zuordnungsparameter verwendet. Um verschiedene Zuordnungen für die Testumgebung festzulegen, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:

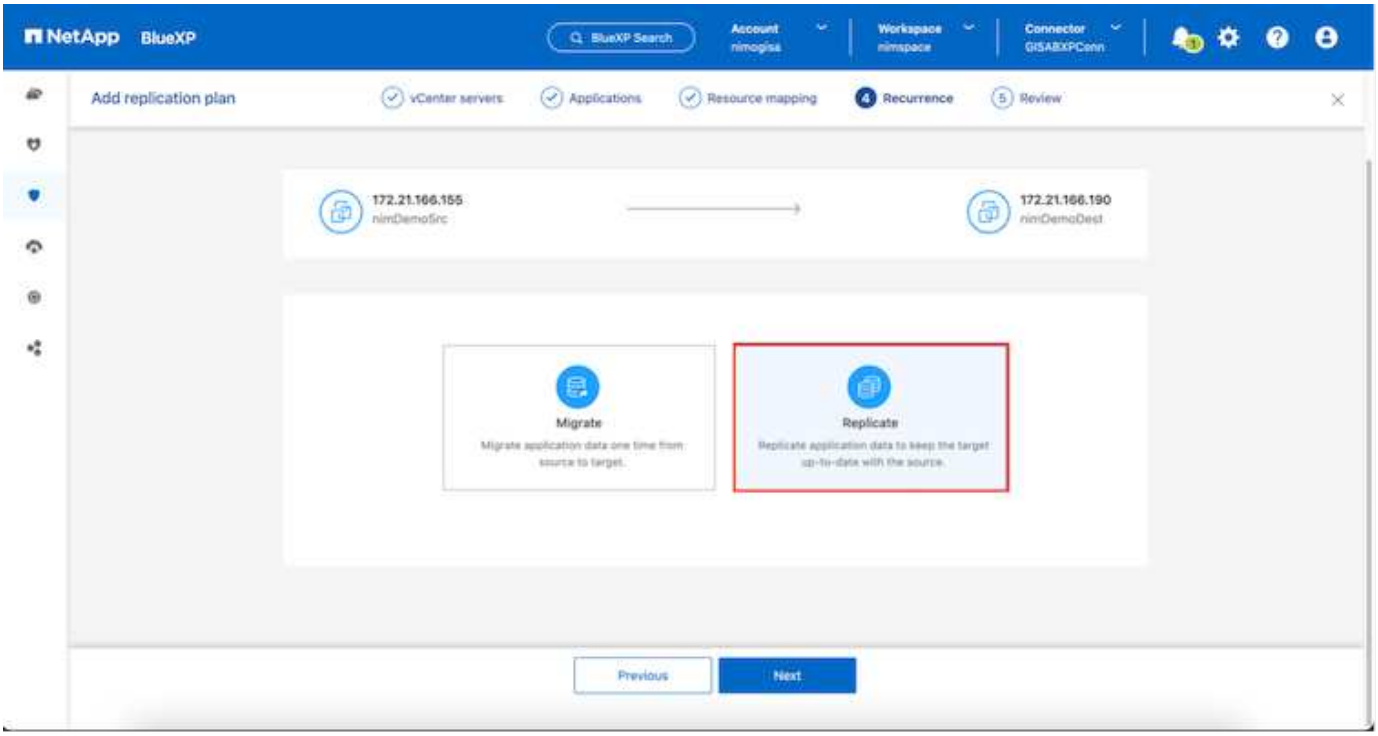


Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.



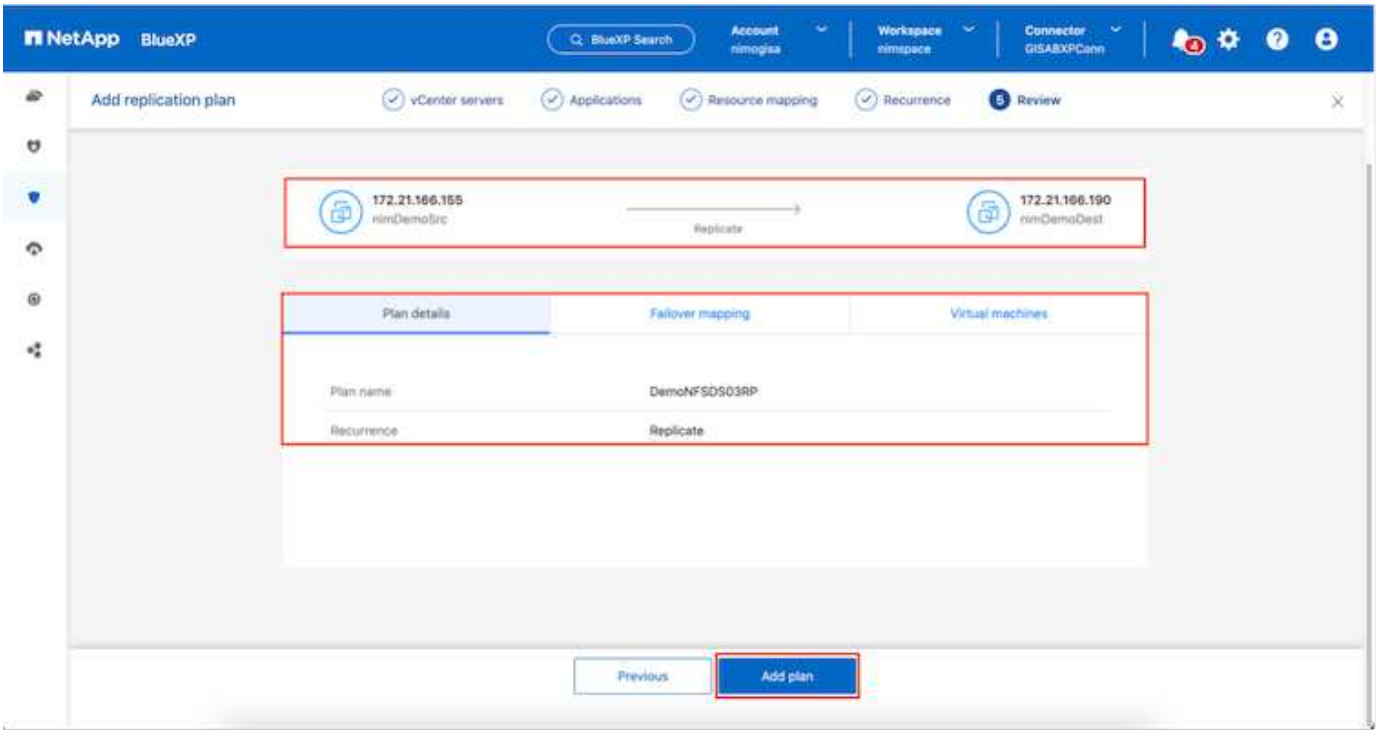
Wählen Sie den Wiederholungstyp aus. Einfach ausgedrückt: Wählen Sie „Migrieren“ (einmalige Migration mit Failover) oder die Option „Wiederkehrende kontinuierliche Replikation“. In dieser exemplarischen

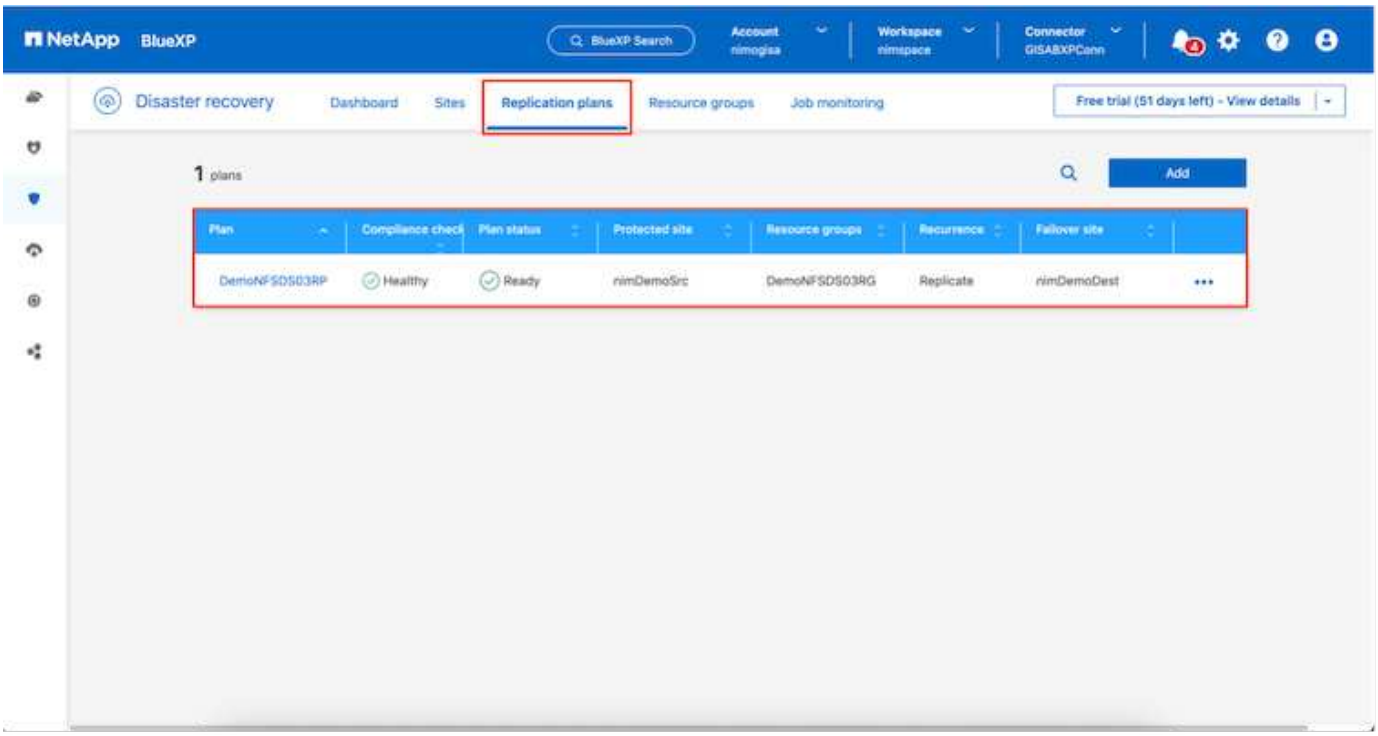
Vorgehensweise ist die Option „Replizieren“ ausgewählt.



Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf **Plan hinzufügen**.

> VMs aus verschiedenen Volumes und SVMs können in einen Replikationsplan aufgenommen werden. Abhängig von der VM-Platzierung (sei es auf demselben Volume oder einem separaten Volume innerhalb derselben SVM, separate Volumes auf verschiedenen SVMs) erstellt die BlueXP disaster recovery einen Consistency Group Snapshot.



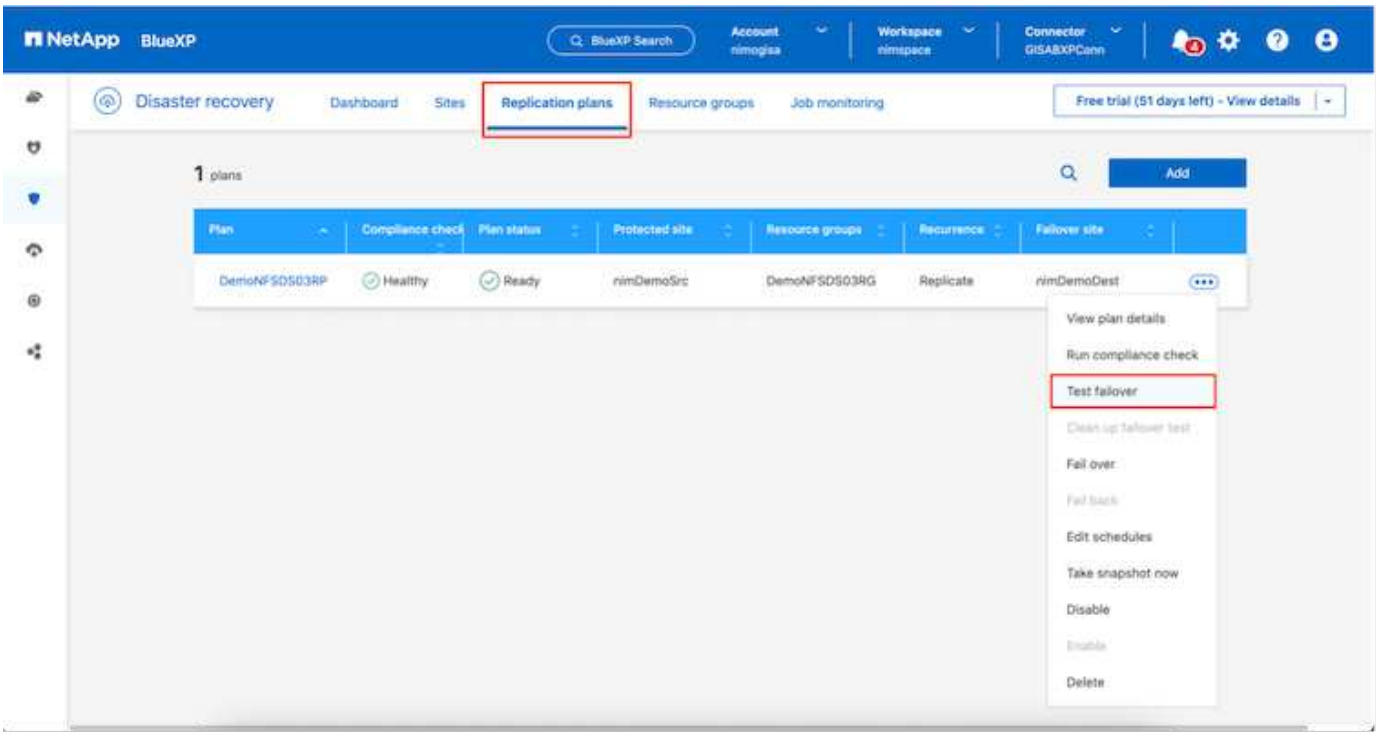


BlueXP DRaaS besteht aus den folgenden Workflows:

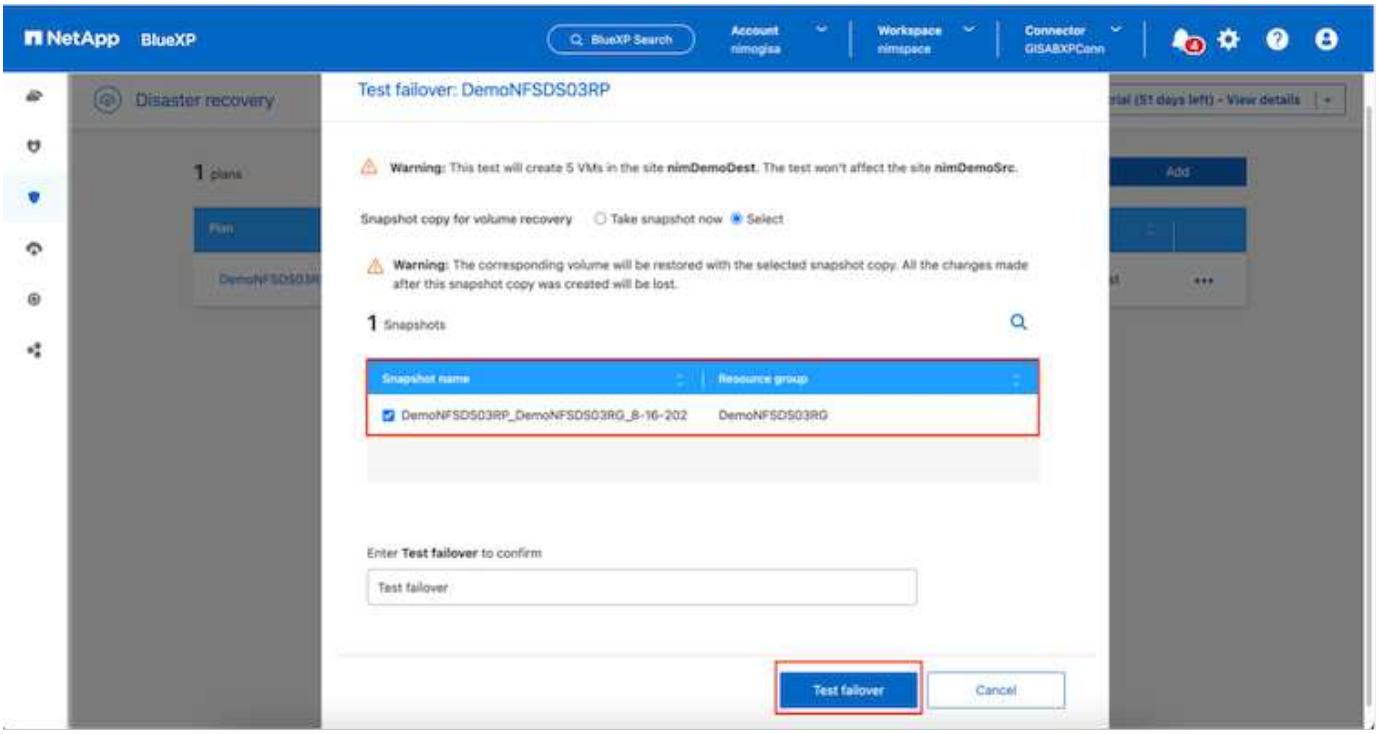
- Test-Failover (einschließlich regelmäßiger automatisierter Simulationen)
- Failovertest bereinigen
- Ausfallsicherung
- Failback

Testen des Failovers

Test-Failover in BlueXP DRaaS ist ein Betriebsverfahren, das es VMware-Administratoren ermöglicht, ihre Wiederherstellungspläne vollständig zu validieren, ohne ihre Produktionsumgebungen zu stören.



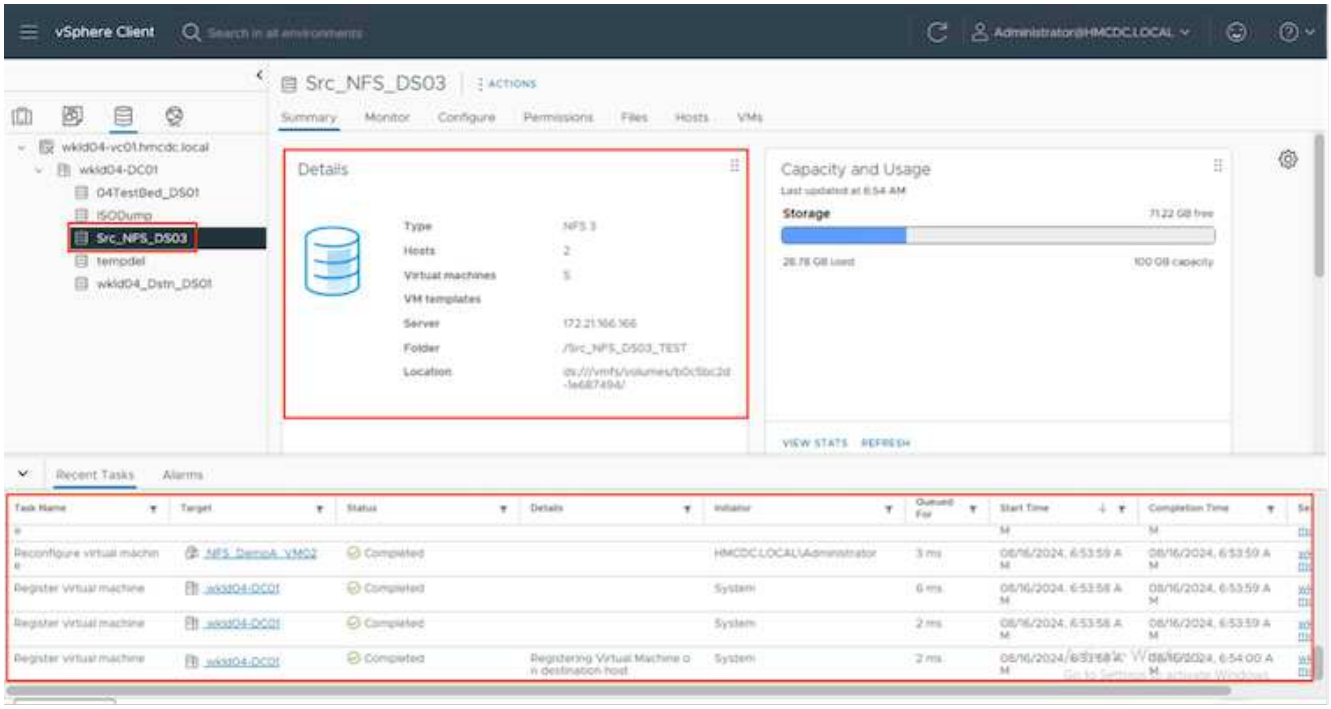
BlueXP DRaaS bietet die Möglichkeit, den Snapshot als optionale Funktion im Test-Failover-Vorgang auszuwählen. Mit dieser Funktion kann der VMware-Administrator überprüfen, ob alle kürzlich in der Umgebung vorgenommenen Änderungen auf die Zielsite repliziert werden und somit während des Tests vorhanden sind. Zu diesen Änderungen gehören Patches für das VM-Gastbetriebssystem



Wenn der VMware-Administrator einen Test-Failover-Vorgang ausführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

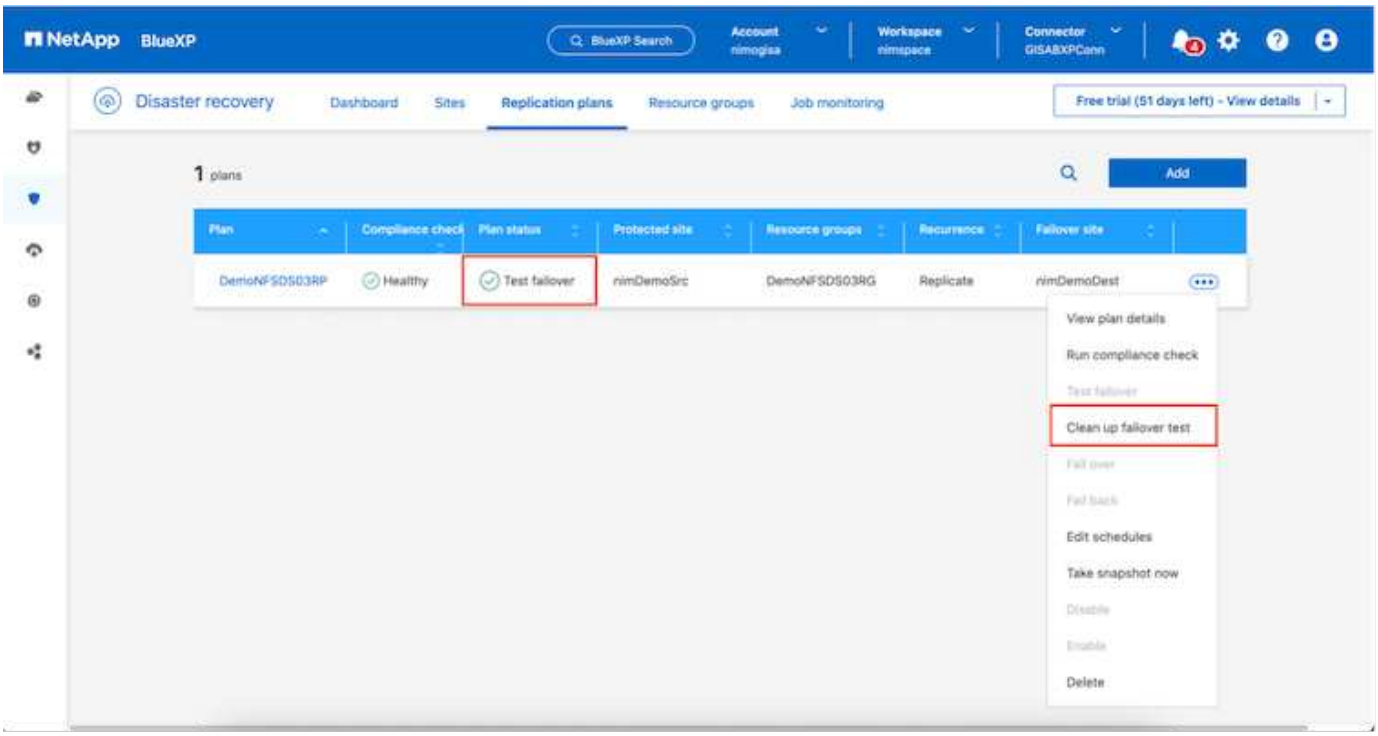
- Auslösen von SnapMirror -Beziehungen, um den Speicher am Zielstandort mit allen kürzlich am Produktionsstandort vorgenommenen Änderungen zu aktualisieren.

- Erstellen von NetApp FlexClone -Volumes der FlexVol -Volumes auf dem DR-Speicherarray.
- Verbinden der NFS-Datenspeicher in den FlexClone -Volumes mit den ESXi-Hosts am DR-Standort.
- Verbinden der VM-Netzwerkadapter mit dem während der Zuordnung angegebenen Testnetzwerk.
- Neukonfigurieren der Netzwerkeinstellungen des VM-Gastbetriebssystems wie für das Netzwerk am DR-Standort definiert.
- Ausführen aller benutzerdefinierten Befehle, die im Replikationsplan gespeichert wurden.
- Einschalten der VMs in der im Replikationsplan festgelegten Reihenfolge.



Bereinigungs-Failover-Testvorgang

Der Bereinigungs-Failover-Testvorgang wird ausgeführt, nachdem der Replikationsplantest abgeschlossen wurde und der VMware-Administrator auf die Bereinigungsaufforderung reagiert.



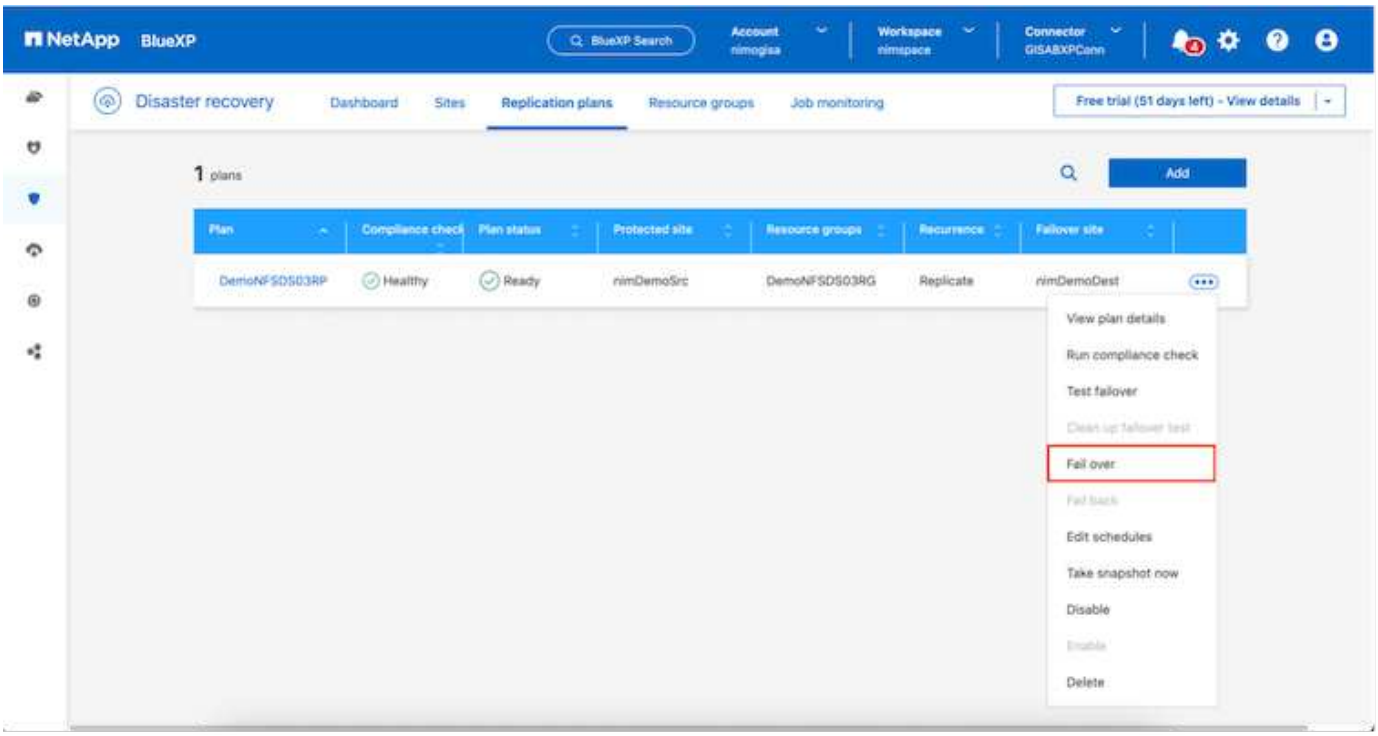
Durch diese Aktion werden die virtuellen Maschinen (VMs) und der Status des Replikationsplans auf den Bereitschaftszustand zurückgesetzt.

Wenn der VMware-Administrator einen Wiederherstellungsvorgang durchführt, führt BlueXP DRaaS den folgenden Prozess durch:

1. Es schaltet jede wiederhergestellte VM in der FlexClone -Kopie aus, die zum Testen verwendet wurde.
2. Es löscht das FlexClone Volume, das während des Tests zum Präsentieren der wiederhergestellten VMs verwendet wurde.

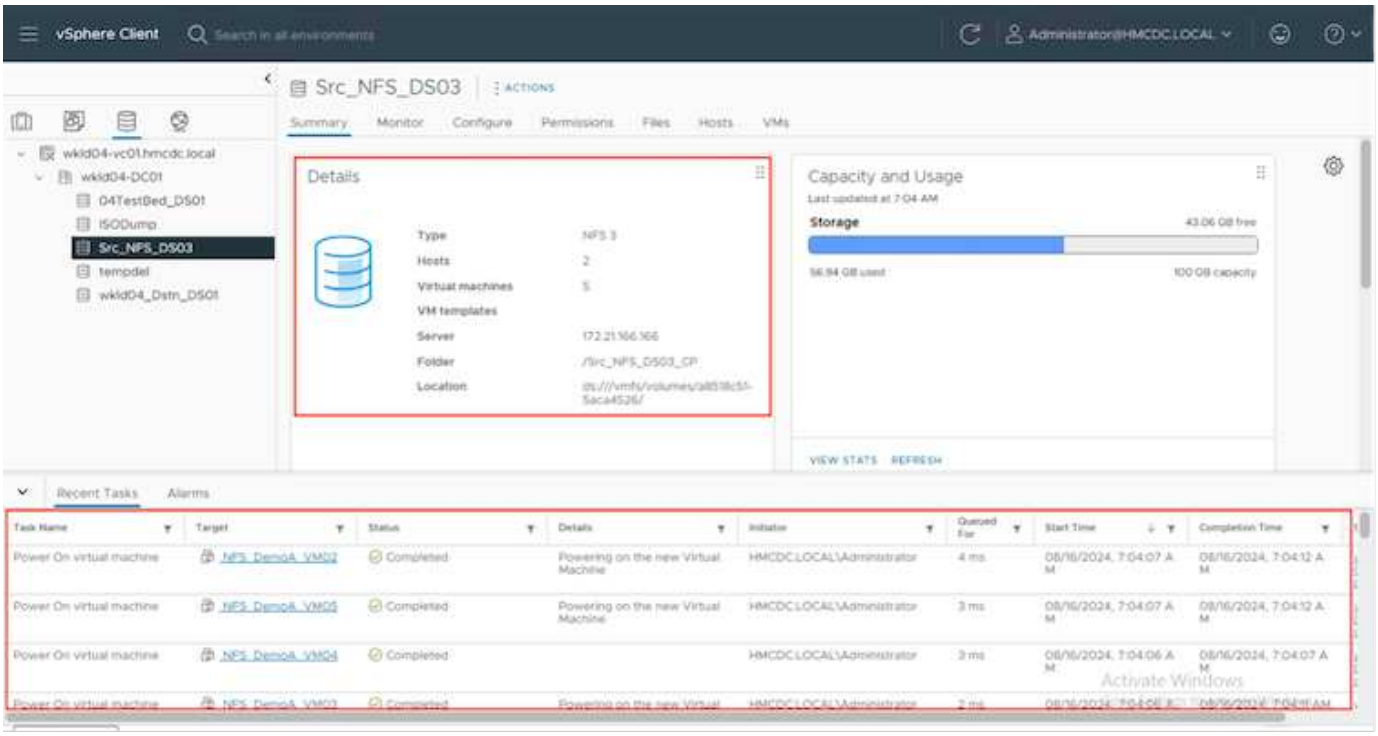
Geplante Migration und Failover

BlueXP DRaaS bietet zwei Methoden zur Durchführung eines echten Failovers: geplante Migration und Failover. Bei der ersten Methode, der geplanten Migration, werden das Herunterfahren der VM und die Synchronisierung der Speicherreplikation in den Prozess integriert, um die VMs wiederherzustellen oder effektiv an den Zielstandort zu verschieben. Für die geplante Migration ist Zugriff auf die Quellsite erforderlich. Die zweite Methode, Failover, ist ein geplantes/ungeplantes Failover, bei dem die VMs am Zielstandort aus dem letzten Speicherreplikationsintervall wiederhergestellt werden, das abgeschlossen werden konnte. Abhängig vom RPO, das in die Lösung integriert wurde, ist im DR-Szenario mit einem gewissen Datenverlust zu rechnen.



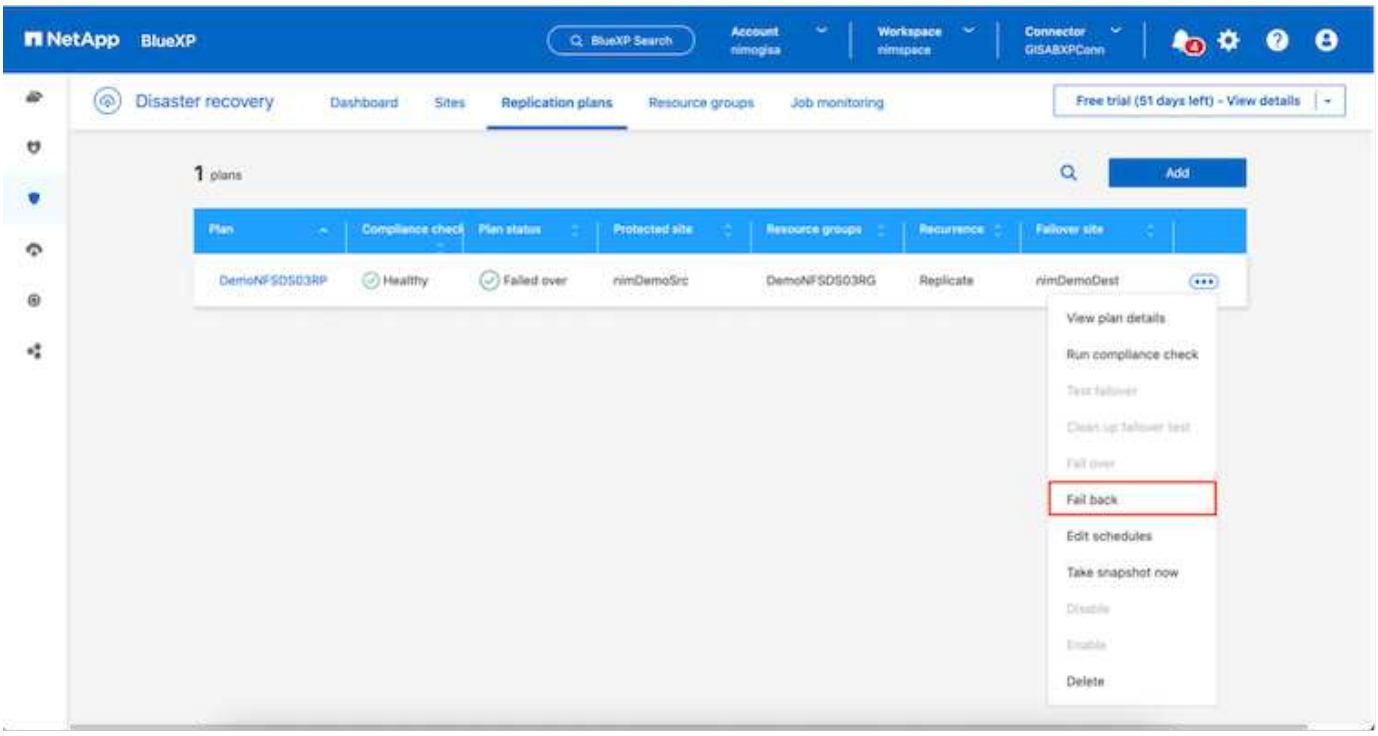
Wenn der VMware-Administrator einen Failover-Vorgang durchführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

- Unterbrechen und Failover der NetApp SnapMirror -Beziehungen.
- Verbinden Sie die replizierten NFS-Datenspeicher mit den ESXi-Hosts am DR-Standort.
- Verbinden Sie die VM-Netzwerkadapter mit dem entsprechenden Zielstandortnetzwerk.
- Konfigurieren Sie die Netzwerkeinstellungen des VM-Gastbetriebssystems neu, wie für das Netzwerk am Zielstandort definiert.
- Führen Sie alle benutzerdefinierten Befehle (sofern vorhanden) aus, die im Replikationsplan gespeichert wurden.
- Schalten Sie die VMs in der im Replikationsplan festgelegten Reihenfolge ein.



Failback

Ein Failback ist ein optionales Verfahren, das nach einer Wiederherstellung die ursprüngliche Konfiguration der Quell- und Zielsites wiederherstellt.



VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie bereit sind, die Dienste auf der ursprünglichen Quellsite wiederherzustellen.

HINWEIS: BlueXP DRaaS repliziert (resynchronisiert) alle Änderungen zurück zur ursprünglichen virtuellen Quellmaschine, bevor die Replikationsrichtung umgekehrt wird. Dieser Prozess beginnt mit einer Beziehung,

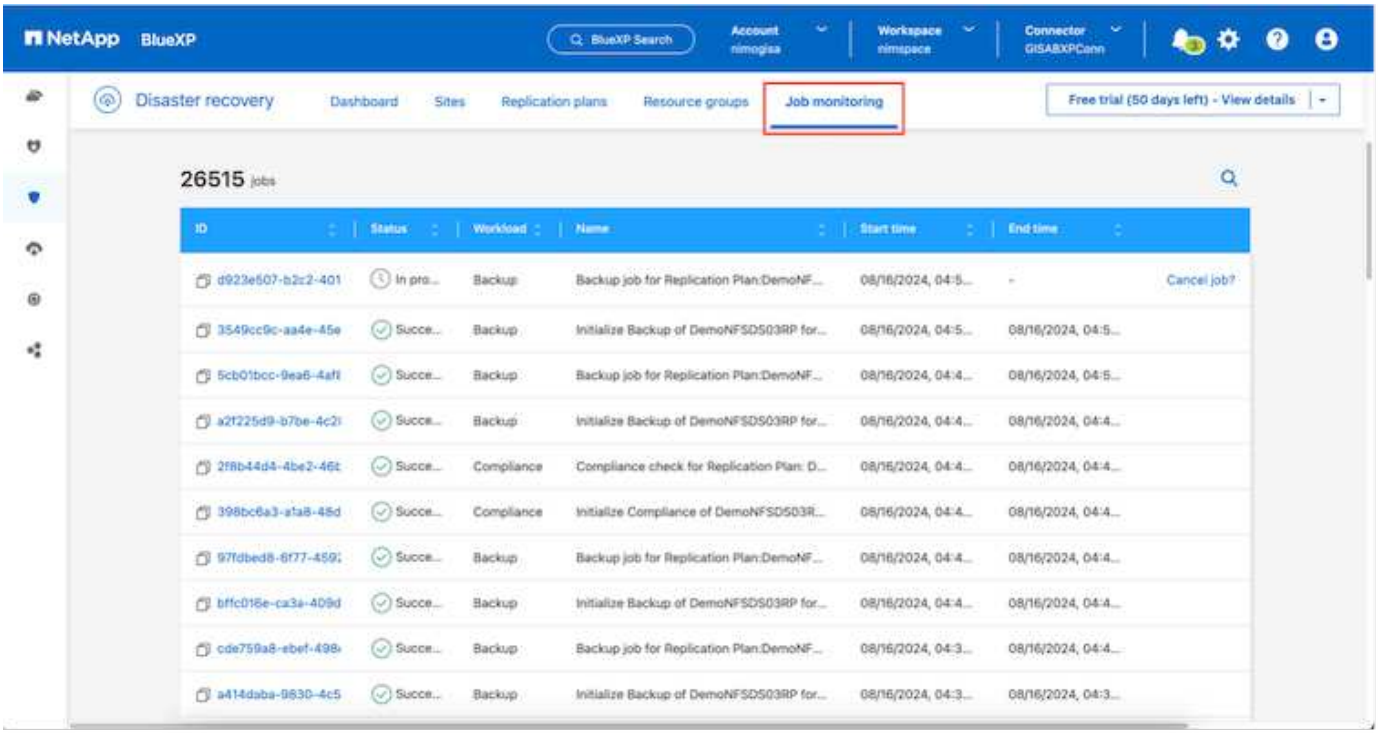
deren Failover zu einem Ziel abgeschlossen ist, und umfasst die folgenden Schritte:

- Schalten Sie die virtuellen Maschinen aus und heben Sie die Registrierung auf. Die Volumes auf der Zielsite werden ausgehängt.
- Unterbrechen Sie die SnapMirror -Beziehung zur Originalquelle, um Lese-/Schreibzugriff zu ermöglichen.
- Synchronisieren Sie die SnapMirror -Beziehung erneut, um die Replikation umzukehren.
- Mounten Sie das Volume auf der Quelle, schalten Sie die virtuellen Quellmaschinen ein und registrieren Sie sie.

Weitere Informationen zum Zugriff auf und zur Konfiguration von BlueXP DRaaS finden Sie im"Erfahren Sie mehr über BlueXP Disaster Recovery für VMware" .

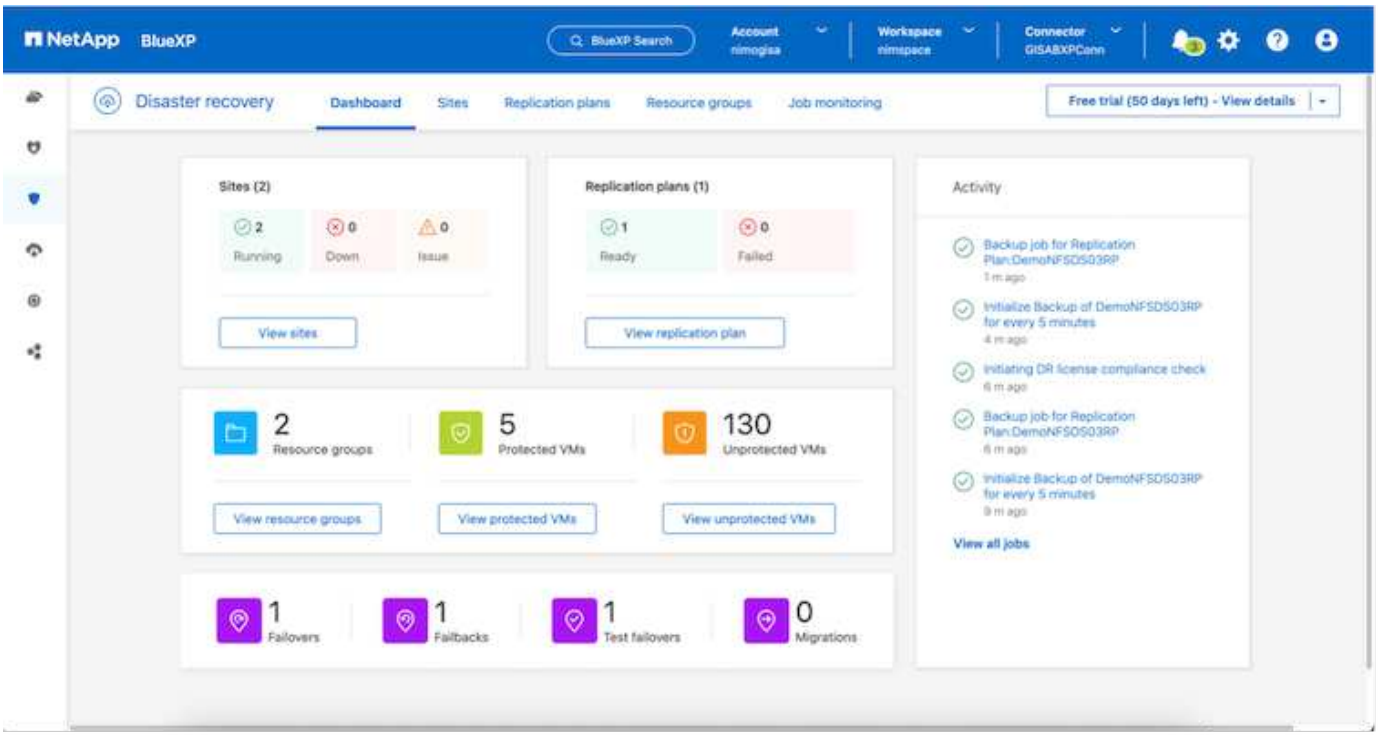
Überwachung und Dashboard

Von BlueXP oder der ONTAP CLI aus können Sie den Replikationszustand für die entsprechenden Datenspeichervolumes überwachen und den Status eines Failovers oder Testfailovers über die Jobüberwachung verfolgen.



Wenn ein Auftrag gerade ausgeführt wird oder sich in der Warteschlange befindet und Sie ihn stoppen möchten, können Sie ihn mit der Option „Abbrechen“ abbrechen.

Mit dem BlueXP disaster recovery können Sie den Status von Notfallwiederherstellungsstandorten und Replikationsplänen zuverlässig bewerten. Dadurch können Administratoren schnell fehlerfreie, nicht verbundene oder beeinträchtigte Sites und Pläne identifizieren.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Prozess zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen oder die"Lösungssimulator" .

Schützen Sie Workloads mit vSphere Metro Storage Cluster

Erfahren Sie mehr über die Integration der hohen Verfügbarkeit von ONTAP mit VMware vSphere Metro Storage Cluster (vMSC).

Informieren Sie sich über die NetApp -Lösungen, mit denen Sie die Hochverfügbarkeit von NetApp ONTAP mit VMware vSphere Metro Storage Cluster (vMSC) integrieren können. Dies bietet robuste Lösungen für die Verwaltung von VMware Cloud Foundation (VCF) und VI-Workloaddomänen.

Diese Kombination gewährleistet kontinuierliche Datenverfügbarkeit, nahtloses Failover und Notfallwiederherstellung an geografisch verteilten Standorten und verbessert so die Ausfallsicherheit und Betriebskontinuität für kritische Workloads. SnapMirror Active Sync ermöglicht die Weiterführung des Betriebs von Geschäftsdiensten auch bei einem vollständigen Site-Ausfall und unterstützt Anwendungen bei einem transparenten Failover mithilfe einer sekundären Kopie. Mit SnapMirror Active Sync sind keine manuellen Eingriffe oder benutzerdefinierten Skripts erforderlich, um ein Failover auszulösen.

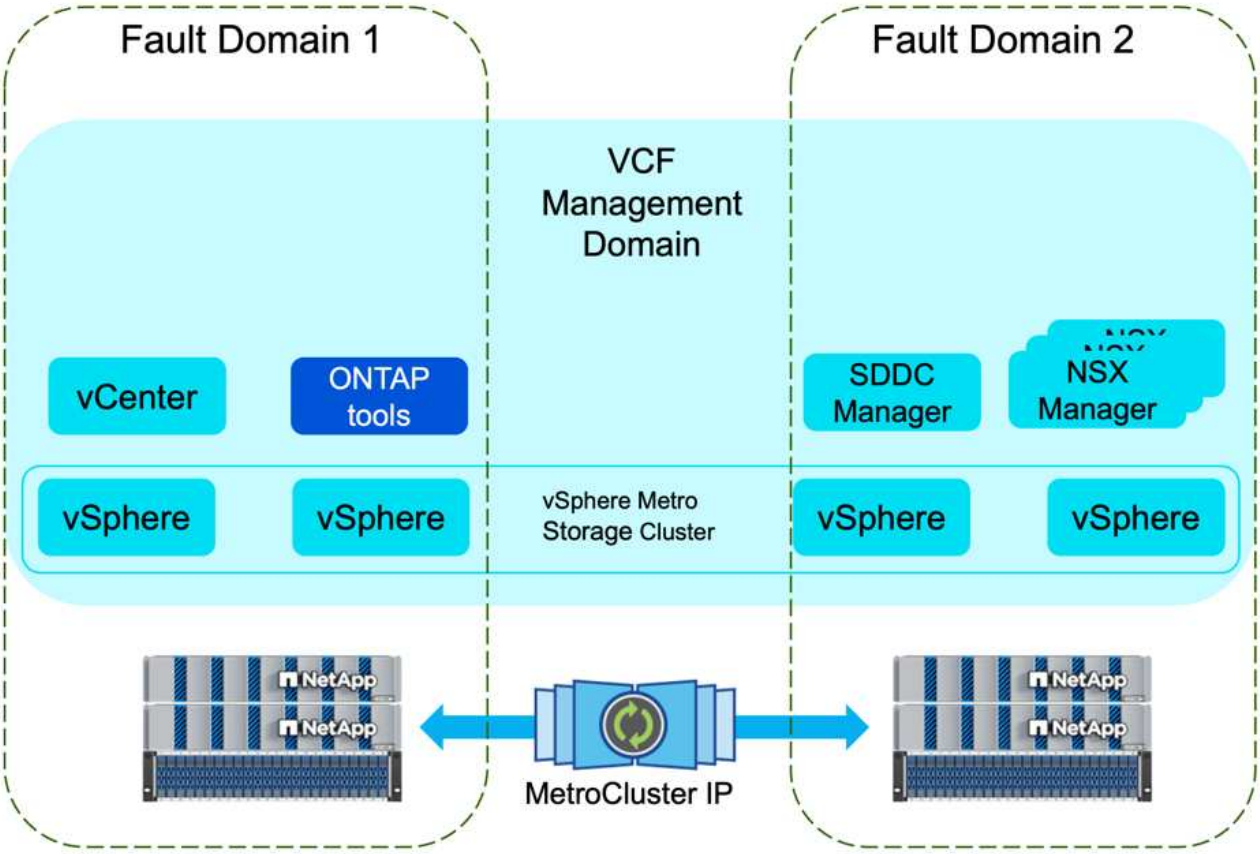
Weitere Einzelheiten finden Sie in den folgenden Lösungen.

- "Stretch-Cluster für die Verwaltungsdomäne mit SnapMirror Active Sync"
- "Stretch-Cluster für die Verwaltungsdomäne mit MetroCluster"
- "Stretch Cluster für VI-Workloaddomäne mit SnapMirror Active Sync"

- "Stretch Cluster für VI-Workloaddomäne mit MetroCluster"

Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne mit MetroCluster

In diesem Anwendungsfall beschreiben wir das Verfahren zum Konfigurieren eines Stretch-Clusters für die VMware Cloud Foundation (VCF)-Verwaltungsdomäne unter Verwendung von ONTAP MetroCluster mit NFS als primärem Datenspeicher. Dieses Verfahren umfasst die Bereitstellung von vSphere-Hosts und vCenter Server, die Bereitstellung von NFS-Datenspeichern, die Validierung des Clusters mit dem VCF-Importtool, die Konfiguration der NSX-Einstellungen und die Konvertierung der Umgebung in eine VCF-Verwaltungsdomäne.



Einführung

In dieser Lösung zeigen wir, wie man eine gestreckte VCF-Verwaltungsdomäne mit NFS als Hauptdatenspeicher unter Verwendung von ONTAP MetroCluster implementiert.

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Stellen Sie vSphere-Hosts und vCenter-Server bereit.
- Stellen Sie den vSphere-Hosts einen NFS-Datenspeicher bereit.

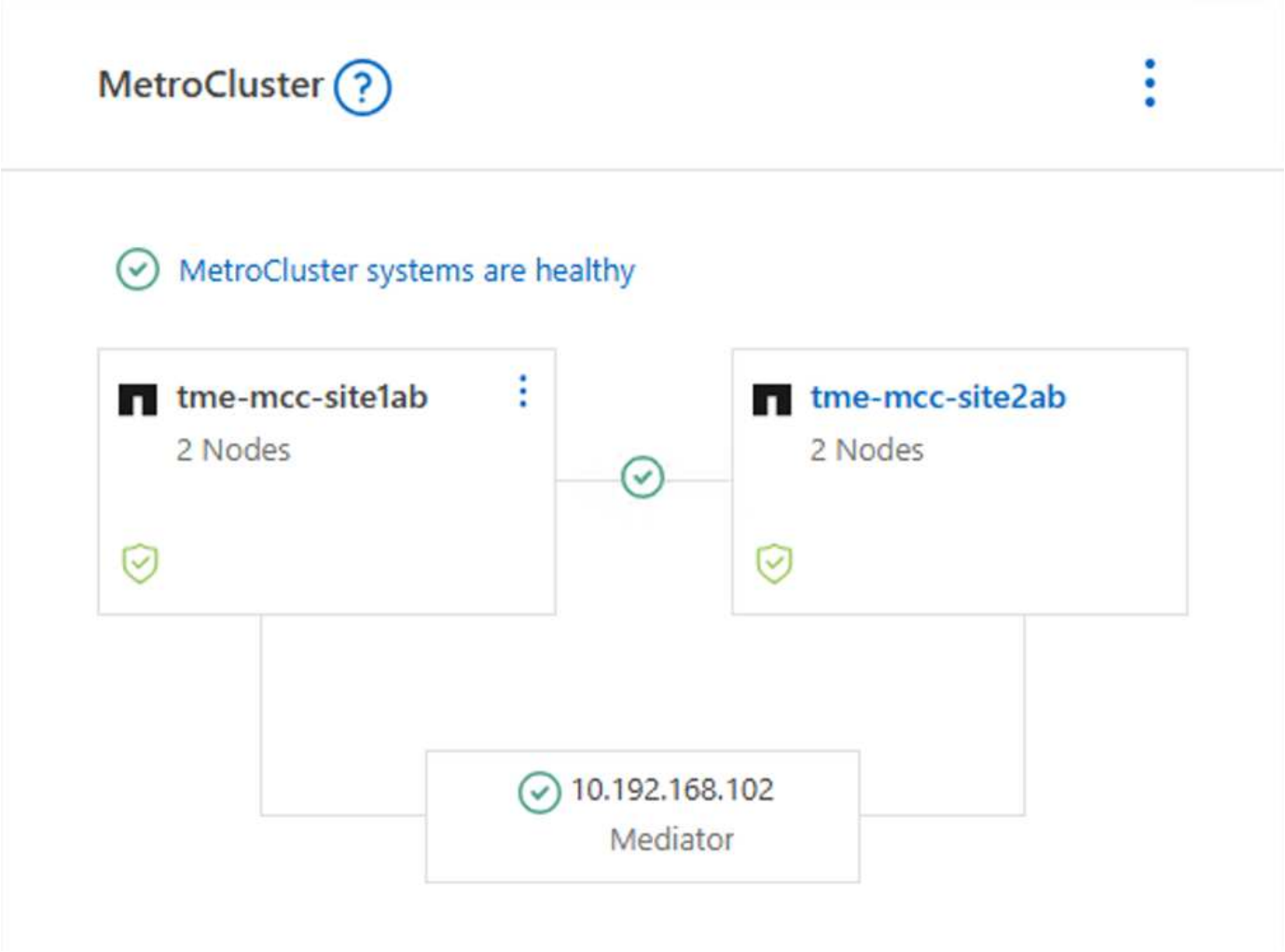
- Stellen Sie den SDDC Manager im vSphere-Cluster bereit.
- Verwenden Sie das VCF-Importtool, um den vSphere-Cluster zu validieren.
- Konfigurieren Sie eine JSON-Datei zum Erstellen eines NSX während der VCF-Konvertierung.
- Verwenden Sie das VCF-Importtool, um die vSphere 8-Umgebung in eine VCF-Verwaltungsdomäne zu konvertieren.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Unterstützte ONTAP MetroCluster Konfiguration
- Storage Virtual Machine (SVM) ist so konfiguriert, dass NFS-Verkehr zugelassen wird.
- Im IP-Netzwerk wurde eine logische Schnittstelle (LIF) erstellt, die den NFS-Verkehr übertragen soll und mit der SVM verknüpft ist.
- Ein vSphere 8-Cluster mit 4 x ESXi-Hosts, die mit einem Netzwerk-Switch verbunden sind.
- Laden Sie die für die VCF-Konvertierung erforderliche Software herunter.

Hier ist der Beispiel-Screenshot vom System Manager, der die MetroCluster -Konfiguration zeigt.



und hier sind die SVM-Netzwerkschnittstellen aus beiden Fehlerdomänen.

Network interfaces Subnets

+ Add

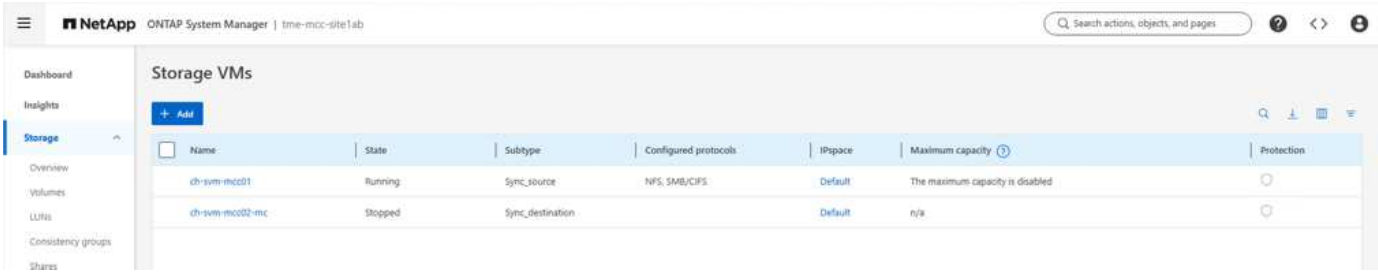
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

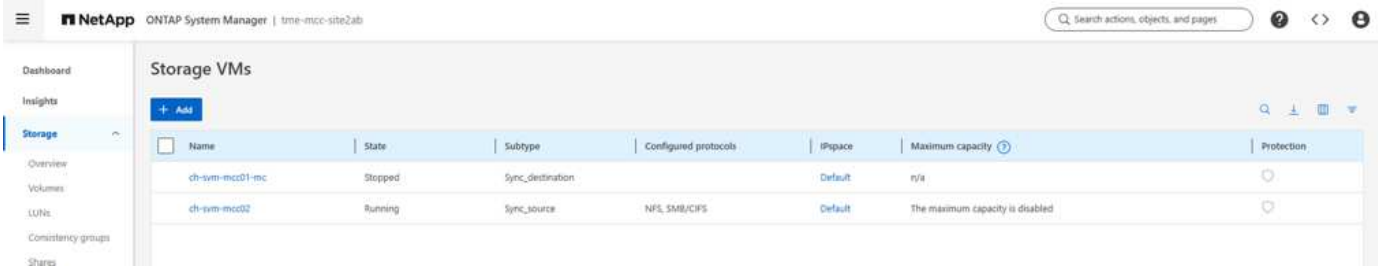
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[HINWEIS] SVM wird auf einer der Fehlerdomänen in MetroCluster aktiv sein.





Verweisen "vMSC mit MetroCluster" .

Informationen zum unterstützten Speicher und andere Überlegungen zum Konvertieren oder Importieren von vSphere in VCF 5.2 finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Bevor Sie einen vSphere-Cluster erstellen, der in eine VCF-Verwaltungsdomäne konvertiert wird, lesen Sie "NSX-Überlegungen für vSphere-Cluster"

Die erforderliche Software finden Sie unter "Laden Sie Software zum Konvertieren oder Importieren vorhandener vSphere-Umgebungen herunter" .

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Bereitstellungsschritte

So stellen Sie eine VCF Stretched Management Domain mit NFS als Hauptdatenspeicher bereit:

Führen Sie die folgenden Schritte aus:

- Stellen Sie vSphere-Hosts und vCenter bereit.
- Erstellen Sie einen vSphere-Cluster.
- Stellen Sie einen NFS-Datenspeicher bereit.
- Kopieren Sie das VCF-Importtool auf die vCenter-Appliance.
- Führen Sie mit dem VCF-Importtool eine Vorprüfung auf der vCenter-Appliance durch.
- Stellen Sie die SDDC-Manager-VM auf dem vCenter-Cluster bereit.
- Erstellen Sie eine JSON-Datei für einen NSX-Cluster, der während des Konvertierungsvorgangs bereitgestellt werden soll.
- Laden Sie die erforderliche Software in den SDDC-Manager hoch.
- Konvertieren Sie den vSphere-Cluster in eine VCF-Verwaltungsdomäne.

Eine Übersicht über den Konvertierungsprozess finden Sie unter "Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workload-Domäne in VMware Cloud Foundation" .

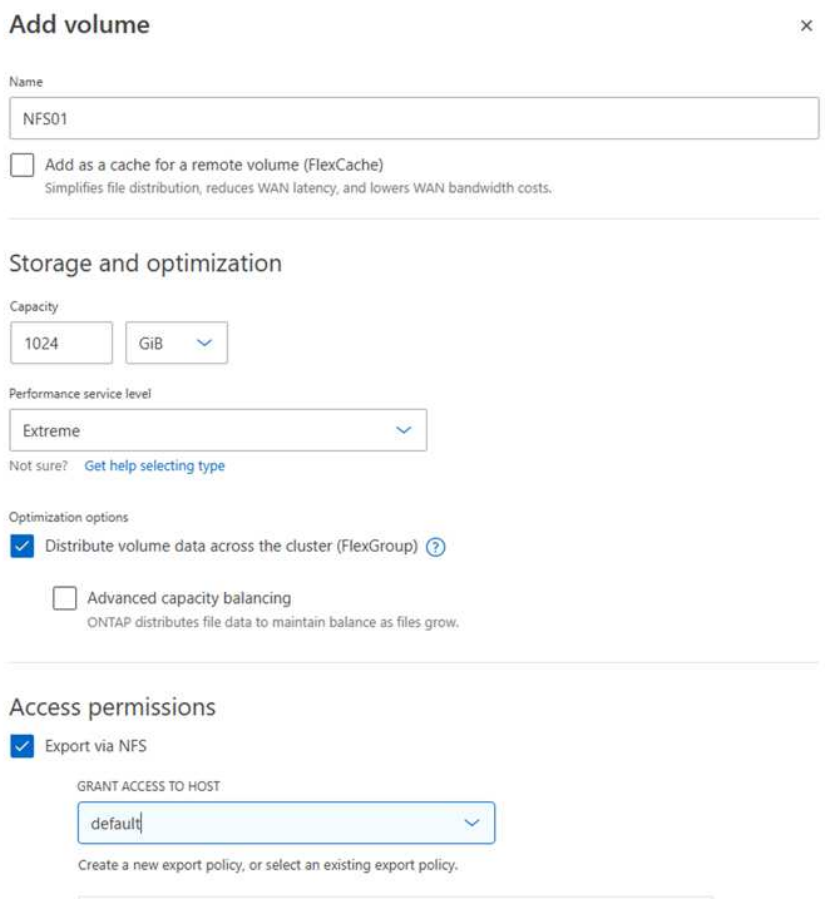
Bereitstellen von vSphere-Hosts und vCenter

Stellen Sie vSphere auf Hosts bereit, indem Sie ISO vom Broadcom-Supportportal herunterladen, oder verwenden Sie die vorhandene Bereitstellungsoption für den vSphere-Host.

Mounten Sie den NFS-Datenspeicher, um VMs zu hosten

In diesem Schritt erstellen wir das NFS-Volume und mounten es als Datenspeicher zum Hosten von VMs.

1. Erstellen Sie mithilfe des System Managers ein Volume und fügen Sie es einer Exportrichtlinie hinzu, die das IP-Subnetz des vSphere-Hosts
   enthält.



2. Stellen Sie eine SSH-Verbindung zum vSphere-Host her und mounten Sie den NFS-Datenspeicher.

```
[root@SiteA-vs01:~] esxcli storage nfs add -c 4 -H 10.192.164.225 -s /NFS01 -v NFS01
[root@SiteA-vs01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Not Supported
[root@SiteA-vs01:~]
```

3. Wiederholen Sie die obigen Schritte für zusätzlichen Datenspeicherbedarf und stellen Sie sicher, dass die Hardwarebeschleunigung unterstützt
   wird.

```
[root@MCCA01:~] esxcli storage nfs list
Volume Name  Host            Share   Vmknic  Accessible  Mounted  Connections  Read-Only   isPE  Hardware Acceleration
-----------  --------------  ------  ------  ----------  -------  -----------  ---------  -----  ---------------------
NFS02        10.192.164.230  /NFS02  None          true     true            4      false  false  Supported
NFS01        10.192.164.225  /NFS01  None          true     true            4      false  false  Supported
[root@MCCA01:~]
```

Stellen Sie vCenter auf einem NFS-Datenspeicher bereit. Stellen Sie sicher, dass SSH und Bash-Shell auf dem vCenter-Gerät aktiviert sind.

vSphere-Cluster erstellen

1. Melden Sie sich beim vSphere-Webclient an. Erstellen Sie das DataCenter und den vSphere-Cluster, indem Sie einen der Hosts hinzufügen, auf dem NFS VAAI bereitgestellt ist. Wir haben uns dafür entschieden, alle Hosts im Cluster mit der Option „Einzelbild“ zu verwalten. [TIPP] Wählen Sie „Konfiguration auf Clusterebene verwalten“ nicht aus. Weitere Einzelheiten finden Sie unter "NSX-Überlegungen für vSphere-Cluster" . Informationen zu vMSC-Best Practices mit ONTAP MetroCluster finden Sie unter "vMSC-Design- und Implementierungsrichtlinien"
2. Fügen Sie dem Cluster weitere vSphere-Hosts hinzu.
3. Erstellen Sie einen verteilten Switch und fügen Sie die Portgruppen hinzu.
4. "Migrieren Sie das Netzwerk vom Standard-vSwitch zum verteilten Switch."

Konvertieren Sie die vSphere-Umgebung in eine VCF-Verwaltungsdomäne

Der folgende Abschnitt behandelt die Schritte zum Bereitstellen des SDDC-Managers und zum Konvertieren des vSphere 8-Clusters in eine VCF 5.2-Verwaltungsdomäne. Gegebenenfalls wird für weitere Einzelheiten auf die VMware-Dokumentation verwiesen.

Das VCF-Importtool von VMware by Broadcom ist ein Dienstprogramm, das sowohl auf der vCenter-Appliance als auch auf dem SDDC-Manager verwendet wird, um Konfigurationen zu validieren und Konvertierungs- und Importdienste für vSphere- und VCF-Umgebungen bereitzustellen.

Weitere Informationen finden Sie unter "Optionen und Parameter des VCF-Importtools" .

VCF-Importtool kopieren und extrahieren

Das VCF-Importtool wird auf der vCenter-Appliance verwendet, um zu überprüfen, ob sich der vSphere-Cluster für den VCF-Konvertierungs- oder Importvorgang in einem fehlerfreien Zustand befindet.

Führen Sie die folgenden Schritte aus:

1. Folgen Sie den Schritten unter "Kopieren Sie das VCF-Importtool auf die Ziel-vCenter-Appliance" bei VMware Docs, um das VCF-Importtool an den richtigen Speicherort zu kopieren.
2. Extrahieren Sie das Paket mit dem folgenden Befehl:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validieren der vCenter-Appliance

Verwenden Sie das VCF-Importtool, um die vCenter-Appliance vor der Konvertierung zu validieren.

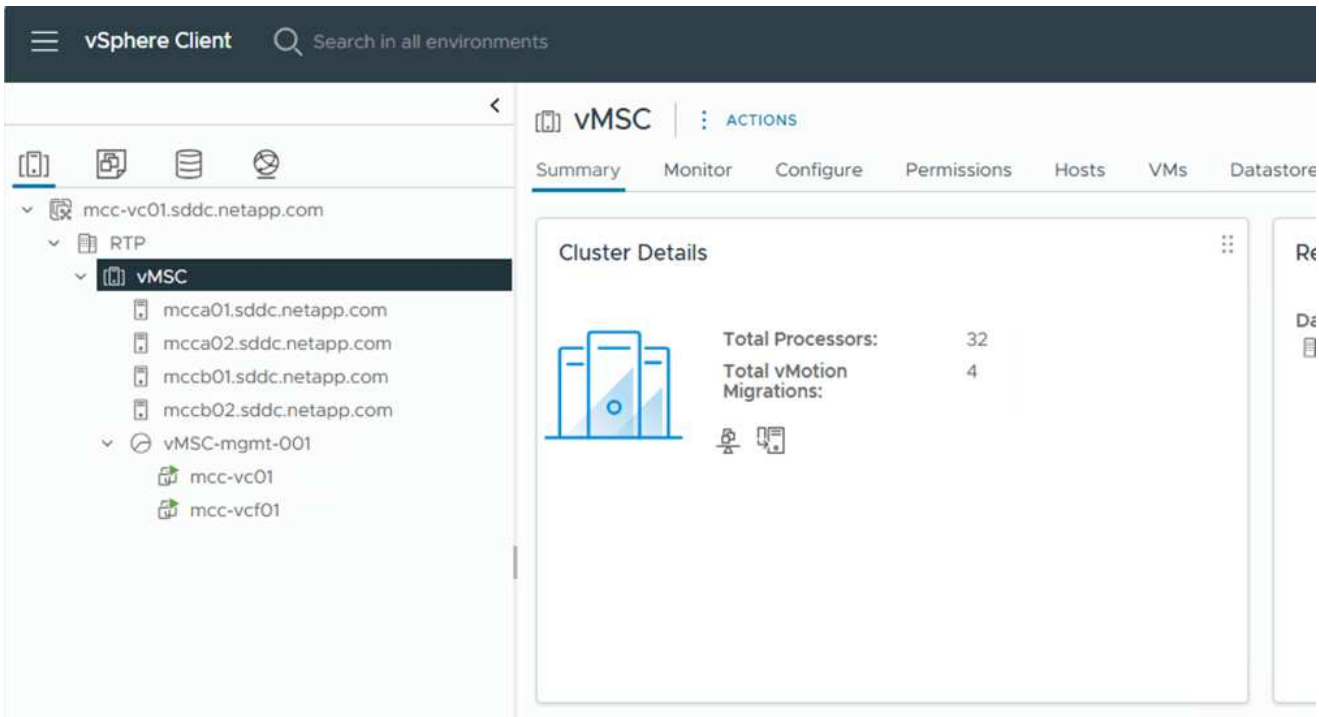
1. Folgen Sie den Schritten unter "Führen Sie vor der Konvertierung eine Vorprüfung des Ziel-vCenters durch" um die Validierung auszuführen.
2. Die folgende Ausgabe zeigt, dass die vCenter-Appliance die Vorprüfung bestanden hat.

```
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]# python3 vcf_brownfield.py precheck --vcenter mcc-vc01.sddc.netapp.com --sso-user administrator@vsphere.local
[2025-03-20 23:02:02,518] [INFO] vcf_brownfield: Brownfield Import main version: 5.2.1.2-24494579
[2025-03-20 23:02:02,521] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
Enter vCenter SSO password:
[2025-03-20 23:02:05,971] [INFO] vc_precheck: Starting VCF Brownfield precheck script version 1.0.0...
[2025-03-20 23:02:06,089] [INFO] vc_precheck: Connected to vCenter mcc-vc01.sddc.netapp.com in 0.12 seconds
[2025-03-20 23:02:06,092] [INFO] vc_precheck: Running pre-checks for vCenter mcc-vc01.sddc.netapp.com...
[2025-03-20 23:02:06,092] [INFO] vc_precheck: [1/10] VC BOM version check...                    PASS
[2025-03-20 23:02:06,135] [INFO] vc_precheck: [2/10] vSAN stretched cluster check...            PASS
[2025-03-20 23:02:06,156] [INFO] vc_precheck: [3/10] Supported storage available check...       PASS
[2025-03-20 23:02:06,170] [INFO] vc_precheck: [4/10] vCenter VM location check...               PASS
[2025-03-20 23:02:06,424] [INFO] vc_precheck: [5/10] VxRail registration check...               PASS
[2025-03-20 23:02:06,614] [INFO] vc_precheck: [6/10] NSX-T registration check...                PASS
[2025-03-20 23:02:06,638] [INFO] vc_precheck: [7/10] Standalone host check...                   PASS
[2025-03-20 23:02:08,820] [INFO] vc_precheck: [8/10] All cluster hosts connected to vDS check...  PASS
[2025-03-20 23:02:10,246] [INFO] vc_precheck: [9/10] ELM ring topology check...                 PASS
[2025-03-20 23:02:10,879] [INFO] vc_precheck: [10/10] WCP import check...                       PASS
[2025-03-20 23:02:10,880] [INFO] vc_precheck: All pre-checks passed!
[2025-03-20 23:02:10,881] [INFO] vc_precheck: Pre-checks for vCenter mcc-vc01.sddc.netapp.com completed in 4.79 seconds
root@mcc-vc01 [ ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset ]#
```

Bereitstellen des SDDC Managers

Der SDDC-Manager muss sich am selben Standort wie der vSphere-Cluster befinden, der in eine VCF-Verwaltungsdomäne umgewandelt wird.

Befolgen Sie die Bereitstellungsanweisungen in den VMware-Dokumenten, um die Bereitstellung abzuschließen.



Siehe "Stellen Sie die SDDC Manager Appliance auf dem Ziel-vCenter bereit" .

Erstellen einer JSON-Datei für die NSX-Bereitstellung

Um NSX Manager bereitzustellen, während Sie eine vSphere-Umgebung in VMware Cloud Foundation importieren oder konvertieren, erstellen Sie eine NSX-Bereitstellungsspezifikation. Für die NSX-Bereitstellung sind mindestens 3 Hosts erforderlich.

> Beim Bereitstellen eines NSX Manager-Clusters in einem Konvertierungs- oder Importvorgang wird ein NSX VLAN-gestütztes Segment verwendet. Einzelheiten zu den Einschränkungen des NSX-VLAN-gestützten Segments finden Sie im Abschnitt „Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation“. Informationen zu NSX-VLAN-Netzwerkbeschränkungen finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Nachfolgend sehen Sie ein Beispiel einer JSON-Datei für die NSX-Bereitstellung:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "******************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.114",
  "cluster_fqdn": "mcc-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-nsxa.sddc.netapp.com",
    "name": "mcc-nsxa",
    "ip_address": "10.61.185.111",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxb.sddc.netapp.com",
    "name": "mcc-nsxb",
    "ip_address": "10.61.185.112",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-nsxc.sddc.netapp.com",
    "name": "mcc-nsxc",
    "ip_address": "10.61.185.113",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Kopieren Sie die JSON-Datei in den VCF-Benutzer-Home-Ordner im SDDC Manager.

Laden Sie Software in den SDDC Manager hoch

Kopieren Sie das VCF-Importtool in den Home-Ordner des VCF-Benutzers und das NSX-Bereitstellungspaket in den Ordner /nfs/vmware/vcf/nfs-mount/bundle/ im SDDC Manager.

Sehen "Laden Sie die erforderliche Software auf die SDDC Manager Appliance hoch" für detaillierte Anweisungen.

Detaillierte Überprüfung von vCenter vor der Konvertierung

Bevor Sie eine Konvertierung der Managementdomäne oder einen Importvorgang für die VI-Workloaddomäne durchführen, müssen Sie eine detaillierte Prüfung durchführen, um sicherzustellen, dass die Konfiguration der vorhandenen vSphere-Umgebung für die Konvertierung oder den Import unterstützt wird. . Stellen Sie als Benutzer vcf eine SSH-Verbindung zum SDDC Manager-Gerät her. . Navigieren Sie zu dem Verzeichnis, in das Sie das VCF-Importtool kopiert haben. . Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die vSphere-Umgebung konvertiert werden kann

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```

Konvertieren Sie den vSphere-Cluster in eine VCF-Verwaltungsdomäne

Zur Durchführung des Konvertierungsprozesses wird das VCF-Importtool verwendet.

Der folgende Befehl wird ausgeführt, um den vSphere-Cluster in eine VCF-Verwaltungsdomäne zu konvertieren und den NSX-Cluster bereitzustellen:

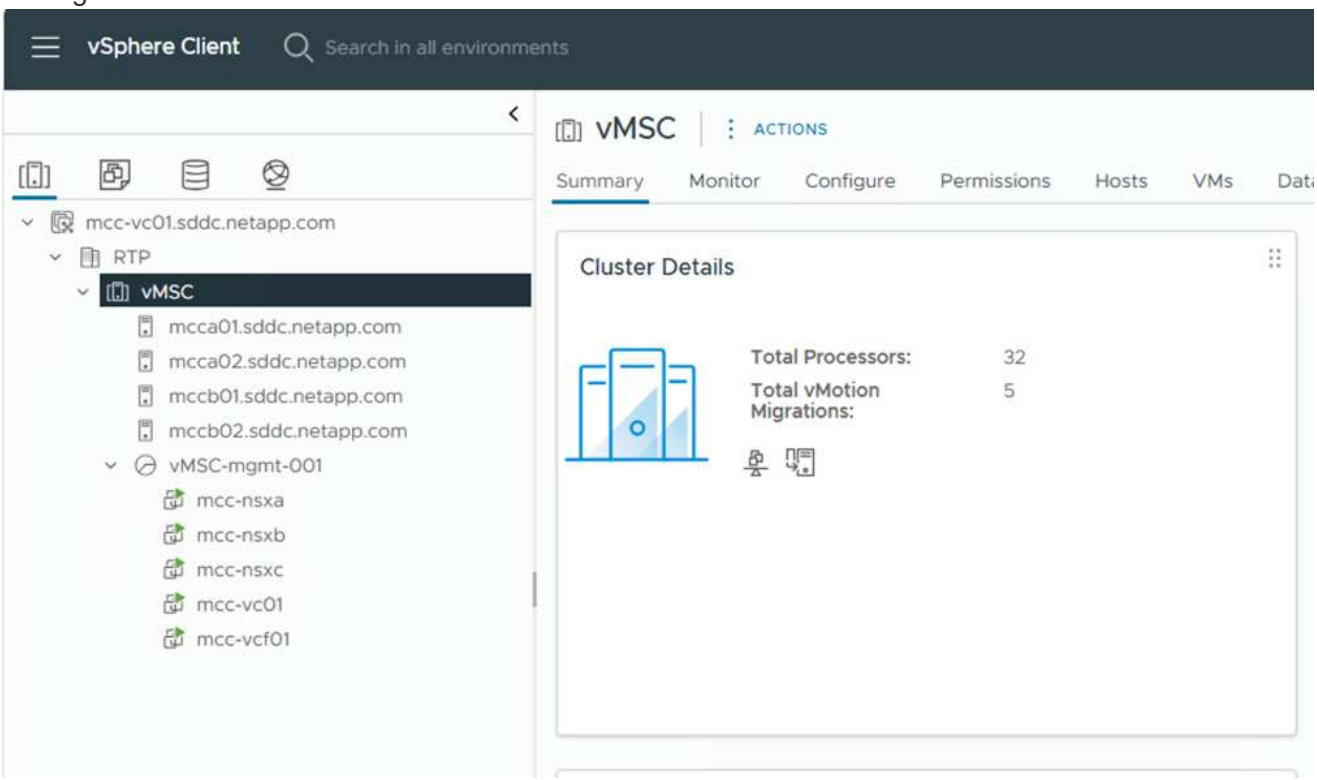
```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

Wenn auf dem vSphere-Host mehrere Datenspeicher verfügbar sind, wird gefragt, welcher Datenspeicher als primärer Datenspeicher betrachtet werden soll, auf dem standardmäßig NSX-VMs bereitgestellt werden.

```
[2025-03-24 19:29:00,394] [INFO] vcenter_connection: Connecting to mcc-vc01.sddc.netapp.com as administrator@vsphere.local
[2025-03-24 19:29:00,583] [INFO] discover_domain: ==============================================================
[2025-03-24 19:29:00,583] [INFO] discover_domain: Starting inventory payload generation for vCenter: mcc-vc01.sddc.netapp.com, as domain of type: MANAGEMENT
[2025-03-24 19:29:00,586] [INFO] discover_domain: [1/5] Starting discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,596] [INFO] discover_domain: [1/5] Completed discovery of PSC and vCenter configuration data from vCenter: mcc-vc01.sddc.netapp.com in 0.01s
[2025-03-24 19:29:00,596] [INFO] discover_domain: ==============================================================
[2025-03-24 19:29:00,596] [INFO] discover_domain: [2/5] Starting discovery of clusters in vCenter: mcc-vc01.sddc.netapp.com
[2025-03-24 19:29:00,613] [INFO] discover_domain: >>>>>> [1/1] Starting discovery of cluster: vMSC
Please select a primary datastore for cluster vMSC:
1) NFS01
2) NFS02
Choose a number: 1
[2025-03-24 19:29:25,192] [INFO] discover_domain: >>>>>> [1/1] Discovered cluster: vMSC in 24.58s
[2025-03-24 19:29:25,193] [INFO] discover_domain: [2/5] Completed discovery of 1 clusters in vCenter: mcc-vc01.sddc.netapp.com in 24.6s
```

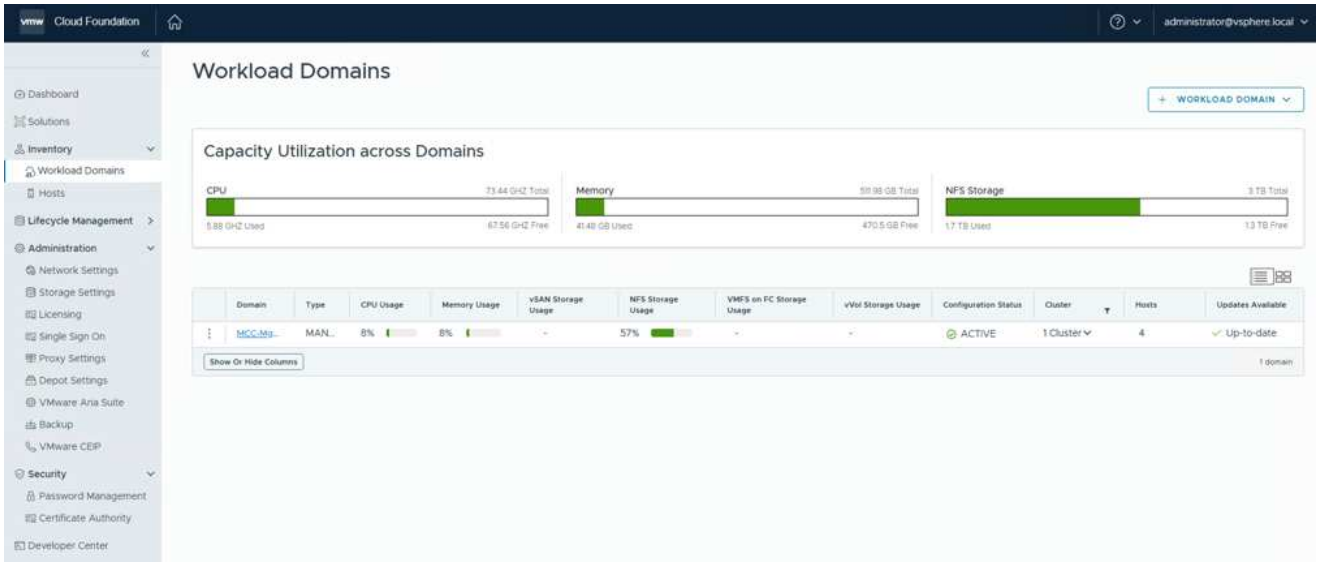
Vollständige Anweisungen finden Sie unter "VCF-Konvertierungsverfahren" .

NSX-VMs werden in vCenter bereitgestellt.

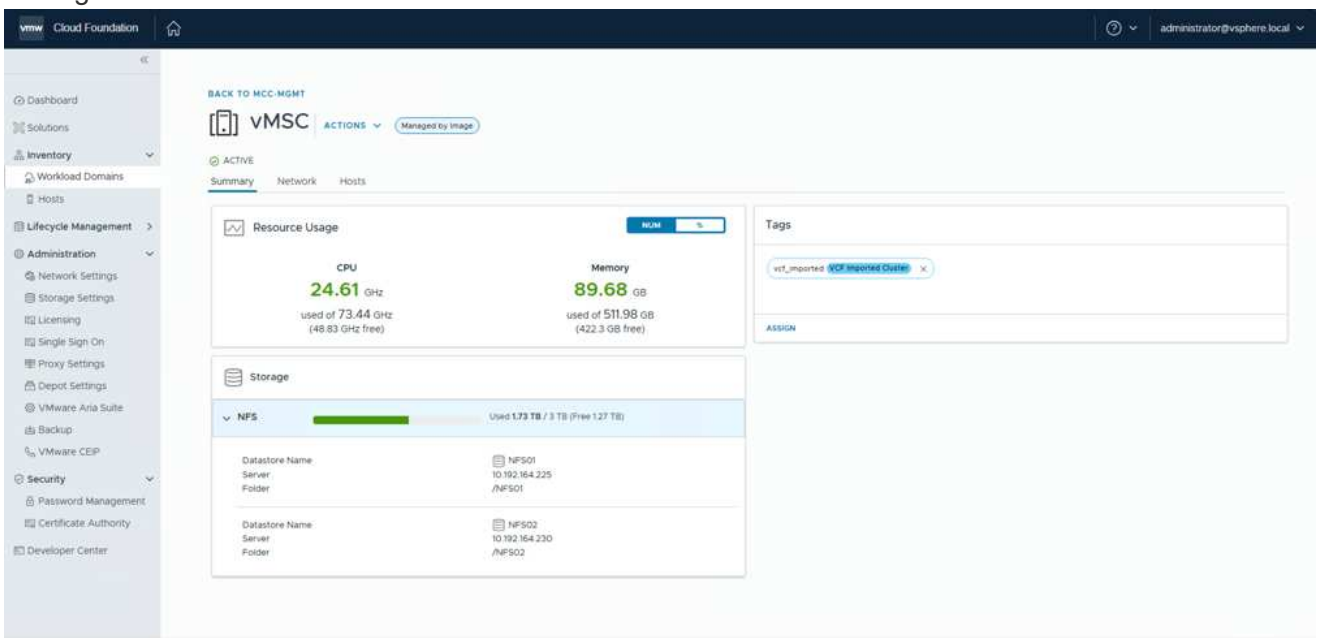


SDDC Manager zeigt die erstellte Verwaltungsdomäne mit dem angegebenen Namen und NFS als

Datenspeicher an.



Bei der Überprüfung des Clusters werden die Informationen zum NFS-Datenspeicher bereitgestellt.



Lizenzierung zu VCF hinzufügen

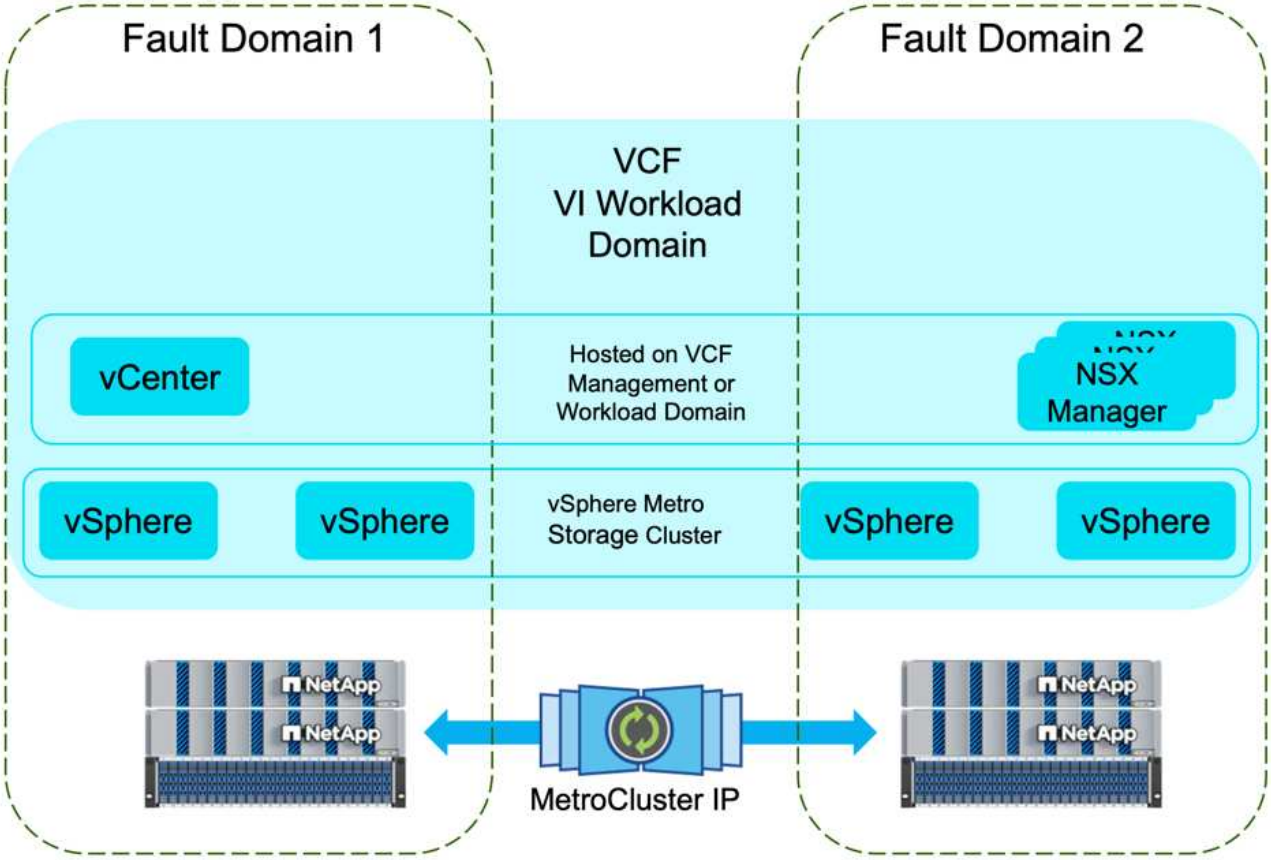
Nach Abschluss der Konvertierung muss der Umgebung eine Lizenzierung hinzugefügt werden.

1. Melden Sie sich bei der SDDC Manager-Benutzeroberfläche an.
2. Navigieren Sie im Navigationsbereich zu **Administration > Lizenzierung**.
3. Klicken Sie auf **+ Lizenzschlüssel**.
4. Wählen Sie ein Produkt aus dem Dropdown-Menü.
5. Geben Sie den Lizenzschlüssel ein.
6. Geben Sie eine Beschreibung für die Lizenz ein.
7. Klicken Sie auf **Hinzufügen**.
8. Wiederholen Sie diese Schritte für jede Lizenz.

Konfigurieren eines Stretch-Clusters für eine VI-Workloaddomäne mit MetroCluster

In diesem Anwendungsfall beschreiben wir das Verfahren zum Konfigurieren einer gestreckten VCF VI-Workloaddomäne mit NFS als Hauptdatenspeicher unter Verwendung von ONTAP MetroCluster. Dieses Verfahren umfasst die Bereitstellung von vSphere-Hosts und vCenter Server, die Bereitstellung von NFS-Datenspeichern, die Validierung des vSphere-Clusters, die Konfiguration von NSX während der VCF-Konvertierung und den Import der vSphere-Umgebung in eine vorhandene VCF-Verwaltungsdomäne.

Die Workloads auf VCF werden durch vSphere Metro Storage Cluster (vMSC) geschützt. ONTAP MetroCluster mit FC- oder IP-Bereitstellung wird normalerweise verwendet, um Fehlertoleranz von VMFS- und NFS-Datenspeichern bereitzustellen.



Einführung

In dieser Lösung zeigen wir, wie man eine gestreckte VCF VI-Workload-Domäne mit NFS als Hauptdatenspeicher unter Verwendung von ONTAP MetroCluster implementiert. Die VI-Workload-Domäne kann mithilfe von SDDC Manager bereitgestellt oder eine vorhandene vSphere-Umgebung als VI-Workload-Domäne importiert werden.

Szenarioübersicht

Dieses Szenario umfasst die folgenden allgemeinen Schritte:

- Stellen Sie vSphere-Hosts und vCenter-Server bereit.
- Stellen Sie den vSphere-Hosts einen NFS-Datenspeicher bereit.
- Verwenden Sie das VCF-Importtool, um den vSphere-Cluster zu validieren.
- Konfigurieren Sie eine JSON-Datei zum Erstellen eines NSX während der VCF-Konvertierung.
- Verwenden Sie das VCF-Importtool, um die vSphere 8-Umgebung als VCF VI-Workload-Domäne in eine vorhandene VCF-Verwaltungsdomäne zu importieren.

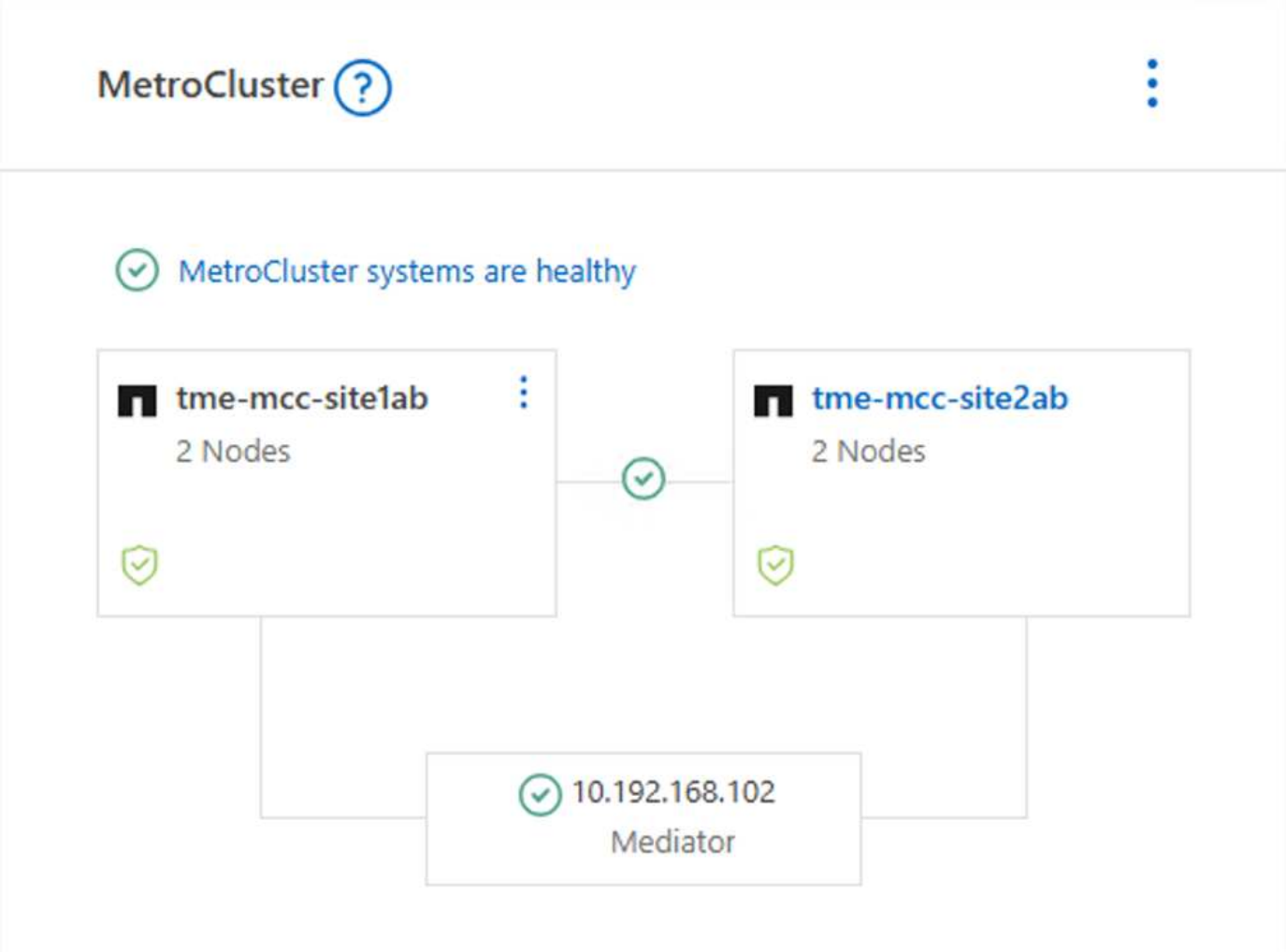
Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Unterstützte ONTAP MetroCluster Konfiguration

- Storage Virtual Machine (SVM) ist so konfiguriert, dass NFS-Verkehr zugelassen wird.
- Im IP-Netzwerk wurde eine logische Schnittstelle (LIF) erstellt, die den NFS-Verkehr übertragen soll und mit der SVM verknüpft ist.
- Ein vSphere 8-Cluster mit 4 x ESXi-Hosts, die mit einem Netzwerk-Switch verbunden sind.
- Laden Sie die für die VCF-Konvertierung erforderliche Software herunter.

Hier ist der Beispiel-Screenshot vom System Manager, der die MetroCluster -Konfiguration zeigt.



und hier sind die SVM-Netzwerkschnittstellen aus beiden Fehlerdomänen.

Network interfaces Subnets

+ Add

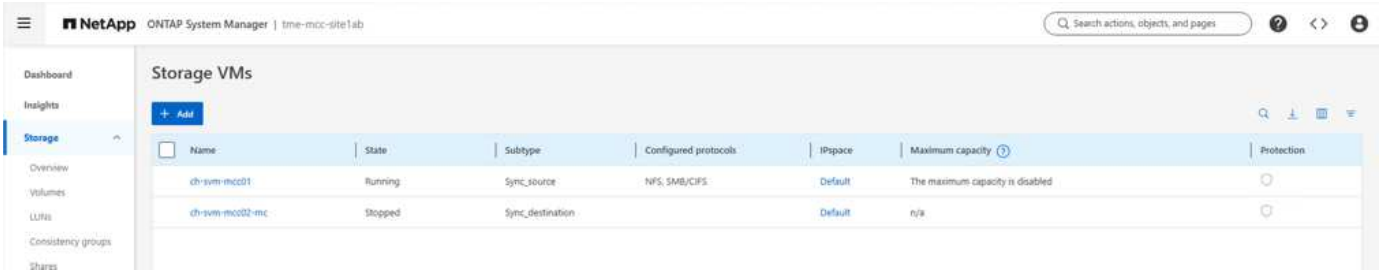
Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc02_8775		ch-svm-mcc02-mc	Default	10.192.164.230	tme-mcc-site1a
lif_ch-svm-mcc01_3118		ch-svm-mcc01	Default	10.192.164.225	tme-mcc-site1a
lif_ch-svm-mcc02_9778		ch-svm-mcc02-mc	Default	10.192.164.231	tme-mcc-site1b
lif_ch-svm-mcc01_6783		ch-svm-mcc01	Default	10.192.164.226	tme-mcc-site1b

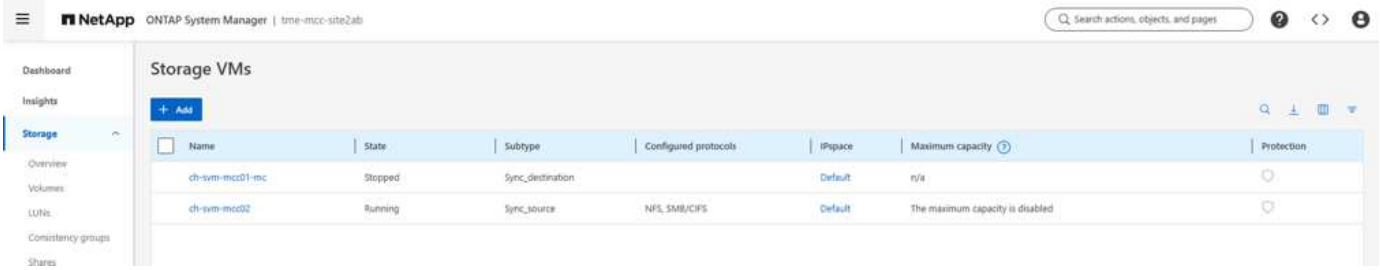
Network interfaces Subnets

+ Add

Name	Status	Storage VM	IPspace	Address	Current node
		ch-svm			
lif_ch-svm-mcc01_3118		ch-svm-mcc01-mc	Default	10.192.164.225	tme-mcc-site2a
lif_ch-svm-mcc02_8775		ch-svm-mcc02	Default	10.192.164.230	tme-mcc-site2a
lif_ch-svm-mcc01_6783		ch-svm-mcc01-mc	Default	10.192.164.226	tme-mcc-site2b
lif_ch-svm-mcc02_9778		ch-svm-mcc02	Default	10.192.164.231	tme-mcc-site2b

[HINWEIS] SVM wird auf einer der Fehlerdomänen in MetroCluster aktiv sein.





Verweisen "vMSC mit MetroCluster" .

Informationen zum unterstützten Speicher und andere Überlegungen zum Konvertieren oder Importieren von vSphere in VCF 5.2 finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Bevor Sie einen vSphere-Cluster erstellen, der in eine VCF-Verwaltungsdomäne konvertiert wird, lesen Sie "NSX-Überlegungen für vSphere-Cluster"

Die erforderliche Software finden Sie unter "Laden Sie Software zum Konvertieren oder Importieren vorhandener vSphere-Umgebungen herunter" .

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Bereitstellungsschritte

So stellen Sie eine VCF Stretched Management Domain mit NFS als Hauptdatenspeicher bereit:

Führen Sie die folgenden Schritte aus:

- Stellen Sie vSphere-Hosts und vCenter bereit.
- Erstellen Sie einen vSphere-Cluster.
- Stellen Sie einen NFS-Datenspeicher bereit.
- Kopieren Sie das VCF-Importtool auf die vCenter-Appliance.
- Führen Sie mit dem VCF-Importtool eine Vorprüfung auf der vCenter-Appliance durch.
- Erstellen Sie eine JSON-Datei für einen NSX-Cluster, der während des Importvorgangs bereitgestellt werden soll.
- Laden Sie die erforderliche Software in den SDDC-Manager hoch.
- Konvertieren Sie den vSphere-Cluster in eine VCF VI-Workload-Domäne.

Eine Übersicht über den Konvertierungsprozess finden Sie unter "Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workload-Domäne in VMware Cloud Foundation" .

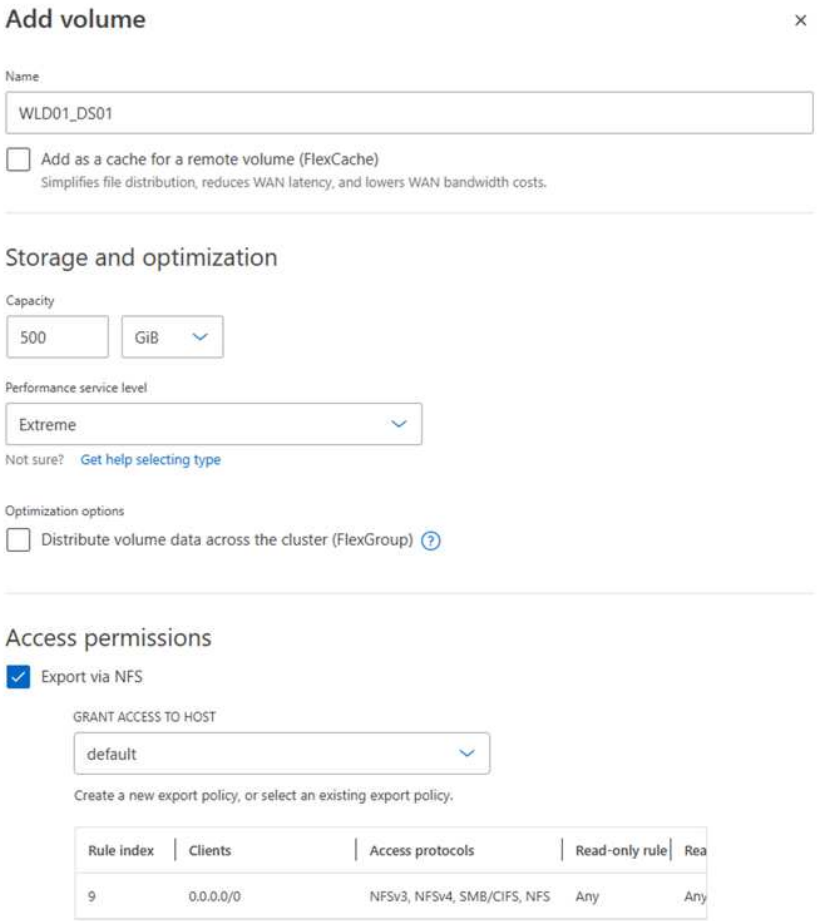
Bereitstellen von vSphere-Hosts und vCenter

Stellen Sie vSphere auf Hosts bereit, indem Sie ISO vom Broadcom-Supportportal herunterladen, oder verwenden Sie die vorhandene Bereitstellungsoption für den vSphere-Host.

Mounten Sie den NFS-Datenspeicher, um VMs zu hosten

In diesem Schritt erstellen wir das NFS-Volume und mounten es als Datenspeicher zum Hosten von VMs.

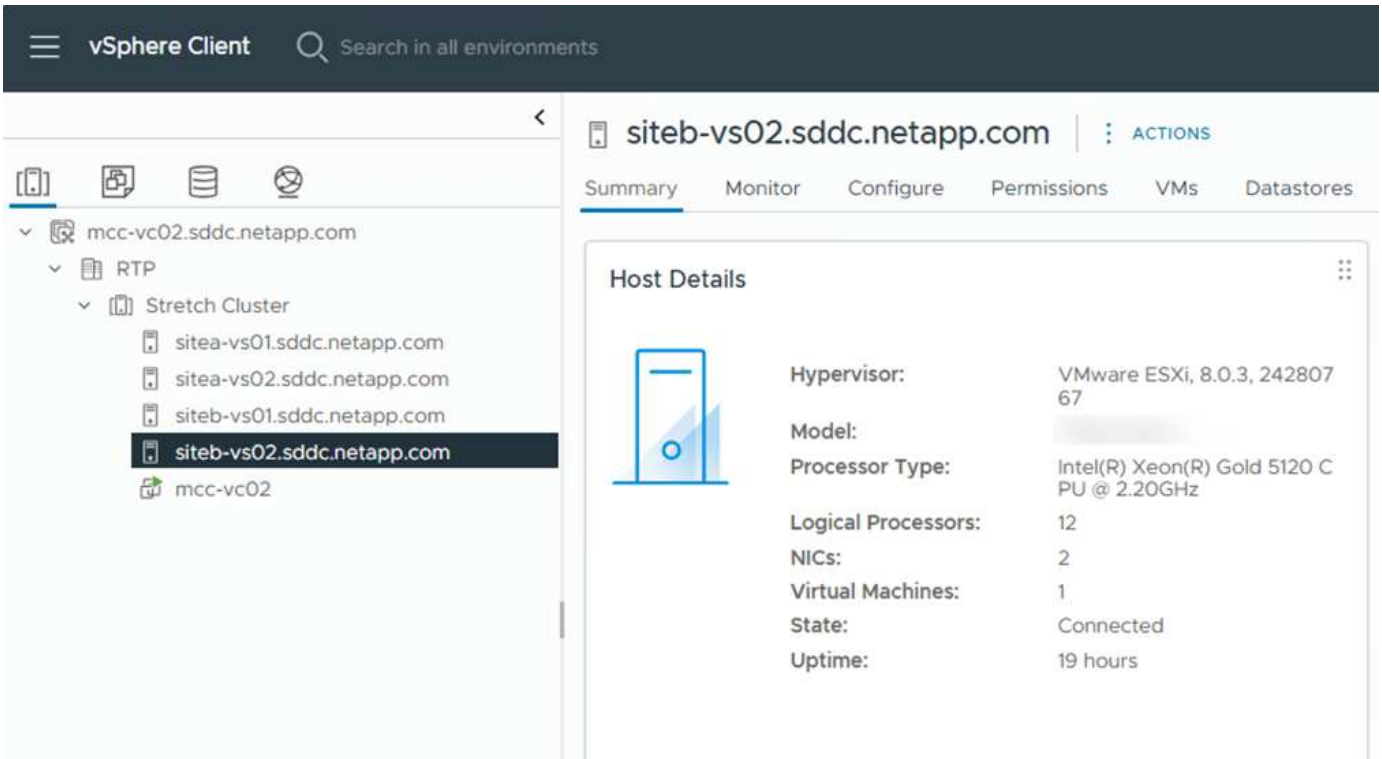
1. Erstellen Sie mithilfe des System Managers ein Volume und fügen Sie es einer Exportrichtlinie hinzu, die das IP-Subnetz des vSphere-Hosts
   enthält.



2. Stellen Sie eine SSH-Verbindung zum vSphere-Host her und mounten Sie den NFS-Datenspeicher.

```
esxcli storage nfs add -c 4 -H 10.192.164.225 -s /WLD01_DS01 -v DS01
esxcli storage nfs add -c 4 -H 10.192.164.230 -s /WLD01_DS02 -v DS02
esxcli storage nfs list
```

Stellen Sie vCenter auf einem NFS-Datenspeicher bereit. Stellen Sie sicher, dass SSH und Bash-Shell auf dem vCenter-Gerät aktiviert
sind.



vSphere-Cluster erstellen

1. Melden Sie sich beim vSphere-Webclient an. Erstellen Sie das DataCenter und den vSphere-Cluster, indem Sie einen der Hosts hinzufügen, auf dem NFS VAAI bereitgestellt ist. Wir haben uns dafür entschieden, alle Hosts im Cluster mit der Option „Einzelbild verwalten“ zu verwalten. [TIPP] Wählen Sie „Konfiguration auf Clusterebene verwalten“ nicht aus. Weitere Einzelheiten finden Sie unter "NSX-Überlegungen für vSphere-Cluster" . Informationen zu vMSC-Best Practices mit ONTAP MetroCluster finden Sie unter "vMSC-Design- und Implementierungsrichtlinien"
2. Fügen Sie dem Cluster weitere vSphere-Hosts hinzu.
3. Erstellen Sie einen verteilten Switch und fügen Sie die Portgruppen hinzu.
4. "Migrieren Sie das Netzwerk vom Standard-vSwitch zum verteilten Switch."

Konvertieren Sie die vSphere-Umgebung in eine VCF VI-Workload-Domäne

Der folgende Abschnitt behandelt die Schritte zum Bereitstellen des SDDC-Managers und zum Konvertieren des vSphere 8-Clusters in eine VCF 5.2-Verwaltungsdomäne. Gegebenenfalls wird für weitere Einzelheiten auf die VMware-Dokumentation verwiesen.

Das VCF-Importtool von VMware by Broadcom ist ein Dienstprogramm, das sowohl auf der vCenter-Appliance als auch auf dem SDDC-Manager verwendet wird, um Konfigurationen zu validieren und Konvertierungs- und Importdienste für vSphere- und VCF-Umgebungen bereitzustellen.

Weitere Informationen finden Sie unter "Optionen und Parameter des VCF-Importtools" .

VCF-Importtool kopieren und extrahieren

Das VCF-Importtool wird auf der vCenter-Appliance verwendet, um zu überprüfen, ob sich der vSphere-Cluster für den VCF-Konvertierungs- oder Importvorgang in einem fehlerfreien Zustand befindet.

Führen Sie die folgenden Schritte aus:

1. Folgen Sie den Schritten unter "Kopieren Sie das VCF-Importtool auf die Ziel-vCenter-Appliance" bei VMware Docs, um das VCF-Importtool an den richtigen Speicherort zu kopieren.
2. Extrahieren Sie das Paket mit dem folgenden Befehl:

```
tar -xvf vcf-brownfield-import-<buildnumber>.tar.gz
```

Validieren der vCenter-Appliance

Verwenden Sie das VCF-Importtool, um die vCenter-Appliance vor dem Import als VI-Workload-Domäne zu validieren.

1. Folgen Sie den Schritten unter "Führen Sie vor der Konvertierung eine Vorprüfung des Ziel-vCenters durch" um die Validierung auszuführen.

Erstellen einer JSON-Datei für die NSX-Bereitstellung

Um NSX Manager bereitzustellen, während Sie eine vSphere-Umgebung in VMware Cloud Foundation importieren oder konvertieren, erstellen Sie eine NSX-Bereitstellungsspezifikation. Für die NSX-Bereitstellung sind mindestens 3 Hosts erforderlich.

> Beim Bereitstellen eines NSX Manager-Clusters in einem Konvertierungs- oder Importvorgang wird ein NSX VLAN-gestütztes Segment verwendet. Einzelheiten zu den Einschränkungen des NSX-VLAN-gestützten Segments finden Sie im Abschnitt „Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation“. Informationen zu NSX-VLAN-Netzwerkbeschränkungen finden Sie unter "Überlegungen vor dem Konvertieren oder Importieren vorhandener vSphere-Umgebungen in VMware Cloud Foundation" .

Nachfolgend sehen Sie ein Beispiel einer JSON-Datei für die NSX-Bereitstellung:

```
{
  "deploy_without_license_keys": true,
  "form_factor": "small",
  "admin_password": "****************",
  "install_bundle_path": "/nfs/vmware/vcf/nfs-mount/bundle/bundle-
133764.zip",
  "cluster_ip": "10.61.185.105",
  "cluster_fqdn": "mcc-wld01-nsx.sddc.netapp.com",
  "manager_specs": [{
    "fqdn": "mcc-wld01-nsxa.sddc.netapp.com",
    "name": "mcc-wld01-nsxa",
    "ip_address": "10.61.185.106",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxb.sddc.netapp.com",
    "name": "mcc-wld01-nsxb",
    "ip_address": "10.61.185.107",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  },
  {
    "fqdn": "mcc-wld01-nsxc.sddc.netapp.com",
    "name": "mcc-wld01-nsxc",
    "ip_address": "10.61.185.108",
    "gateway": "10.61.185.1",
    "subnet_mask": "255.255.255.0"
  }]
}
```

Kopieren Sie die JSON-Datei in den VCF-Benutzer-Home-Ordner im SDDC Manager.

Laden Sie Software in den SDDC Manager hoch

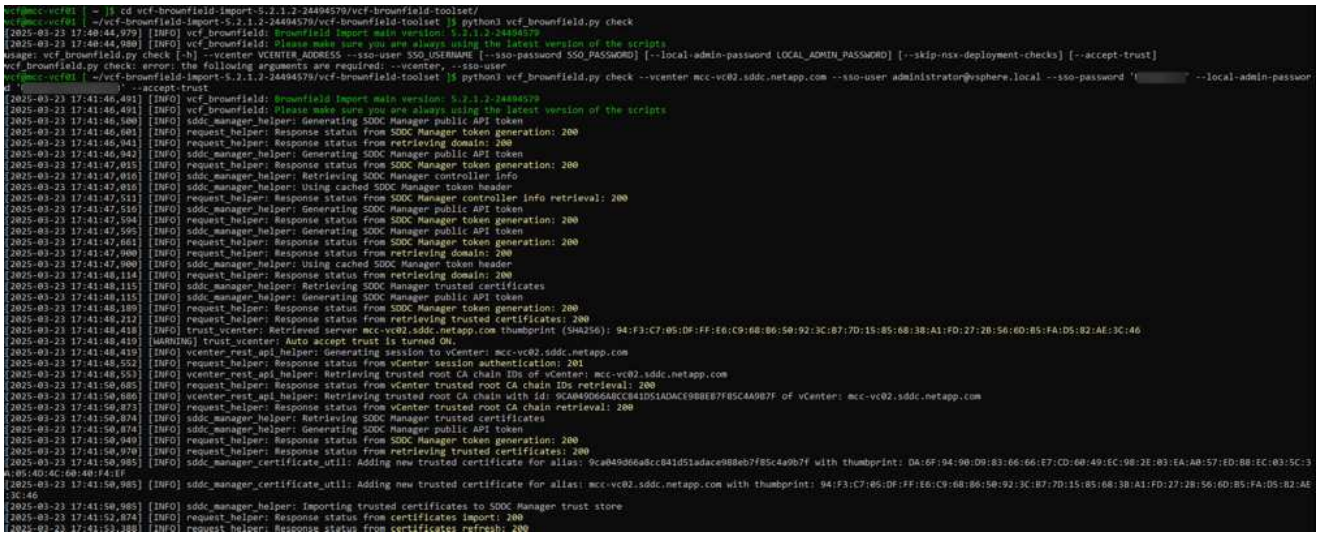
Kopieren Sie das VCF-Importtool in den Home-Ordner des VCF-Benutzers und das NSX-Bereitstellungspaket in den Ordner /nfs/vmware/vcf/nfs-mount/bundle/ im SDDC Manager.

Sehen "Laden Sie die erforderliche Software auf die SDDC Manager Appliance hoch" für detaillierte Anweisungen.

Detaillierte Überprüfung von vCenter vor der Konvertierung

Bevor Sie eine Konvertierung der Managementdomäne oder einen Importvorgang für die VI-Workloaddomäne durchführen, müssen Sie eine detaillierte Prüfung durchführen, um sicherzustellen, dass die Konfiguration der vorhandenen vSphere-Umgebung für die Konvertierung oder den Import unterstützt wird. . Stellen Sie als Benutzer vcf eine SSH-Verbindung zum SDDC Manager-Gerät her. . Navigieren Sie zu dem Verzeichnis, in das Sie das VCF-Importtool kopiert haben. . Führen Sie den folgenden Befehl aus, um zu überprüfen, ob die vSphere-Umgebung konvertiert werden kann

```
python3 vcf_brownfield.py check --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '********' --local-admin-password
'****************' --accept-trust
```



Konvertieren Sie den vSphere-Cluster in eine VCF VI-Workloaddomäne

Zur Durchführung des Konvertierungsprozesses wird das VCF-Importtool verwendet.

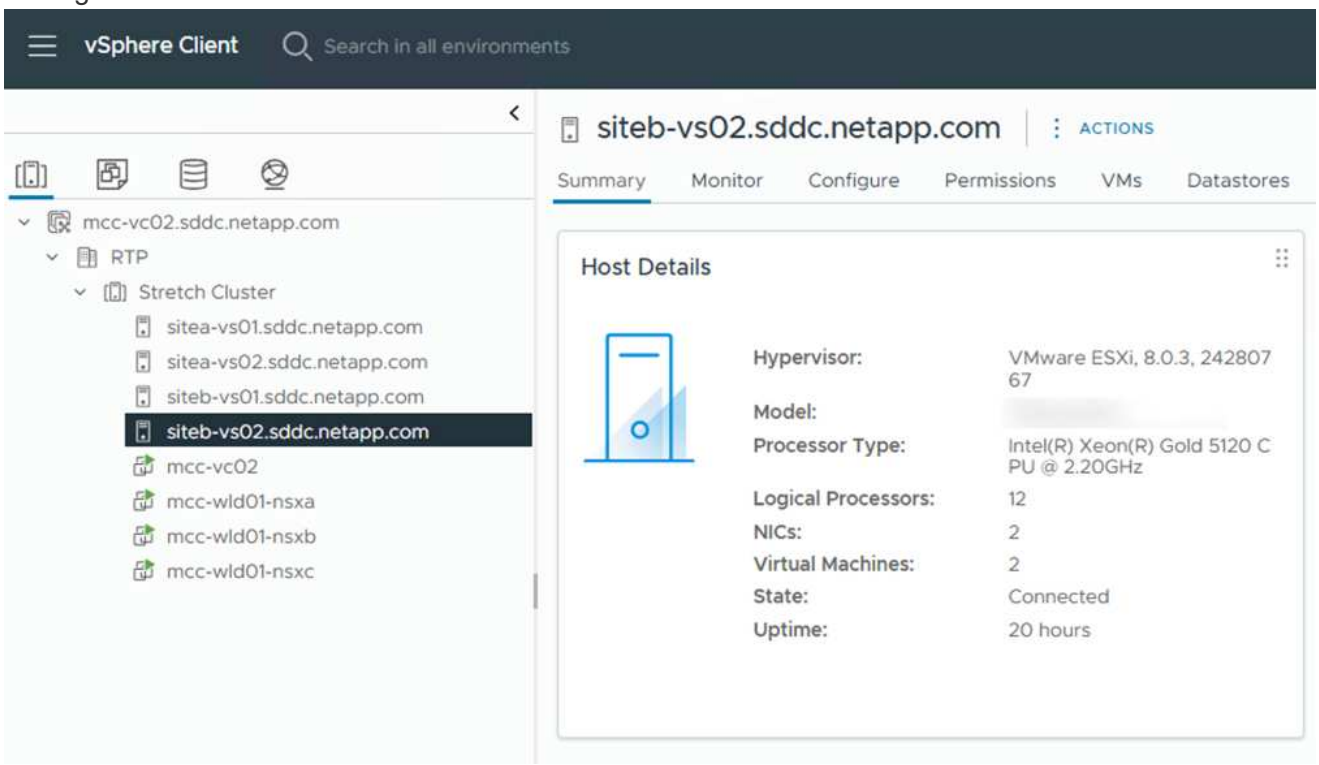
Der folgende Befehl wird ausgeführt, um den vSphere-Cluster in eine VCF-Verwaltungsdomäne zu konvertieren und den NSX-Cluster bereitzustellen:

```
python3 vcf_brownfield.py import --vcenter '<vcenter-fqdn>' --sso-user
'<sso-user>' --sso-password '******' --vcenter-root-password '********'
--local-admin-password '****************' --backup-password
'****************' --domain-name '<Mgmt-domain-name>' --accept-trust
--nsx-deployment-spec-path /home/vcf/nsx.json
```

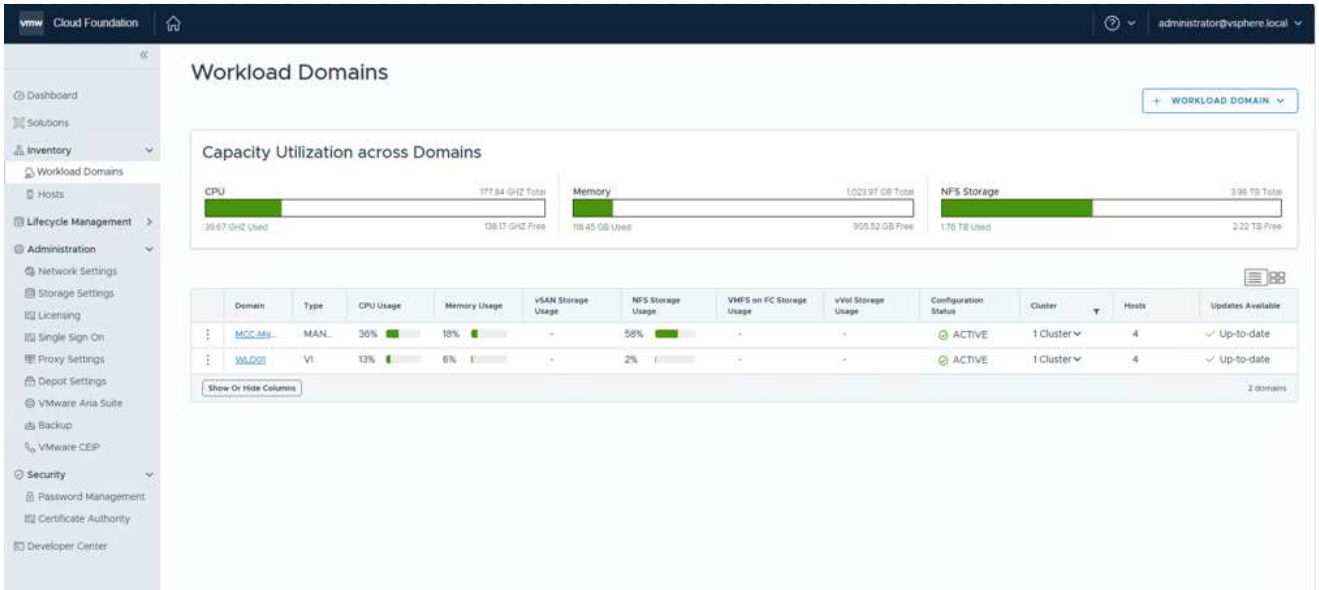
Auch wenn auf dem vSphere-Host mehrere Datenspeicher verfügbar sind, muss nicht abgefragt werden, welcher Datenspeicher als primärer Datenspeicher betrachtet werden soll.

Vollständige Anweisungen finden Sie unter "VCF-Konvertierungsverfahren" .

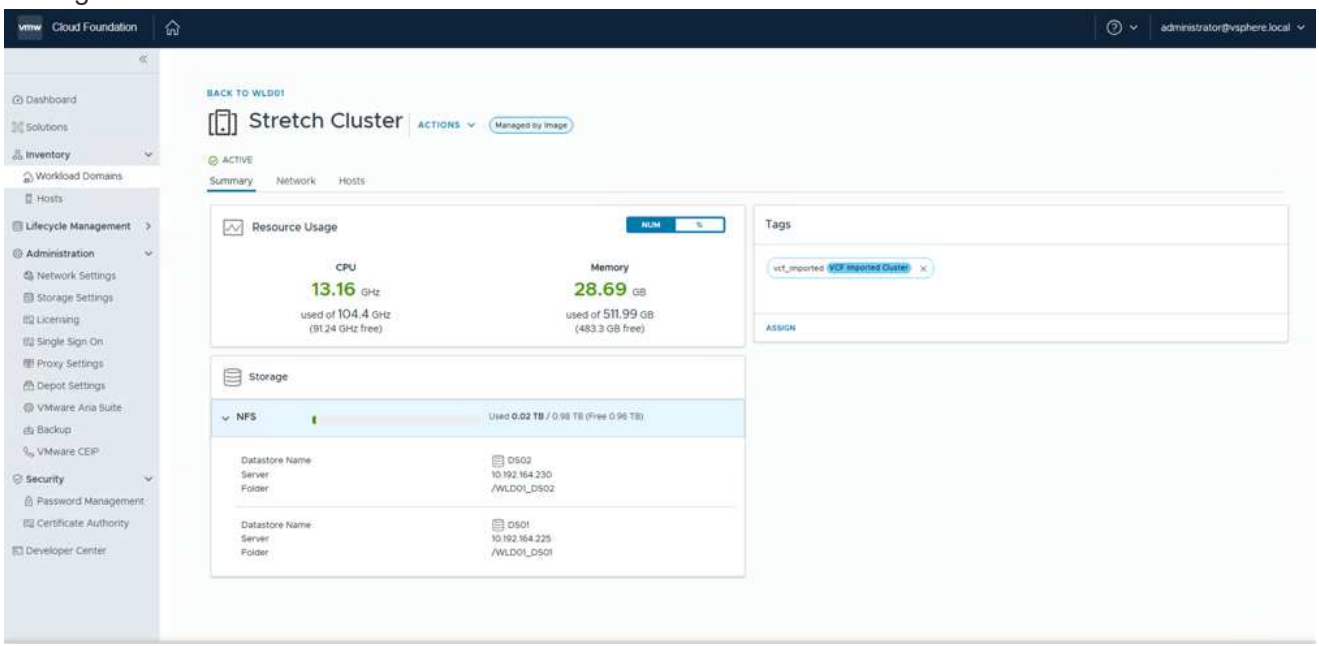
NSX-VMs werden in vCenter
bereitgestellt.



SDDC Manager zeigt die erstellte VI-Workload-Domäne mit dem angegebenen Namen und NFS als Datenspeicher
an.



Bei der Überprüfung des Clusters werden Informationen zu NFS-Datenspeichern bereitgestellt.



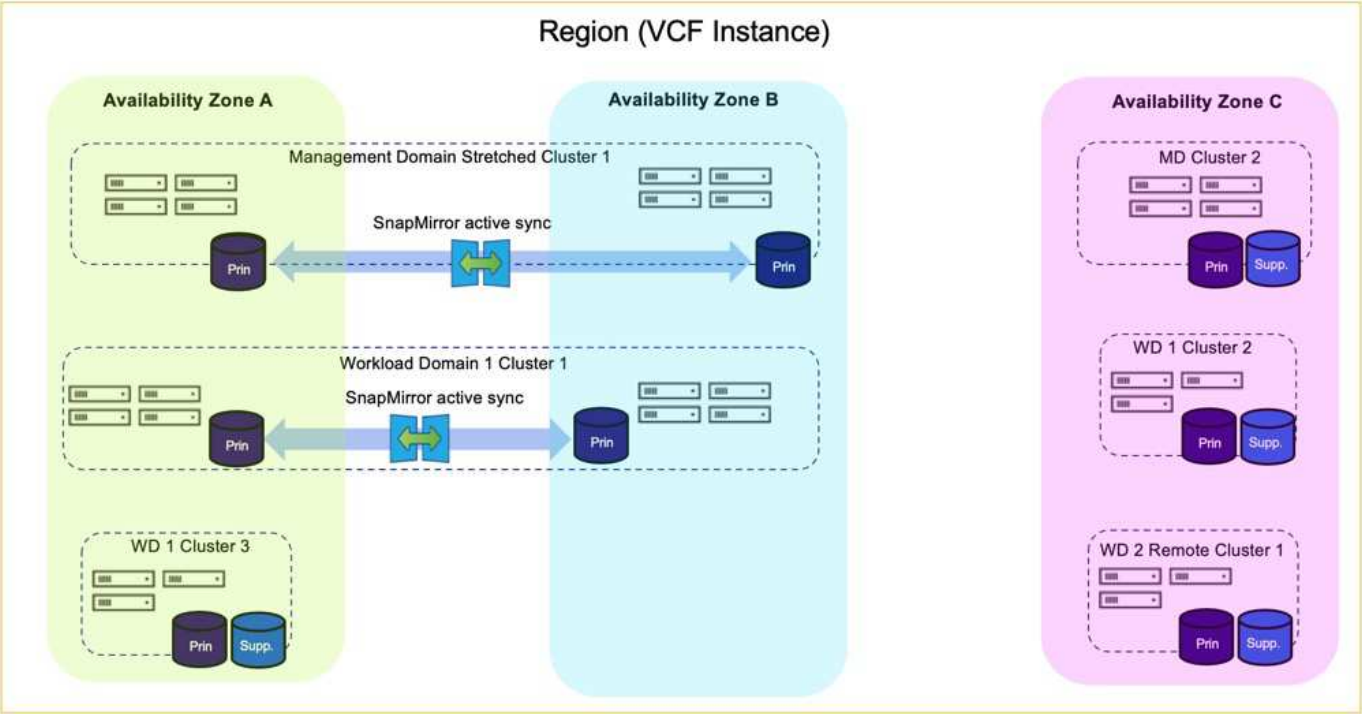
Lizenzierung zu VCF hinzufügen

Nach Abschluss der Konvertierung muss der Umgebung eine Lizenzierung hinzugefügt werden.

1. Melden Sie sich bei der SDDC Manager-Benutzeroberfläche an.
2. Navigieren Sie im Navigationsbereich zu **Administration > Lizenzierung**.
3. Klicken Sie auf **+ Lizenzschlüssel**.
4. Wählen Sie ein Produkt aus dem Dropdown-Menü.
5. Geben Sie den Lizenzschlüssel ein.
6. Geben Sie eine Beschreibung für die Lizenz ein.
7. Klicken Sie auf **Hinzufügen**.
8. Wiederholen Sie diese Schritte für jede Lizenz.

Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne mit SnapMirror Active Sync

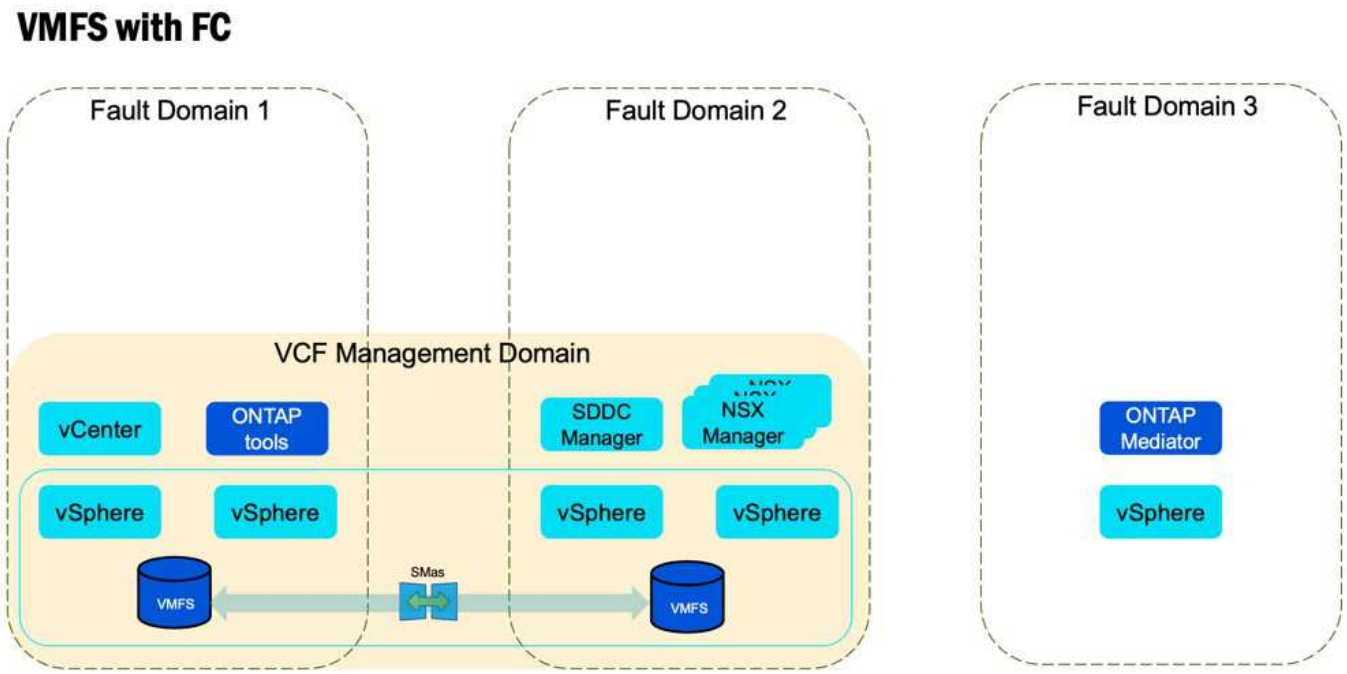
In diesem Anwendungsfall beschreiben wir das Verfahren zur Verwendung von ONTAP tools for VMware vSphere zum Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne. Dieses Verfahren umfasst die Bereitstellung von vSphere-Hosts und vCenter Server, die Installation von ONTAP Tools, den Schutz von Datenspeichern mit SnapMirror Active Sync, die Migration von VMs zu geschützten Datenspeichern und die Konfiguration von zusätzlichem Speicher.



Szenarioübersicht

Die Stretch-Cluster-Lösung kann auf einem Standardcluster oder einem zusätzlichen Cluster in VCF-

Verwaltungs- oder Workloaddomänen implementiert werden. VMFS auf FC wird sowohl auf dem Hauptdatenspeicher als auch auf zusätzlichen Datenspeichern unterstützt. VMFS auf iSCSI wird nur mit zusätzlichen Datenspeichern unterstützt. Informationen zur Unterstützung von VMFS auf NVMe-oF mit SnapMirror Active Sync erhalten Sie bei IMT .



Hauptspeicher in der Verwaltungsdomäne

Ab VCF 5.2 kann die Verwaltungsdomäne mithilfe des VCF-Importtools ohne VSAN bereitgestellt werden. Die Konvertierungsoption des VCF-Importtools ermöglicht"eine vorhandene vCenter-Bereitstellung in eine Verwaltungsdomäne" . Alle Cluster in vCenter werden Teil der Verwaltungsdomäne.

1. Bereitstellen von vSphere-Hosts
2. Stellen Sie den vCenter-Server auf einem lokalen Datenspeicher bereit (vCenter muss auf vSphere-Hosts koexistieren, die in eine Verwaltungsdomäne umgewandelt werden).
3. Bereitstellen von ONTAP tools for VMware vSphere
4. SnapCenter -Plugin für VMware vSphere bereitstellen (optional)
5. Datenspeicher erstellen (FC-Zonenkonfiguration sollte vorhanden sein)
6. Schützen Sie den vSphere-Cluster
7. Migrieren Sie VMs in einen neu erstellten Datenspeicher

> Wenn der Cluster erweitert oder verkleinert wird, muss die Host-Cluster-Beziehung in den ONTAP Tools für den Cluster aktualisiert werden, um die an der Quelle oder dem Ziel vorgenommenen Änderungen anzuzeigen.

Zusätzlicher Speicher in der Verwaltungsdomäne

Sobald die Verwaltungsdomäne betriebsbereit ist, können mithilfe von ONTAP -Tools zusätzliche Datenspeicher erstellt werden, die die Erweiterung der Konsistenzgruppe auslösen.

> Wenn ein vSphere-Cluster geschützt ist, sind alle Datenspeicher im Cluster geschützt.

Wenn die VCF-Umgebung mit dem Cloud Builder-Tool bereitgestellt wird, stellen Sie zum Erstellen des zusätzlichen Speichers mit iSCSI ONTAP -Tools bereit, um den iSCSI-Datenspeicher zu erstellen und den vSphere-Cluster zu schützen.

> Wenn der Cluster erweitert oder verkleinert wird, muss die Host-Cluster-Beziehung in den ONTAP Tools für den Cluster aktualisiert werden, um die an der Quelle oder dem Ziel vorgenommenen Änderungen anzuzeigen.

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

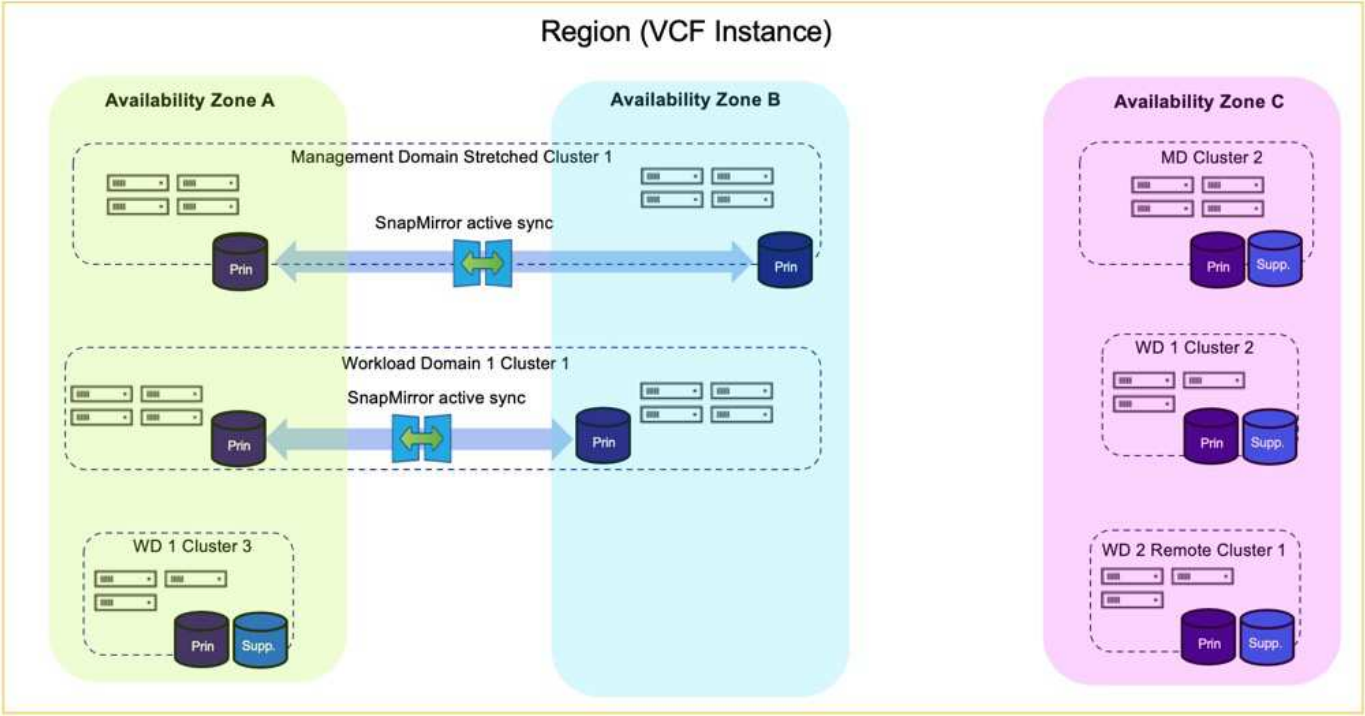
Informationen zur Konfiguration von VCF finden Sie unter"Dokumentation zu VMware Cloud Foundation 5.2" .

Videodemo für diese Lösung

Stretch-Cluster für VCF mit ONTAP -Tools

Konfigurieren eines Stretch-Clusters für eine VI-Workloaddomäne mit SnapMirror Active Sync

In diesem Anwendungsfall beschreiben wir das Verfahren zum Konfigurieren eines Stretch-Clusters für eine Virtual Infrastructure (VI)-Workload-Domäne unter Verwendung von SnapMirror Active Sync mit ONTAP tools for VMware vSphere. Dieses Verfahren umfasst das Erstellen einer VCF-Workload-Domäne mit VMFS auf Fibre Channel, das Registrieren des vCenter mit ONTAP Tools, das Registrieren von Speichersystemen und das Schützen des vSphere-Clusters.



Szenarioübersicht

Die Datenspeicher in der VCF-Workload-Domäne können mit SnapMirror Active Sync geschützt werden, um eine Stretch-Cluster-Lösung bereitzustellen. Der Schutz wird auf vSphere-Clusterebene aktiviert und alle ONTAP Blockdatenspeicher im Cluster werden geschützt.

Hauptspeicher in der Workloaddomäne

Die Workloaddomäne kann entweder durch Importieren mit dem VCF-Importtool oder durch Bereitstellen mit dem SDDC-Manager erstellt werden. Die Bereitstellung mit dem SDDC-Manager bietet mehr Netzwerkoptionen als das Importieren einer vorhandenen Umgebung.

1. Erstellen Sie eine Workload-Domäne mit VMFS auf FC
2. "Registrieren Sie das Workload-Domänen-vCenter beim ONTAP Tools-Manager, um das vCenter-Plugin bereitzustellen"
3. "Registrieren Sie Speichersysteme auf ONTAP -Tools"
4. "Schützen Sie den vSphere-Cluster"

> Wenn der Cluster erweitert oder verkleinert wird, muss die Host-Cluster-Beziehung in den ONTAP Tools für den Cluster aktualisiert werden, um die an der Quelle oder dem Ziel vorgenommenen Änderungen anzuzeigen.

Zusätzlicher Speicher in der Workloaddomäne

Sobald die Workload-Domäne betriebsbereit ist, können mithilfe von ONTAP -Tools zusätzliche Datenspeicher erstellt werden, die die Erweiterung der Konsistenzgruppe auslösen.

> Wenn ein vSphere-Cluster geschützt ist, sind alle Datenspeicher im Cluster geschützt.

Weitere Informationen

Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im"ONTAP 9 Dokumentation" Center.

Informationen zur Konfiguration von VCF finden Sie unter"VMware Cloud Foundation-Dokumentation" .

Videodemo für diese Lösung

Stretch-Cluster für VCF mit ONTAP -Tools

Migrieren Sie VMs von VMware vSphere zu ONTAP -Datenspeichern

VMware vSphere-Umgebungen können erheblich von der Migration virtueller Maschinen auf NetApp ONTAP-gestützte Datenspeicher profitieren. Egal, ob Sie von vSAN oder Speichersystemen von Drittanbietern wechseln oder Ihre vorhandene Infrastruktur aktualisieren, erkunden Sie verschiedene vMotion-Szenarien und Migrationsstrategien, um Ihre VMs nahtlos auf ONTAP Datenspeicher umzustellen. Dadurch wird die Geschäftskontinuität sichergestellt und gleichzeitig werden die Speicherfunktionen der Enterprise-Klasse von ONTAP genutzt.

VMware vSphere von Broadcom unterstützt VMFS-, NFS- und vVol-Datenspeicher zum Hosten virtueller Maschinen. Kunden haben die Möglichkeit, diese Datenspeicher mit hyperkonvergenten Infrastrukturen oder mit zentralisierten gemeinsam genutzten Speichersystemen zu erstellen.

Kunden erkennen häufig den Wert des Hostings auf ONTAP -basierten Speichersystemen, da diese platzsparende Snapshots und Klone virtueller Maschinen bereitstellen, die Flexibilität bieten, zwischen verschiedenen Bereitstellungsmodellen in den Rechenzentren und Clouds zu wählen, die Betriebseffizienz durch Überwachungs- und Warntools steigern, Sicherheit, Governance und optionale Compliance-Tools zur Überprüfung von VM-Daten bieten und so weiter.

Auf ONTAP Datenspeichern gehostete VMs können mit dem SnapCenter Plugin für VMware vSphere (SCV) geschützt werden. SCV erstellt speicherbasierte Snapshots und repliziert auch auf das Remote ONTAP Speichersystem. Wiederherstellungen können entweder von primären oder sekundären Speichersystemen durchgeführt werden.

Kunden haben die Flexibilität, zwischen Cloud Insights oder Aria Operations oder einer Kombination aus beiden oder anderen Tools von Drittanbietern zu wählen, die die ONTAP API zur Fehlerbehebung, Leistungsüberwachung, Berichterstellung und Warnbenachrichtigungsfunktionen verwenden.

Kunden können Datenspeicher problemlos mithilfe des ONTAP Tools vCenter Plug-ins oder seiner API bereitstellen und VMs können auch im eingeschalteten Zustand zu ONTAP Datenspeichern migriert werden.

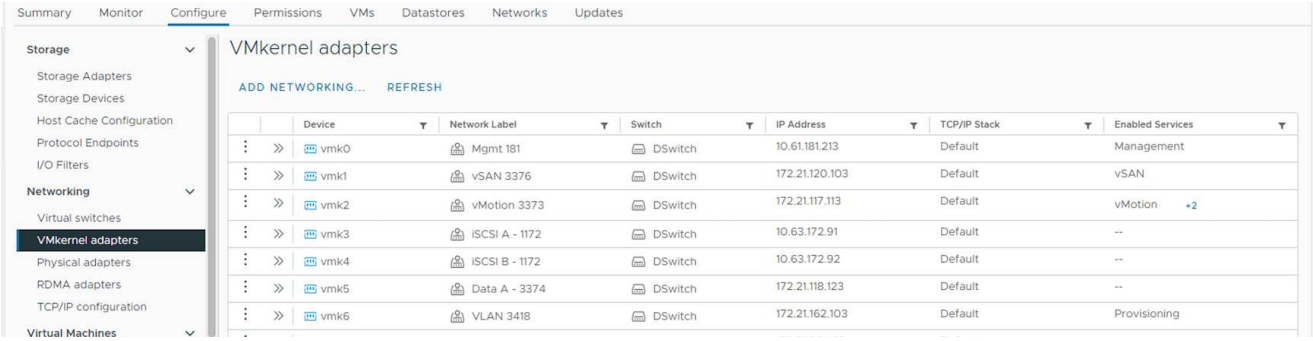
> Einige VMs, die mit externen Verwaltungstools wie Aria Automation, Tanzu (oder anderen Kubernetes-Varianten) bereitgestellt werden, hängen normalerweise von der VM-Speicherrichtlinie ab. Bei der Migration zwischen den Datenspeichern innerhalb derselben VM-Speicherrichtlinie sollte dies weniger Auswirkungen auf die Anwendungen haben. Wenden Sie sich an die Anwendungsbesitzer, um diese VMs ordnungsgemäß in den neuen Datenspeicher zu migrieren. vSphere 8 eingeführt "vSphere vMotion-Benachrichtigungen für latenzempfindliche Anwendungen" um Anwendungen für vMotion vorzubereiten.

Netzwerkanforderungen

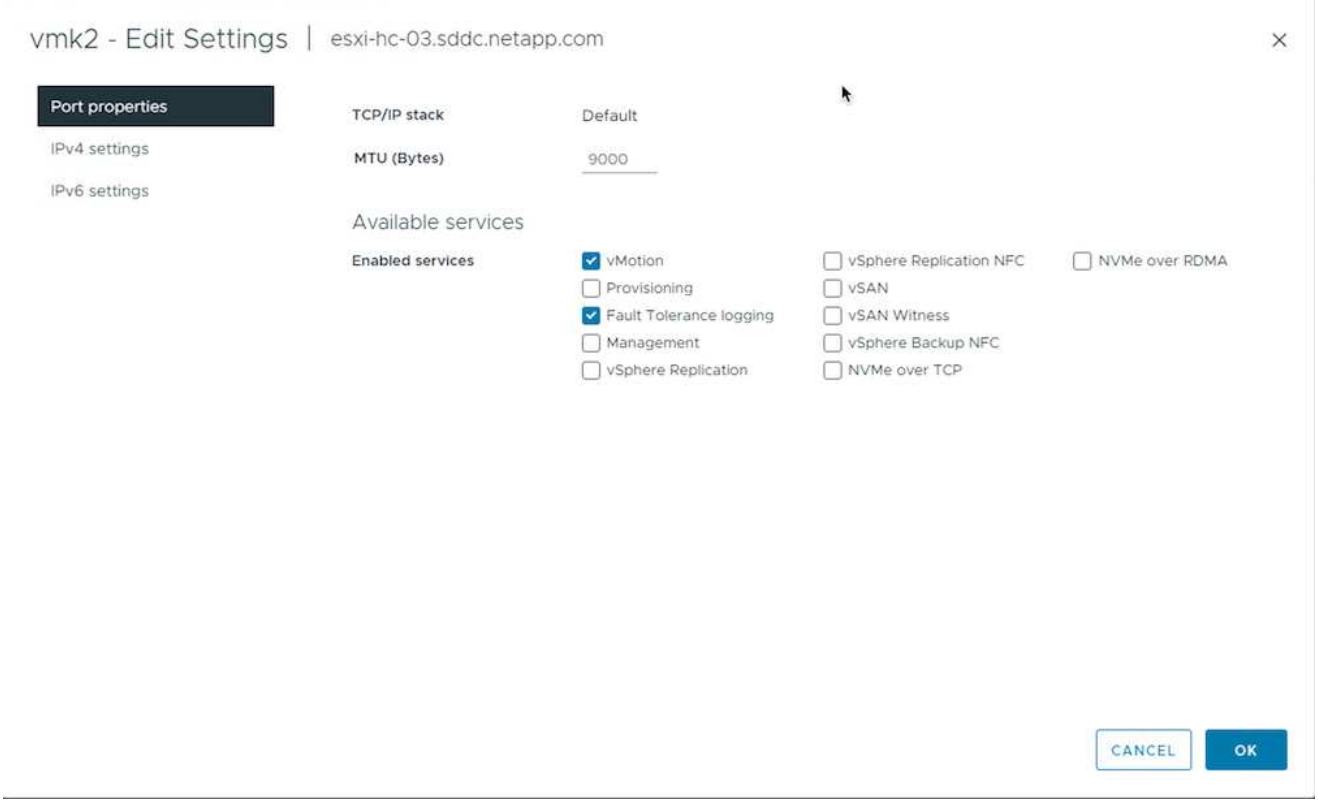
VM-Migration mit vMotion

Es wird davon ausgegangen, dass für den ONTAP Datenspeicher bereits ein duales Speichernetzwerk vorhanden ist, um Konnektivität, Fehlertoleranz und Leistungssteigerung zu gewährleisten.

Die Migration von VMs über die vSphere-Hosts wird ebenfalls von der VMKernel-Schnittstelle des vSphere-Hosts abgewickelt. Für die Hot-Migration (eingeschaltete VMs) wird die VMKernel-Schnittstelle mit aktiviertem vMotion-Dienst verwendet, und für die Cold-Migration (ausgeschaltete VMs) wird die VMKernel-Schnittstelle mit aktiviertem Provisioning-Dienst zum Verschieben der Daten verwendet. Wenn keine gültige Schnittstelle gefunden wurde, wird die Verwaltungsschnittstelle zum Verschieben der Daten verwendet, was für bestimmte Anwendungsfälle möglicherweise nicht wünschenswert ist.



Wenn Sie die VMKernel-Schnittstelle bearbeiten, besteht hier die Möglichkeit, die erforderlichen Dienste zu aktivieren.



Stellen Sie sicher, dass mindestens zwei aktive Hochgeschwindigkeits-Uplink-Netzwerkkarten für die von vMotion- und Provisioning-VMkernel-Schnittstellen verwendete Portgruppe verfügbar sind.

VM-Migrationsszenarien

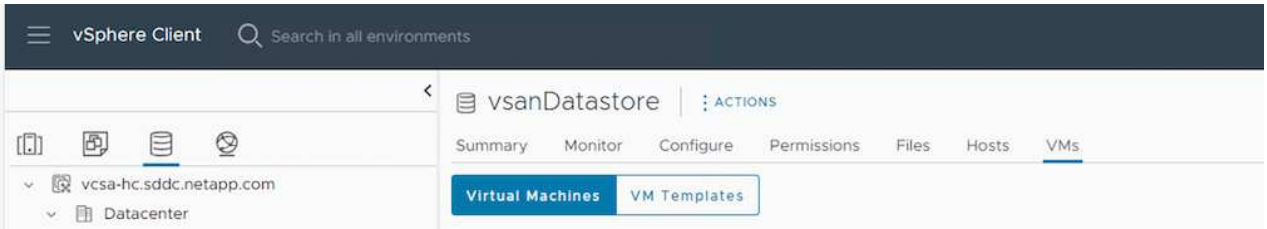
vMotion wird häufig verwendet, um die VMs unabhängig von ihrem Energiezustand zu migrieren. Weitere Überlegungen und Migrationsverfahren für bestimmte Szenarien finden Sie weiter unten.

> Verstehen "VM-Bedingungen und Einschränkungen von vSphere vMotion" bevor Sie mit VM-Migrationsoptionen fortfahren.

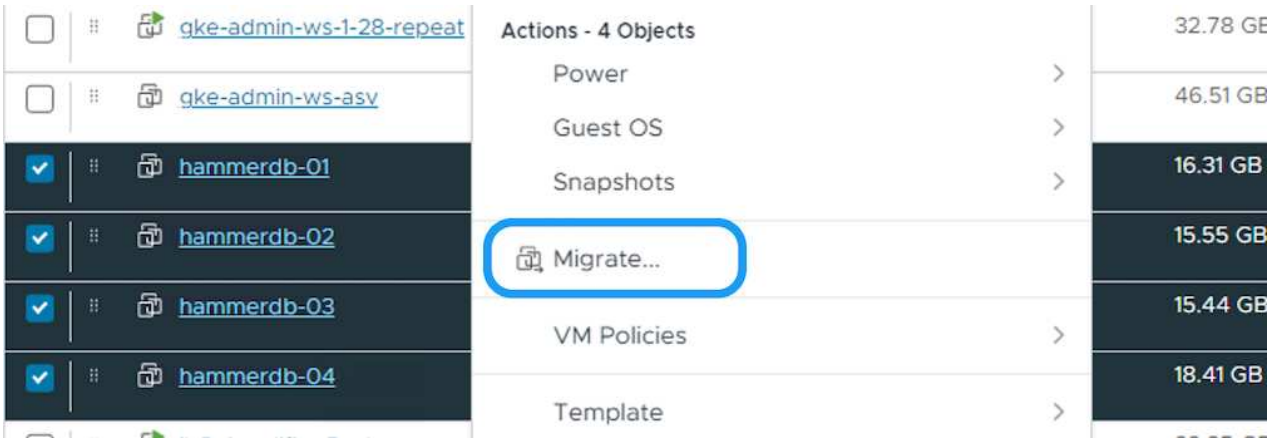
Migration von VMs aus einem bestimmten vSphere-Datenspeicher

Befolgen Sie die nachstehenden Schritte, um VMs mithilfe der Benutzeroberfläche in einen neuen Datenspeicher zu migrieren.

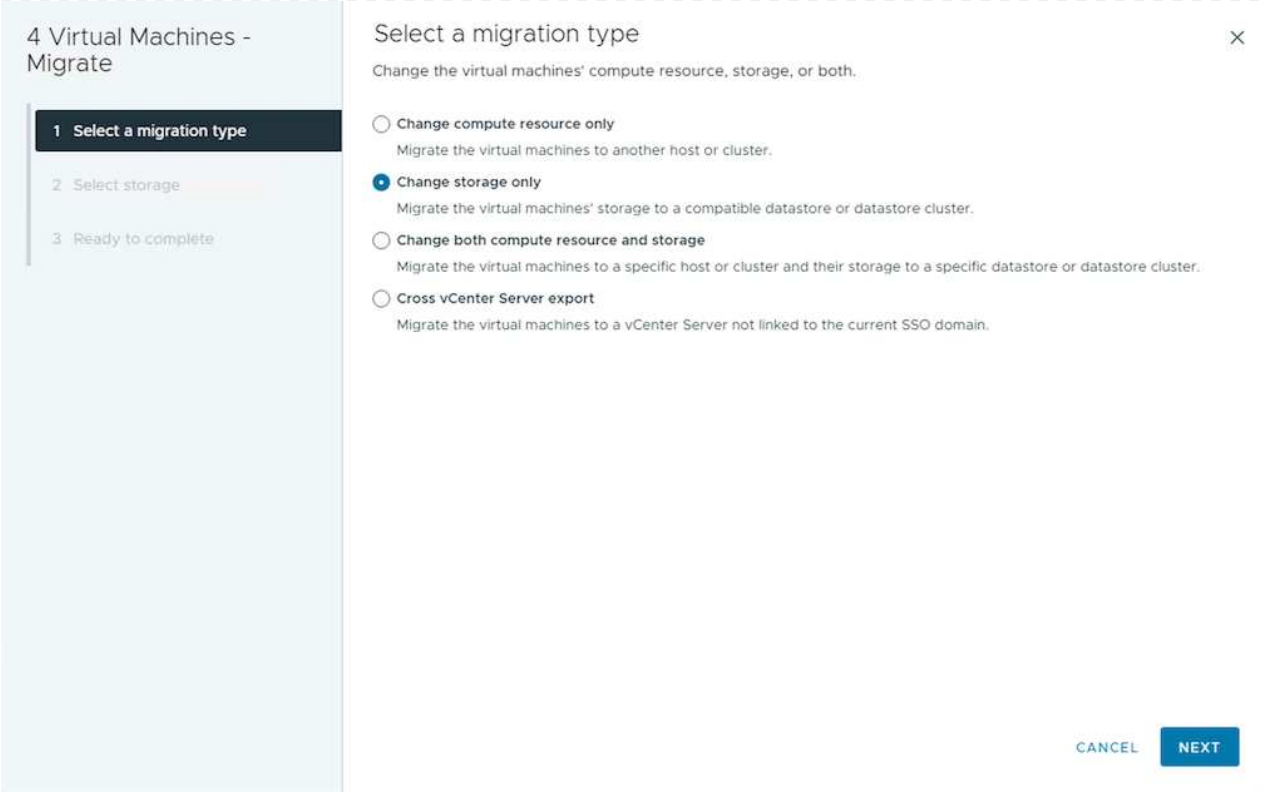
1. Wählen Sie mit dem vSphere Web Client den Datenspeicher aus dem Speicherinventar aus und klicken Sie auf die Registerkarte „VMs“.



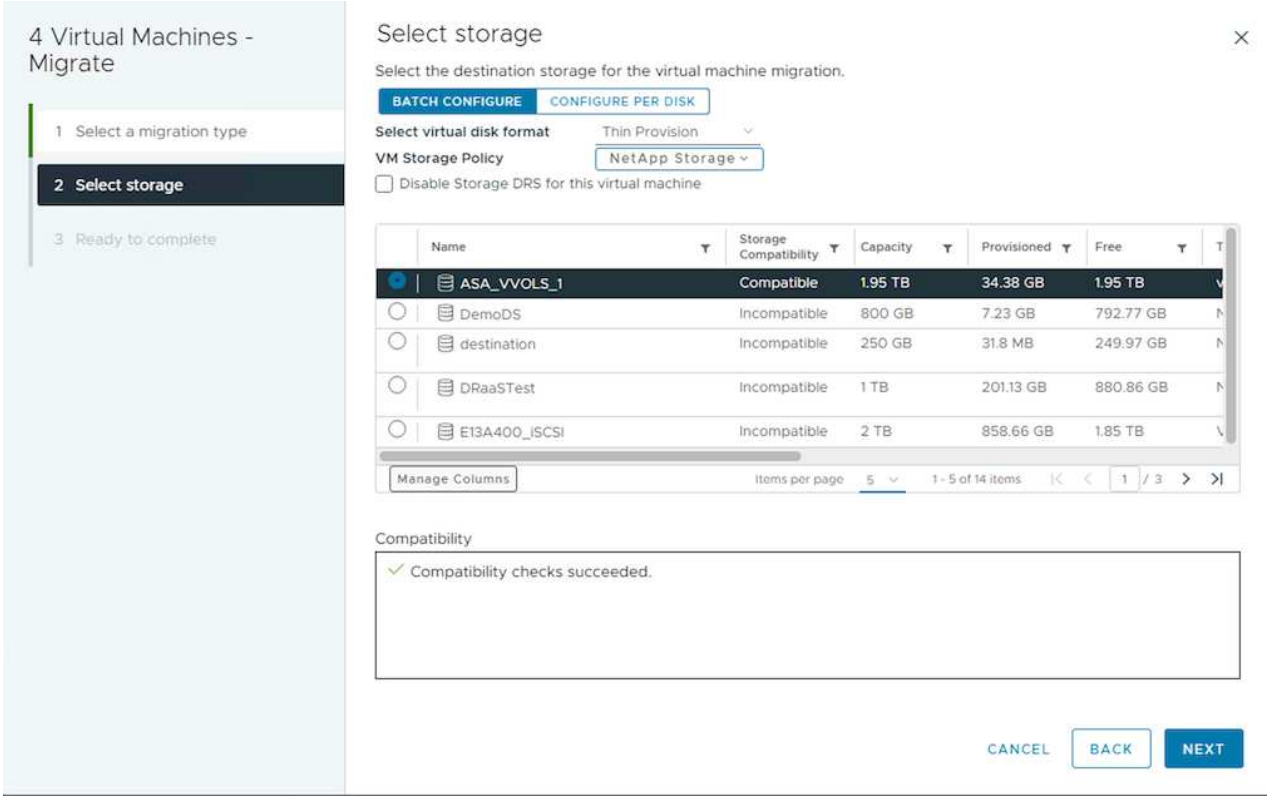
2. Wählen Sie die VMs aus, die migriert werden müssen, und klicken Sie mit der rechten Maustaste, um die Option „Migrieren“ auszuwählen.



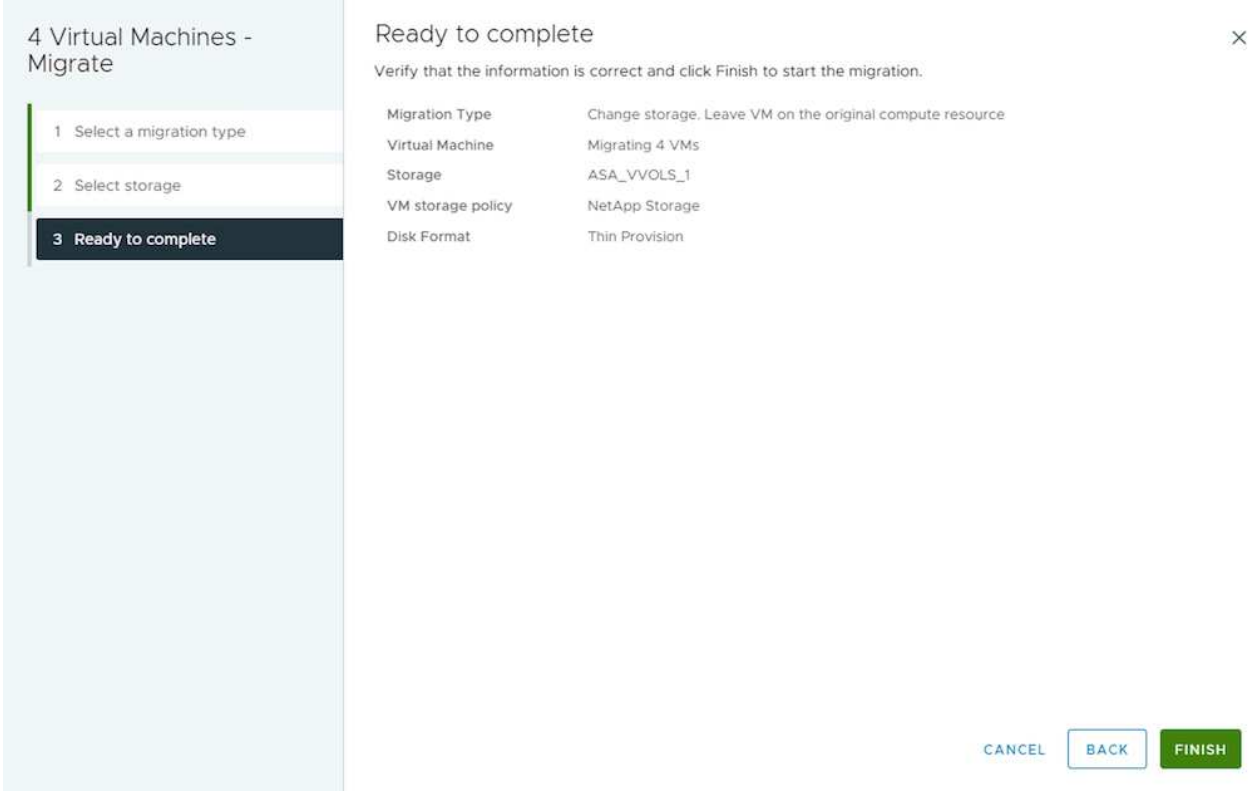
3. Wählen Sie die Option, nur den Speicher zu ändern, und klicken Sie auf „Weiter“.



4. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.



5. Überprüfen Sie den Eintrag und klicken Sie auf „Fertig stellen“.



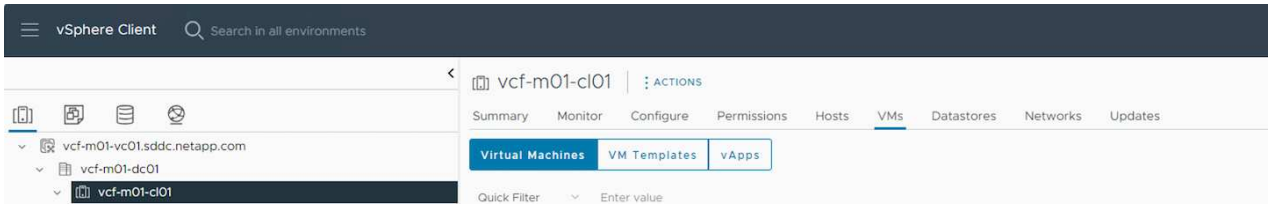
Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific datastore
$vm = Get-DataStore 'vSanDatastore' | Get-VM Har*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

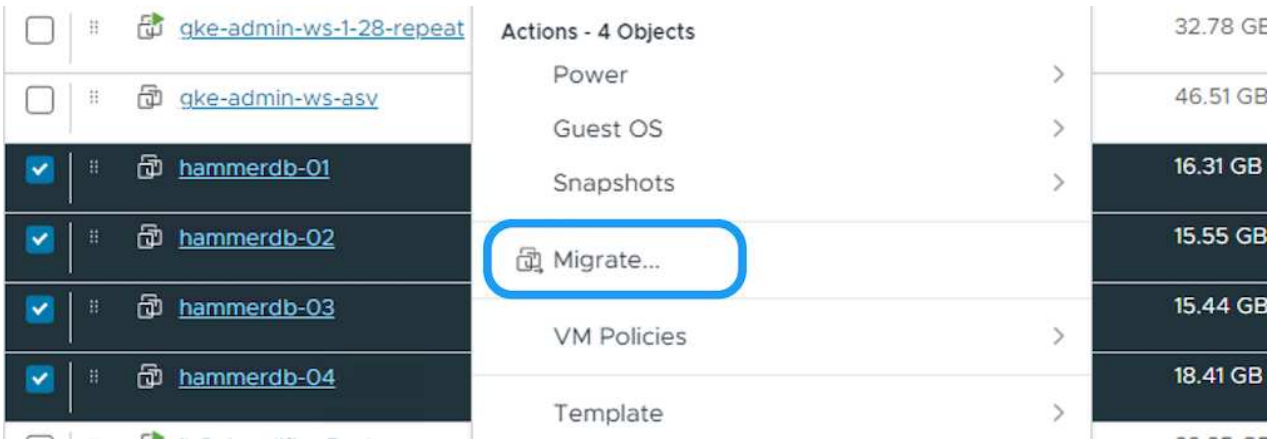
Migration von VMs im selben vSphere-Cluster

Befolgen Sie die nachstehenden Schritte, um VMs mithilfe der Benutzeroberfläche in einen neuen Datenspeicher zu migrieren.

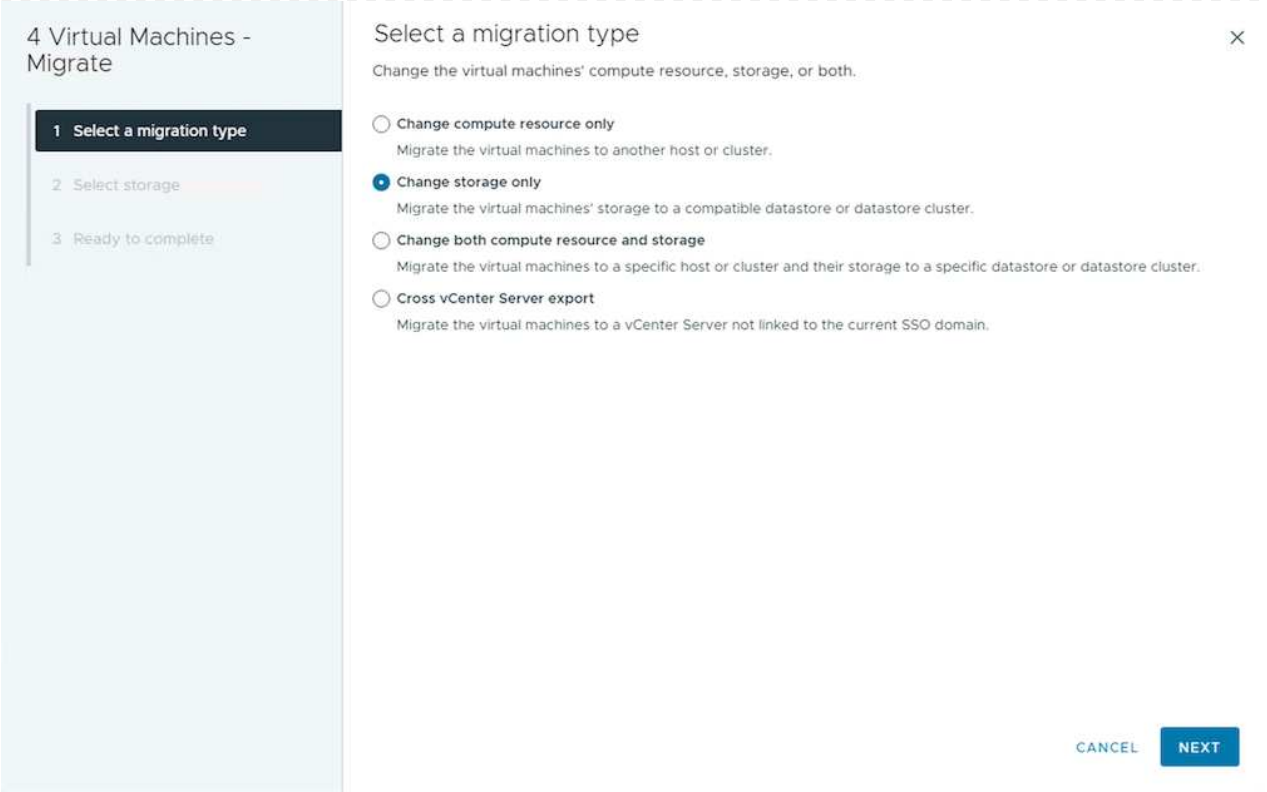
1. Wählen Sie mit dem vSphere Web Client den Cluster aus dem Host- und Cluster-Inventar aus und klicken Sie auf die Registerkarte „VMs“.



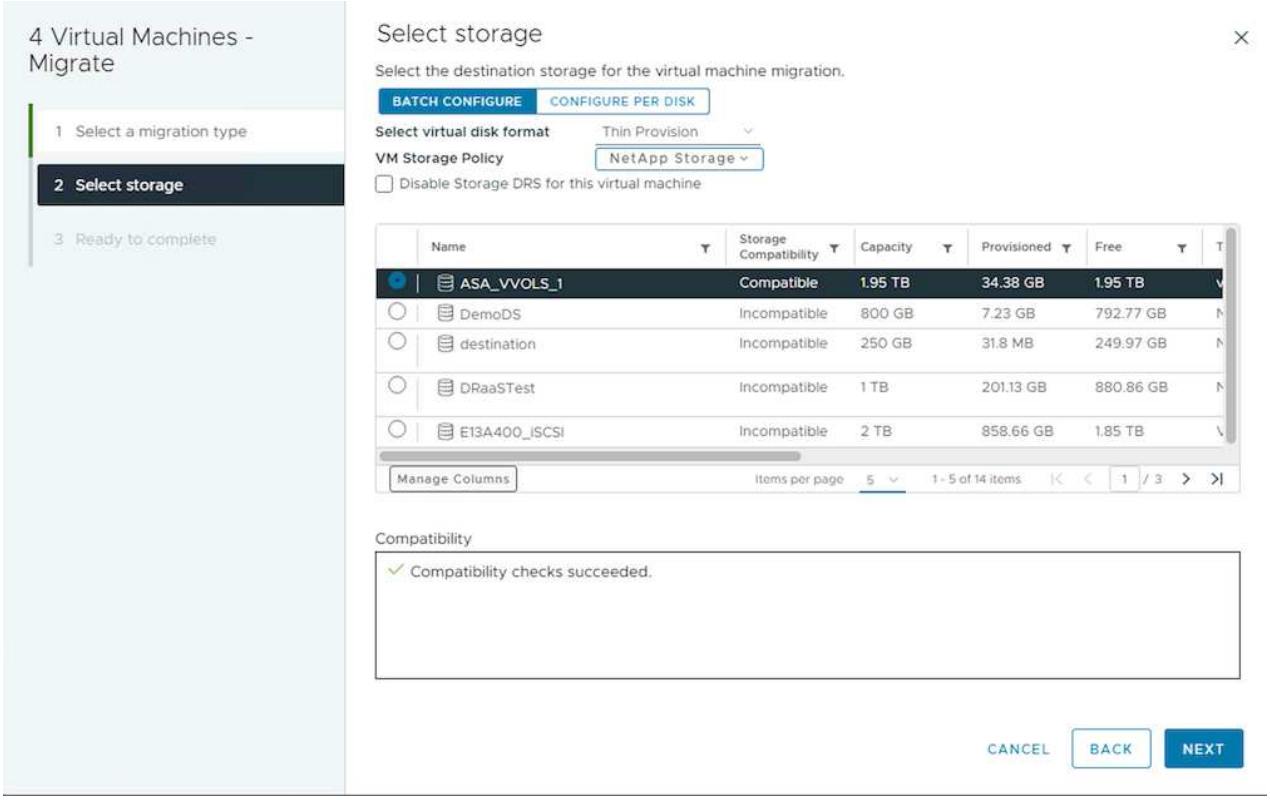
2. Wählen Sie die VMs aus, die migriert werden müssen, und klicken Sie mit der rechten Maustaste, um die Option „Migrieren“ auszuwählen.



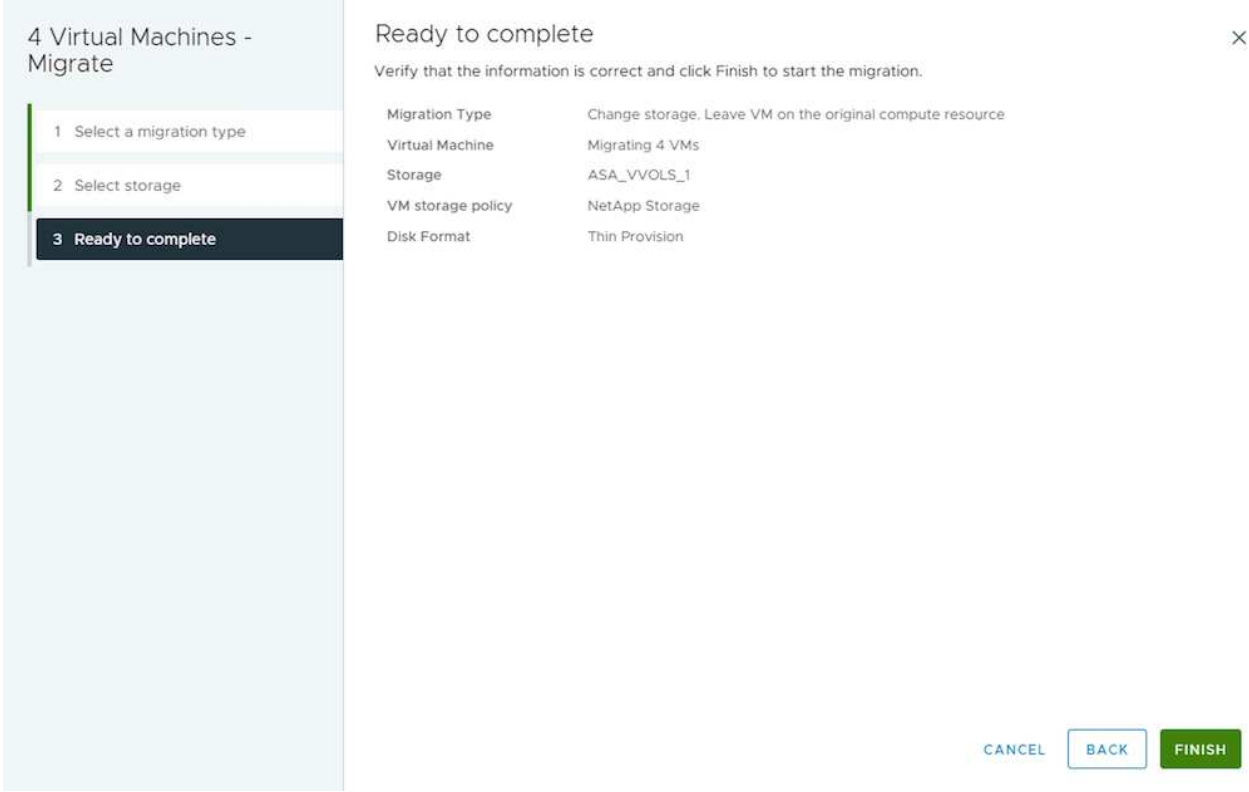
3. Wählen Sie die Option, nur den Speicher zu ändern, und klicken Sie auf „Weiter“.



4. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.



5. Überprüfen Sie den Eintrag und klicken Sie auf „Fertig stellen“.



Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to Datastore specified by Policy
$vm | Move-VM -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy)

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

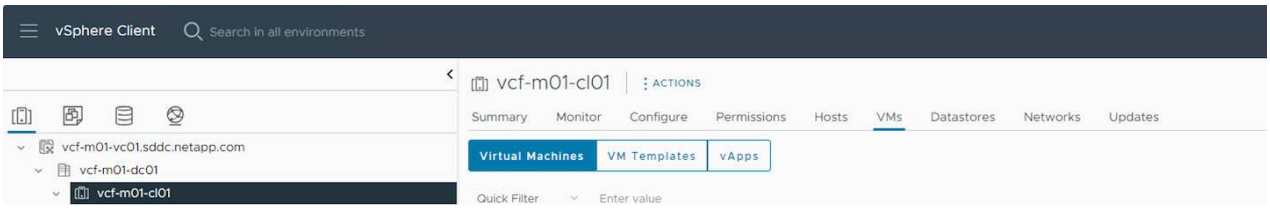
Wenn ein Datastore-Cluster mit vollautomatischem Storage DRS (Dynamic Resource Scheduling) verwendet wird und beide Datastores (Quell- und Ziel-Datastores) vom gleichen Typ (VMFS/NFS/vVol) sind, behalten Sie beide Datastores im selben Storage-Cluster und migrieren Sie VMs vom Quell-Datastore, indem Sie den Wartungsmodus auf der Quelle aktivieren. Die Erfahrung wird ähnlich sein wie bei der Wartung von Compute-Hosts.

Migration von VMs über mehrere vSphere-Cluster

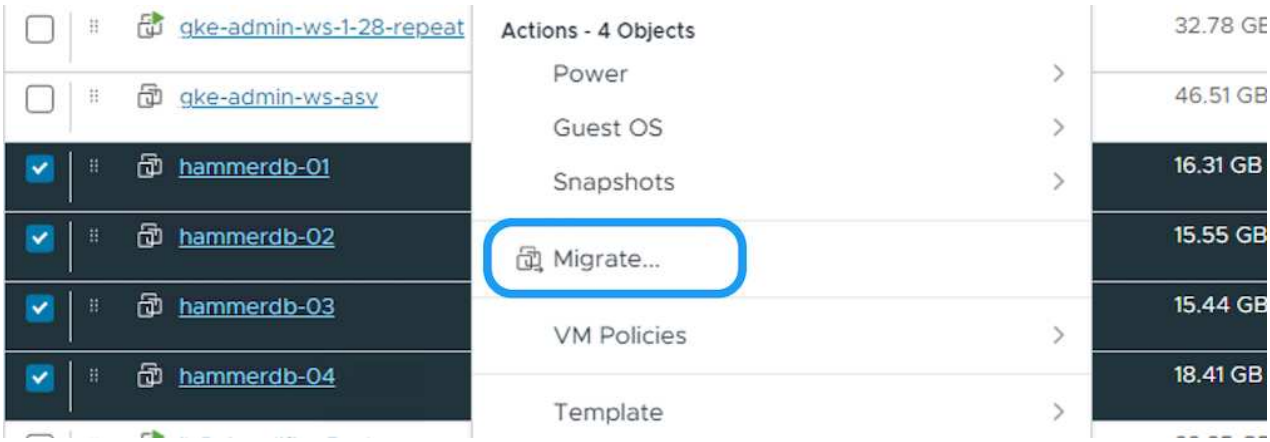
> Verweisen "CPU-Kompatibilität und vSphere Enhanced vMotion-Kompatibilität" wenn Quell- und Zielhosts zu unterschiedlichen CPU-Familien oder Modellen gehören.

Befolgen Sie die nachstehenden Schritte, um VMs mithilfe der Benutzeroberfläche in einen neuen Datenspeicher zu migrieren.

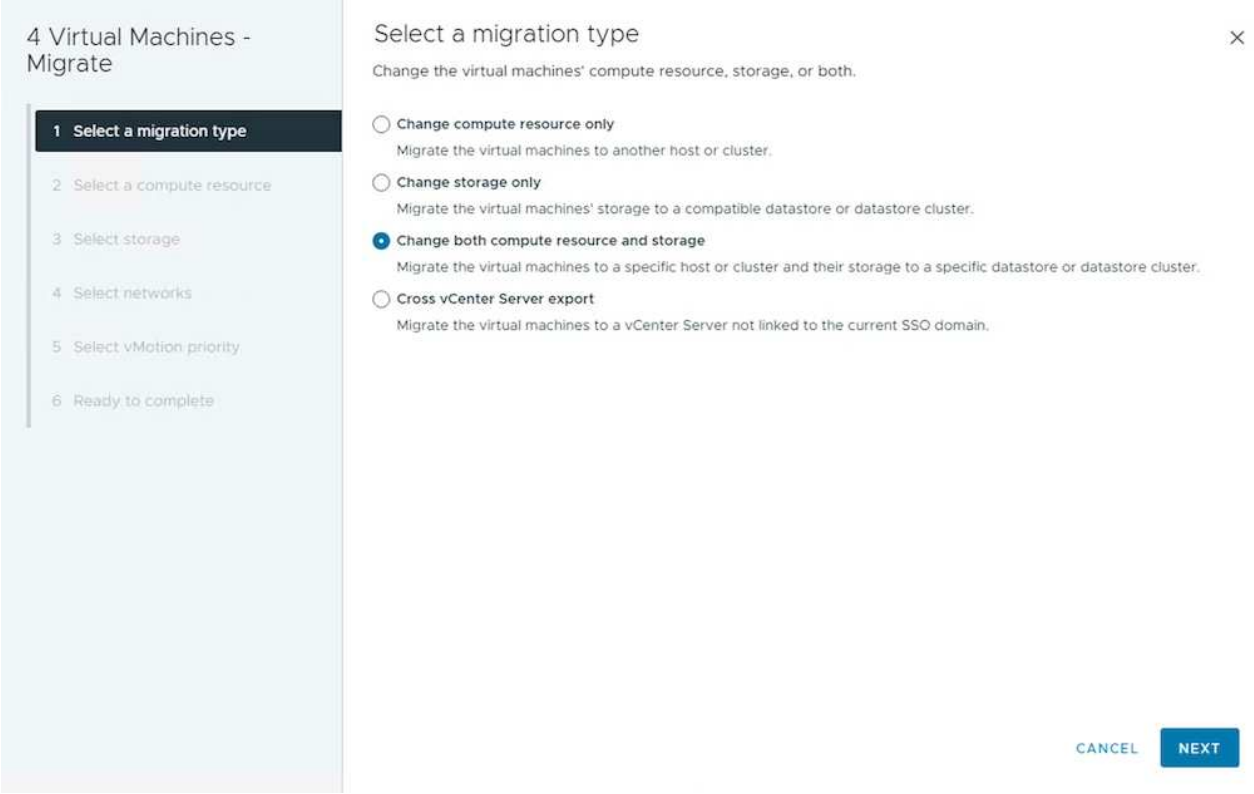
1. Wählen Sie mit dem vSphere Web Client den Cluster aus dem Host- und Cluster-Inventar aus und klicken Sie auf die Registerkarte „VMs“.



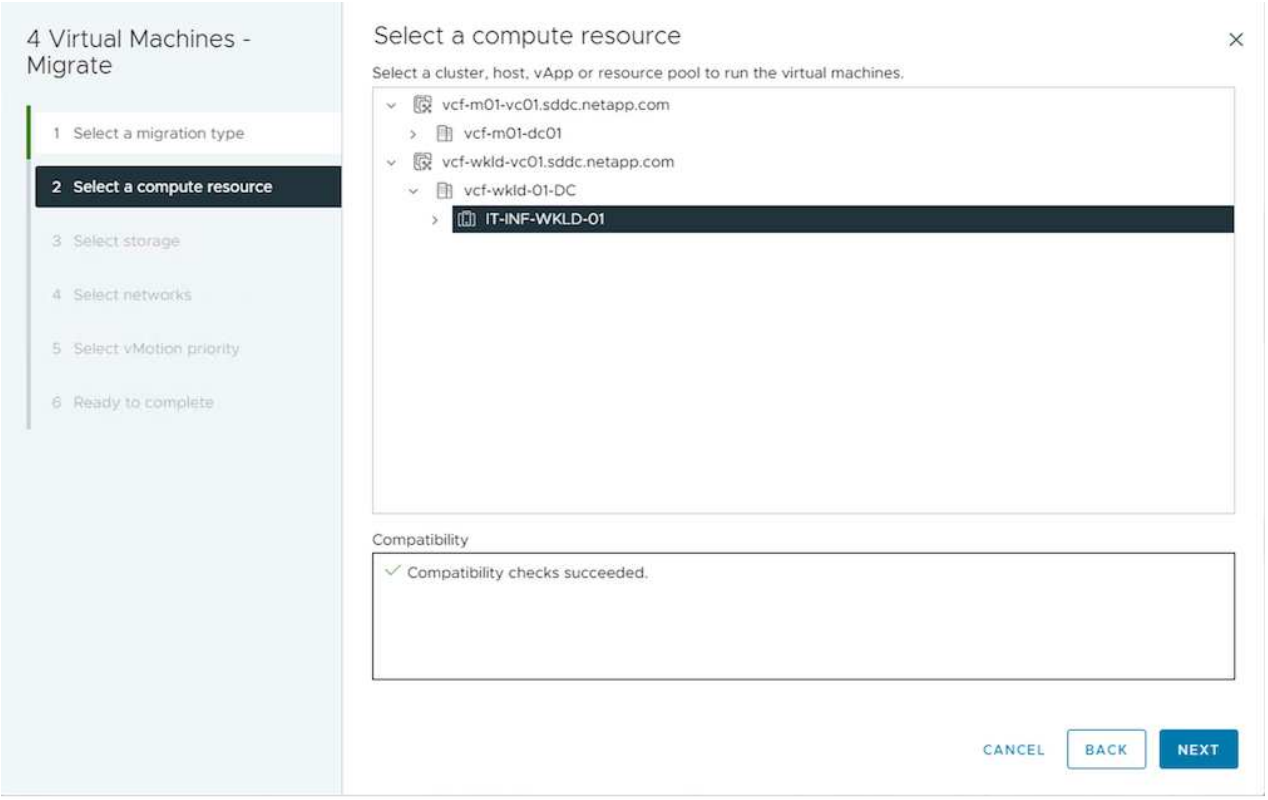
2. Wählen Sie die VMs aus, die migriert werden müssen, und klicken Sie mit der rechten Maustaste, um die Option „Migrieren“ auszuwählen.



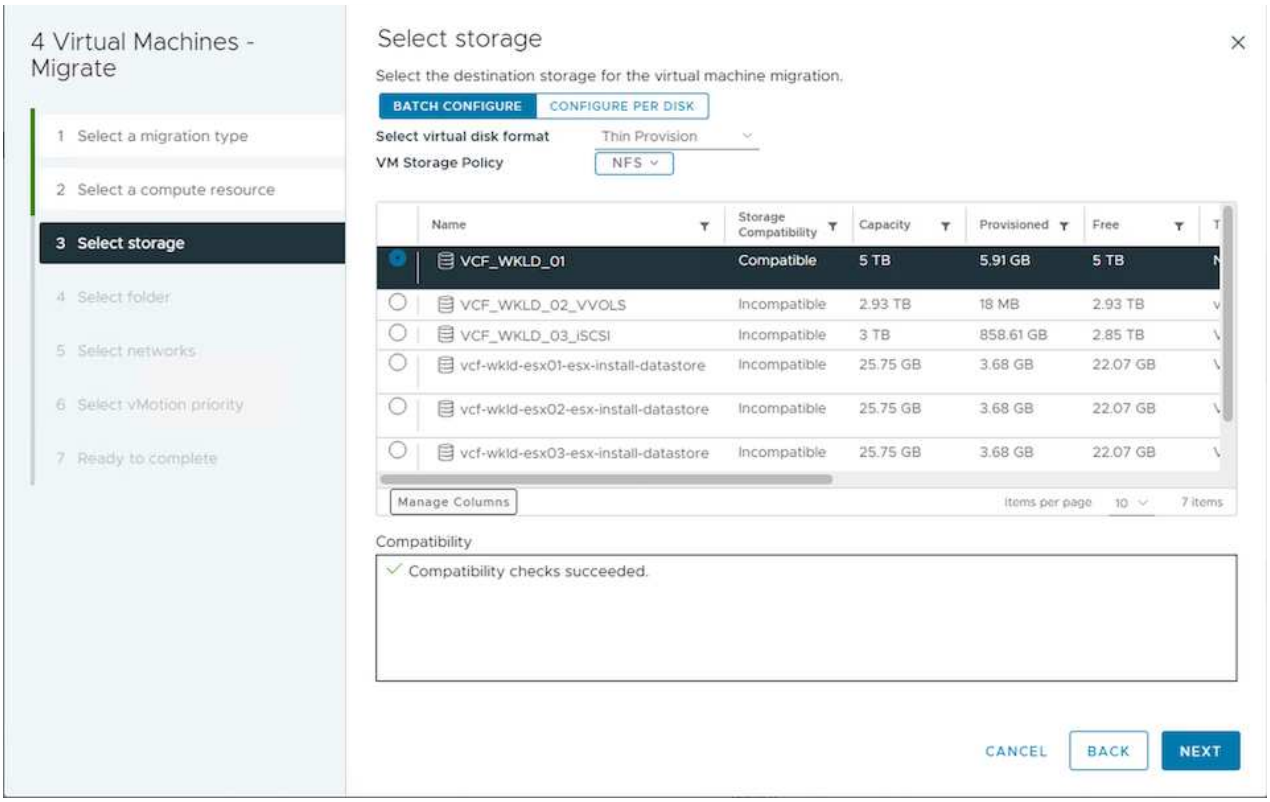
3. Wählen Sie die Option zum Ändern der Rechenressourcen und des Speichers und klicken Sie auf „Weiter“.



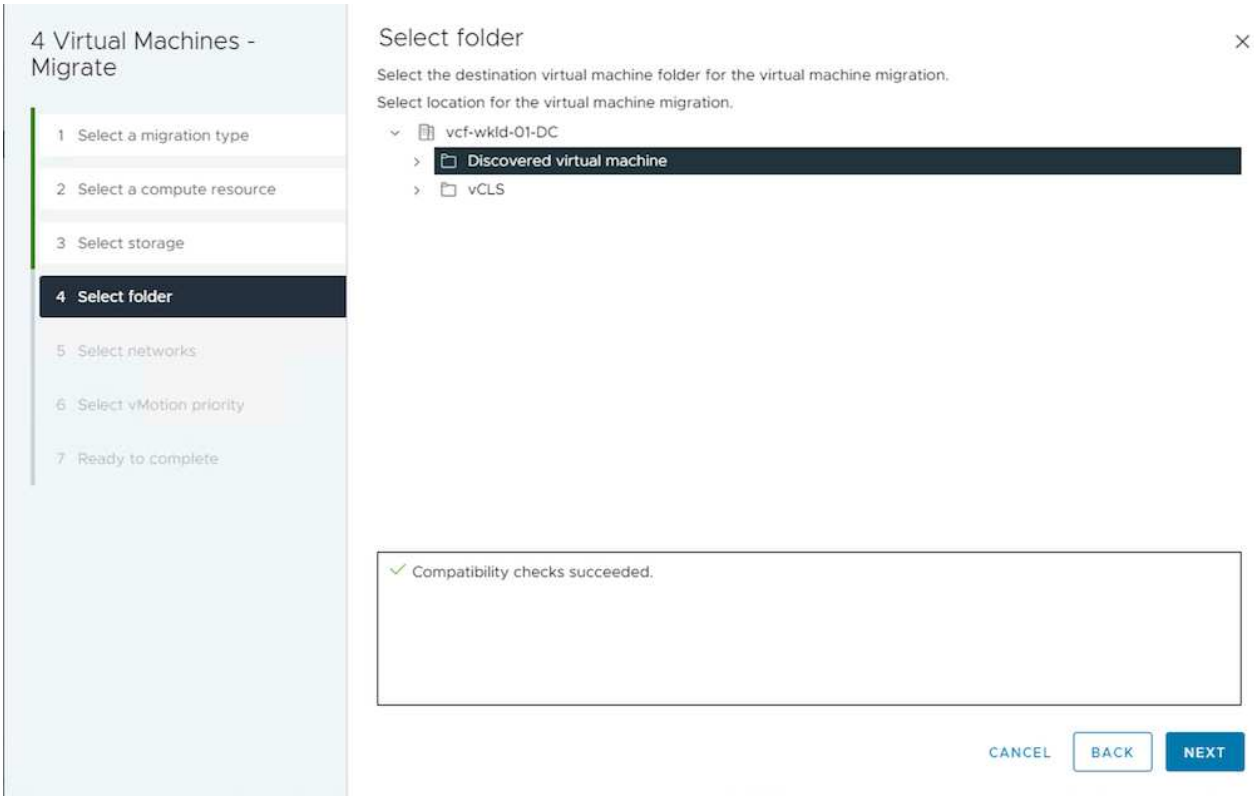
4. Navigieren Sie und wählen Sie den richtigen Cluster für die Migration aus.



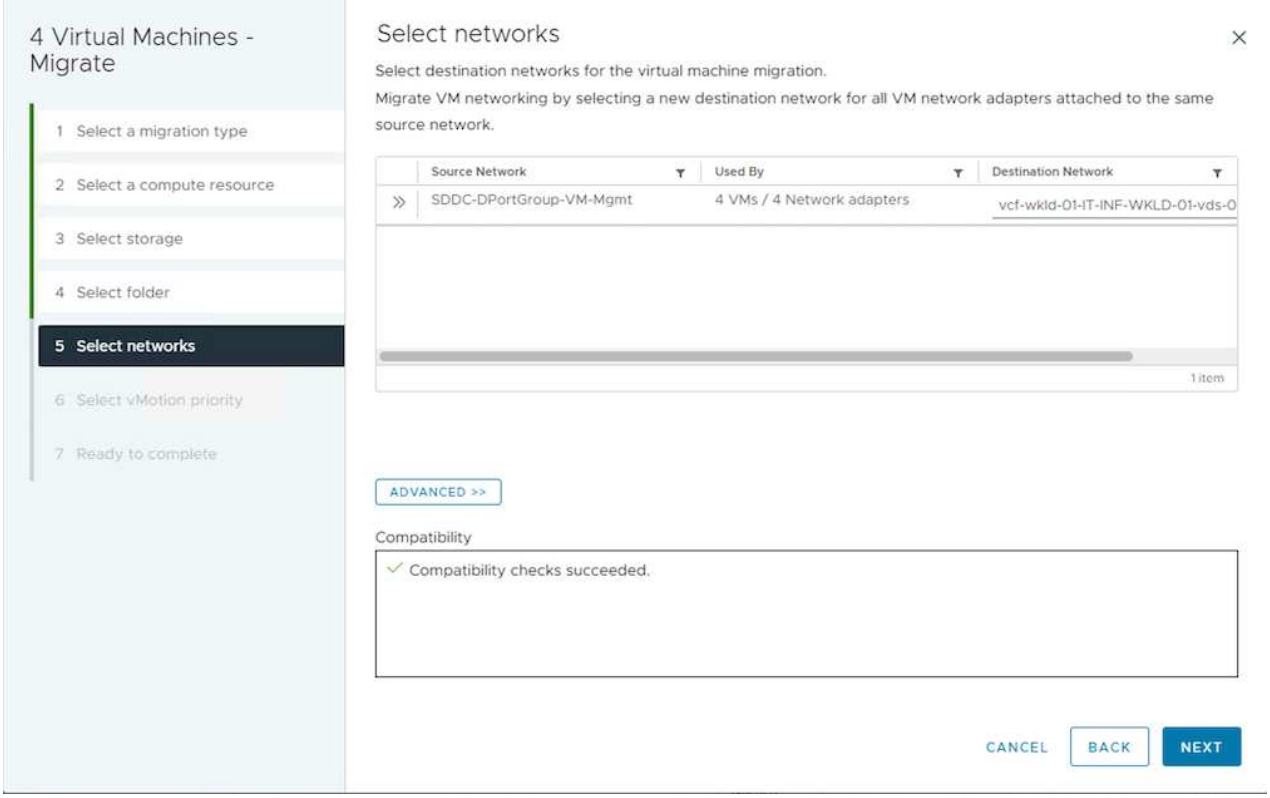
5. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.



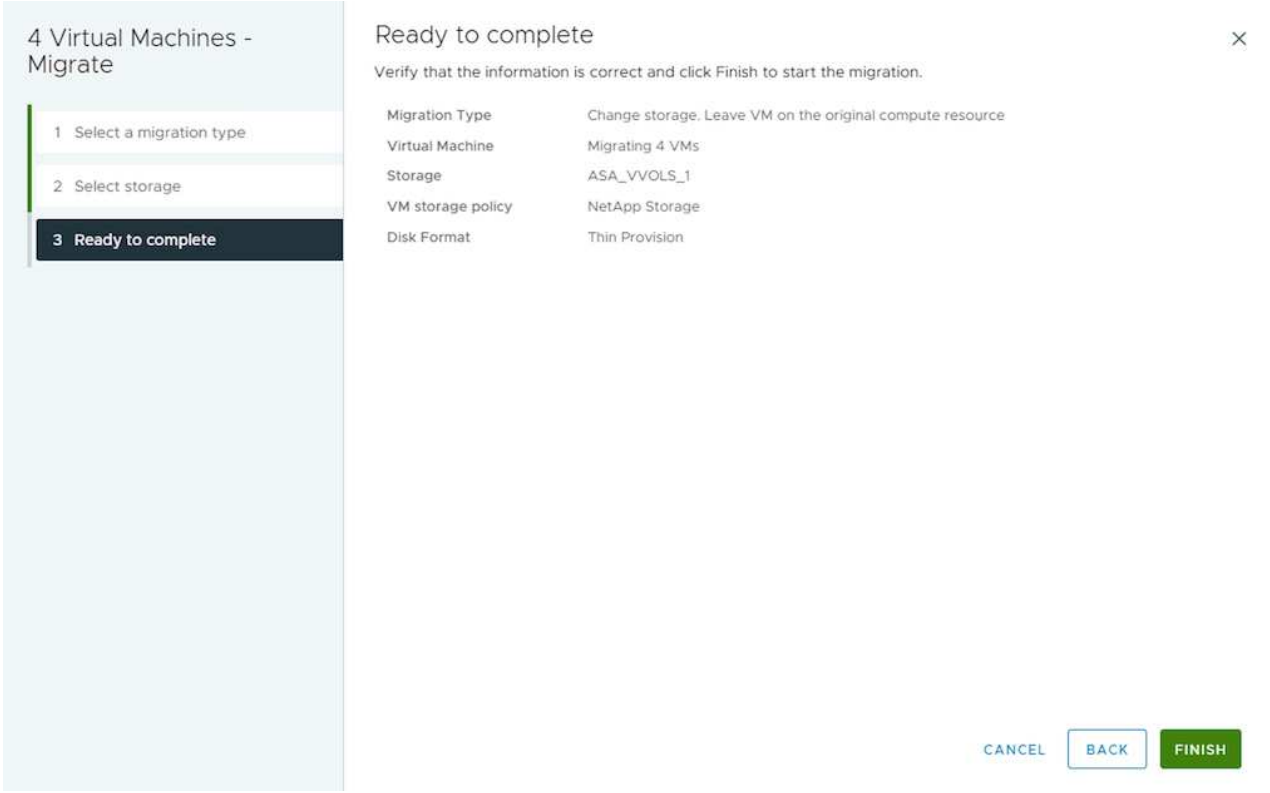
6. Wählen Sie den VM-Ordner aus, in dem die Ziel-VMs platziert werden sollen.



7. Wählen Sie die Zielportgruppe aus.



8. Überprüfen Sie den Eintrag und klicken Sie auf „Fertig stellen“.



Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

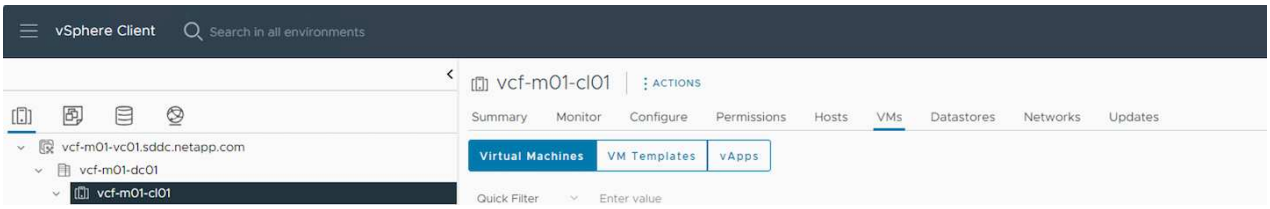
```
#Authenticate to vCenter
Connect-VIServer -server vcsa.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01' | Get-VM Aria*

#Gather VM Disk info
$vmdisk = $vm | Get-HardDisk

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'NetApp Storage'

#set VM Storage Policy for VM config and its data disks.
$vm, $vmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Migrate VMs to another cluster and Datastore specified by Policy
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy)

#When Portgroup is specific to each cluster, replace the above command
with
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster') -Datastore
(Get-SPBMCompatibleStorage -StoragePolicy $storagepolicy) -PortGroup
(Get-VirtualPortGroup 'VLAN 101')

#Ensure VM Storage Policy remains compliant.
$vm, $vmdisk | Get-SPBMEntityConfiguration
```

Migration von VMs über vCenter-Server in derselben SSO-Domäne

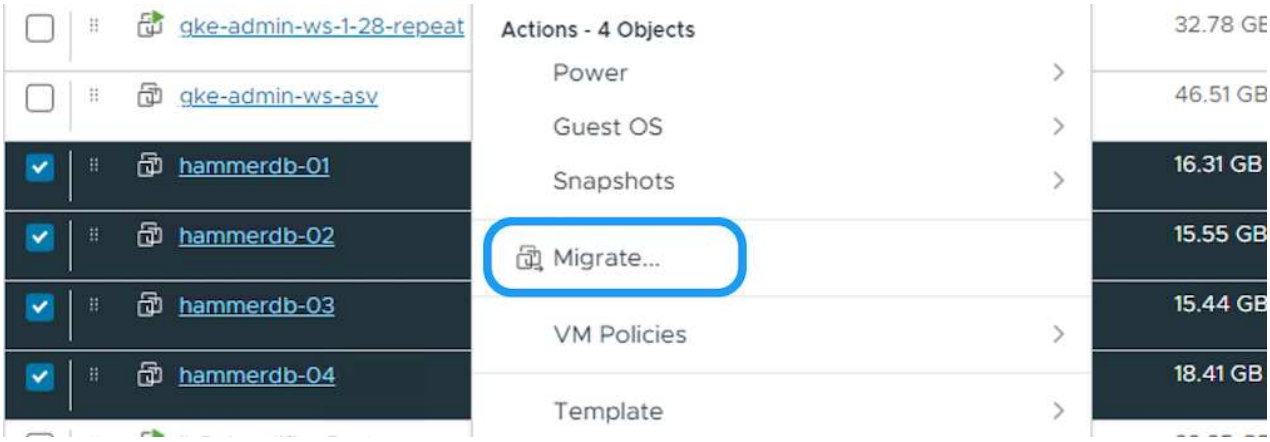
Befolgen Sie die nachstehenden Schritte, um VMs auf einen neuen vCenter-Server zu migrieren, der auf derselben vSphere-Client-Benutzeroberfläche aufgeführt ist.

> Weitere Anforderungen wie Quell- und Ziel-vCenter-Versionen usw. finden Sie unter "vSphere-Dokumentation zu den Anforderungen für vMotion zwischen vCenter-Serverinstanzen"

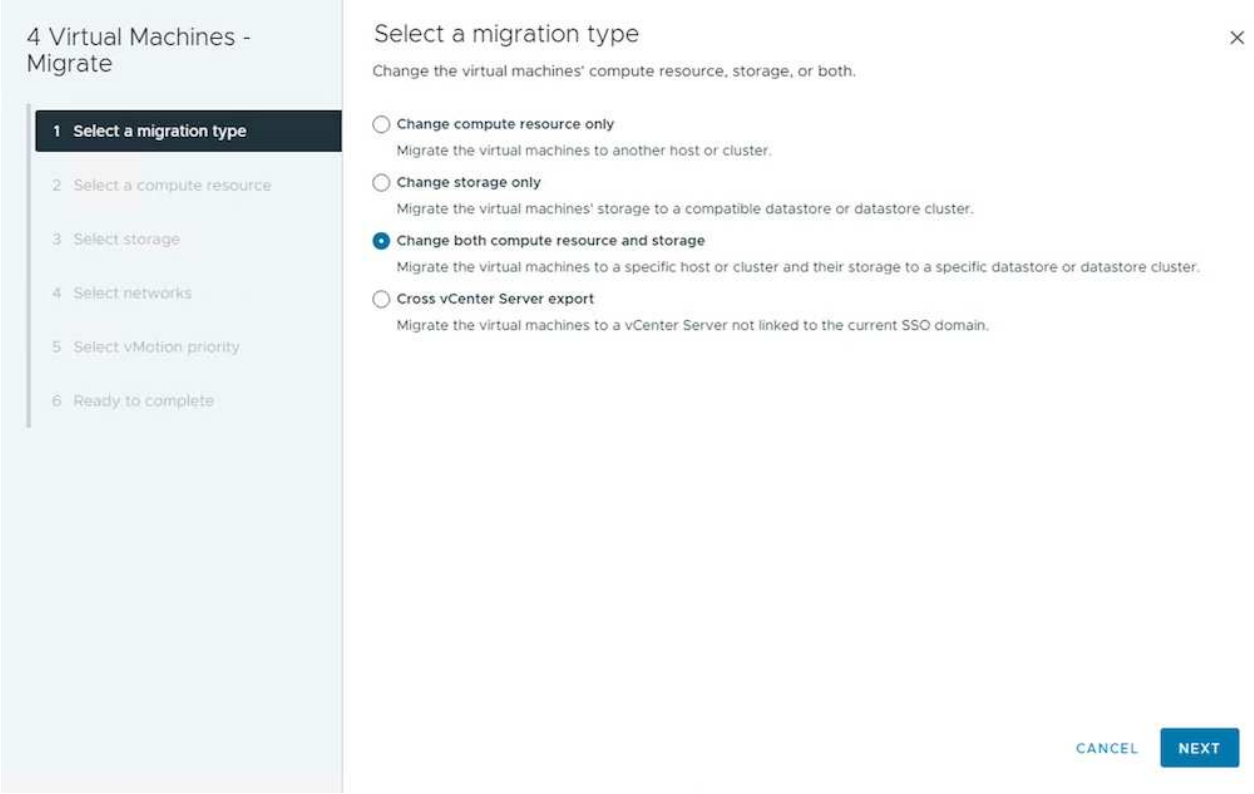
1. Wählen Sie mit dem vSphere Web Client den Cluster aus dem Host- und Cluster-Inventar aus und klicken Sie auf die Registerkarte „VMs“.



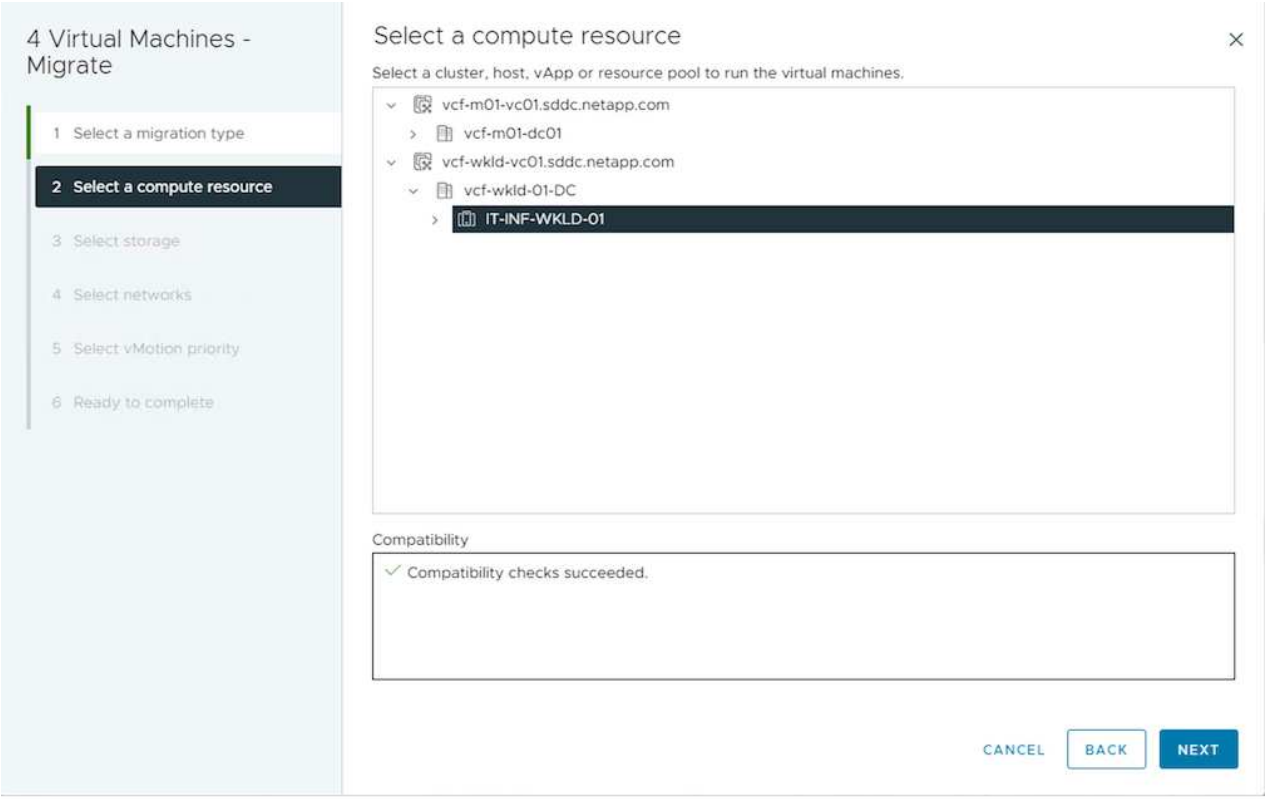
2. Wählen Sie die VMs aus, die migriert werden müssen, und klicken Sie mit der rechten Maustaste, um die Option „Migrieren“ auszuwählen.



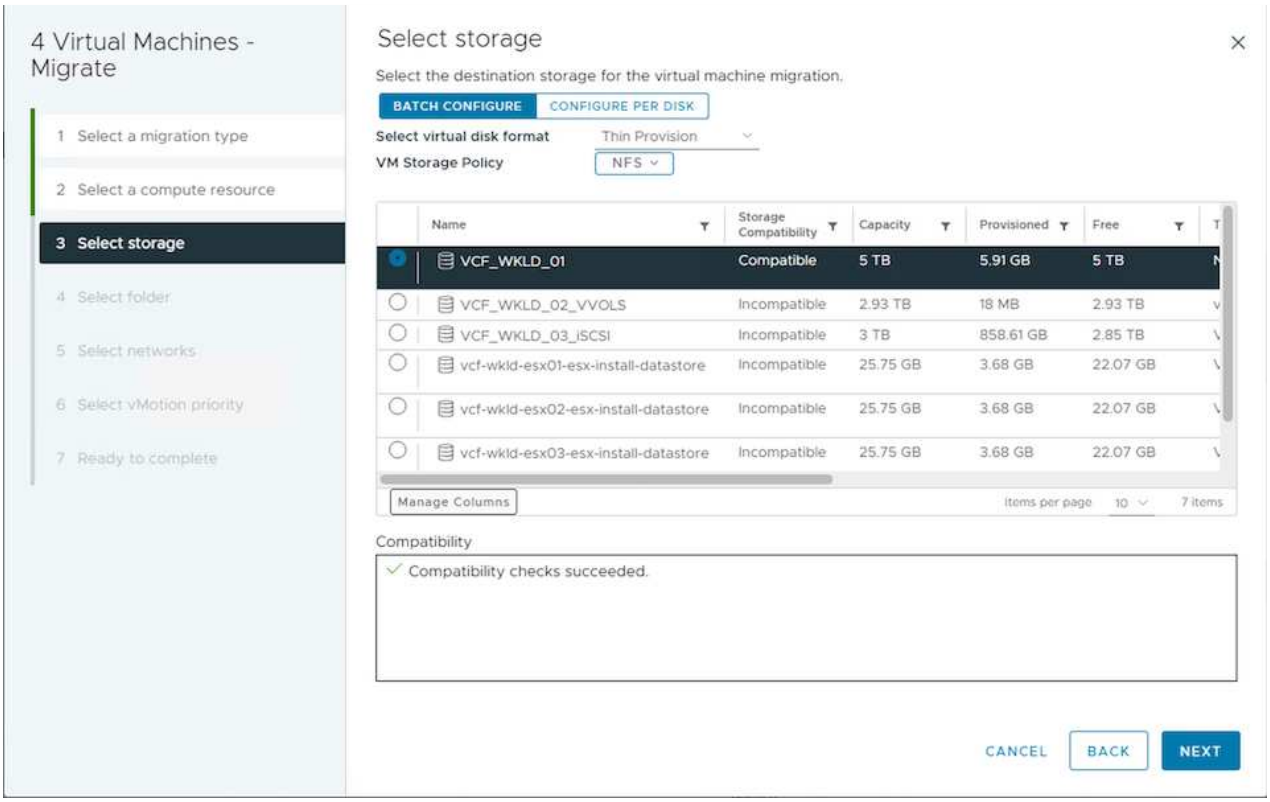
3. Wählen Sie die Option zum Ändern der Rechenressourcen und des Speichers und klicken Sie auf „Weiter“.



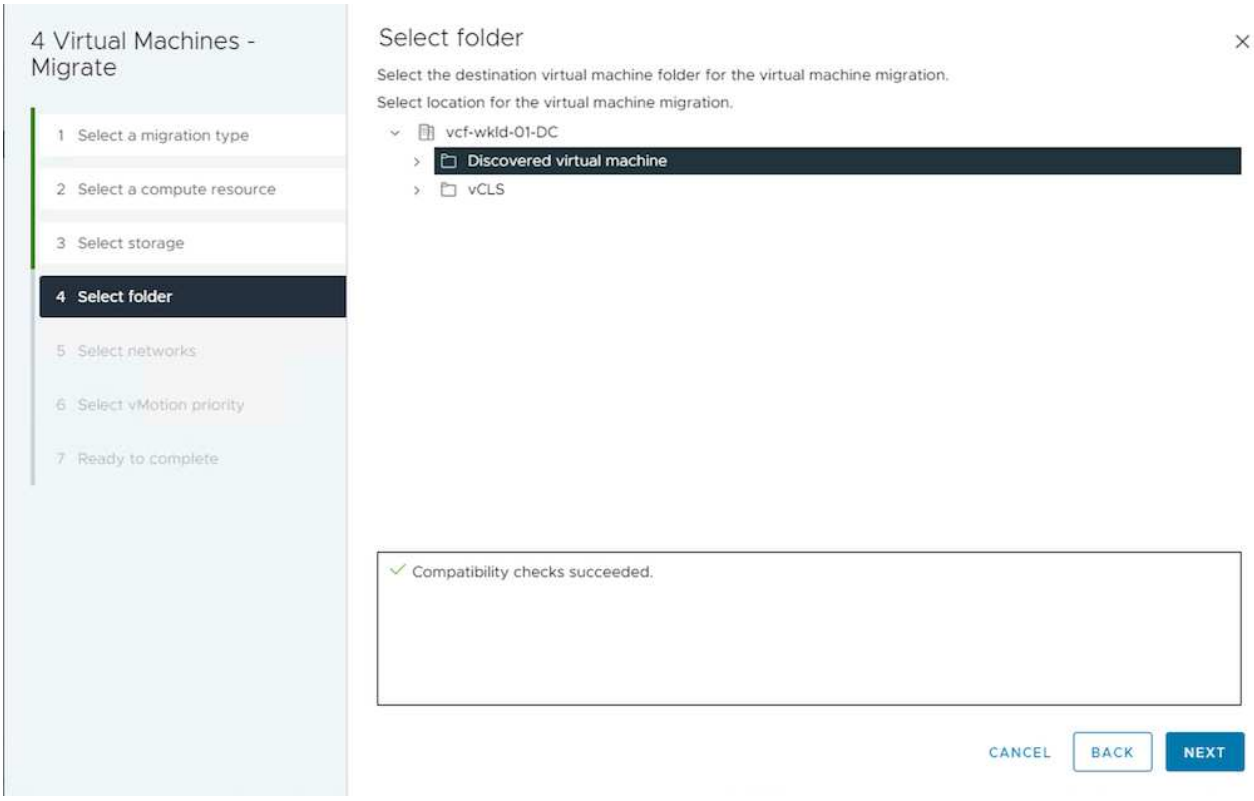
4. Wählen Sie den Zielcluster im Ziel-vCenter-Server aus.



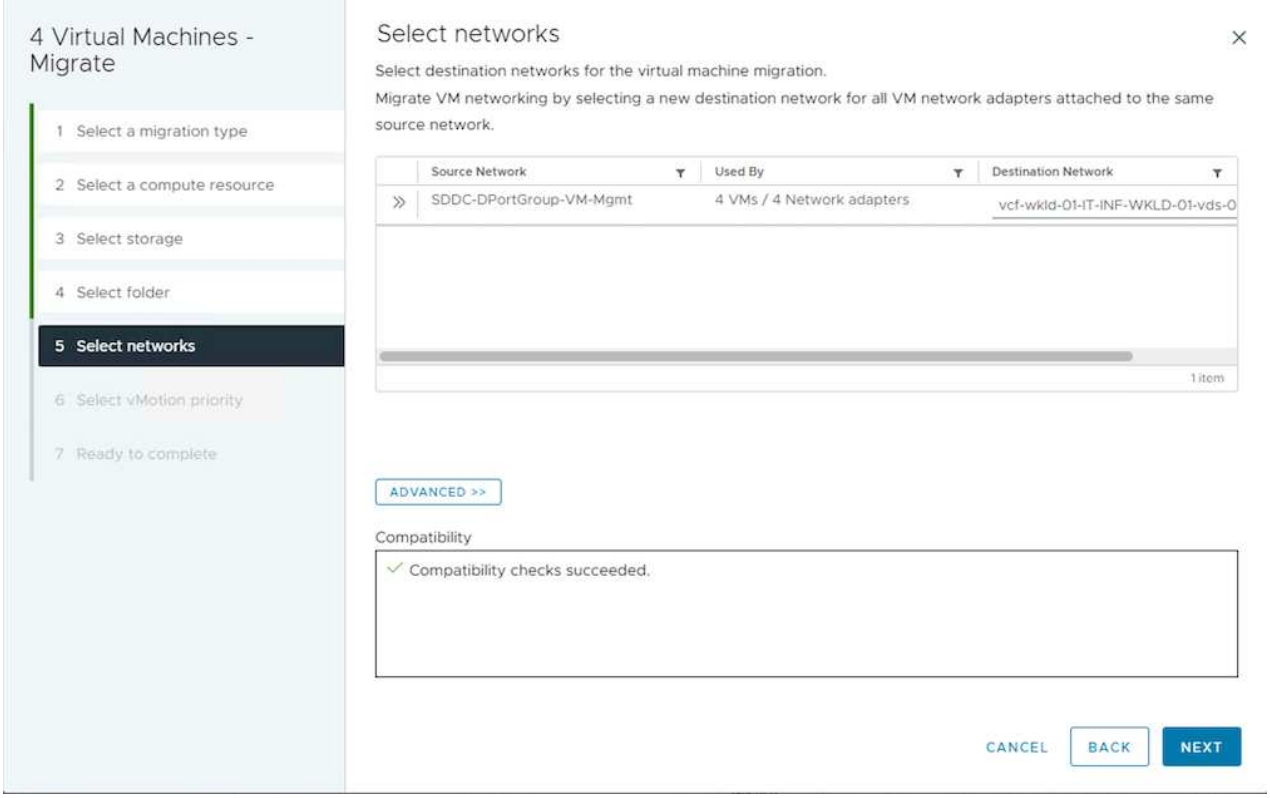
5. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.



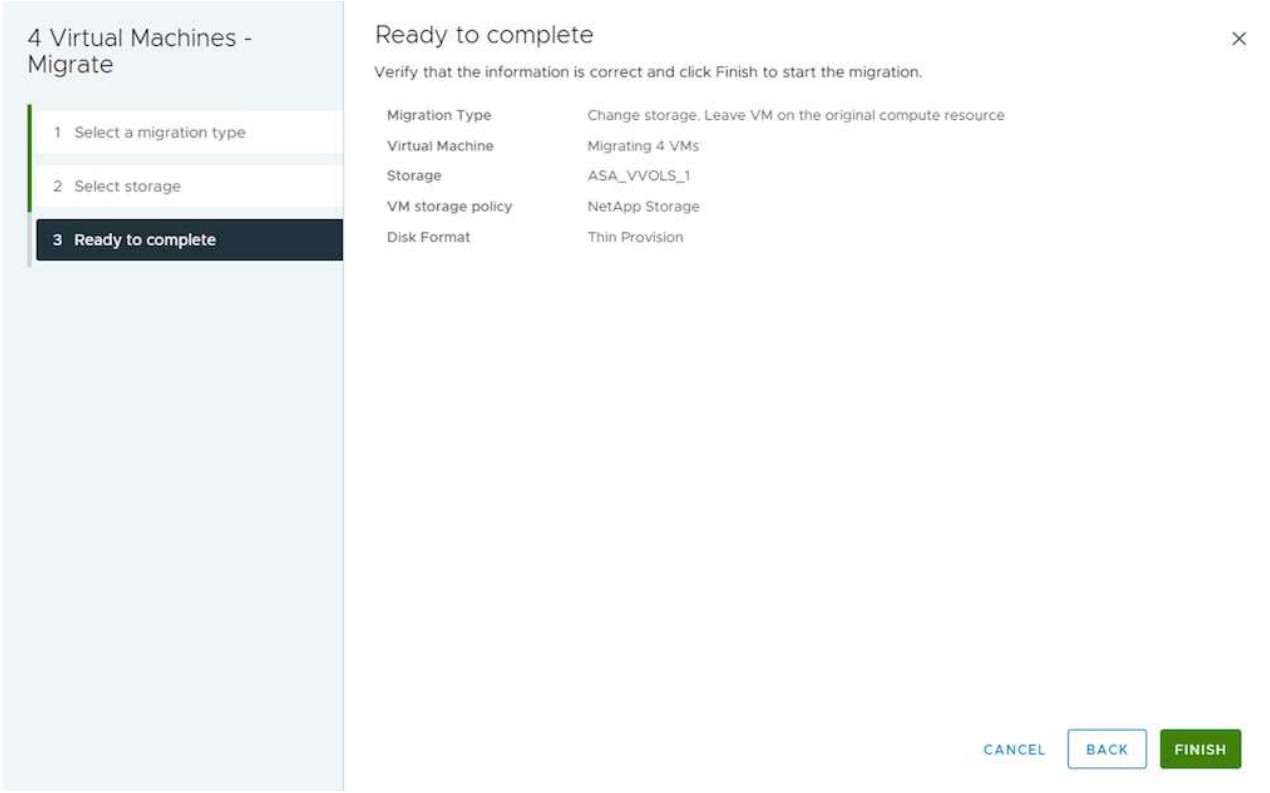
6. Wählen Sie den VM-Ordner aus, in dem die Ziel-VMs platziert werden sollen.



7. Wählen Sie die Zielportgruppe aus.



8. Überprüfen Sie die Migrationsoptionen und klicken Sie auf „Fertig stellen“.



Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

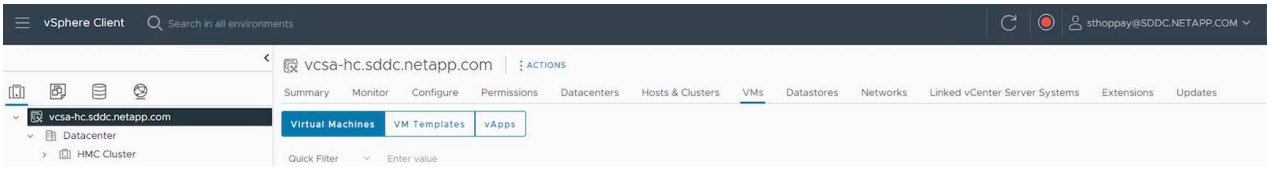
```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'vcf-m01-cl01'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migration von VMs über vCenter-Server in verschiedenen SSO-Domänen

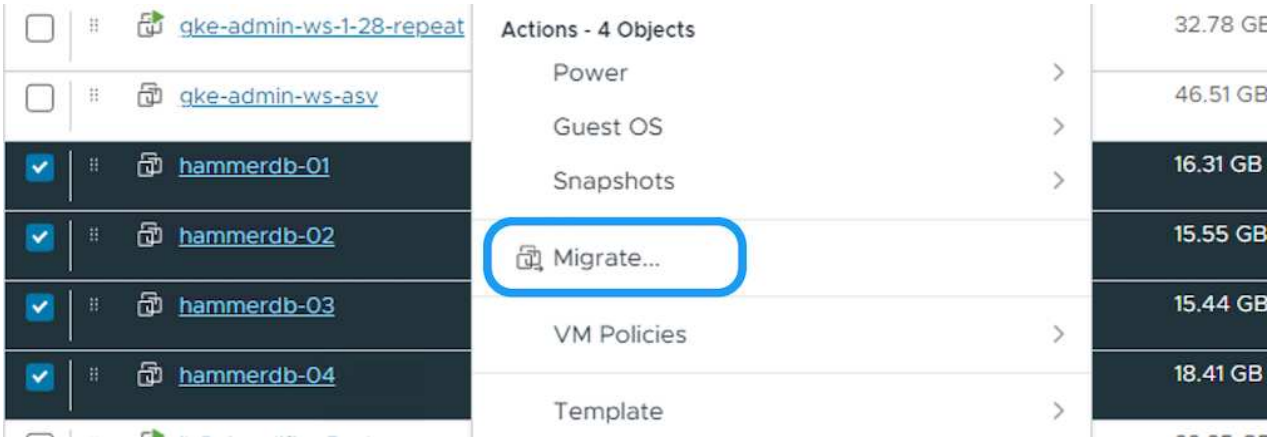
> Dieses Szenario geht davon aus, dass die Kommunikation zwischen den vCenter-Servern besteht. Andernfalls prüfen Sie das unten aufgeführte Szenario für mehrere Rechenzentrumsstandorte. Voraussetzungen finden Sie unter "vSphere-Dokumentation zu Advanced Cross vCenter vMotion"

Befolgen Sie die nachstehenden Schritte, um VMs mithilfe der Benutzeroberfläche auf einen anderen vCenter-Server zu migrieren.

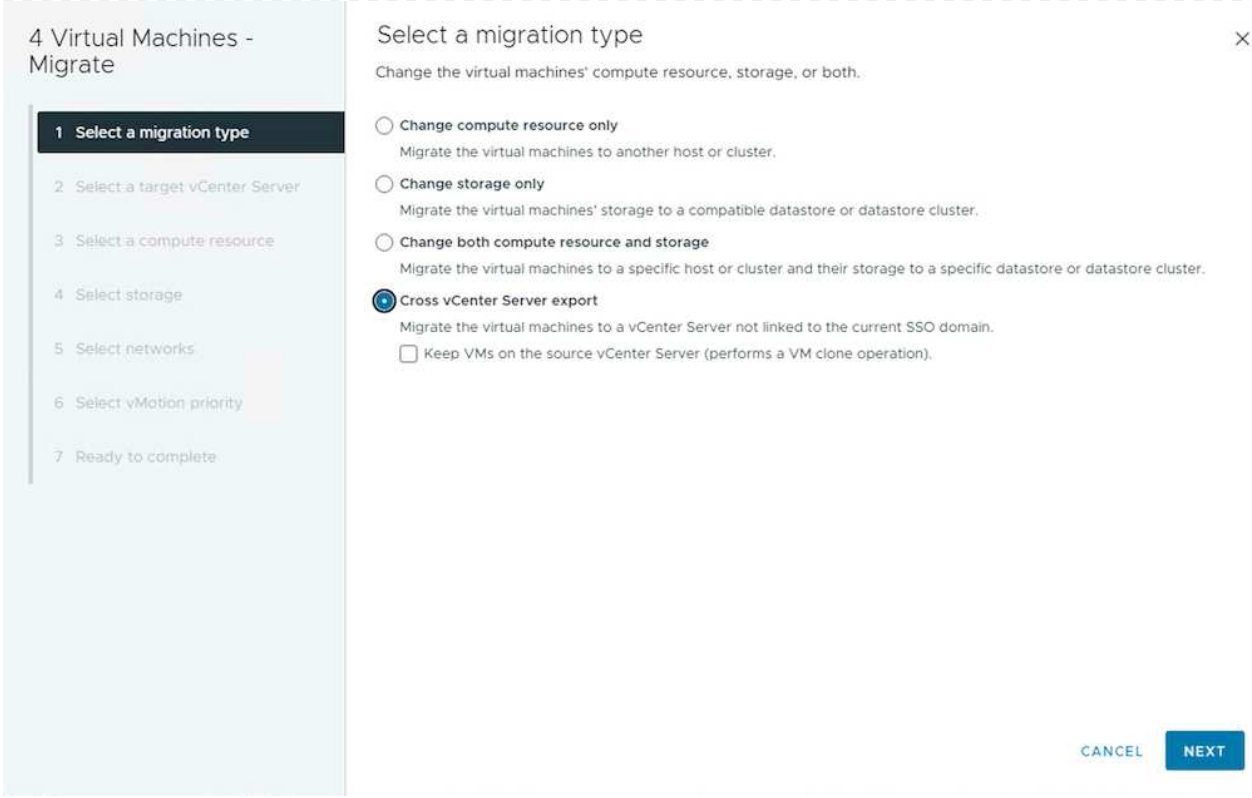
1. Wählen Sie mit dem vSphere Web Client den Quell-vCenter-Server aus und klicken Sie auf die Registerkarte „VMs“.



2. Wählen Sie die VMs aus, die migriert werden müssen, und klicken Sie mit der rechten Maustaste, um die Option „Migrieren“ auszuwählen.

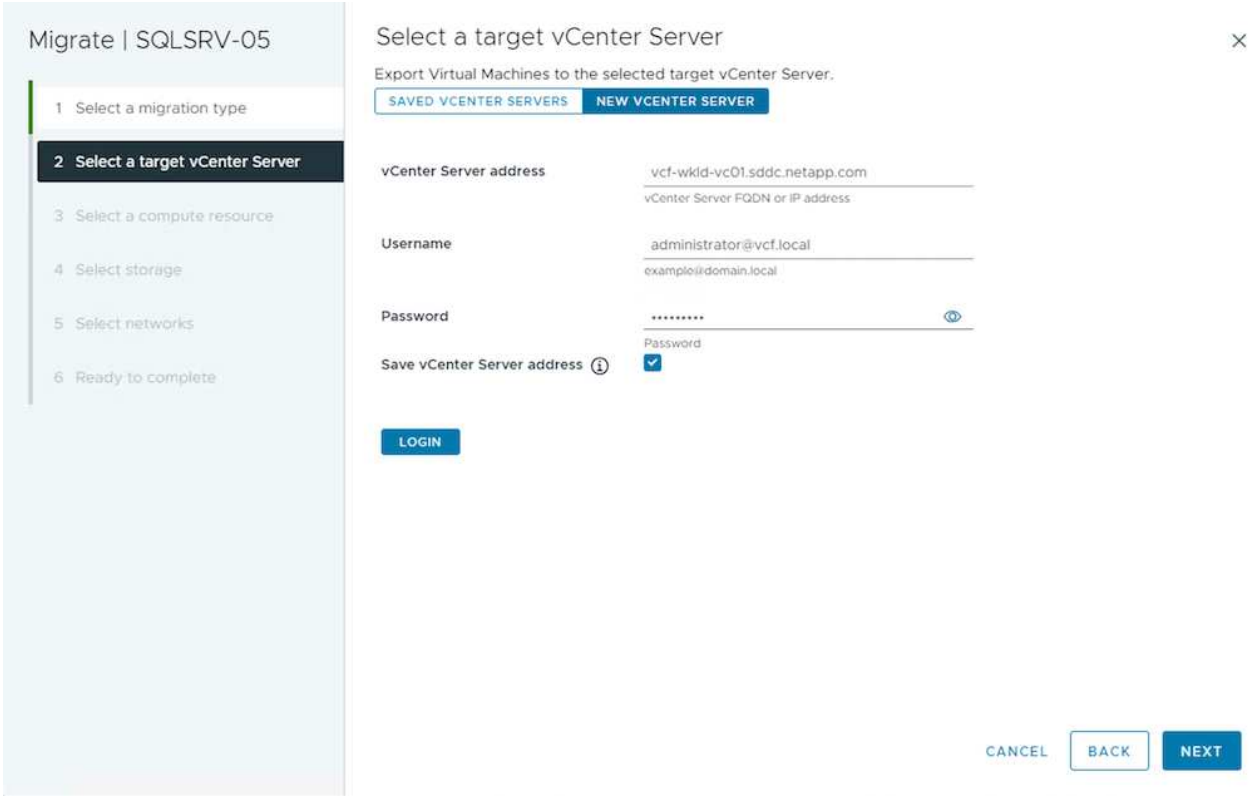


3. Wählen Sie die Option Cross vCenter Server-Export und klicken Sie auf Weiter

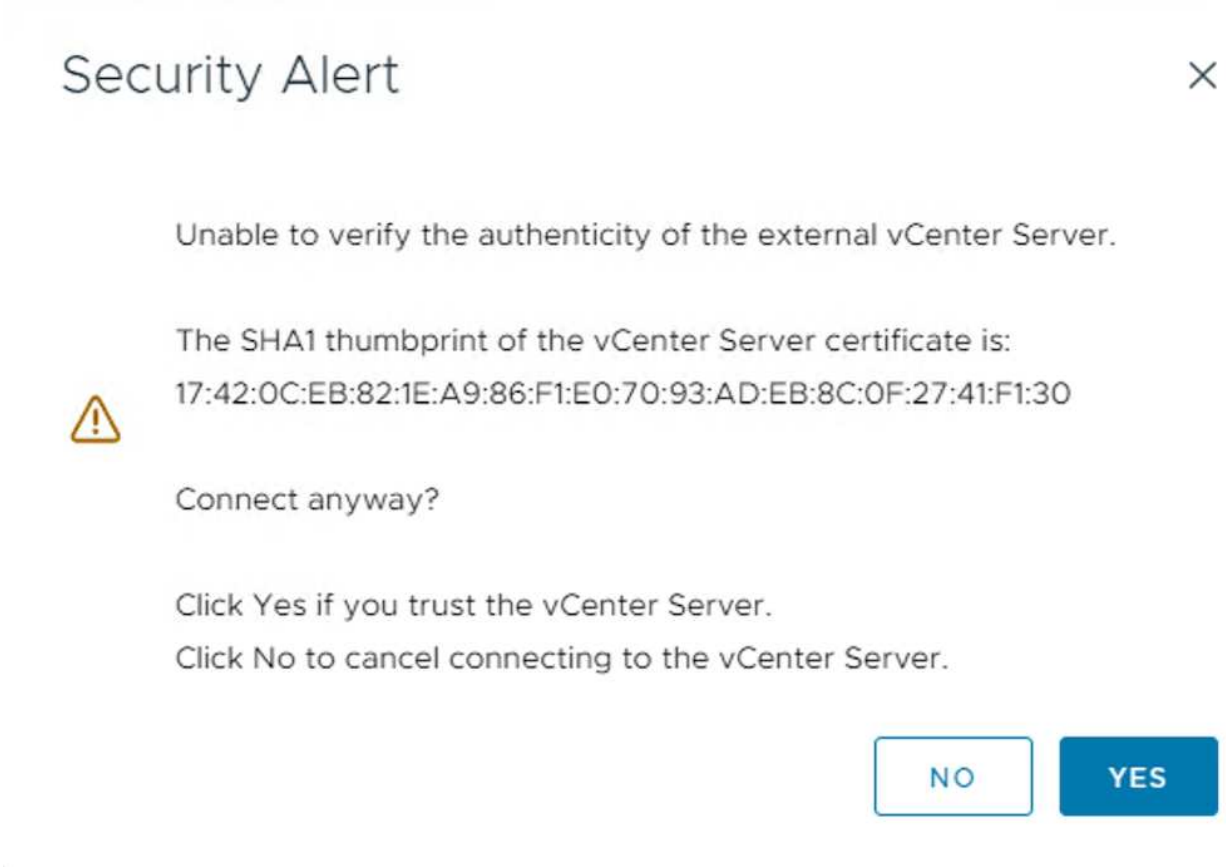


VM kann auch vom Ziel-vCenter-Server importiert werden. Überprüfen Sie für dieses Verfahren "Importieren oder Klonen einer virtuellen Maschine mit Advanced Cross vCenter vMotion"

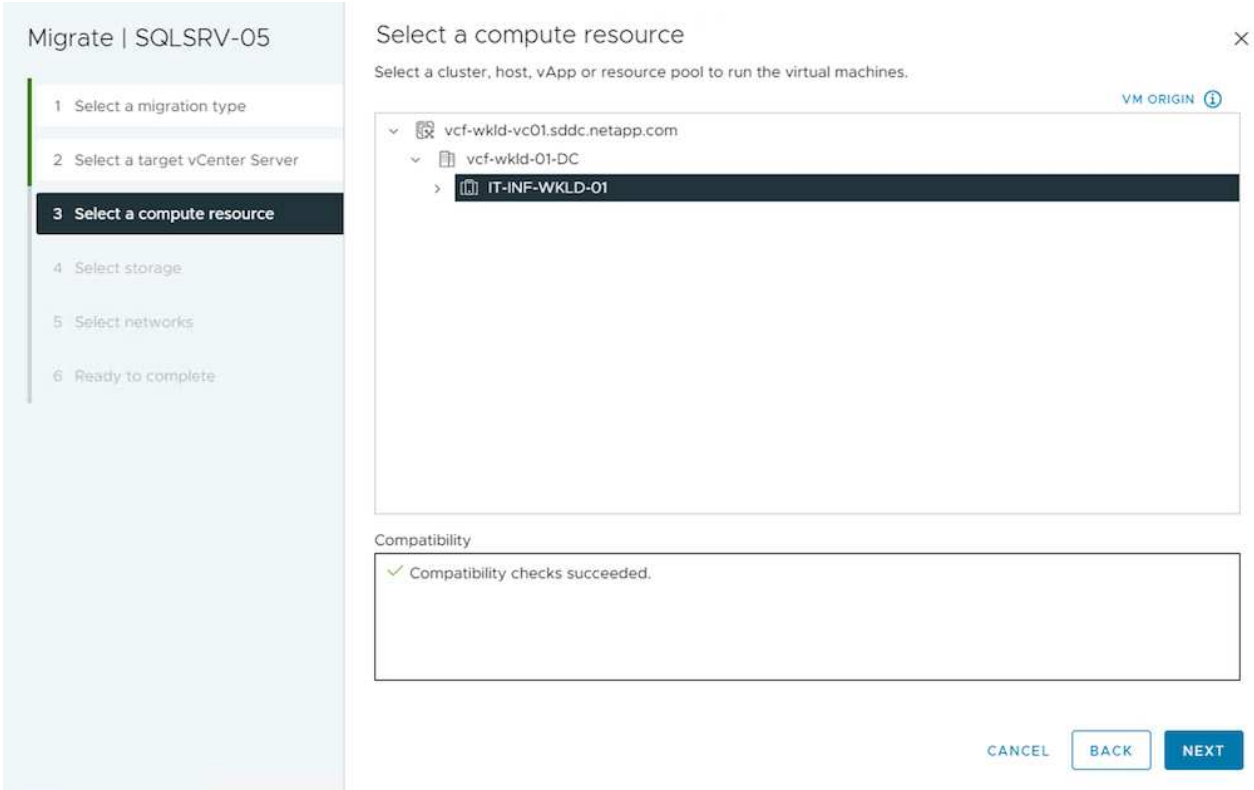
4. Geben Sie die vCenter-Anmeldeinformationen ein und klicken Sie auf „Anmelden“.



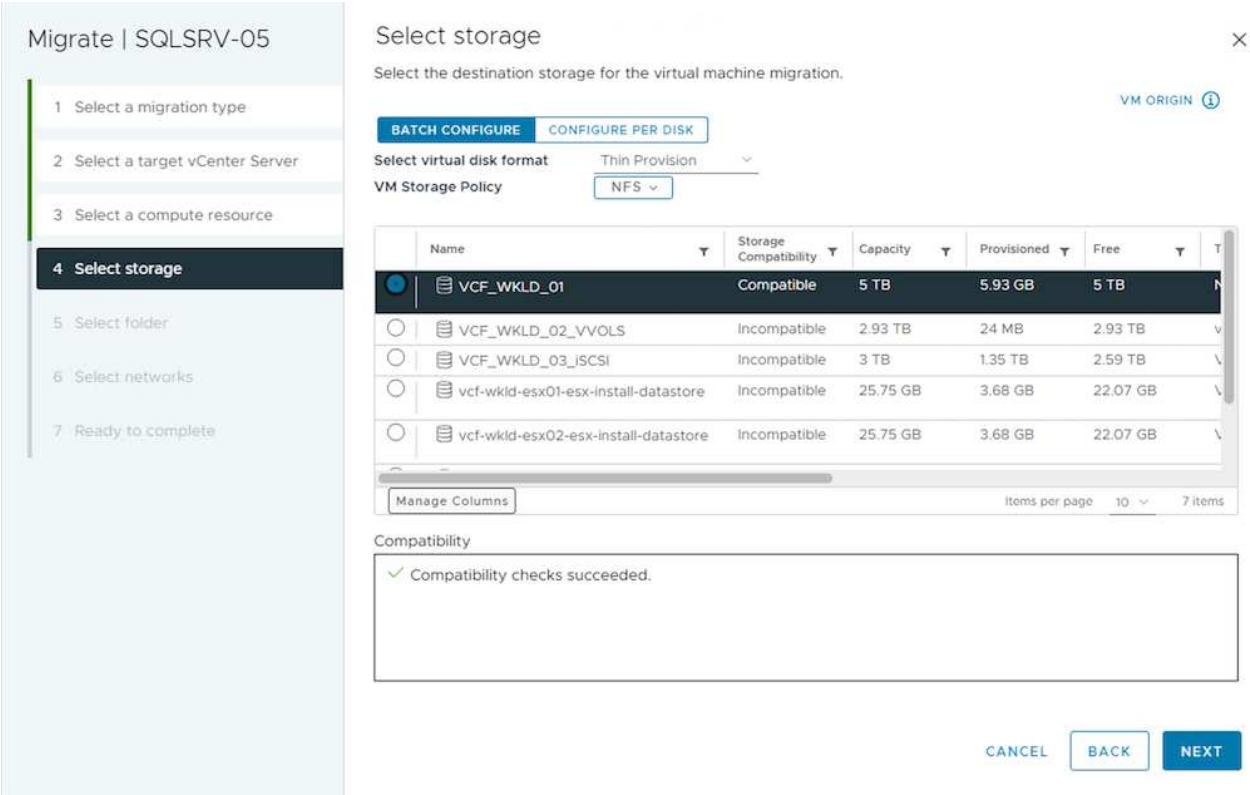
5. Bestätigen und akzeptieren Sie den Fingerabdruck des SSL-Zertifikats des vCenter-Servers



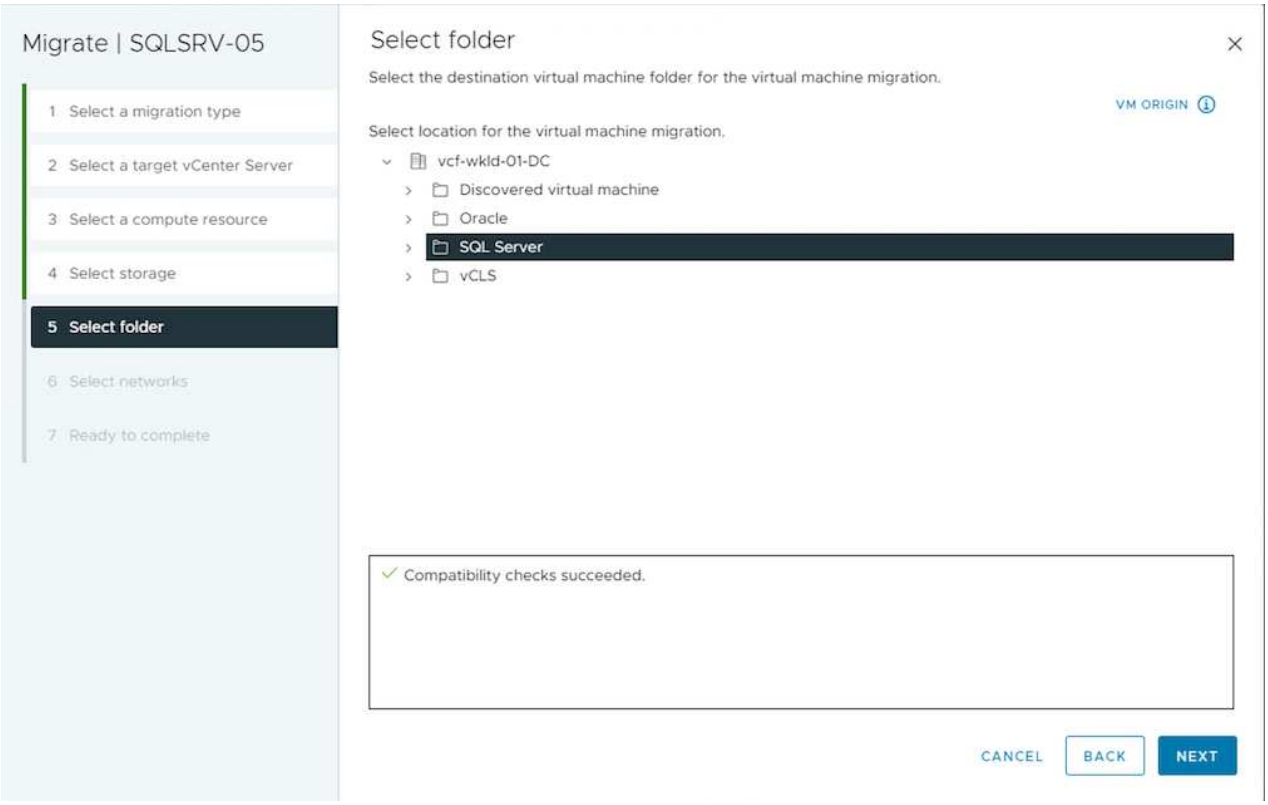
6. Erweitern Sie das Ziel-vCenter und wählen Sie den Ziel-Compute-Cluster aus.



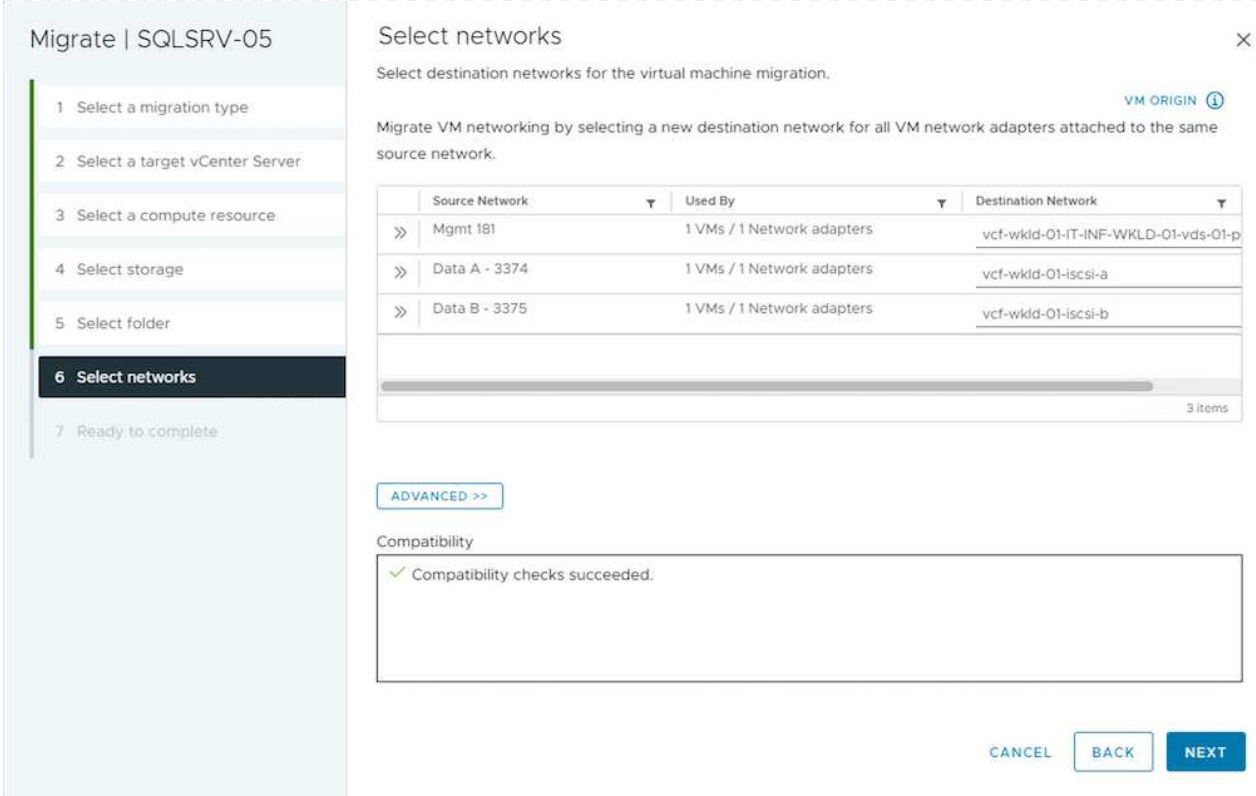
7. Wählen Sie den Zieldatenspeicher basierend auf der VM-Speicherrichtlinie aus.



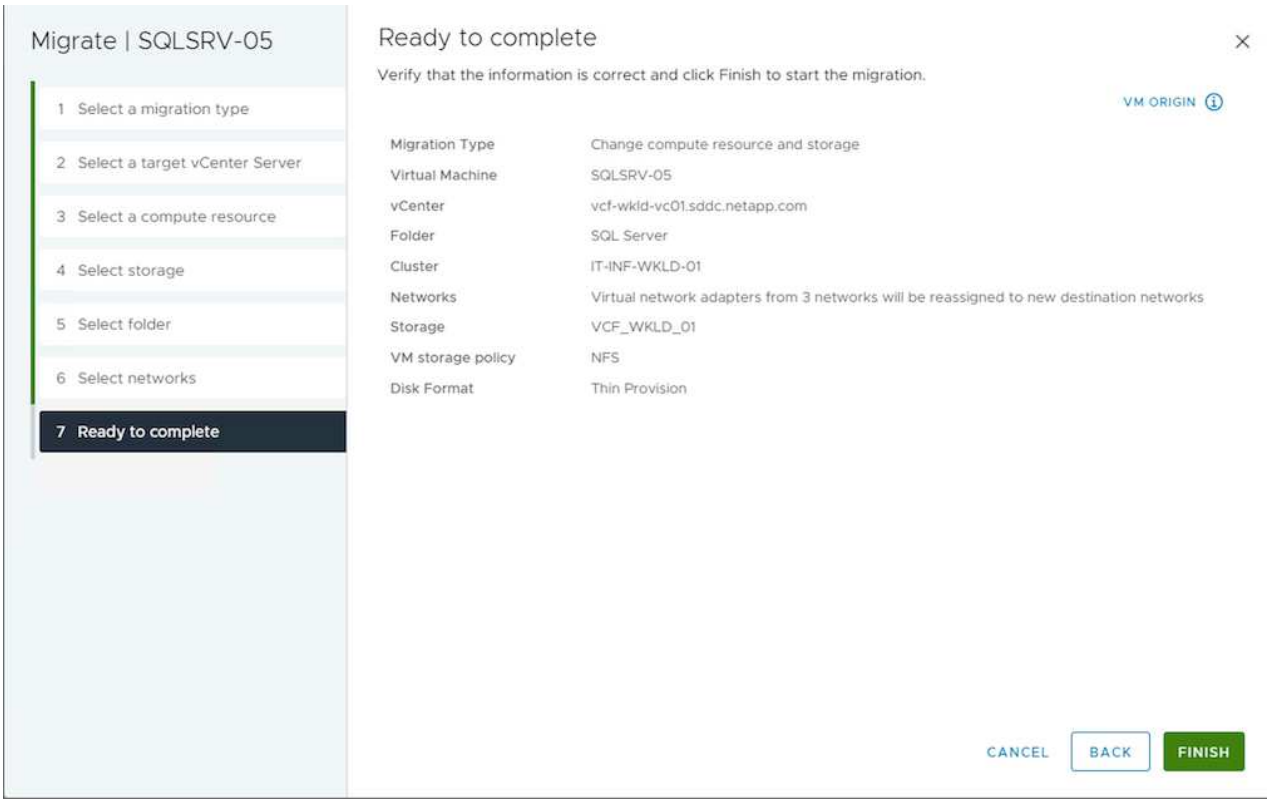
8. Wählen Sie den Ziel-VM-Ordner aus.



9. Wählen Sie die VM-Portgruppe für jede Netzwerkschnittstellenkartenzuordnung aus.



10. Überprüfen Sie die Angaben und klicken Sie auf „Fertig stellen“, um vMotion auf den vCenter-Servern zu starten.



Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

```
#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vcsa01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vcsa02.sddc.netapp.local -force

# Get all VMs with filter applied for a specific cluster
$vm = Get-Cluster 'Source Cluster'  -server $sourcevc| Get-VM Win*

#Gather the desired Storage Policy to set for the VMs. Policy should be
available with valid datastores.
$storagepolicy = Get-SPBMStoragePolicy 'iSCSI' -server $targetvc

#Migrate VMs to target vCenter
$vm | Move-VM -Destination (Get-Cluster 'Target Cluster' -server
$targetvc) -Datastore (Get-SPBMCompatibleStorage -StoragePolicy
$storagepolicy -server $targetvc) -PortGroup (Get-VirtualPortGroup
'VLAN 101' -server $targetvc)

$targetvm = Get-Cluster 'Target Cluster' -server $targetvc | Get-VM
Win*

#Gather VM Disk info
$targetvmdisk = $targetvm | Get-HardDisk

#set VM Storage Policy for VM config and its data disks.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration | Set-
SPBMEntityConfiguration -StoragePolicy $storagepolicy

#Ensure VM Storage Policy remains compliant.
$targetvm, $targetvmdisk | Get-SPBMEntityConfiguration
```

Migration von VMs zwischen Rechenzentrumsstandorten

- Wenn der Layer-2-Datenverkehr über mehrere Rechenzentren verteilt wird, entweder mithilfe von NSX Federation oder anderen Optionen, befolgen Sie das Verfahren zum Migrieren von VMs über vCenter-Server.
- HCX bietet verschiedene "Migrationstypen" einschließlich Replication Assisted vMotion über die Rechenzentren hinweg, um VM ohne Ausfallzeiten zu verschieben.
- "Site Recovery Manager (SRM)"ist in der Regel für die Notfallwiederherstellung gedacht und wird auch häufig für die geplante Migration unter Verwendung einer auf Speicher-Arrays basierenden Replikation verwendet.
- Continous Data Protection (CDP) Produkte verwenden "vSphere API für IO (VAIO)" um die Daten abzufangen und eine Kopie an einen entfernten Standort zu senden, für eine RPO-Lösung nahe Null.
- Es können auch Backup- und Wiederherstellungsprodukte verwendet werden. Führt aber oft zu einer längeren RTO.
- "BlueXP Disaster Recovery als Service (DRaaS)"nutzt die auf Speicherarrays basierende Replikation und automatisiert bestimmte Aufgaben, um die VMs am Zielstandort wiederherzustellen.

Migration von VMs in Hybrid-Cloud-Umgebungen

- "Konfigurieren des Hybrid Linked Mode"und befolgen Sie das Verfahren von"Migration von VMs über vCenter-Server in derselben SSO-Domäne"
- HCX bietet verschiedene "Migrationstypen" einschließlich Replication Assisted vMotion über die Rechenzentren hinweg, um VMs zu verschieben, während sie eingeschaltet sind.
  - "TR 4942: Migrieren Sie Workloads mit VMware HCX zum FSx ONTAP Datenspeicher"
  - "TR-4940: Migrieren von Workloads zum Azure NetApp Files Datenspeicher mithilfe von VMware HCX – Kurzanleitung"
  - "Migrieren Sie Workloads mit VMware HCX zum Google Cloud NetApp Volumes -Datenspeicher auf Google Cloud VMware Engine – Kurzanleitung"
- "BlueXP Disaster Recovery als Service (DRaaS)"nutzt die auf Speicherarrays basierende Replikation und automatisiert bestimmte Aufgaben, um die VMs am Zielstandort wiederherzustellen.
- Mit unterstützten Continous Data Protection (CDP)-Produkten, die "vSphere API für IO (VAIO)" um die Daten abzufangen und eine Kopie an einen entfernten Standort zu senden, für eine RPO-Lösung nahe Null.

> Wenn sich die Quell-VM auf einem Block-vVol-Datenspeicher befindet, kann sie mit SnapMirror auf Amazon FSx ONTAP oder Cloud Volumes ONTAP (CVO) bei anderen unterstützten Cloud-Anbietern repliziert und als iSCSI-Volume mit Cloud-nativen VMs genutzt werden.

Szenarien für die Migration von VM-Vorlagen

VM-Vorlagen können von vCenter Server oder einer Inhaltsbibliothek verwaltet werden. Die Verteilung von VM-Vorlagen, OVF- und OVA-Vorlagen und anderen Dateitypen erfolgt durch Veröffentlichung in der lokalen Inhaltsbibliothek und Remote-Inhaltsbibliotheken können diese abonnieren.

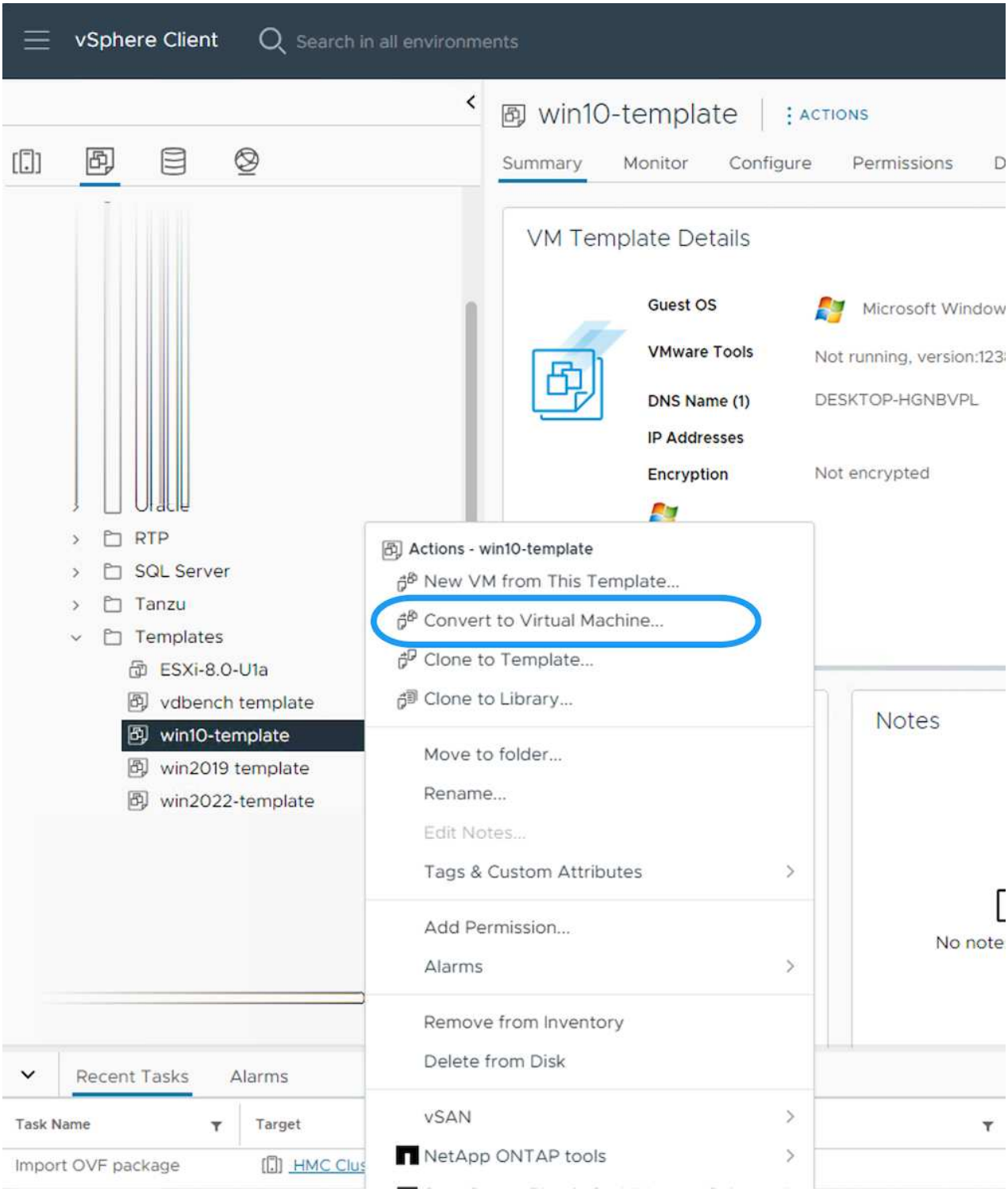
- Im vCenter-Inventar gespeicherte VM-Vorlagen können in VMs konvertiert werden und die VM-

Migrationsoptionen nutzen.

- OVF- und OVA-Vorlagen sowie andere in der Inhaltsbibliothek gespeicherte Dateitypen können in andere Inhaltsbibliotheken geklont werden.
- VM-Vorlagen für Inhaltsbibliotheken können auf jedem Datenspeicher gehostet werden und müssen einer neuen Inhaltsbibliothek hinzugefügt werden.

Migration von VM-Vorlagen, die auf einem Datenspeicher gehostet werden

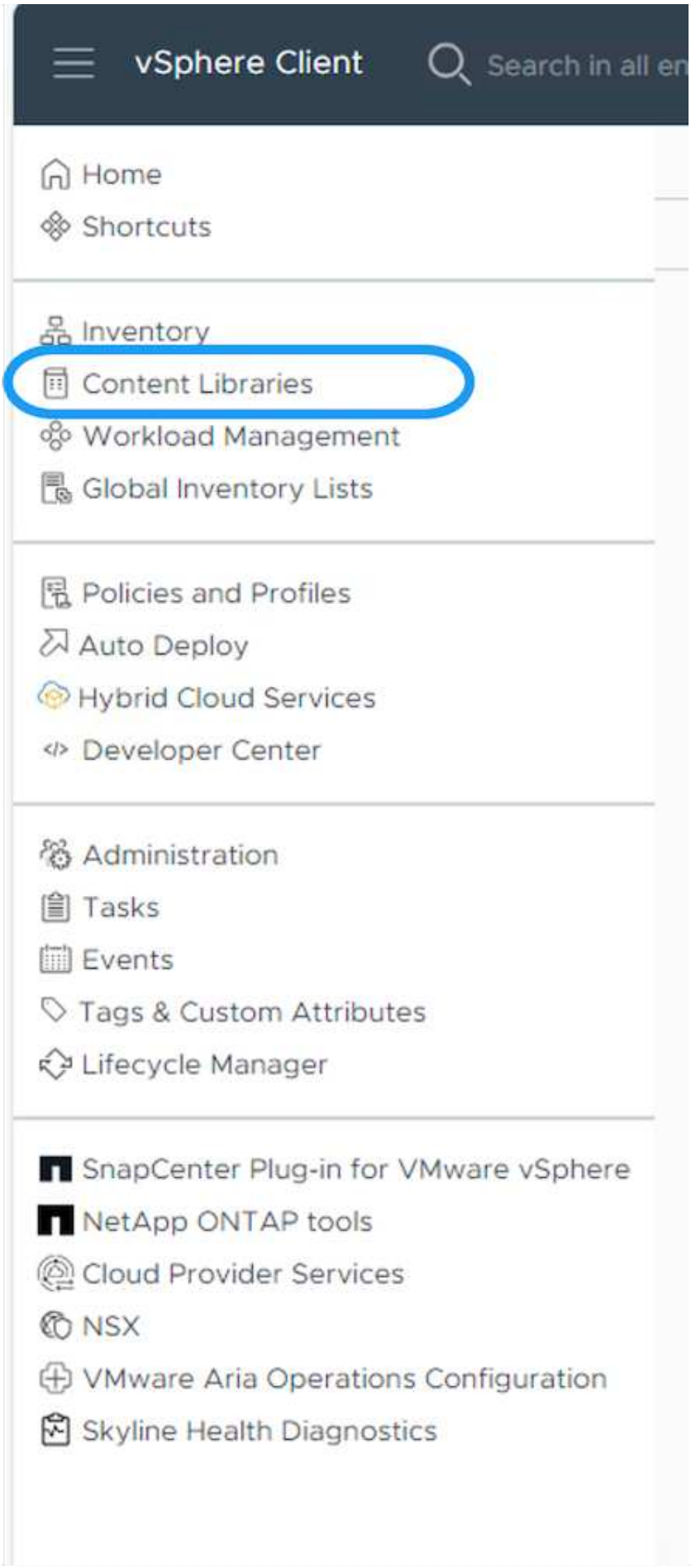
1. Klicken Sie im vSphere Web Client mit der rechten Maustaste auf die VM-Vorlage unter der Ordneransicht „VM und Vorlagen“ und wählen Sie die Option zum Konvertieren in VM.



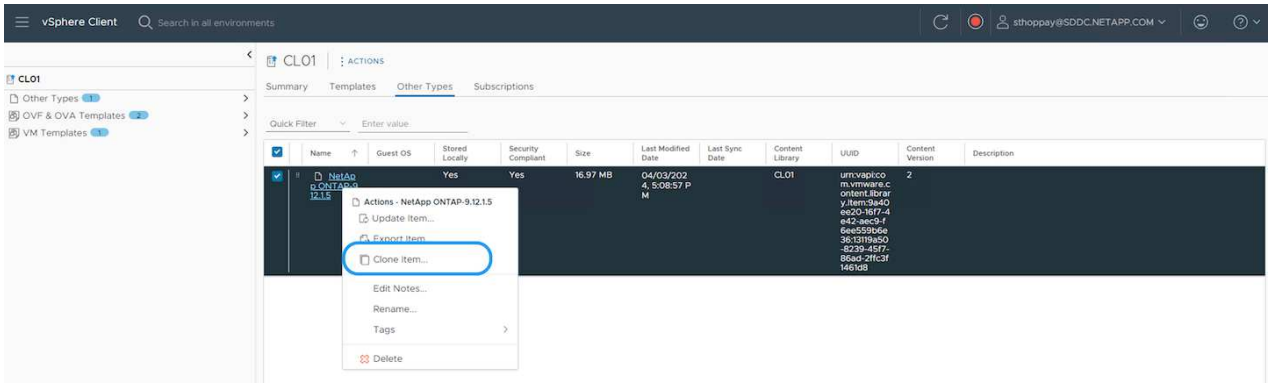
2. Sobald es als VM konvertiert ist, folgen Sie den VM-Migrationsoptionen.

Klonen von Elementen der Inhaltsbibliothek

1. Wählen Sie im vSphere Web Client Inhaltsbibliotheken aus

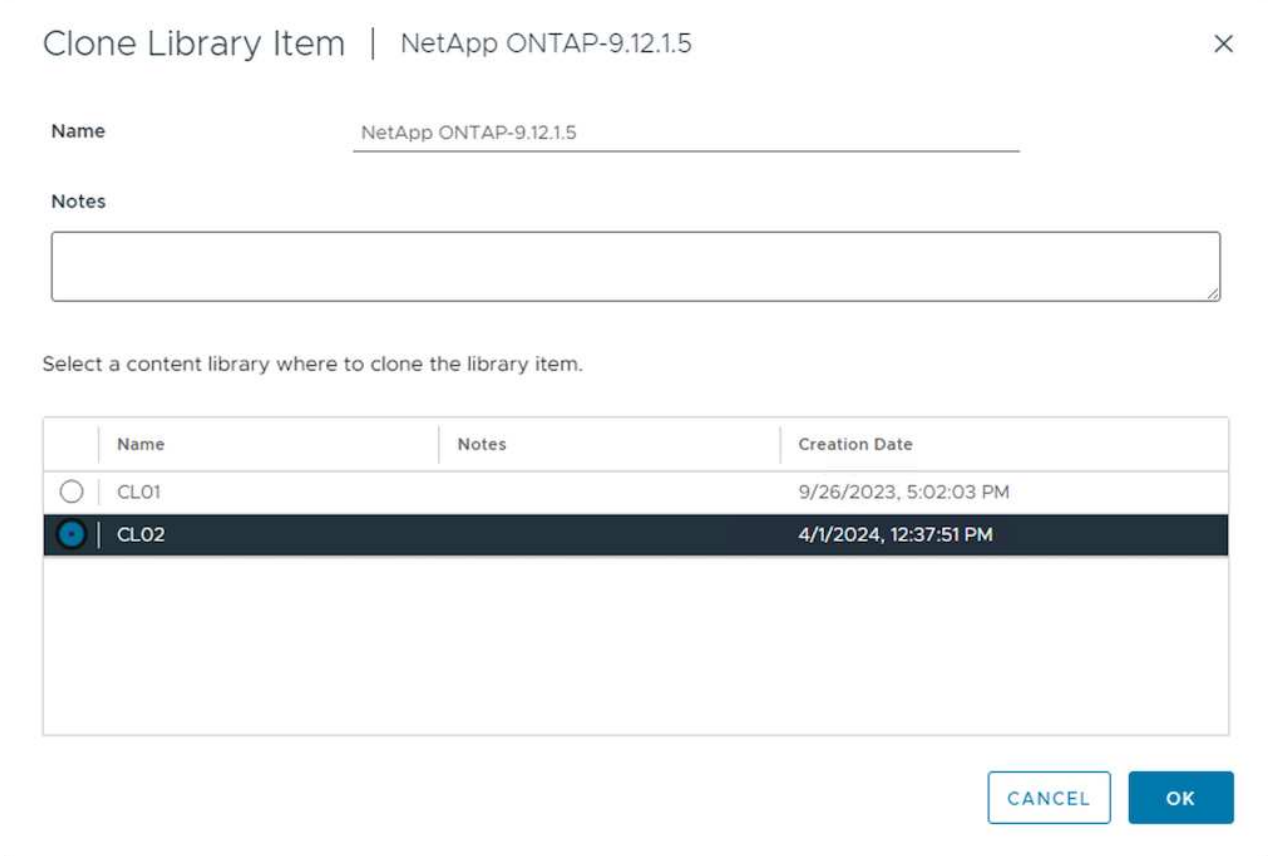

vSphere Client
Search in all en
Home
Shortcuts
Inventory
Content Libraries
Workload Management
Global Inventory Lists
Policies and Profiles
Auto Deploy
Hybrid Cloud Services
Developer Center
Administration
Tasks
Events
Tags & Custom Attributes
Lifecycle Manager
SnapCenter Plug-in for VMware vSphere
NetApp ONTAP tools
Cloud Provider Services
NSX
VMware Aria Operations Configuration
Skyline Health Diagnostics

2. Wählen Sie die Inhaltsbibliothek aus, in der sich das Element befindet, das Sie klonen möchten
3. Klicken Sie mit der rechten Maustaste auf das Element und klicken Sie auf „Element klonen“.

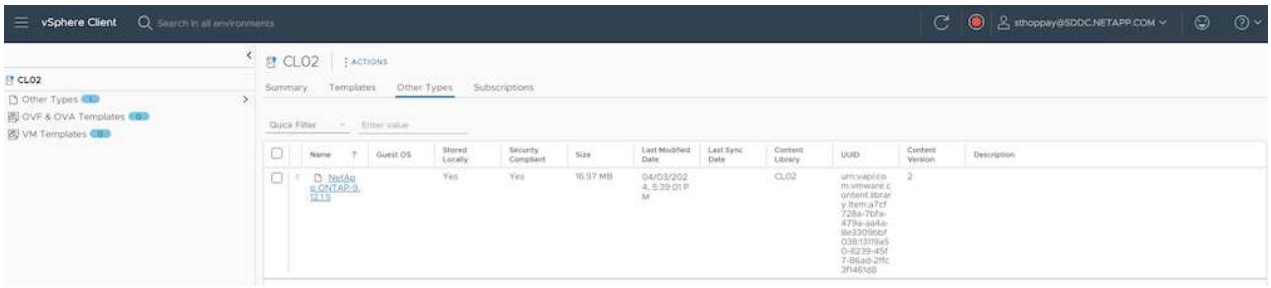


> Wenn Sie das Aktionsmenü verwenden, stellen Sie sicher, dass das richtige Zielobjekt zum Ausführen der Aktion aufgelistet ist.

4. Wählen Sie die Zielinhaltsbibliothek aus und klicken Sie auf OK.



5. Überprüfen Sie, ob das Element in der Zielinhaltsbibliothek verfügbar ist.

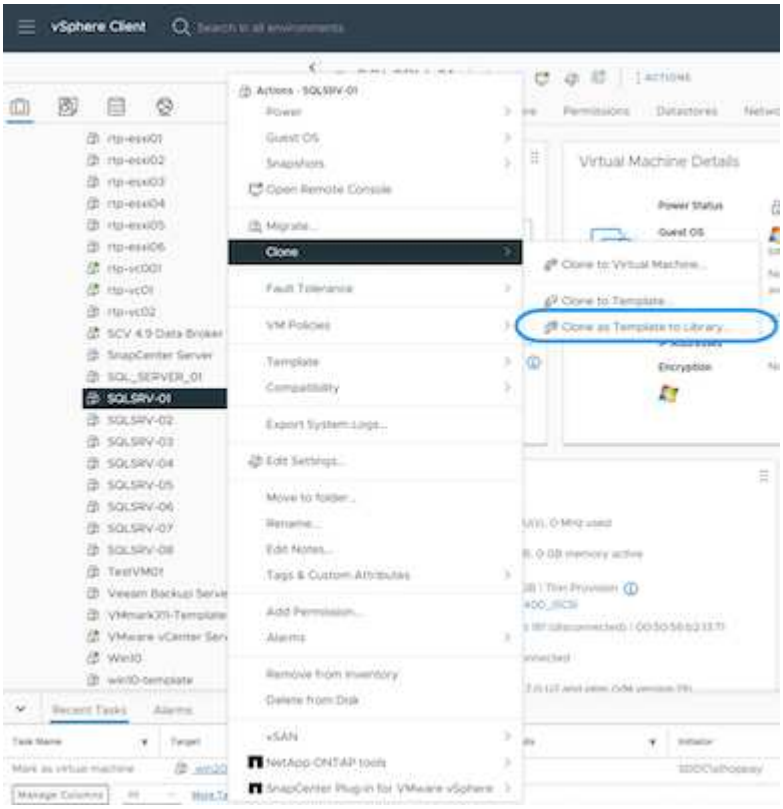


Hier ist das PowerCLI-Beispielskript zum Kopieren der Inhaltsbibliothekselemente von der Inhaltsbibliothek CL01 nach CL02.

```
#Authenticate to vCenter Server(s)
$sourcevc = Connect-VIServer -server 'vcenter01.domain' -force
$targetvc = Connect-VIServer -server 'vcenter02.domain' -force

#Copy content library items from source vCenter content library CL01 to
target vCenter content library CL02.
Get-ContentLibaryItem -ContentLibary (Get-ContentLibary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibaryItem -ContentLibrary (Get-ContentLibary 'CL02' -Server
$targetvc)
```

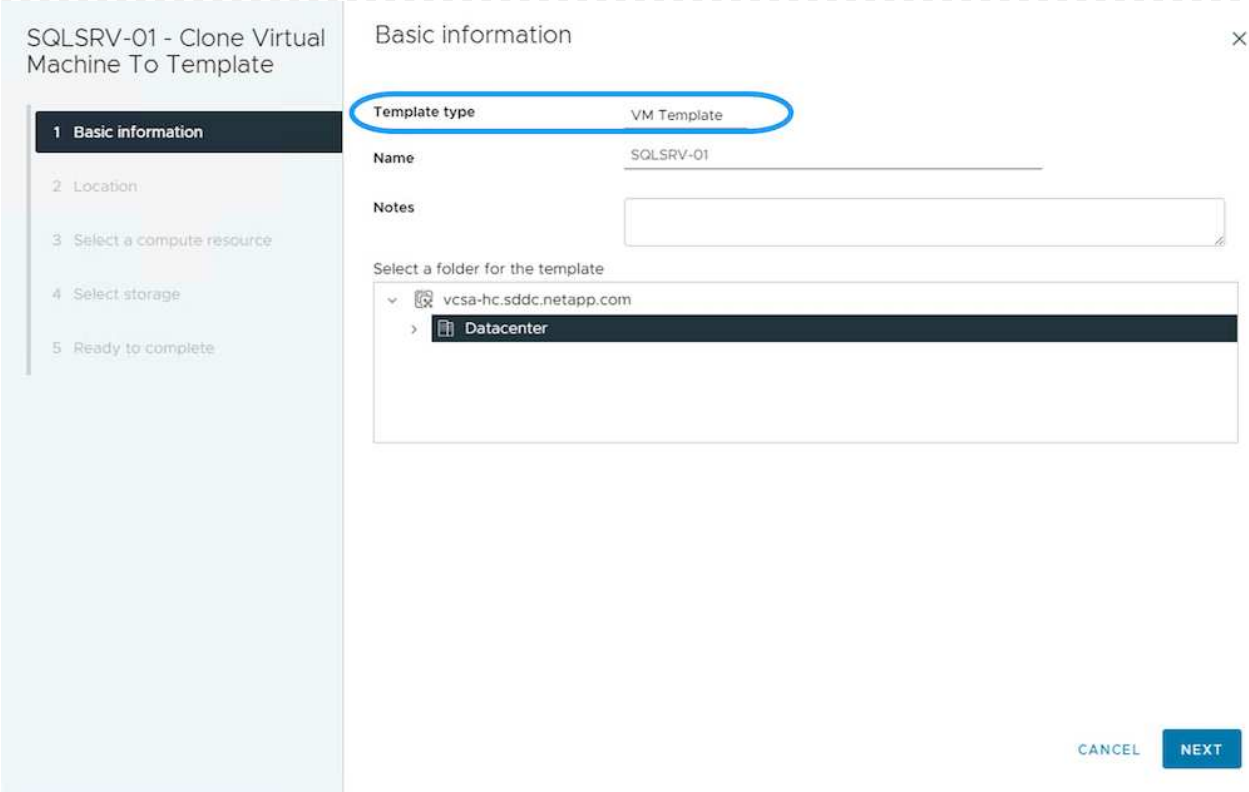
Hinzufügen von VM als Vorlagen zur Inhaltsbibliothek

1. Wählen Sie im vSphere Web Client die VM aus und klicken Sie mit der rechten Maustaste, um „Als Vorlage in Bibliothek klonen“ auszuwählen.



> Wenn in der Bibliothek eine VM-Vorlage zum Klonen ausgewählt wird, kann sie nur als OVF- und OVA-Vorlage und nicht als VM-Vorlage gespeichert werden.

2. Bestätigen Sie, dass als Vorlagentyp „VM-Vorlage“ ausgewählt ist, und folgen Sie den Antworten des Assistenten, um den Vorgang abzuschließen.



Weitere Informationen zu VM-Vorlagen in der Inhaltsbibliothek finden Sie unter "vSphere VM-Administrationshandbuch"

Anwendungsfälle

Migration von Speichersystemen von Drittanbietern (einschließlich vSAN) zu ONTAP -Datenspeichern.

- Wählen Sie basierend darauf, wo der ONTAP -Datenspeicher bereitgestellt wird, die oben genannten VM-Migrationsoptionen aus.

Migration von der vorherigen Version zur neuesten Version von vSphere.

- Wenn ein direktes Upgrade nicht möglich ist, können Sie eine neue Umgebung einrichten und die oben genannten Migrationsoptionen verwenden.

Importieren Sie bei der Cross-vCenter-Migrationsoption vom Ziel, wenn die Exportoption auf der Quelle nicht verfügbar ist. Überprüfen Sie für dieses Verfahren"Importieren oder Klonen einer virtuellen Maschine mit Advanced Cross vCenter vMotion"

Migration zur VCF-Workload-Domäne.

- Migrieren Sie VMs von jedem vSphere-Cluster zur Ziel-Workloaddomäne.

> Um die Netzwerkkommunikation mit vorhandenen VMs auf anderen Clustern im Quell-vCenter zu ermöglichen, erweitern Sie entweder das NSX-Segment, indem Sie die vSphere-Hosts des Quell-vCenters zur Transportzone hinzufügen, oder verwenden Sie die L2-Bridge am Edge, um die L2-Kommunikation im VLAN zu ermöglichen. Überprüfen Sie die NSX-Dokumentation von "Konfigurieren einer Edge-VM für Bridging"

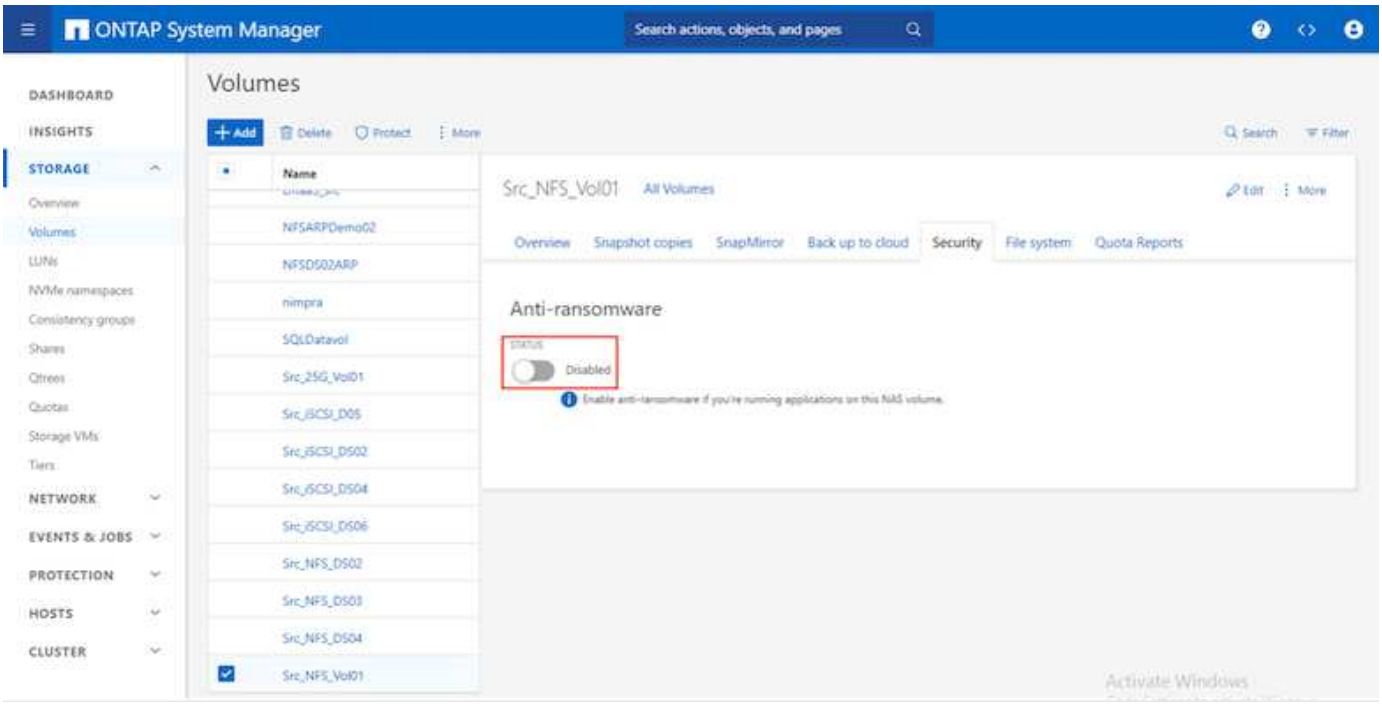
Weitere Ressourcen

- "Migration virtueller vSphere-Maschinen"
- "Migrieren virtueller Maschinen mit vSphere vMotion"
- "Tier-0-Gateway-Konfigurationen in der NSX-Föderation"
- "HCX 4.8 Benutzerhandbuch"
- "VMware Live Recovery-Dokumentation"
- "BlueXP disaster recovery für VMware"

Autonomer Ransomware-Schutz für NFS-Speicher

Um die Verbreitung von Ransomware zu verhindern und kostspielige Ausfallzeiten zu vermeiden, ist es entscheidend, sie so früh wie möglich zu erkennen. Eine wirksame 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 gegen Ransomware-Angriffe zu schaffen, ermöglicht ONTAP das Hinzufügen weiterer Schutzebenen zum allgemeinen Verteidigungsansatz. Um nur einige Funktionen zu nennen: Es beginnt mit Snapshots, autonomem Ransomware-Schutz, manipulationssicheren Snapshots und so weiter.

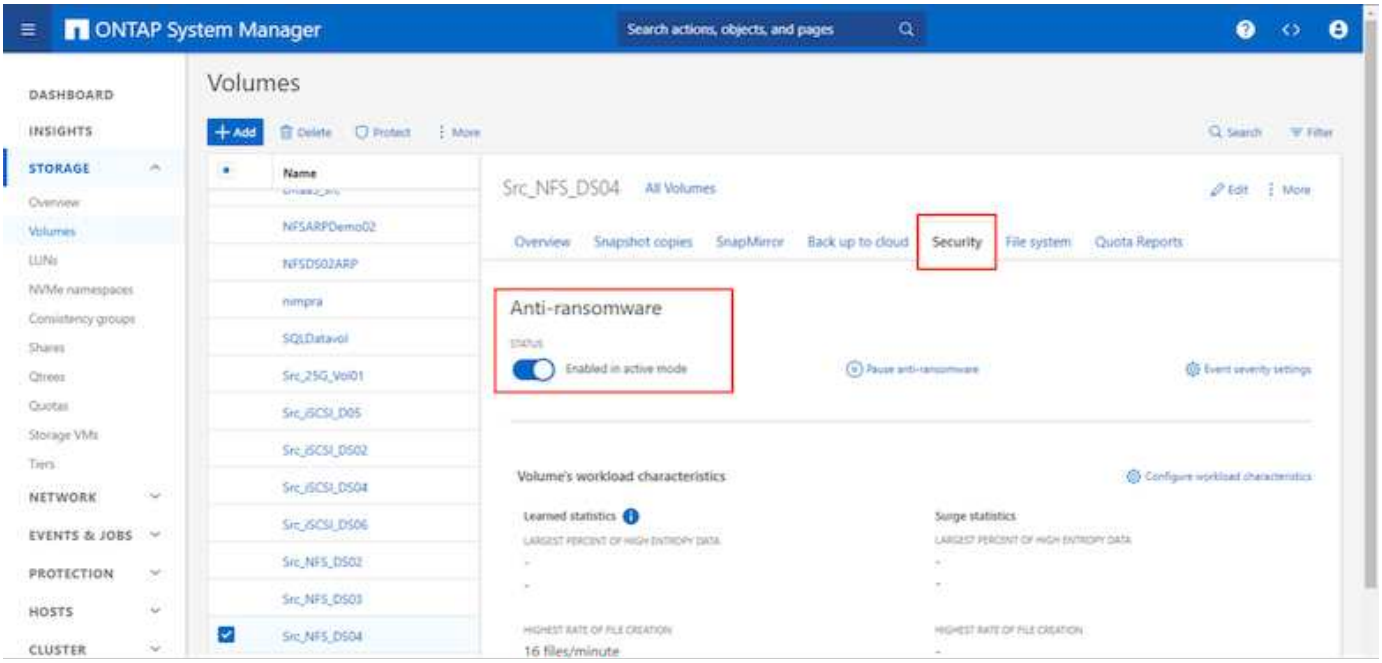
Sehen wir uns an, wie die oben genannten Funktionen mit VMware zusammenarbeiten, um die Daten vor Ransomware zu schützen und wiederherzustellen. Um vSphere und Gast-VMs vor Angriffen zu schützen, müssen verschiedene Maßnahmen ergriffen werden, darunter Segmentierung, die Verwendung von EDR/XDR/SIEM für Endpunkte, die Installation von Sicherheitsupdates und die Einhaltung der entsprechenden Härtungsrichtlinien. Jede virtuelle Maschine, die sich auf einem Datenspeicher befindet, hostet auch ein Standardbetriebssystem. Stellen Sie sicher, dass auf den Unternehmensservern Anti-Malware-Produktpakete installiert und regelmäßig aktualisiert werden. Dies ist ein wesentlicher Bestandteil einer mehrschichtigen Ransomware-Schutzstrategie. Aktivieren Sie außerdem Autonomous Ransomware Protection (ARP) auf dem NFS-Volume, das den Datenspeicher mit Strom versorgt. ARP nutzt integriertes Onbox-ML, das die Workload-Aktivität des Volumens sowie die Datenentropie betrachtet, um Ransomware automatisch zu erkennen. ARP kann über die integrierte Verwaltungsschnittstelle von ONTAP oder den Systemmanager konfiguriert und pro Volume aktiviert werden.



Mit dem neuen NetApp ARP/AI, das sich derzeit in der Tech Preview befindet, ist kein Lernmodus erforderlich. Stattdessen kann es mit seiner KI-gestützten Ransomware-Erkennungsfunktion direkt in den aktiven Modus wechseln.

Mit ONTAP One sind alle diese Funktionssätze völlig kostenlos. Greifen Sie auf die robuste Datenschutz- und Sicherheitssuite von NetApp sowie auf alle Funktionen von ONTAP zu, ohne sich um Lizenzbarrieren Gedanken machen zu müssen.

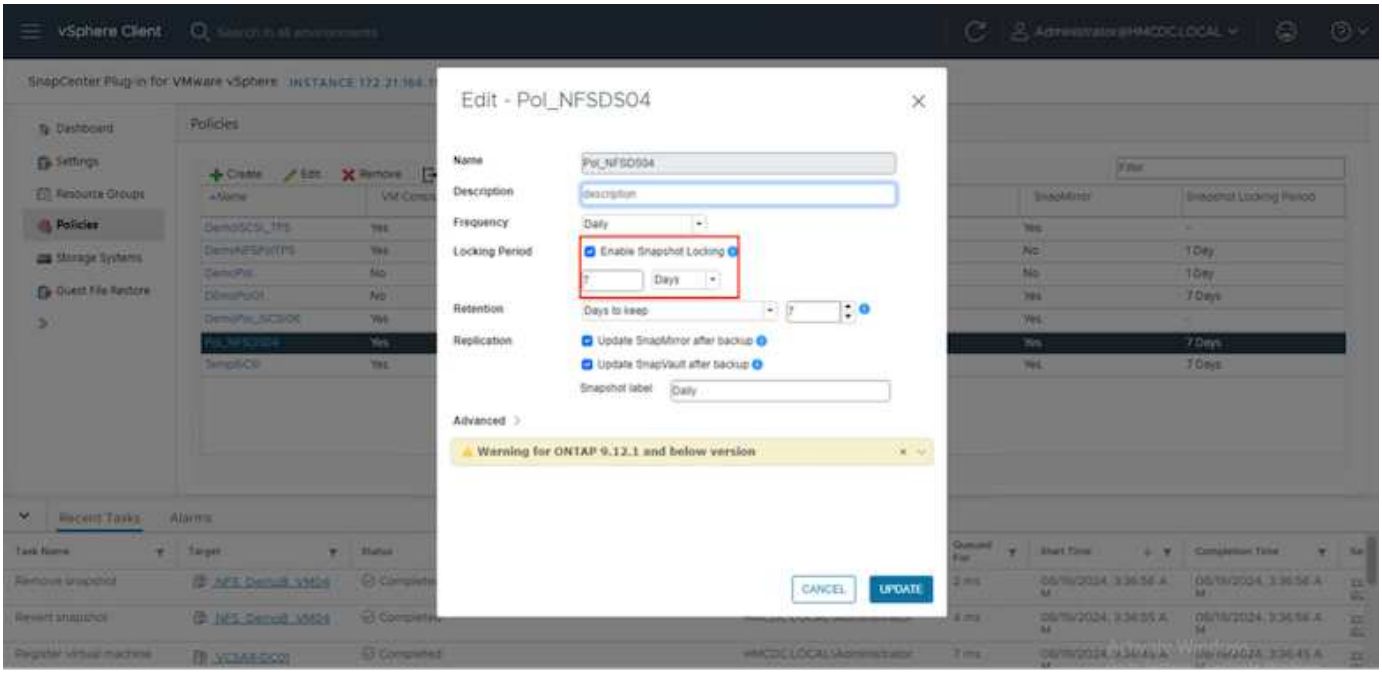
Sobald es sich im aktiven Modus befindet, beginnt es mit der Suche nach abnormaler Volumenaktivität, bei der es sich möglicherweise um Ransomware handeln könnte. Wenn eine ungewöhnliche Aktivität erkannt wird, wird sofort automatisch eine Snapshot-Kopie erstellt, die einen Wiederherstellungspunkt bereitstellt, der möglichst nahe an der Dateiinfektion liegt. ARP kann Änderungen an VM-spezifischen Dateierweiterungen auf einem NFS-Volume außerhalb der VM erkennen, wenn dem verschlüsselten Volume eine neue Erweiterung hinzugefügt oder die Erweiterung einer Datei geändert wird.



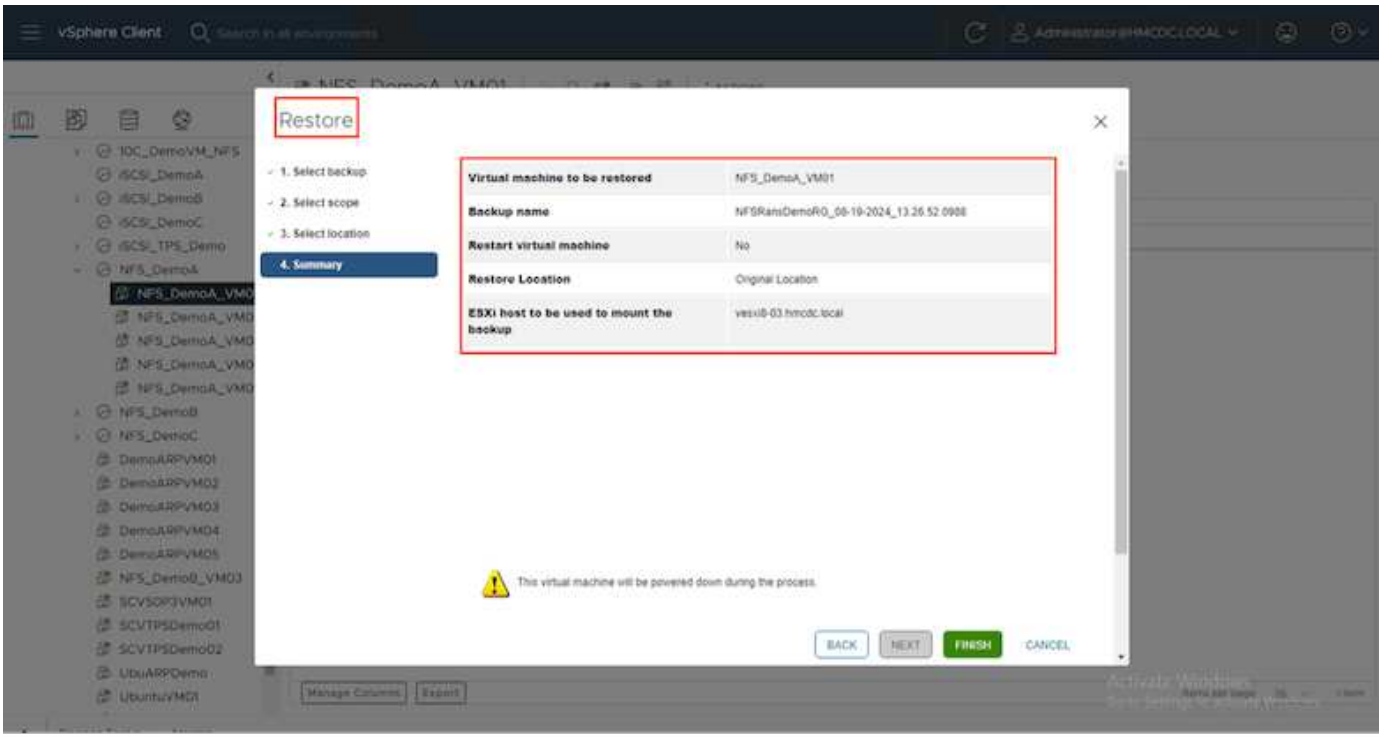
Wenn ein Ransomware-Angriff auf die virtuelle Maschine (VM) abzielt und Dateien innerhalb der VM ändert, ohne Änderungen außerhalb der VM vorzunehmen, erkennt Advanced Ransomware Protection (ARP) die Bedrohung dennoch, wenn die Standardentropie der VM niedrig ist, beispielsweise bei Dateitypen wie .txt-, .docx- oder .mp4-Dateien. Obwohl ARP in diesem Szenario einen schützenden Snapshot erstellt, wird keine Bedrohungswarnung generiert, da die Dateierweiterungen außerhalb der VM nicht manipuliert wurden. In solchen Szenarien würden die ersten Verteidigungsebenen 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-Anwendungsfälle und Überlegungen" .

Ransomware-Angriffe konzentrieren sich nicht mehr nur auf Dateien, sondern auch auf Sicherungsdaten. Sie zielen nun zunehmend auf Sicherungskopien und Snapshot-Wiederherstellungspunkte ab, indem sie versuchen, diese zu löschen, bevor sie mit der Verschlüsselung der Dateien beginnen. Mit ONTAP kann dies jedoch verhindert werden, indem manipulationssichere Snapshots auf primären oder sekundären Systemen mit"NetApp Snapshot-Kopiersperre" .



Diese Snapshot-Kopien können von Ransomware-Angreifern oder betrügerischen Administratoren weder gelöscht noch geändert werden, sodass sie auch nach einem Angriff verfügbar sind. Wenn der Datenspeicher oder bestimmte virtuelle Maschinen betroffen sind, kann SnapCenter die Daten der virtuellen Maschinen in Sekundenschnelle wiederherstellen und so die Ausfallzeit des Unternehmens minimieren.



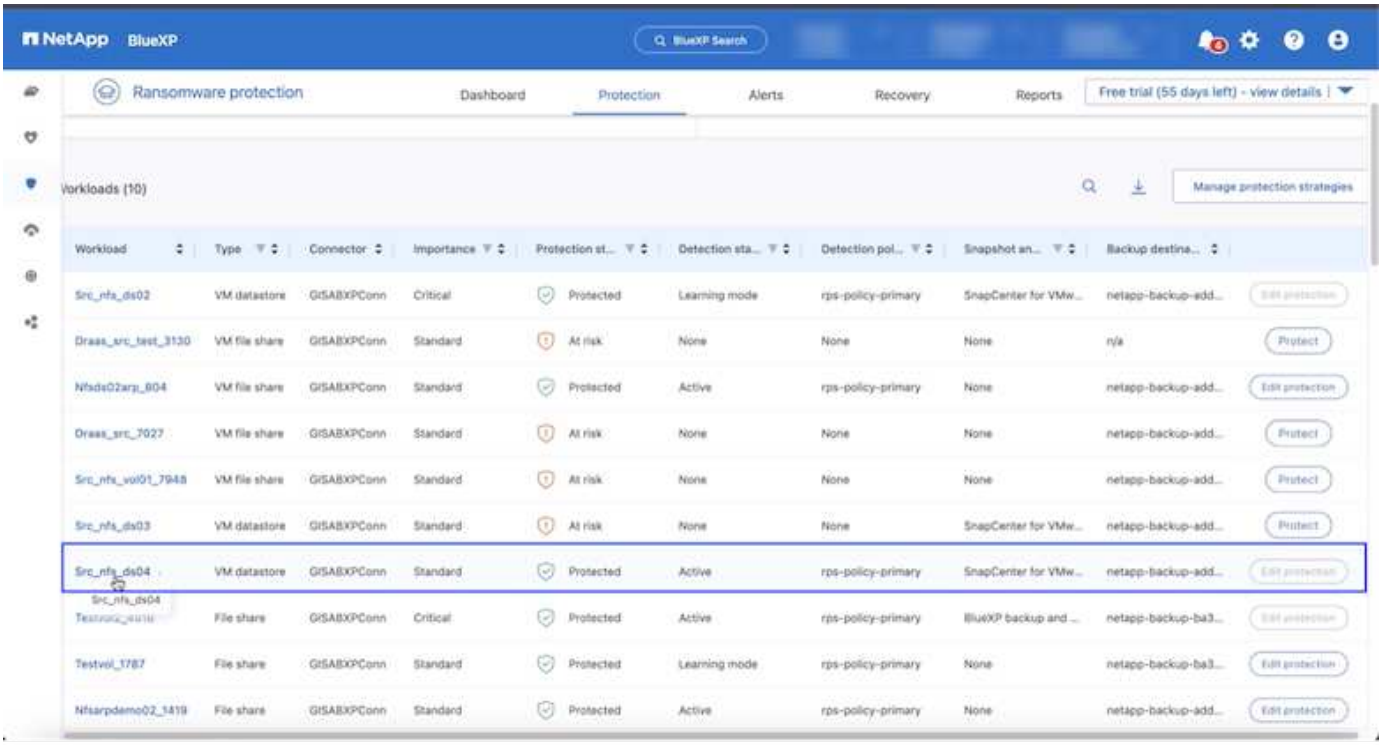
Das Obige zeigt, wie ONTAP Speicher den vorhandenen Techniken eine zusätzliche Ebene hinzufügt und so die Zukunftssicherheit der Umgebung verbessert.

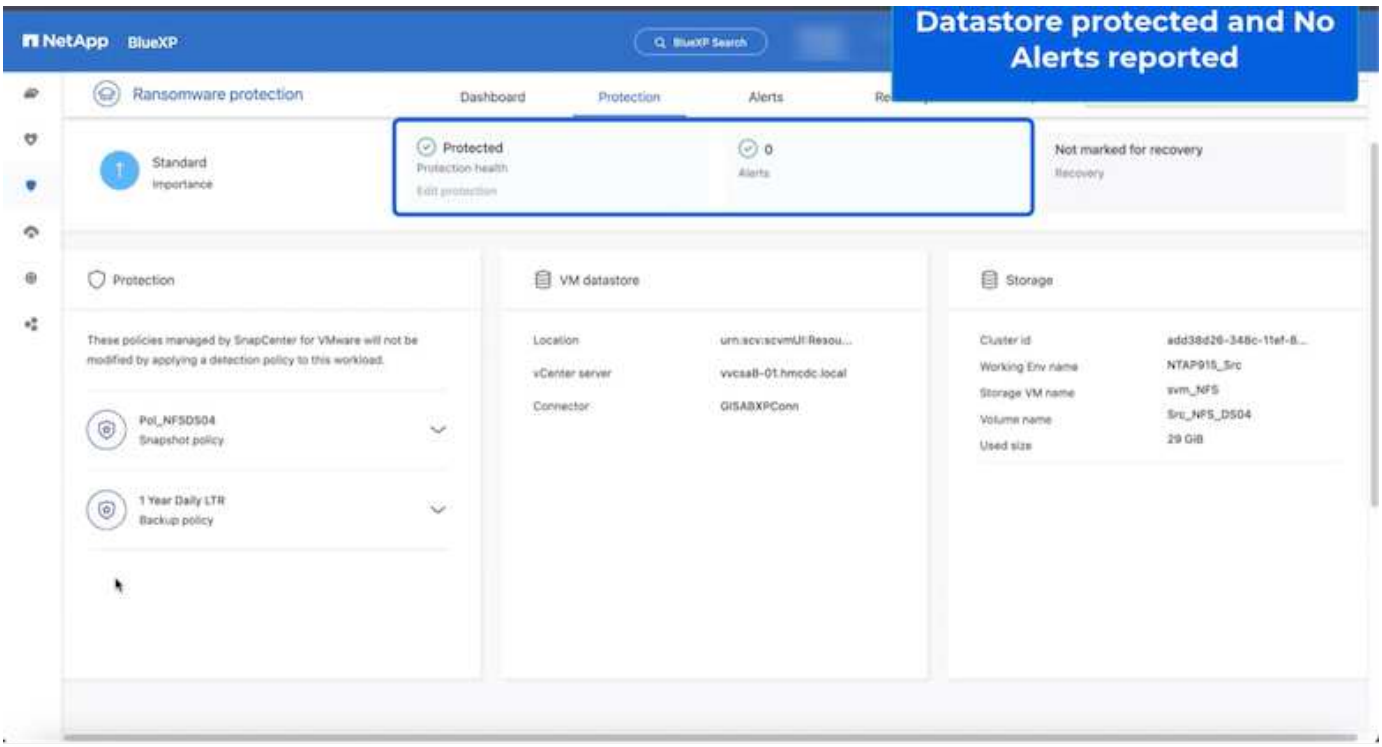
Weitere Informationen finden Sie in der Anleitung für"NetApp -Lösungen für Ransomware" .

Wenn all dies nun orchestriert und mit SIEM-Tools integriert werden muss, kann ein Offtap-Dienst wie der BlueXP ransomware protection verwendet werden. Es handelt sich um einen Dienst zum Schutz von Daten vor

Ransomware. Dieser Dienst bietet Schutz für anwendungsbasierte Workloads wie Oracle, MySQL, VM-Datenspeicher und Dateifreigaben auf lokalem NFS-Speicher.

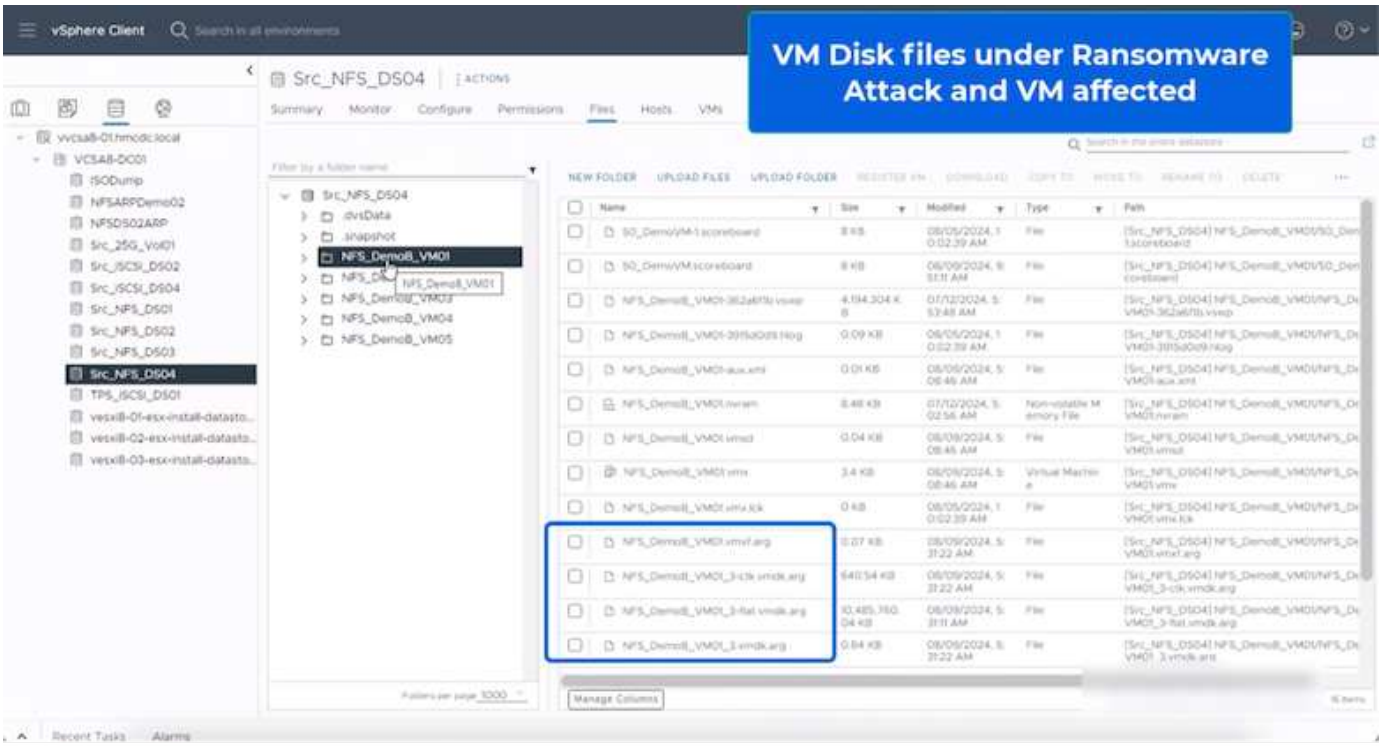
In diesem Beispiel wird der NFS-Datenspeicher „Src_NFS_DS04“ mit dem BlueXP ransomware protection geschützt.



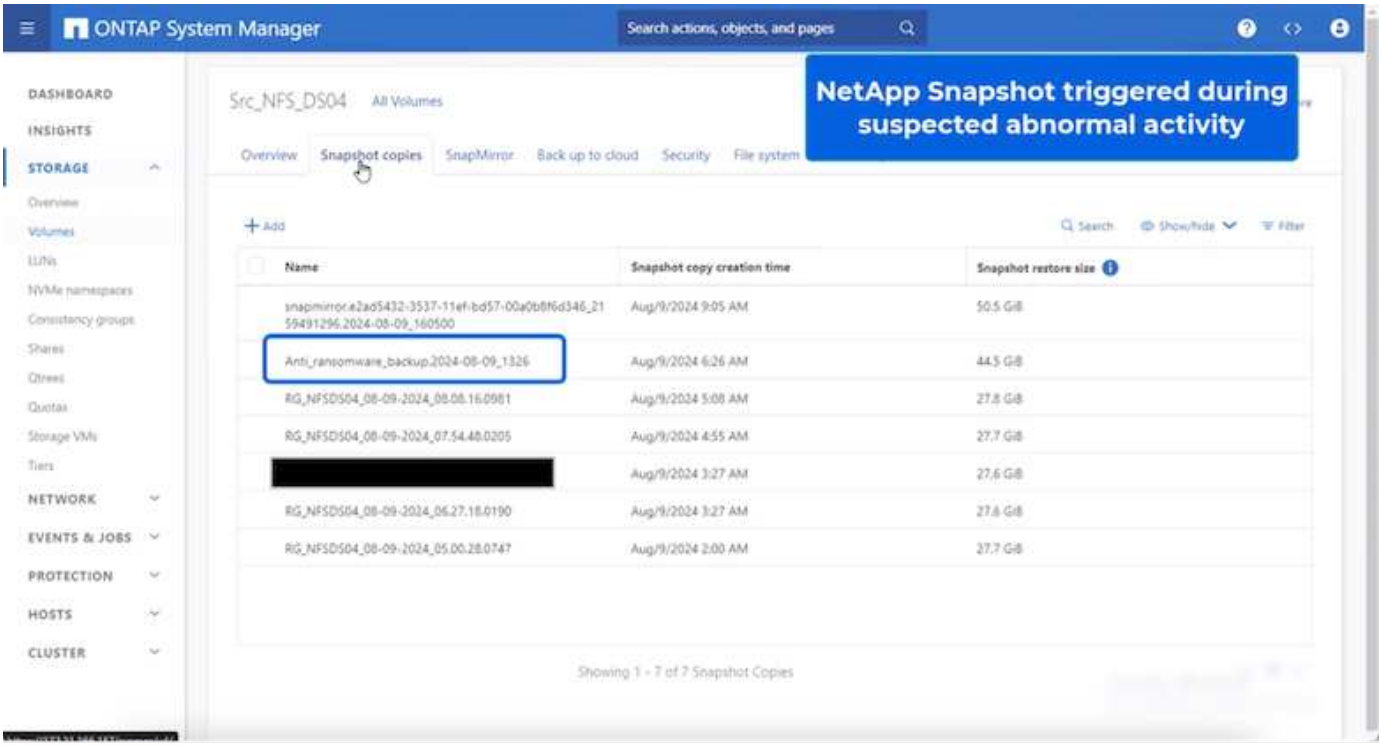


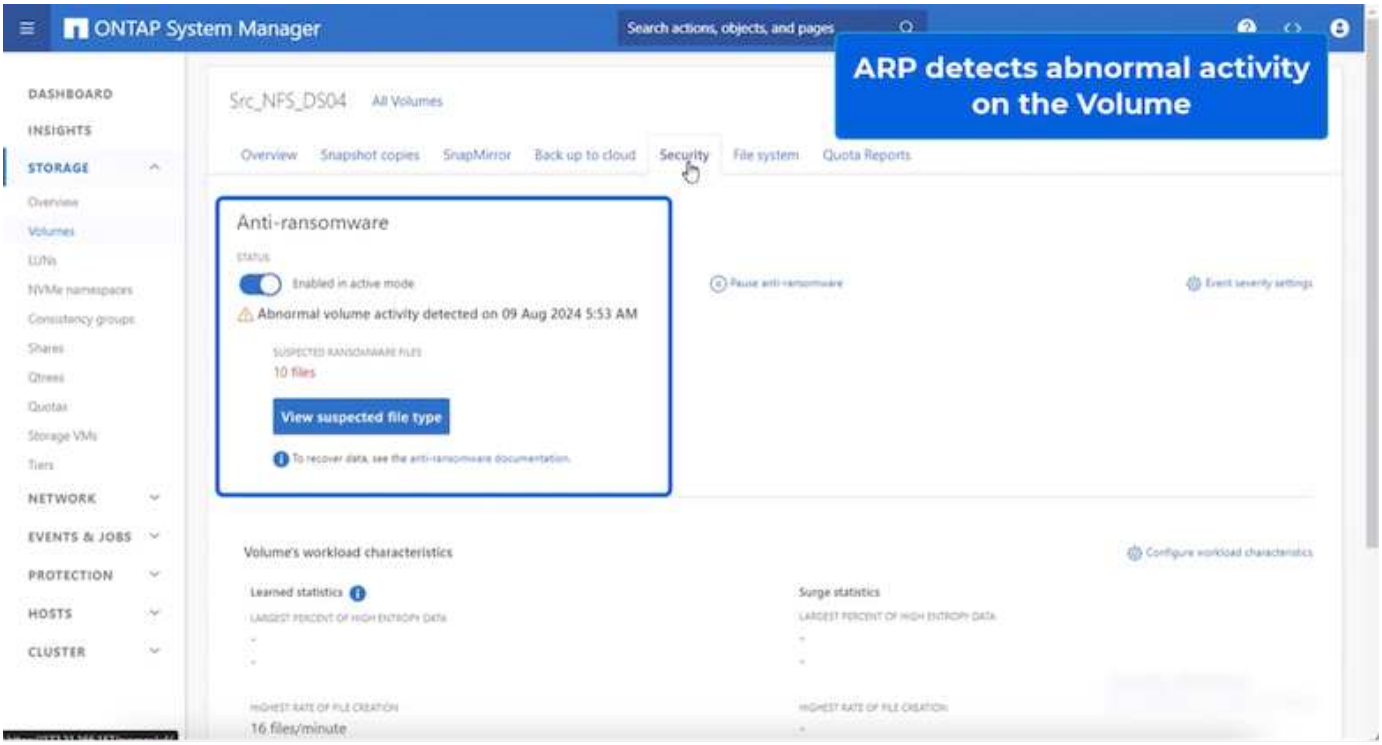
Ausführliche Informationen zum Konfigurieren des BlueXP ransomware protection finden Sie unter"Richten Sie den BlueXP ransomware protection ein" Und"Konfigurieren Sie die BlueXP ransomware protection -Schutzeinstellungen" .

Es ist an der Zeit, dies anhand eines Beispiels zu verdeutlichen. In dieser exemplarischen Vorgehensweise ist der Datenspeicher „Src_NFS_DS04“ betroffen.

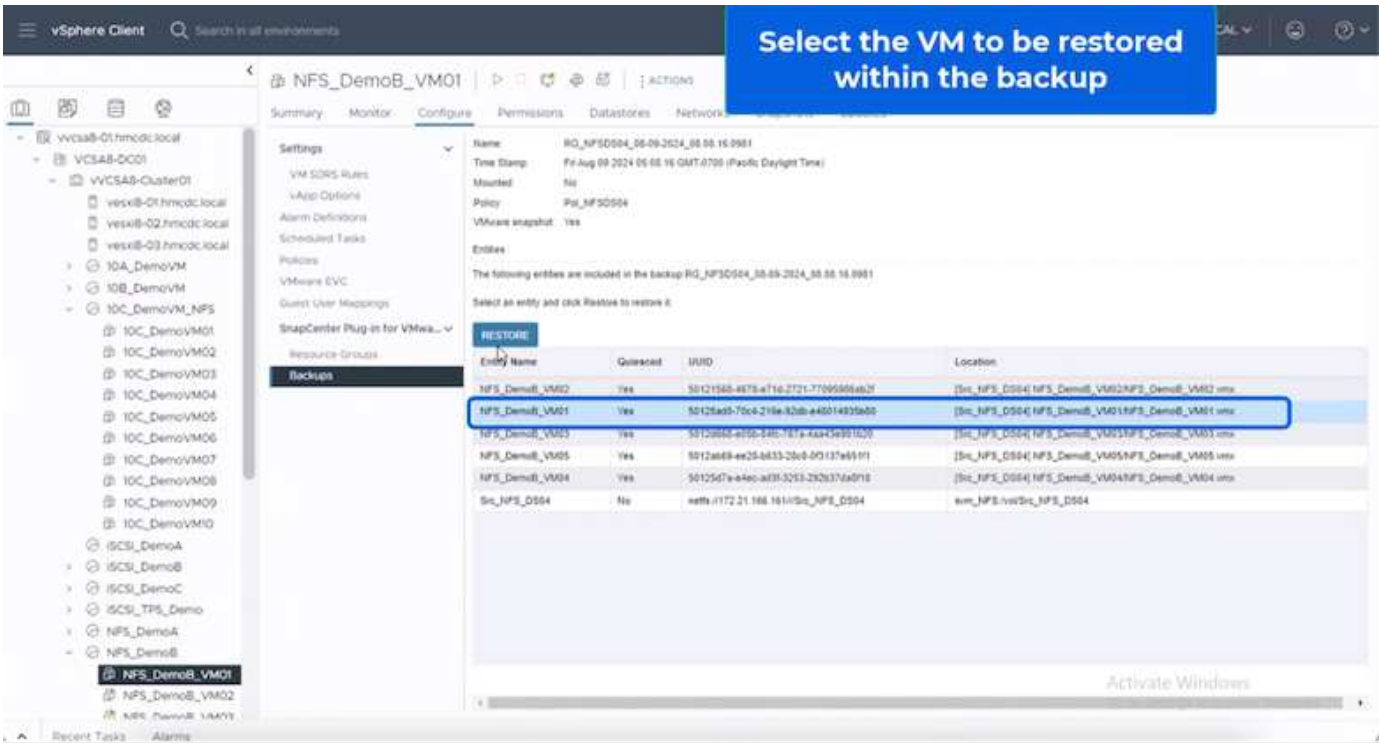


ARP löste bei der Erkennung sofort einen Snapshot auf dem Volume aus.





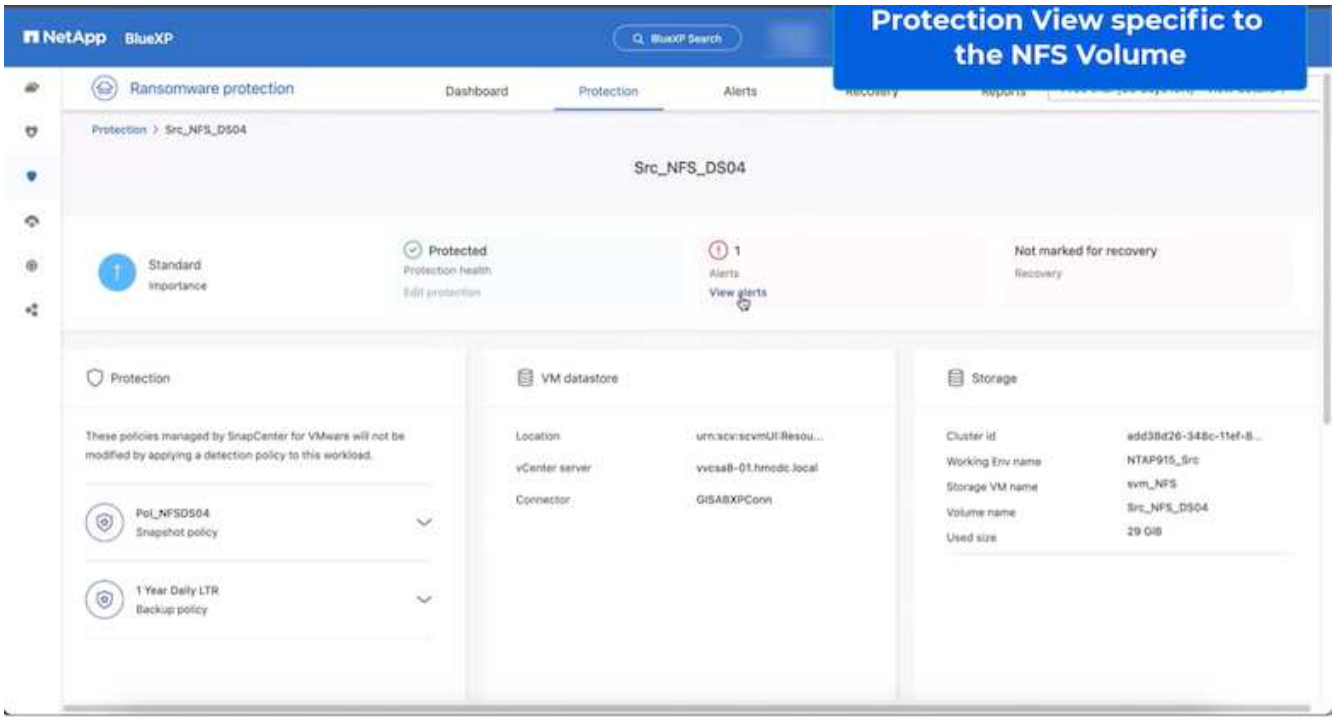
Sobald die forensische Analyse abgeschlossen ist, können die Wiederherstellungen mithilfe des Ransomware-Schutzes SnapCenter oder BlueXP ransomware protection schnell und nahtlos durchgeführt werden. Gehen Sie mit SnapCenter zu den betroffenen virtuellen Maschinen und wählen Sie den entsprechenden Snapshot zur Wiederherstellung aus.



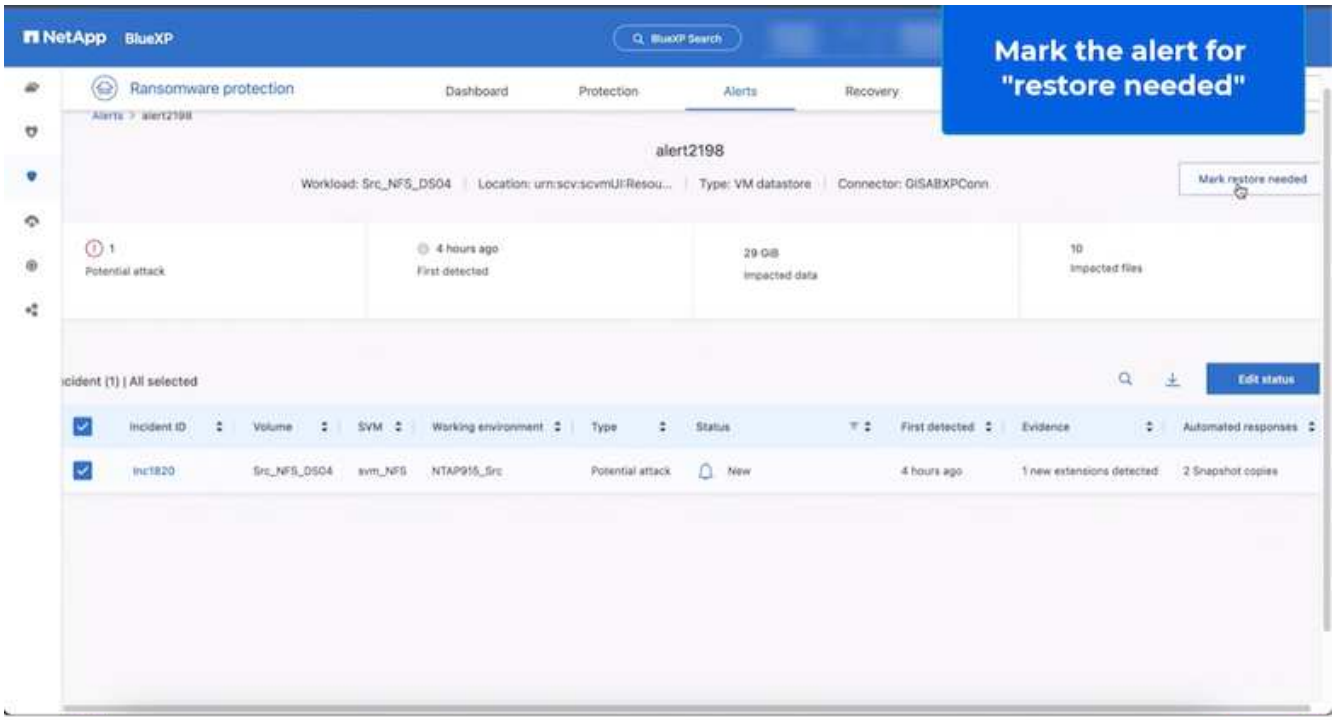
In diesem Abschnitt wird erläutert, wie der BlueXP ransomware protection die Wiederherstellung nach einem Ransomware-Vorfall orchestriert, bei dem die VM-Dateien verschlüsselt sind.

Wenn die VM von SnapCenter verwaltet wird, stellt der BlueXP ransomware protection die VM mithilfe des VM-konsistenten Prozesses in ihren vorherigen Zustand zurück.

1. Greifen Sie auf den BlueXP ransomware protection zu und auf dem BlueXP ransomware protection -Dashboard wird eine Warnung angezeigt.
2. Klicken Sie auf die Warnung, um die Vorfälle auf diesem bestimmten Datenträger für die generierte Warnung zu überprüfen

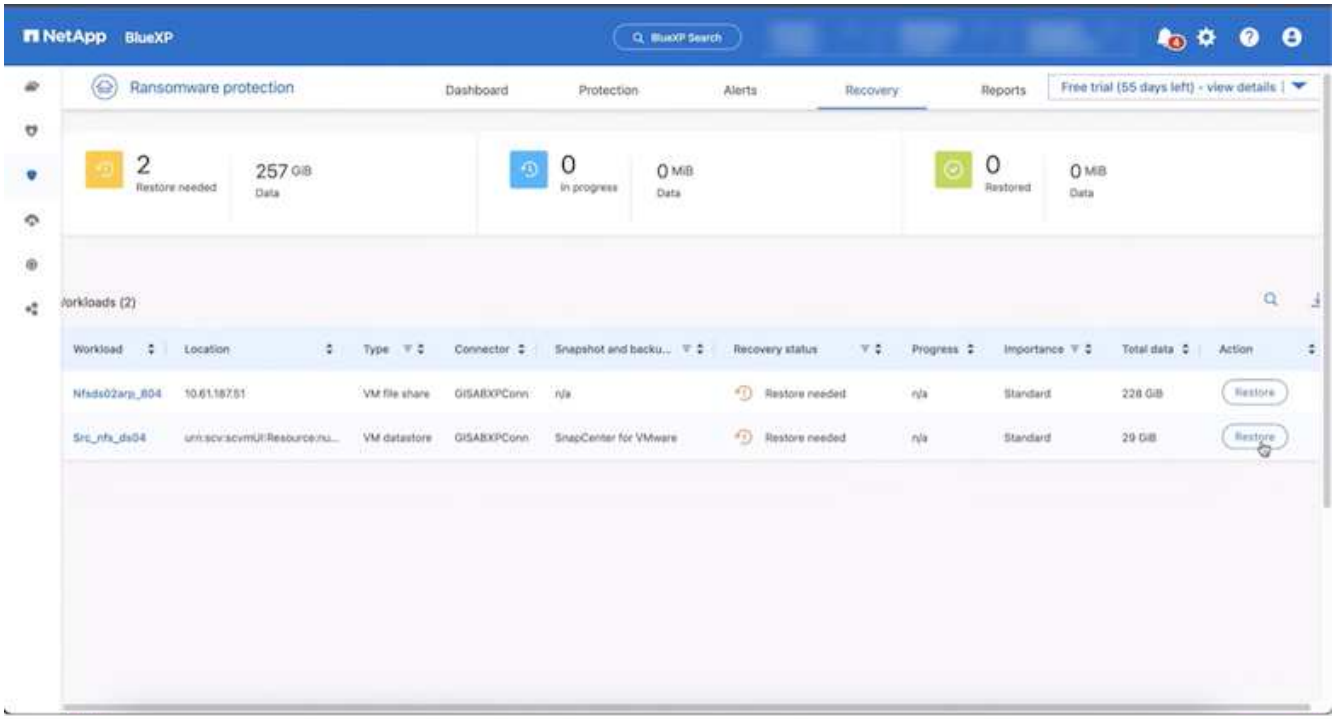


3. Markieren Sie den Ransomware-Vorfall als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden), indem Sie „Als Wiederherstellung erforderlich markieren“ auswählen.

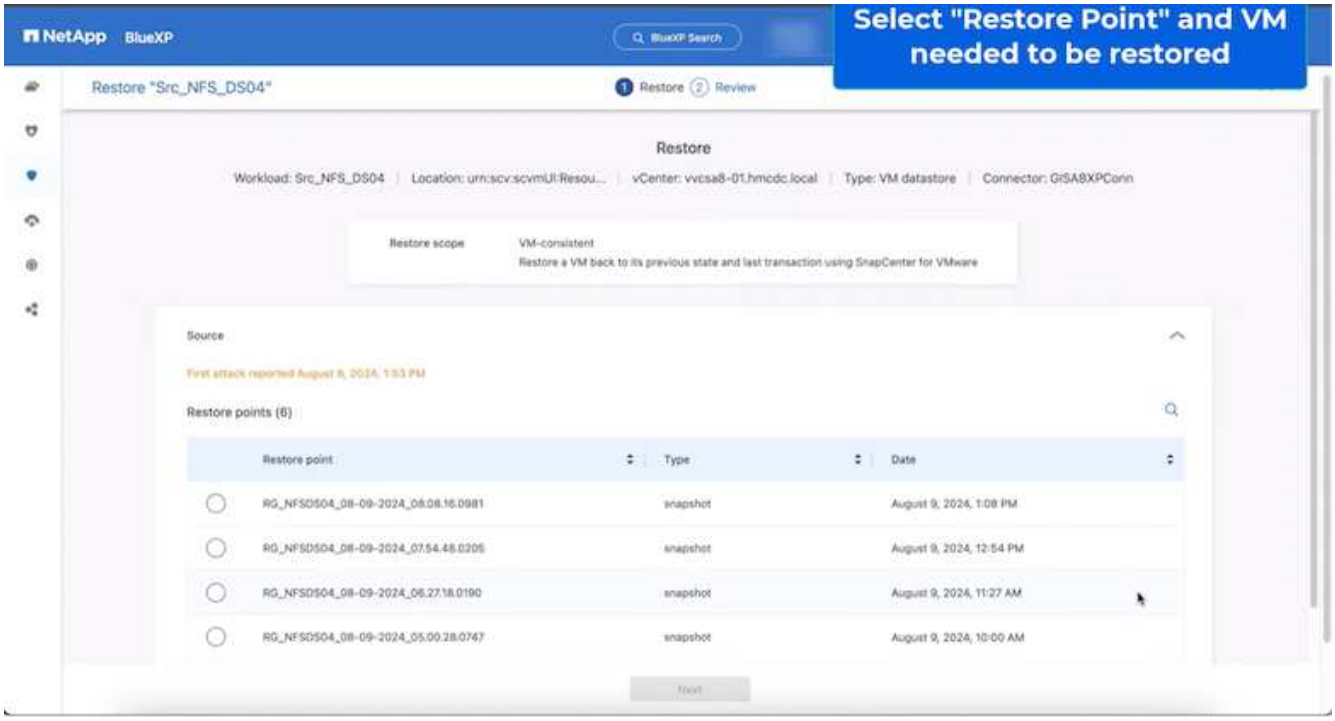


Die Warnung kann verworfen werden, wenn sich der Vorfall als falsch positiv herausstellt.

4. Gehen Sie zur Registerkarte „Wiederherstellung“, überprüfen Sie die Arbeitslastinformationen auf der Seite „Wiederherstellung“, wählen Sie das Datenspeichervolume aus, das sich im Status „Wiederherstellung erforderlich“ befindet, und wählen Sie „Wiederherstellen“ aus.

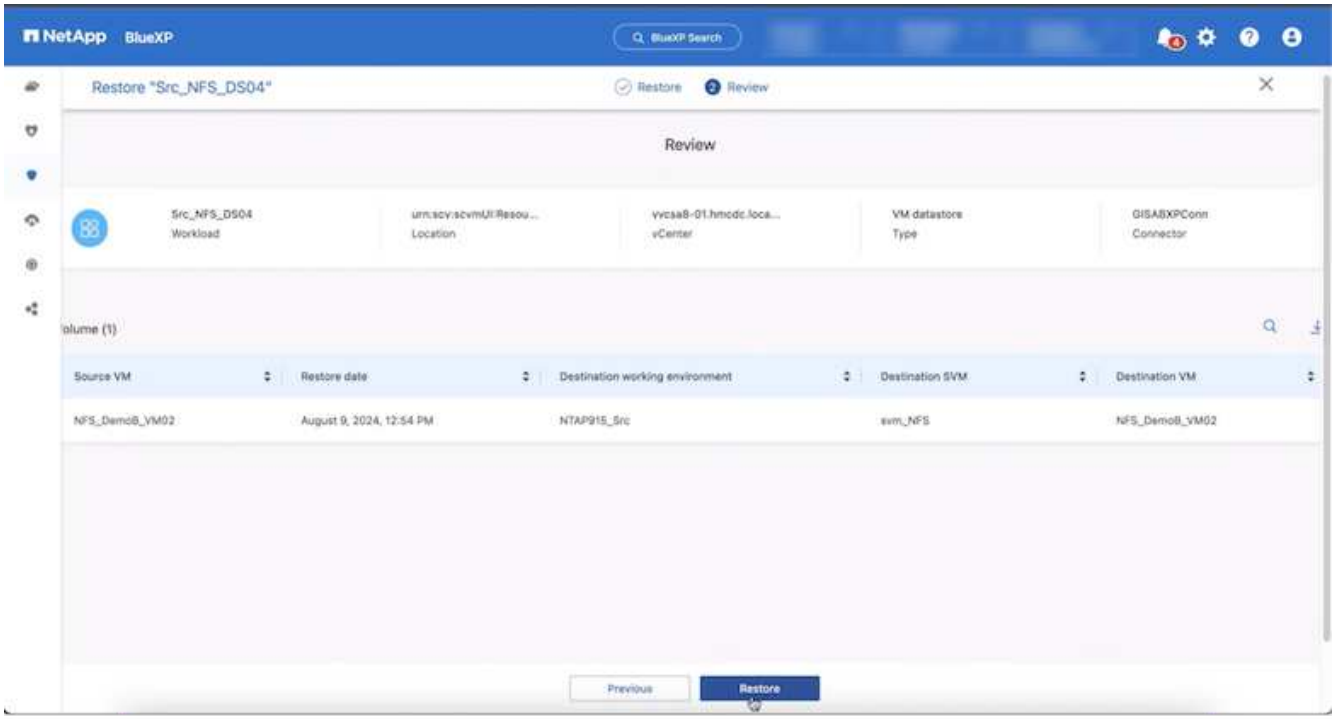


5. In diesem Fall ist der Wiederherstellungsumfang „Nach VM“ (für SnapCenter für VMs ist der Wiederherstellungsumfang „Nach VM“).

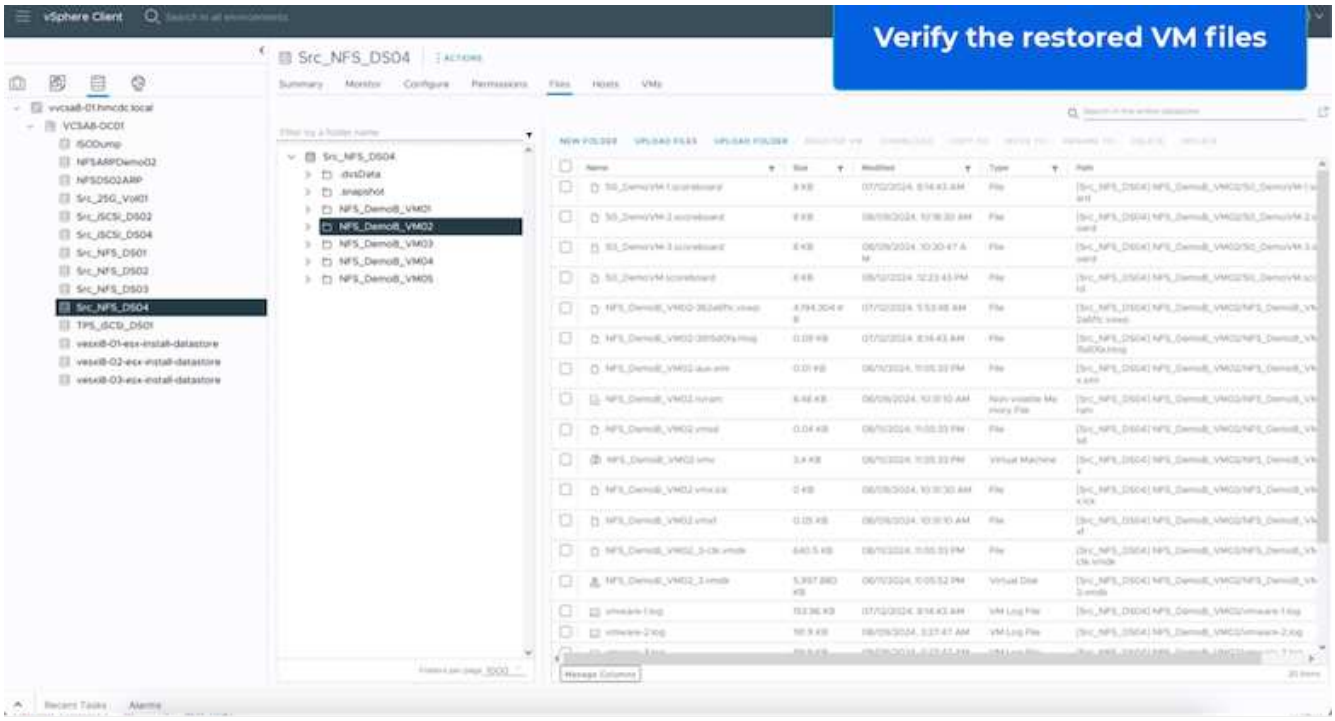


6. Wählen Sie den Wiederherstellungspunkt aus, der zum Wiederherstellen der Daten verwendet werden soll,

wählen Sie Ziel aus und klicken Sie auf Wiederherstellen.



7. Wählen Sie im oberen Menü „Wiederherstellung“ aus, um die Arbeitslast auf der Seite „Wiederherstellung“ zu überprüfen, auf der der Status des Vorgangs durch die verschiedenen Zustände verläuft. Sobald die Wiederherstellung abgeschlossen ist, werden die VM-Dateien wie unten gezeigt wiederhergestellt.



Die Wiederherstellung kann je nach Anwendung über SnapCenter für VMware oder das SnapCenter -Plugin durchgeführt werden.

Die NetApp -Lösung bietet verschiedene effektive Tools für Transparenz, Erkennung und Behebung. Sie helfen

Ihnen, Ransomware frühzeitig zu erkennen, ihre Verbreitung zu verhindern und bei Bedarf eine schnelle Wiederherstellung durchzuführen, um kostspielige Ausfallzeiten zu vermeiden. Herkömmliche mehrschichtige Verteidigungslösungen sind weiterhin weit verbreitet, ebenso wie Lösungen von Drittanbietern und Partnern für Sichtbarkeit und Erkennung. Eine wirksame Sanierung bleibt ein entscheidender Teil der Reaktion auf jede Bedrohung.

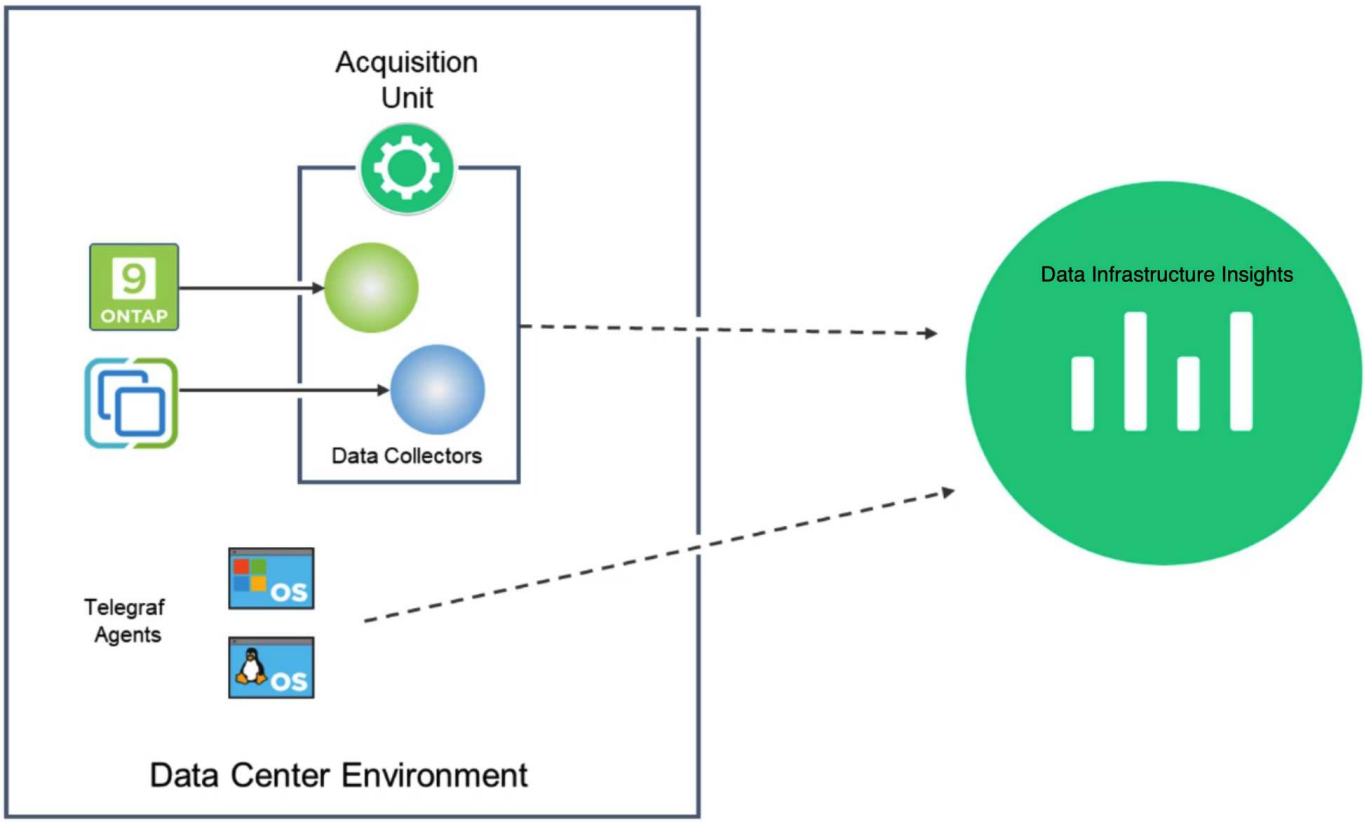
Überwachen Sie den lokalen Speicher mit Data Infrastructure Insights

NetApp Data Infrastructure Insights (ehemals Cloud Insights) ist eine Cloud-basierte Plattform zur Überwachung und Analyse der Leistung, des Zustands und der Kosten von IT-Infrastrukturen sowohl vor Ort als auch in der Cloud. Erfahren Sie, wie Sie Datensammler bereitstellen, Leistungsmetriken analysieren und Dashboards verwenden, um Probleme zu identifizieren und Ressourcen zu optimieren.

Überwachung des lokalen Speichers mit Data Infrastructure Insights

Data Infrastructure Insights funktioniert über die Acquisition Unit-Software, die mit Datensammlern für Assets wie VMware vSphere und NetApp ONTAP Speichersysteme eingerichtet ist. Diese Collector sammeln Daten und übermitteln sie an Data Infrastructure Insights. Die Plattform nutzt dann eine Vielzahl von Dashboards, Widgets und Metrikabfragen, um die Daten in aufschlussreiche Analysen zu organisieren, die die Benutzer interpretieren können.

Architekturdiagramm von Data Infrastructure Insights :



Übersicht über die Lösungsbereitstellung

Diese Lösung bietet eine Einführung in die Überwachung lokaler VMware vSphere- und ONTAP -Speichersysteme mithilfe von Data Infrastructure Insights.

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

1. Konfigurieren Sie Data Collector für einen vSphere-Cluster.
2. Konfigurieren Sie Data Collector für ein ONTAP Speichersystem.
3. Verwenden Sie Anmerkungsregeln, um Assets zu markieren.
4. Erkunden und korrelieren Sie Vermögenswerte.
5. Verwenden Sie ein Top-VM-Latenz-Dashboard, um laute Nachbarn zu isolieren.
6. Identifizieren Sie Möglichkeiten zur richtigen Größe von VMs.
7. Verwenden Sie Abfragen, um Metriken zu isolieren und zu sortieren.

Voraussetzungen

Diese Lösung verwendet die folgenden Komponenten:

1. NetApp All-Flash SAN Array A400 mit ONTAP 9.13.
2. VMware vSphere 8.0-Cluster.
3. NetApp BlueXP Konto.
4. Auf einer lokalen VM installierte NetApp Data Infrastructure Insights Acquisition Unit-Software mit Netzwerkkonnektivität zu Assets zur Datenerfassung.

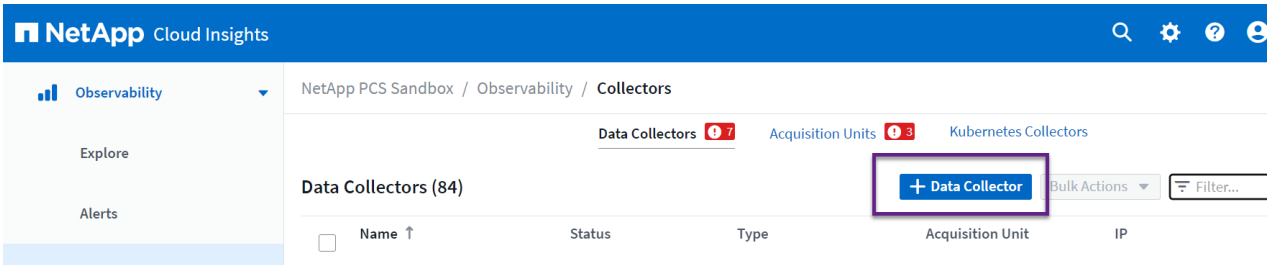
Lösungsbereitstellung

Konfigurieren von Datensammlern

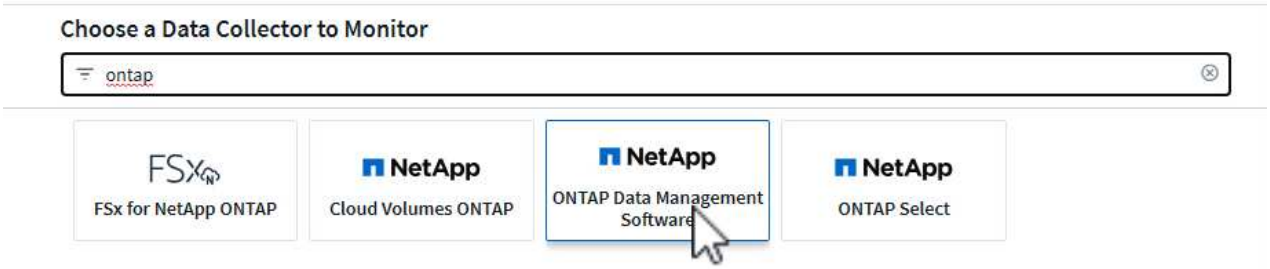
Führen Sie die folgenden Schritte aus, um Datenkollektoren für VMware vSphere- und ONTAP -Speichersysteme zu konfigurieren:

Fügen Sie einen Datensammler für ein ONTAP -Speichersystem hinzu

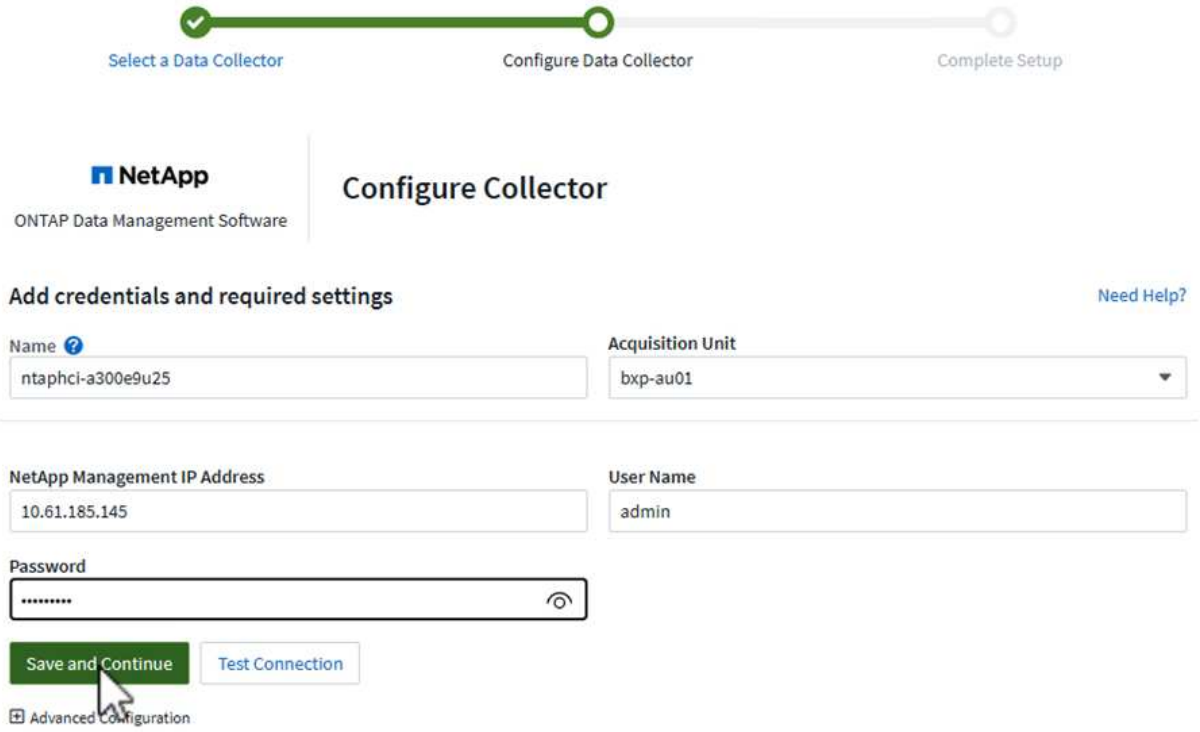
1. Navigieren Sie nach der Anmeldung bei Data Infrastructure Insights zu **Observability > Collectors > Data Collectors** und drücken Sie die Schaltfläche, um einen neuen Data Collector zu installieren.



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

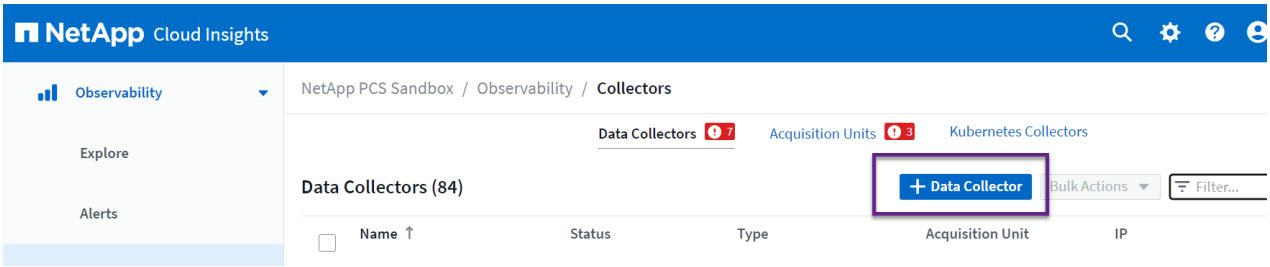


3. Geben Sie auf der Seite **Collector konfigurieren** einen Namen für den Collector ein, geben Sie die richtige **Erfassungseinheit** an und geben Sie die Anmeldeinformationen für das ONTAP -Speichersystem ein. Klicken Sie auf **Speichern und fortfahren** und dann unten auf der Seite auf **Setup abschließen**,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

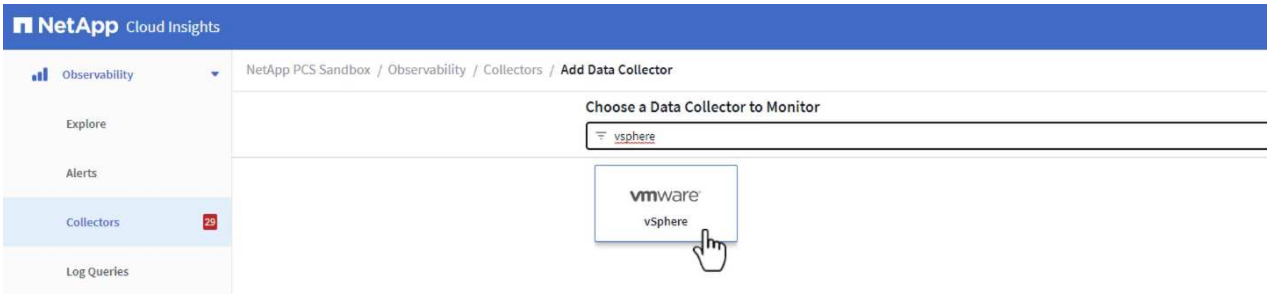


Hinzufügen eines Datensammlers für einen VMware vSphere-Cluster

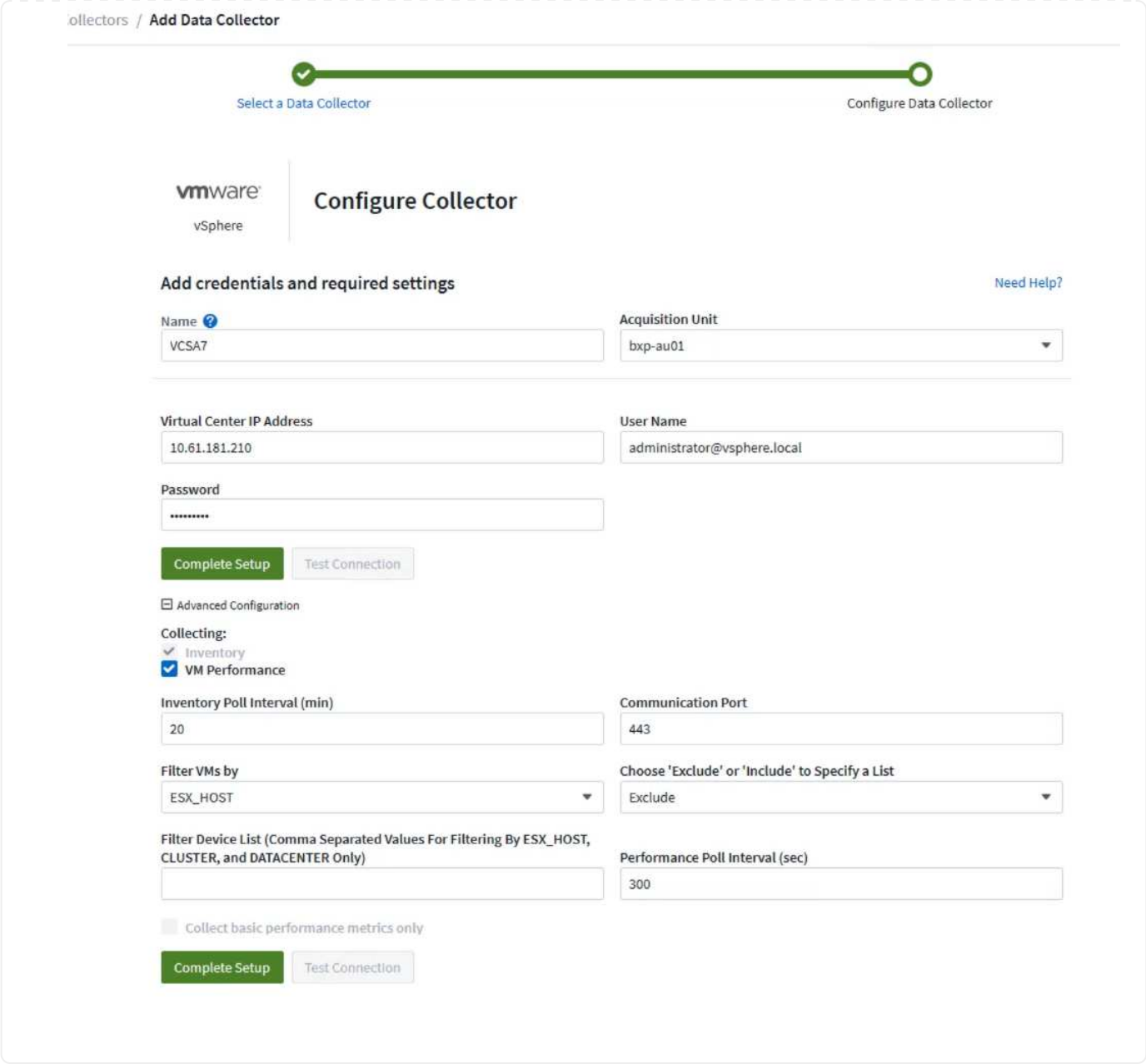
1. Navigieren Sie erneut zu **Observability > Collectors > Data Collectors** und drücken Sie die Schaltfläche, um einen neuen Data Collector zu installieren.



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



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



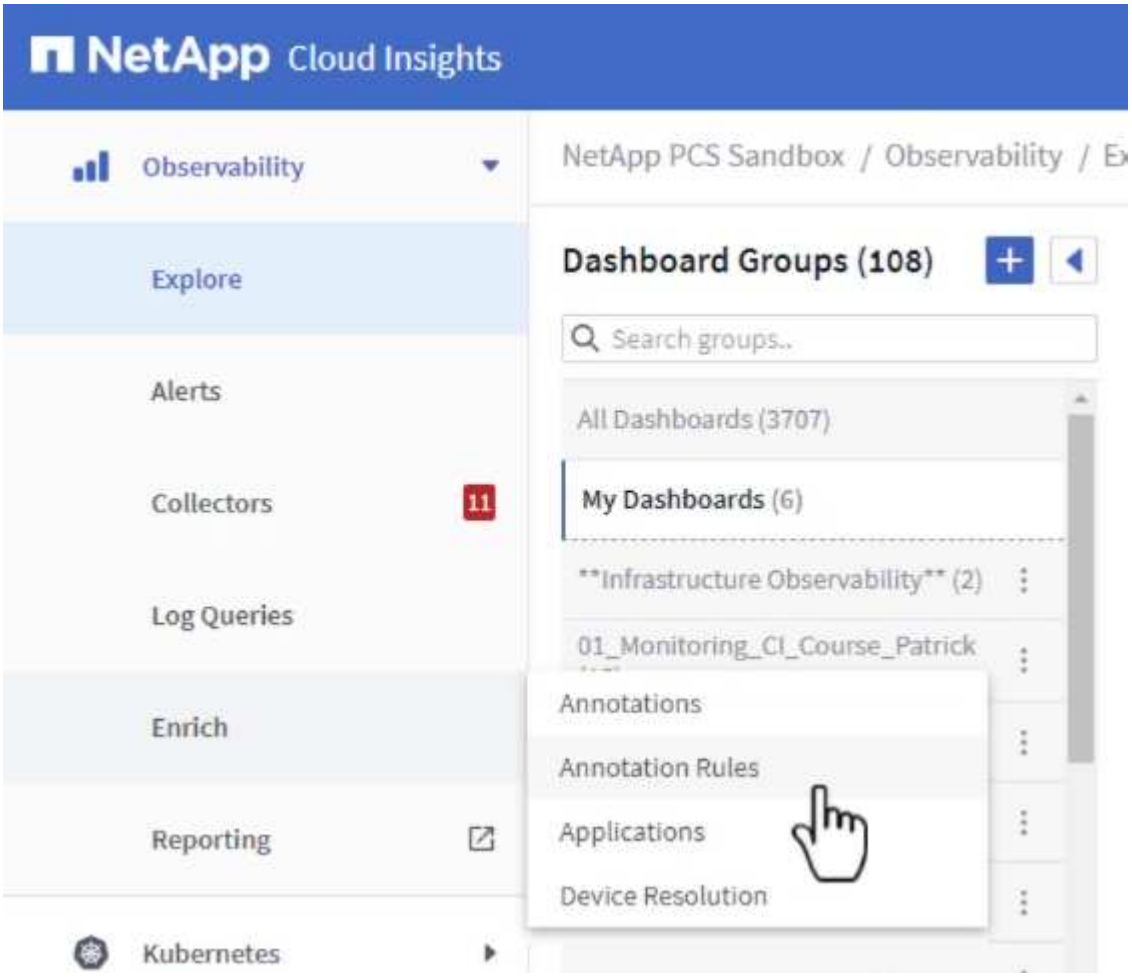
Hinzufügen von Anmerkungen zu Assets

Anmerkungen sind eine nützliche Methode zum Markieren von Assets, sodass sie in den verschiedenen in Cloud Insights verfügbaren Ansichten und Metrikabfragen gefiltert und anderweitig identifiziert werden können.

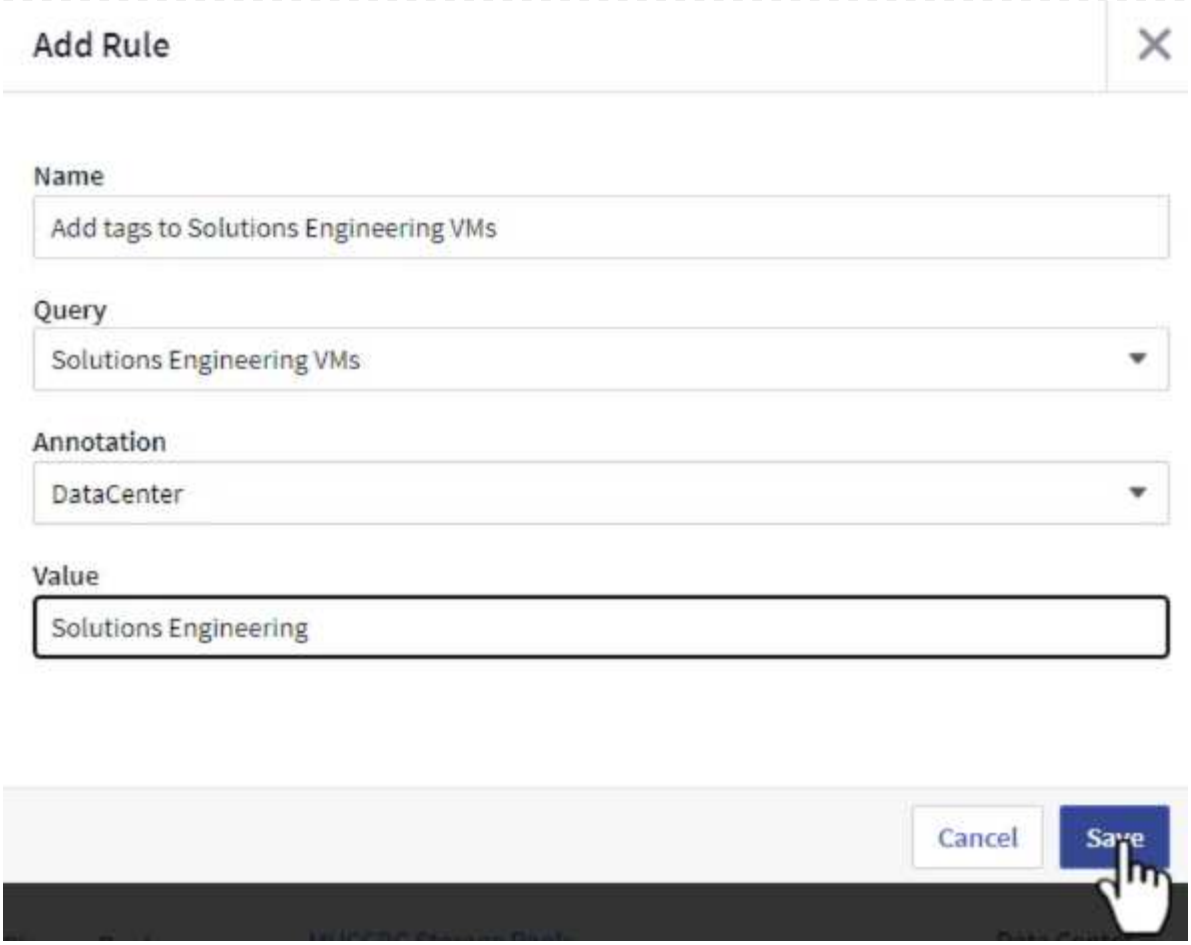
In diesem Abschnitt werden Anmerkungen zu virtuellen Maschinenressourcen hinzugefügt, um sie nach **Rechenzentrum** zu filtern.

Verwenden Sie Anmerkungsregeln zum Markieren von Assets

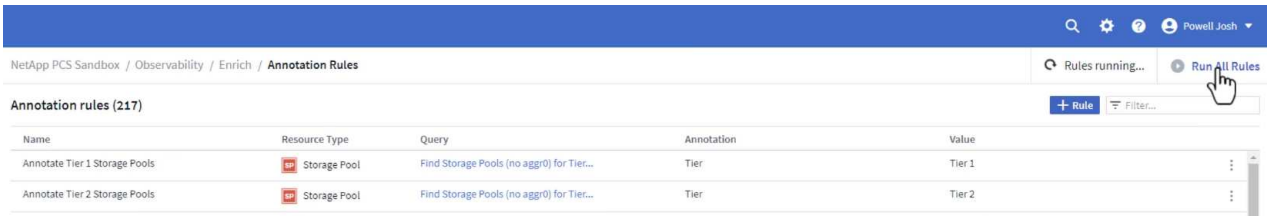
1. Navigieren Sie im linken Menü zu **Observability > Enrich > Annotation Rules** und klicken Sie oben rechts auf die Schaltfläche **+ Rule**, um eine neue Regel hinzuzufügen.



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



3. Klicken Sie abschließend in der oberen rechten Ecke der Seite **Annotation Rules** auf **Run All Rules**, um die Regel auszuführen und die Annotation auf die Assets anzuwenden.



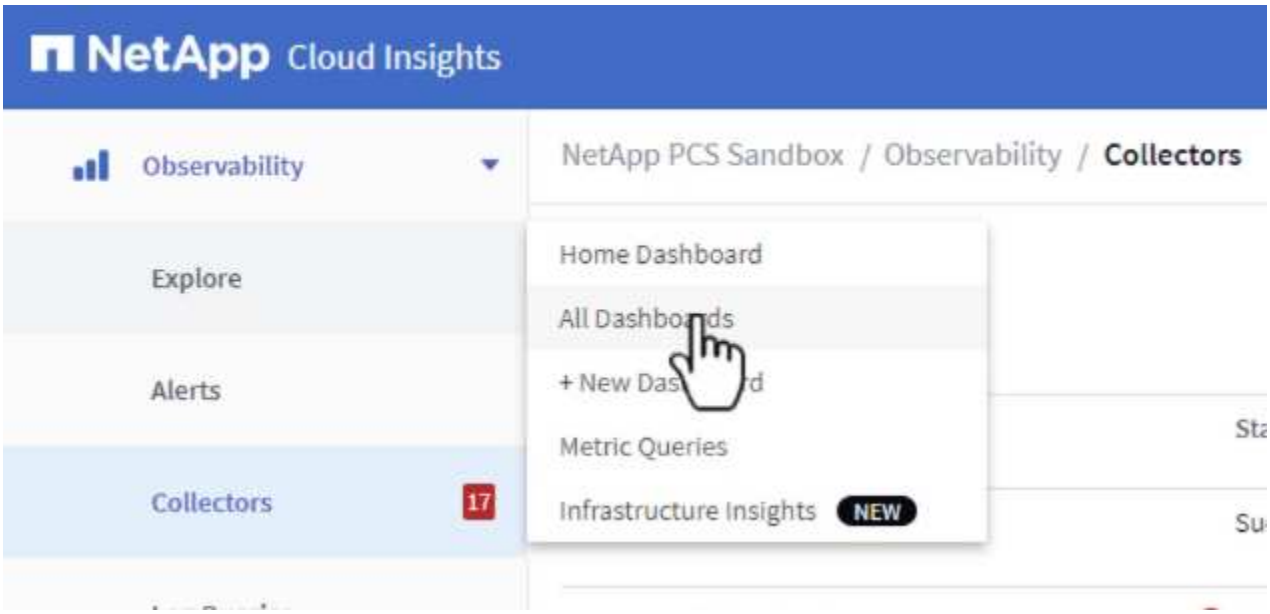
Erkunden und Korrelieren von Assets

Cloud Insights zieht logische Schlussfolgerungen über die Assets, die zusammen auf Ihren Speichersystemen und vSphere-Clustern ausgeführt werden.

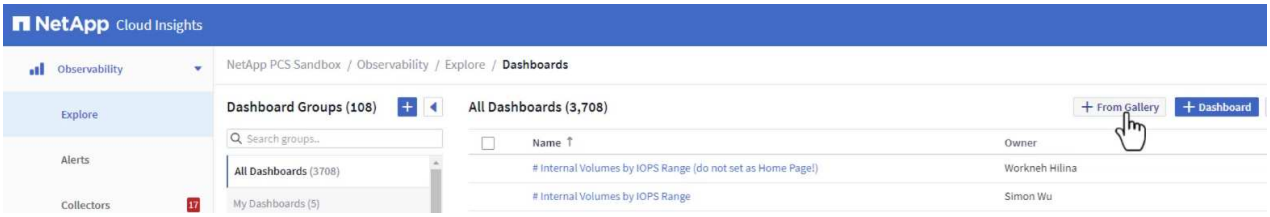
Dieser Abschnitt veranschaulicht, wie Sie Dashboards zum Korrelieren von Assets verwenden.

Korrelieren von Assets über ein Dashboard zur Speicherleistung

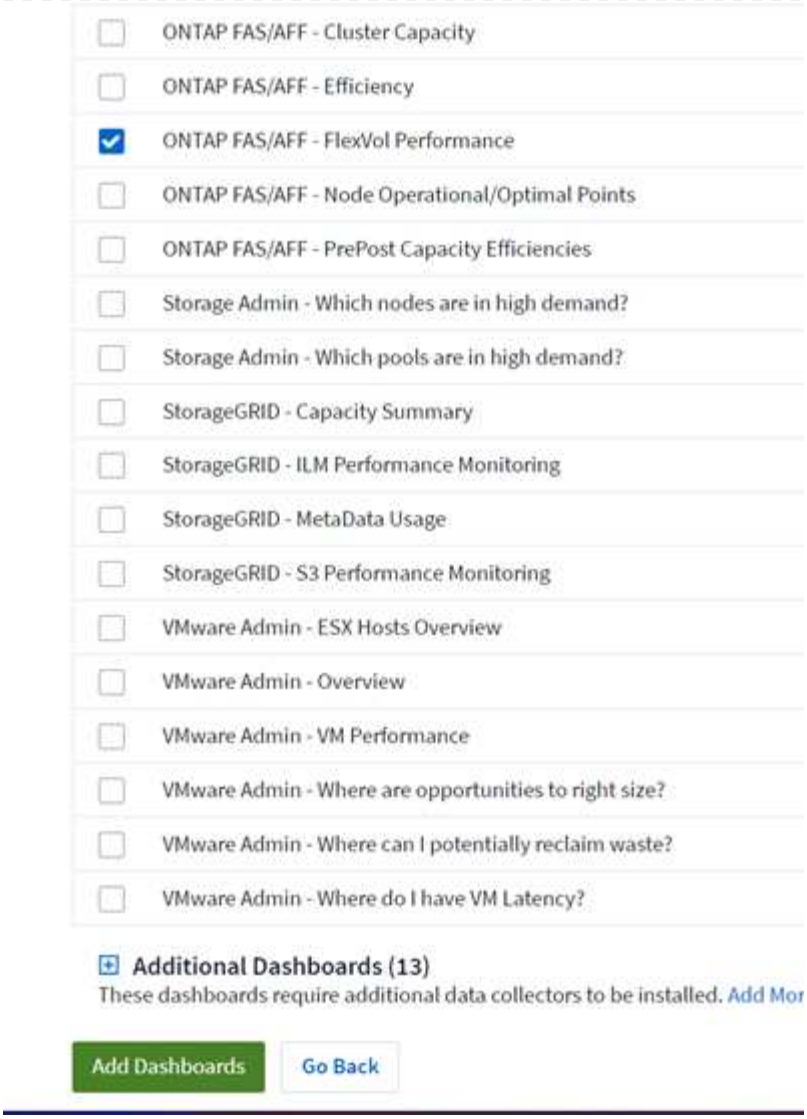
1. Navigieren Sie im linken Menü zu **Observability > Explore > All Dashboards**.



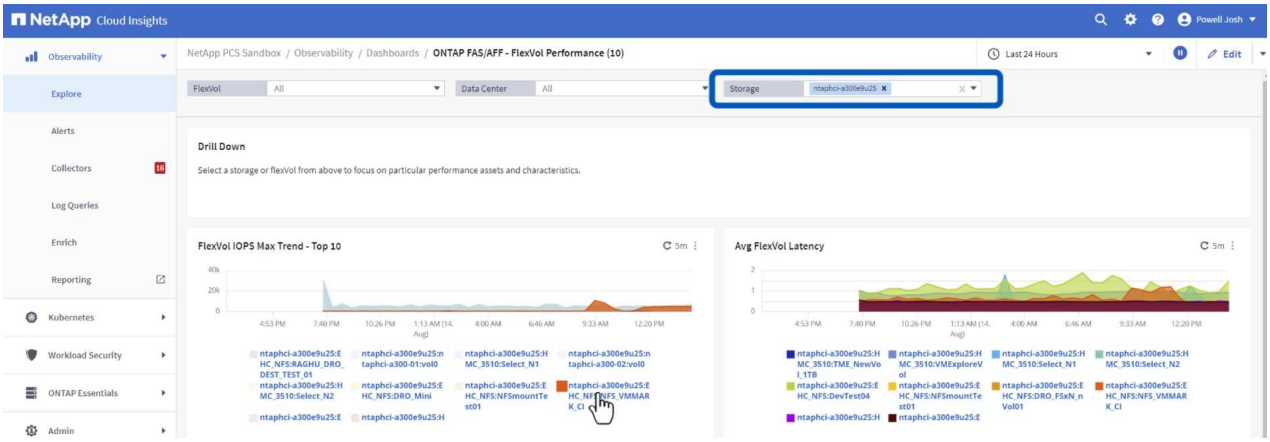
2. Klicken Sie auf die Schaltfläche **+ Aus Galerie**, um eine Liste vorgefertigter Dashboards anzuzeigen, die importiert werden können.



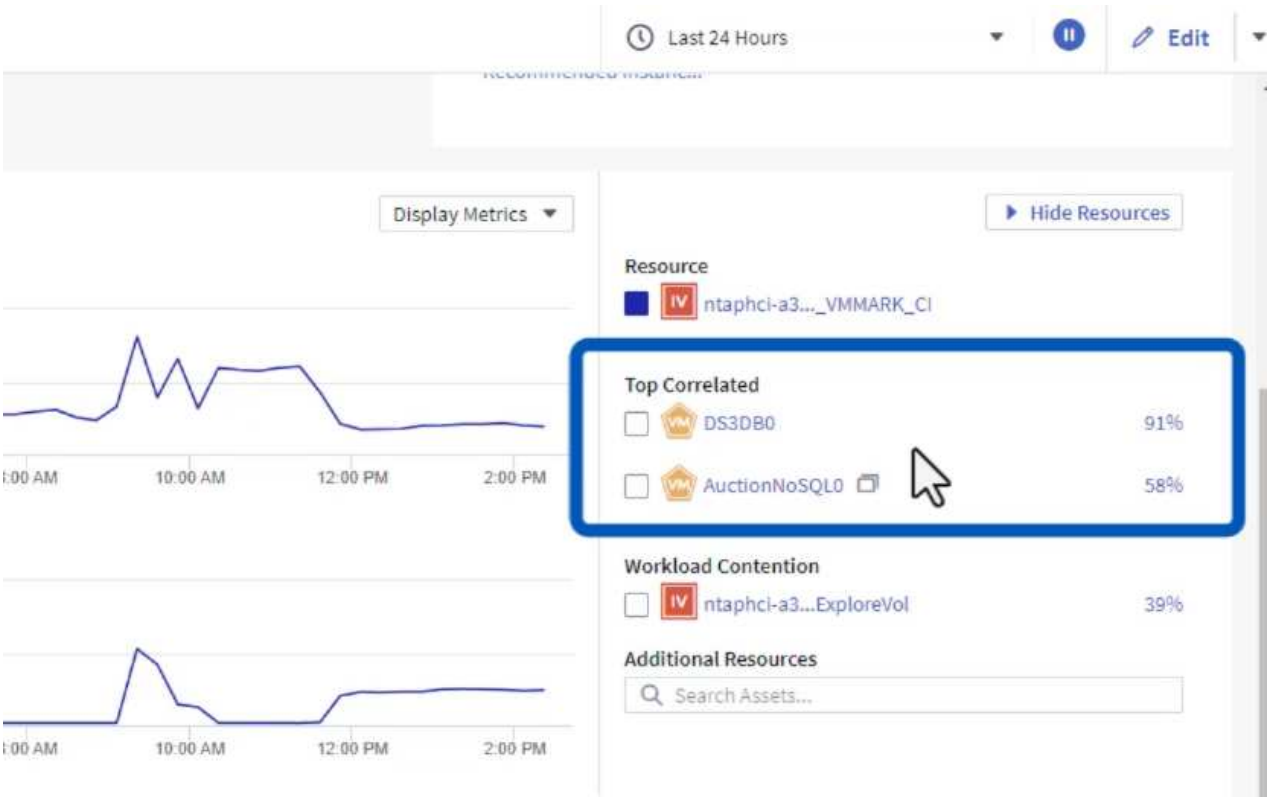
3. Wählen Sie aus der Liste ein Dashboard für die FlexVol -Leistung aus und klicken Sie unten auf der Seite auf die Schaltfläche **Dashboards hinzufügen**.



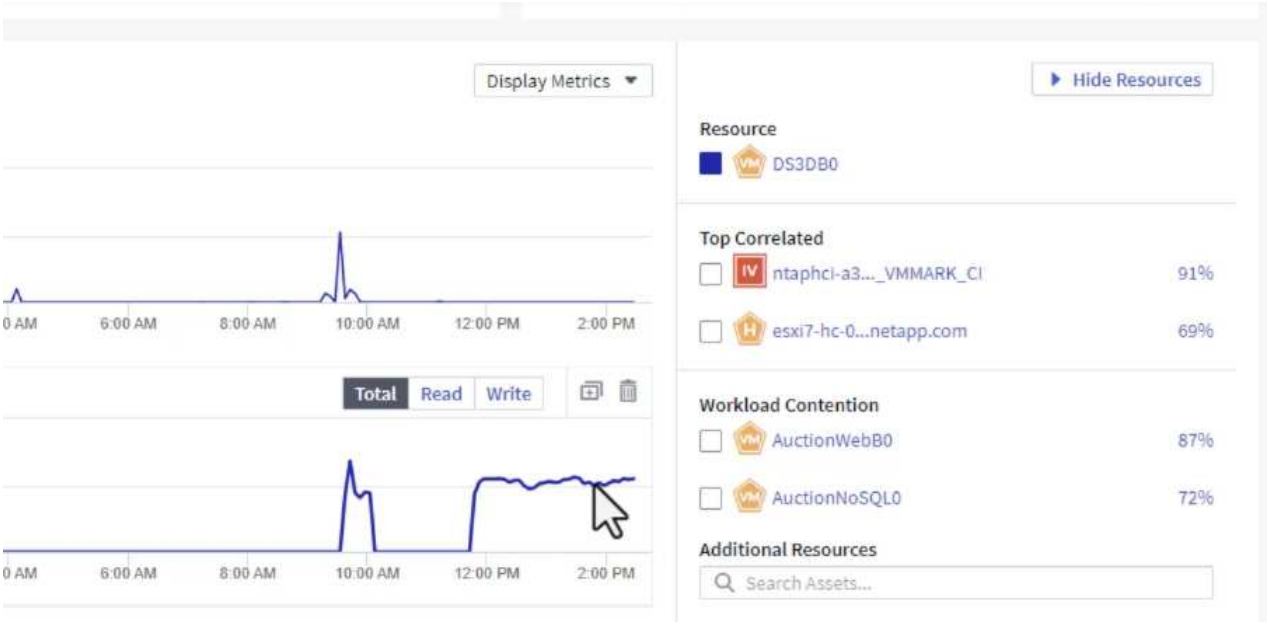
4. Öffnen Sie nach dem Import das Dashboard. Von hier aus können Sie verschiedene Widgets mit detaillierten Leistungsdaten sehen. Fügen Sie einen Filter hinzu, um ein einzelnes Speichersystem anzuzeigen, und wählen Sie ein Speichervolumen aus, um dessen Details zu untersuchen.



5. In dieser Ansicht können Sie verschiedene Kennzahlen zu diesem Speichervolume und den am stärksten genutzten und korrelierten virtuellen Maschinen sehen, die auf dem Volume ausgeführt werden.



6. Durch Klicken auf die VM mit der höchsten Auslastung können Sie die Metriken für diese VM genauer untersuchen, um mögliche Probleme anzuzeigen.



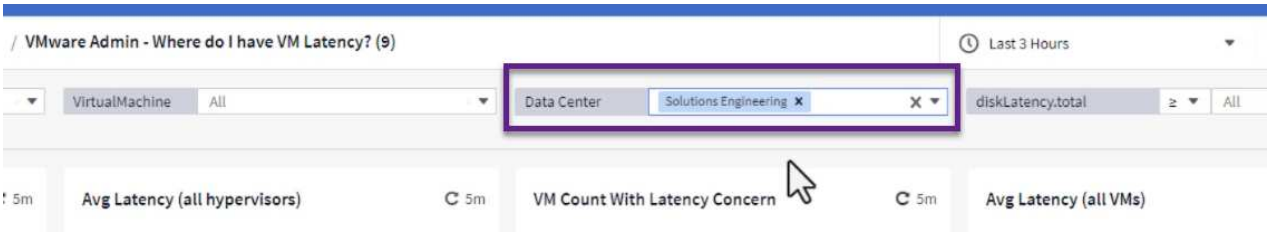
Verwenden Sie Cloud Insights , um laute Nachbarn zu identifizieren

Cloud Insights bietet Dashboards, mit denen sich Peer-VMs, die sich negativ auf andere VMs auswirken, die auf demselben Speichervolume ausgeführt werden, problemlos isolieren lassen.

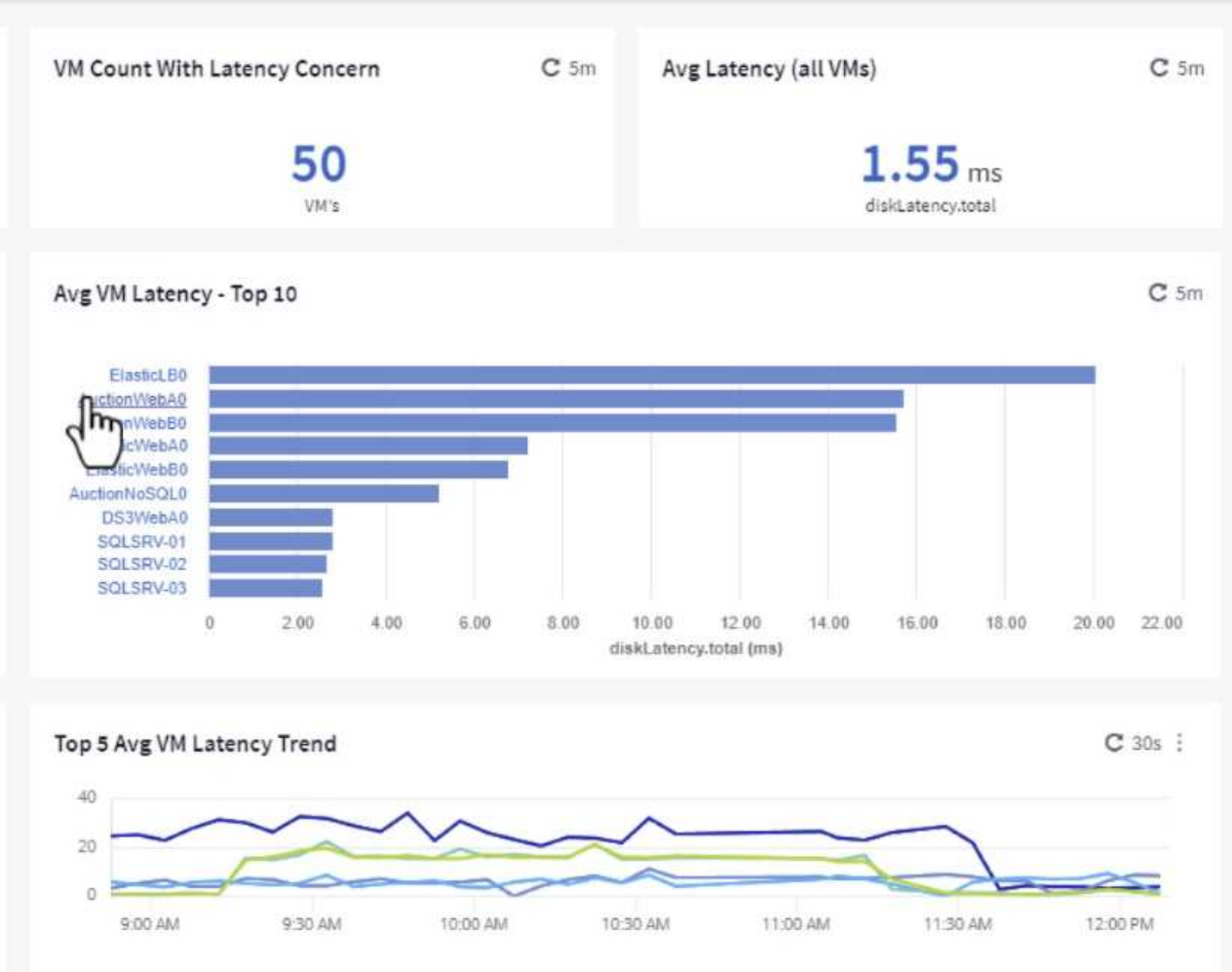
Verwenden Sie ein Top VM Latency-Dashboard, um laute Nachbarn zu isolieren

1. Greifen Sie in diesem Beispiel auf ein in der **Galerie** verfügbares Dashboard mit dem Namen **VMware Admin – Wo habe ich VM-Latenz?** zu.

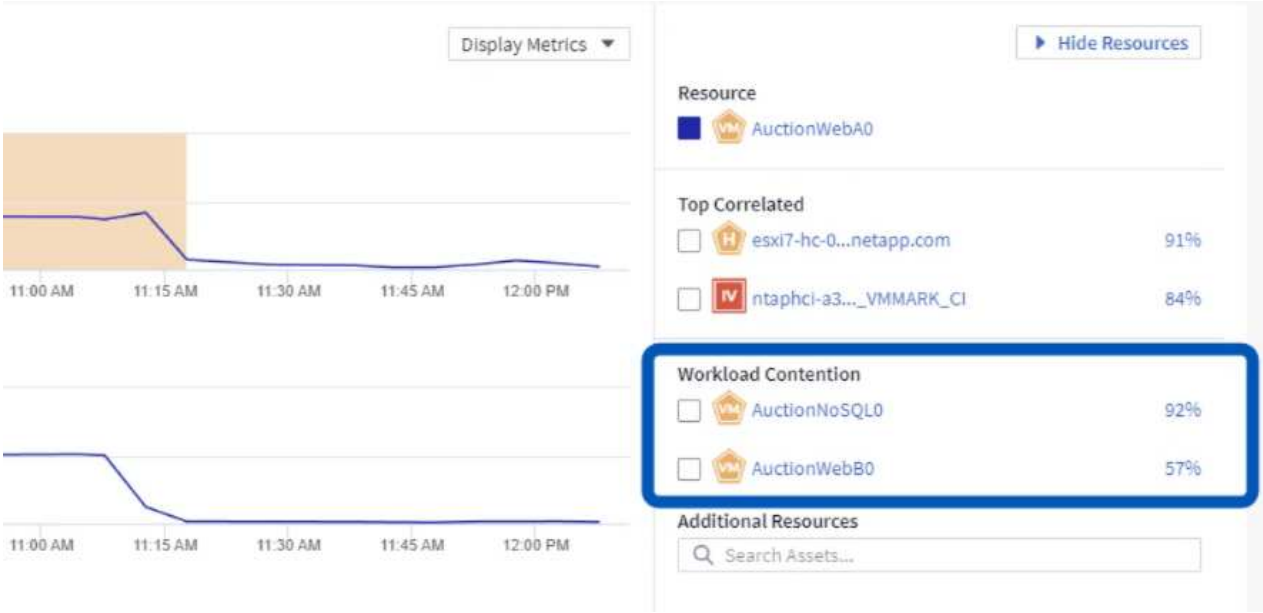
2. Filtern Sie als Nächstes nach der im vorherigen Schritt erstellten Anmerkung **Data Center**, um eine Teilmenge der Assets anzuzeigen.



3. Dieses Dashboard zeigt eine Liste der Top 10 VMs nach durchschnittlicher Latenz. Klicken Sie hier auf die betreffende VM, um sich die Details anzusehen.



4. Die VMs, die möglicherweise zu Workload-Konflikten führen, sind aufgelistet und verfügbar. Untersuchen Sie die Leistungsmetriken dieser VMs, um mögliche Probleme zu untersuchen.

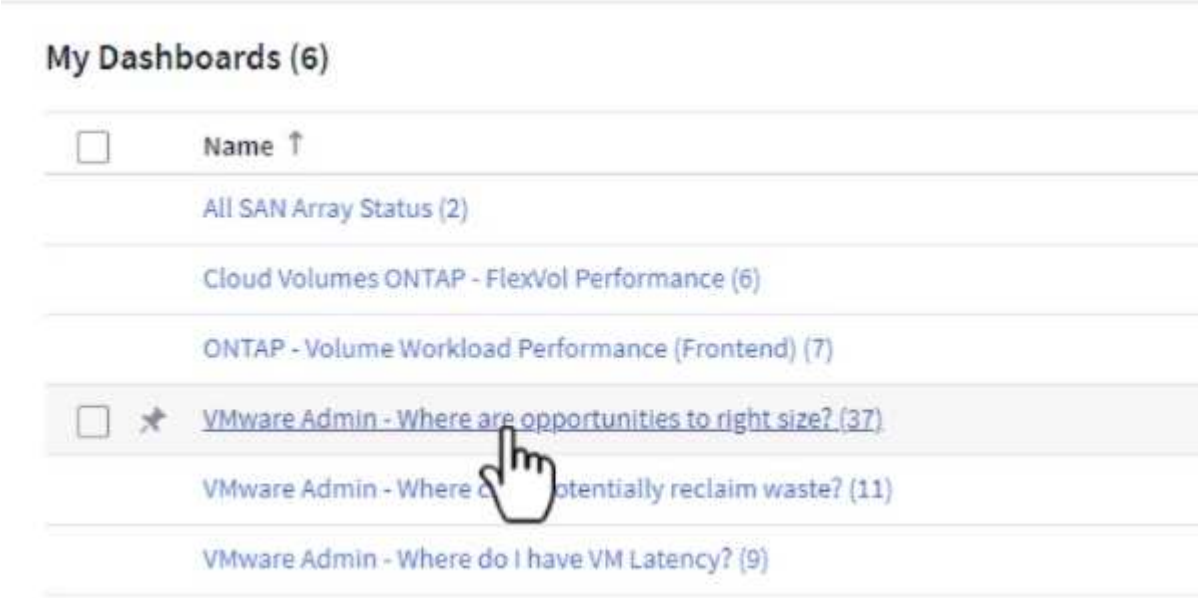


Zeigen Sie über- und unterausgelastete Ressourcen in Cloud Insights an

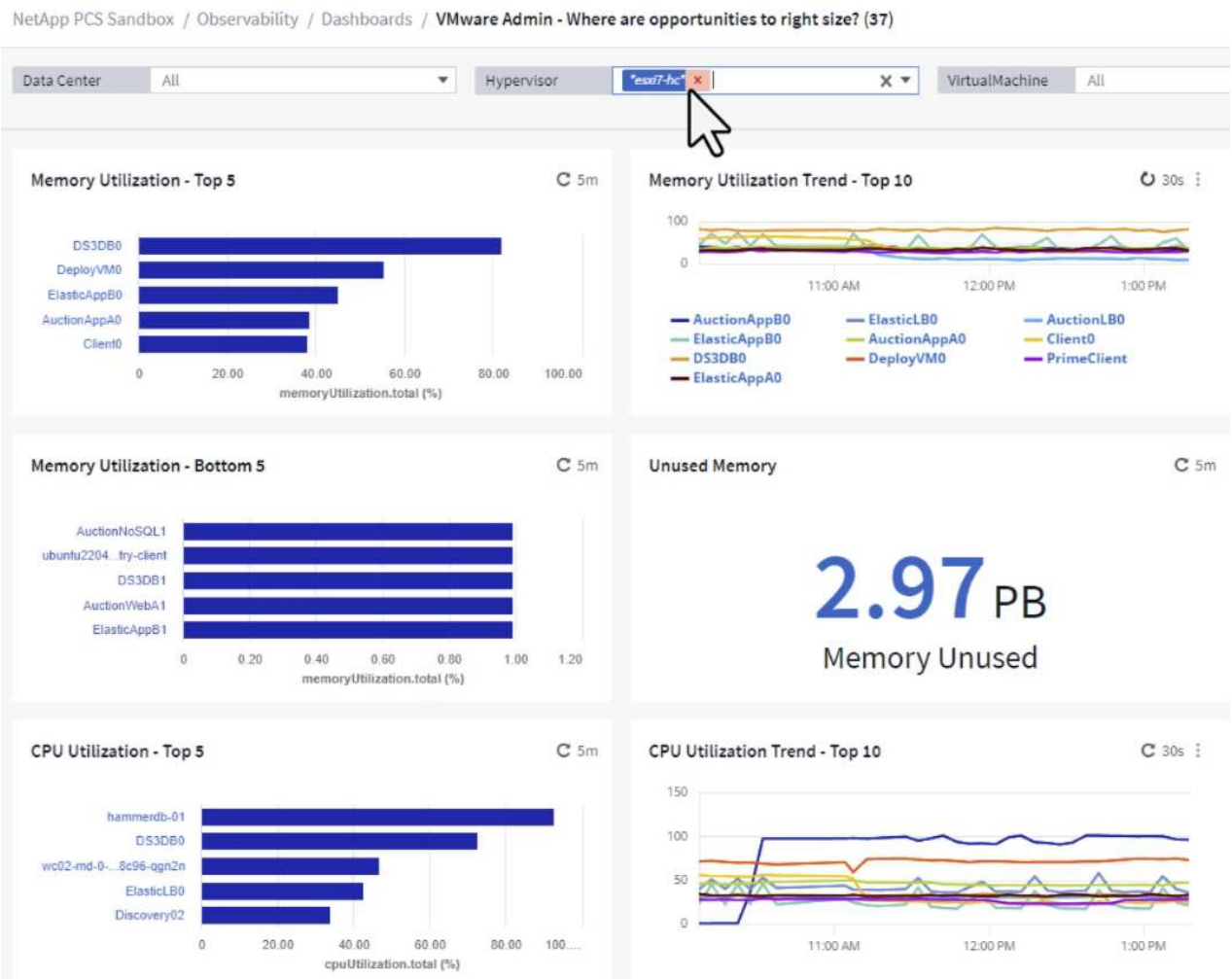
Durch die Anpassung der VM-Ressourcen an die tatsächlichen Arbeitslastanforderungen kann die Ressourcennutzung optimiert werden, was zu Kosteneinsparungen bei Infrastruktur und Cloud-Diensten führt. Daten in Cloud Insights können angepasst werden, um über- oder unterausgelastete VMs einfach anzuzeigen.

Identifizieren Sie Möglichkeiten zur richtigen VM-Größe

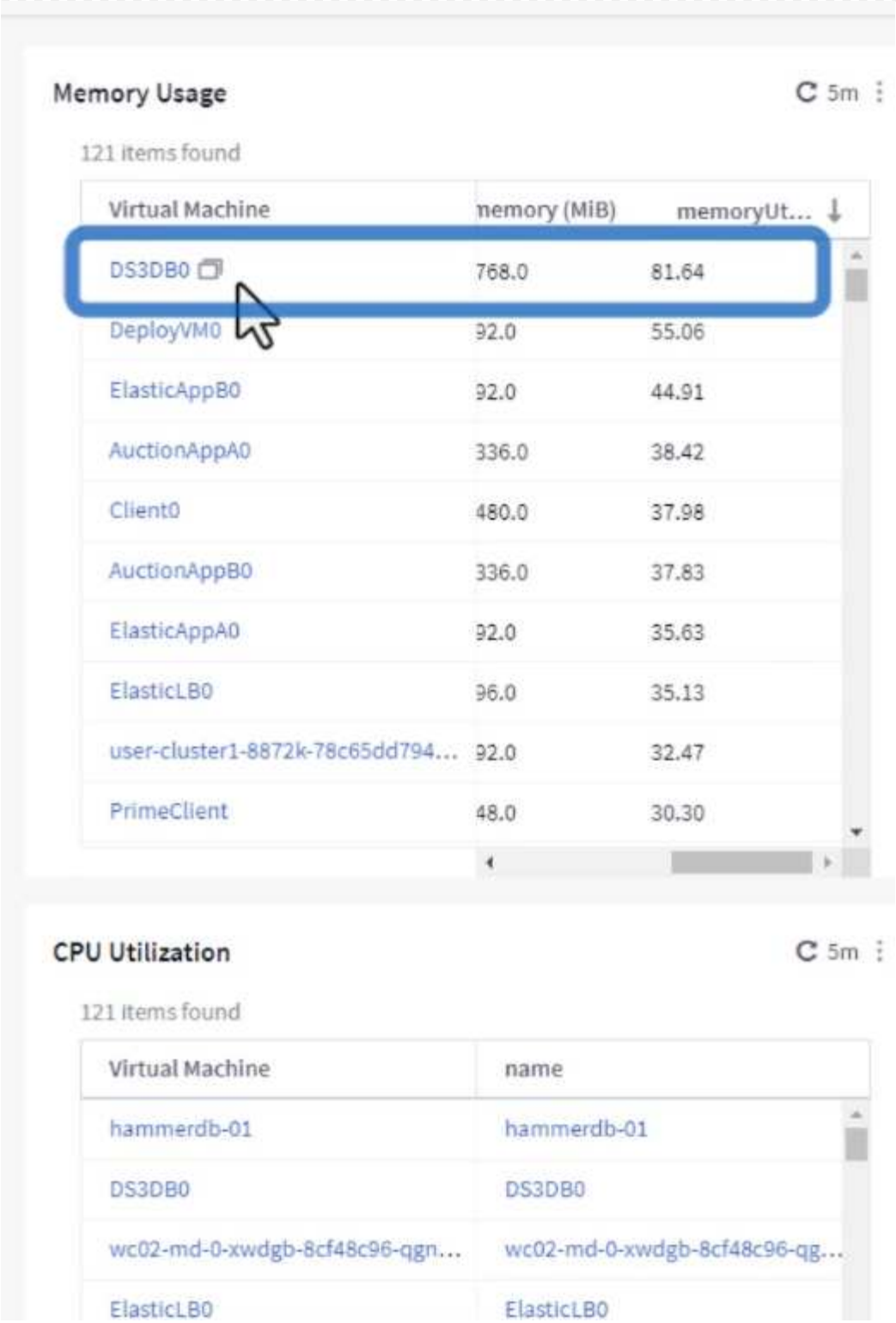
1. Greifen Sie in diesem Beispiel auf ein in der **Galerie** verfügbares Dashboard mit dem Namen **VMware Admin – Wo gibt es Möglichkeiten zur richtigen Dimensionierung?** zu.



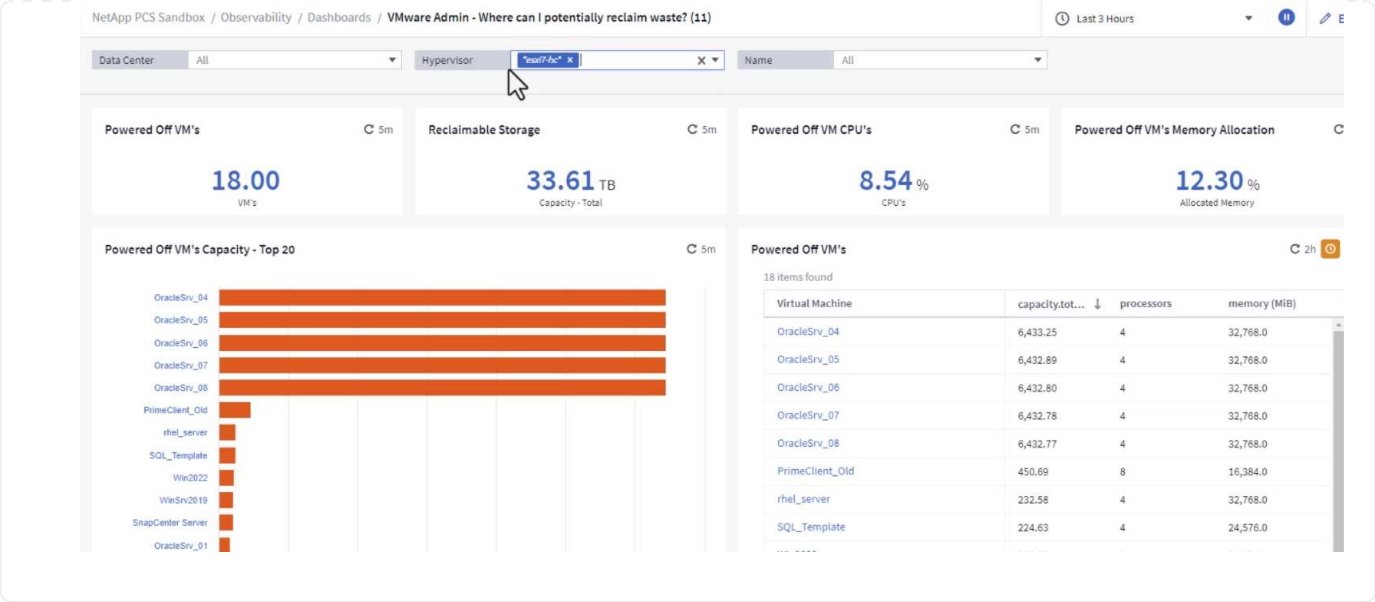
2. Filtern Sie zunächst nach allen ESXi-Hosts im Cluster. Sie können dann die Rangfolge der besten und schlechtesten VMs nach Speicher- und CPU-Auslastung sehen.



3. Tabellen ermöglichen das Sortieren und bieten basierend auf den ausgewählten Datenspalten mehr Details.



4. Ein weiteres Dashboard mit dem Namen **VMware Admin – Wo kann ich möglicherweise Abfall zurückgewinnen?** zeigt ausgeschaltete VMs sortiert nach ihrer Kapazitätsnutzung.

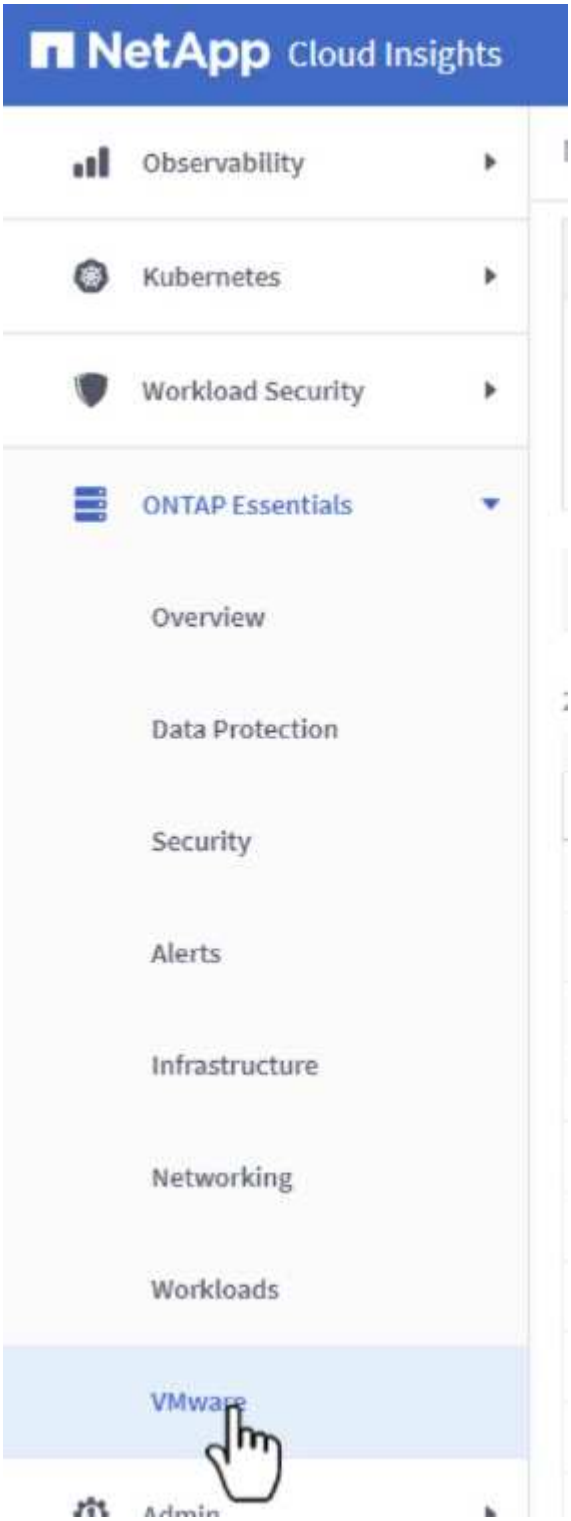


Verwenden Sie Abfragen, um Metriken zu isolieren und zu sortieren

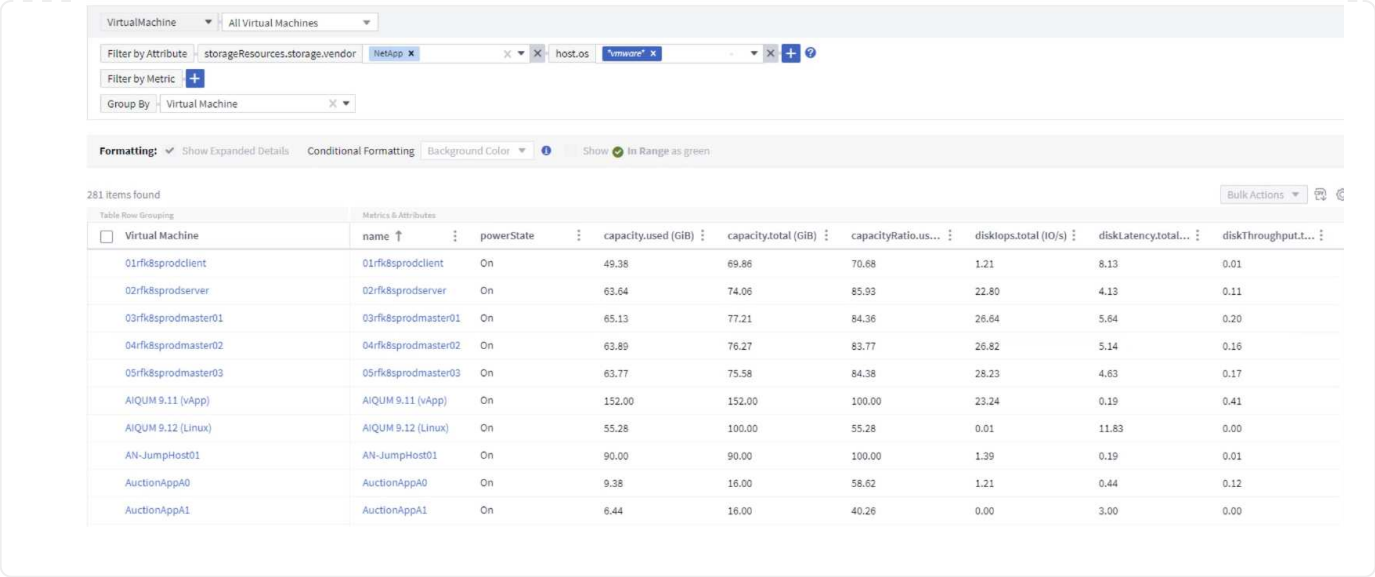
Die von Cloud Insights erfasste Datenmenge ist recht umfangreich. Metrikabfragen bieten eine leistungsstarke Möglichkeit, große Datenmengen auf nützliche Weise zu sortieren und zu organisieren.

Eine detaillierte VMware-Abfrage unter ONTAP Essentials anzeigen

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



2. In dieser Ansicht werden Ihnen oben mehrere Optionen zum Filtern und Gruppieren der Daten angezeigt. Alle Datenspalten sind anpassbar und zusätzliche Spalten können einfach hinzugefügt werden.



Abschluss

Diese Lösung wurde als Einführung in die ersten Schritte mit NetApp Cloud Insights konzipiert und zeigt einige der leistungsstarken Funktionen, die diese Observability-Lösung bietet. Das Produkt verfügt über Hunderte von Dashboards und Metrikabfragen, sodass Sie sofort loslegen können. Die Vollversion von Cloud Insights ist als 30-tägige Testversion verfügbar und die Basisversion ist für NetApp -Kunden kostenlos erhältlich.

Weitere Informationen

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

- "Zielseite zu NetApp BlueXP und Data Infrastructure Insights"
- "Dokumentation zu NetApp Data Infrastructure Insights"

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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