



VMware Cloud Foundation auf NetApp

NetApp virtualization solutions

NetApp

January 12, 2026

This PDF was generated from <https://docs.netapp.com/de-de/netapp-solutions-virtualization/vmware/vmw-vcf-overview.html> on January 12, 2026. 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 der Notfallwiederherstellung mit NetApp Disaster Recovery	14
Erste Schritte	15
NetApp Disaster Recovery -Konfiguration	17
Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array	18
So richten Sie Replikationsbeziehungen für NetApp Disaster Recovery ein	18
Was kann NetApp Disaster Recovery für Sie tun?	18
Testen des Failovers	23
Bereinigungs-Failover-Testvorgang	25
Geplante Migration und Failover	25
Failback	27
Überwachung und Dashboard	28
Konvertieren Sie vorhandene vSphere-Cluster in VCF	29
Erfahren Sie mehr über die Konvertierung einer vSphere-Umgebung mit vorhandenen	
Datenspeichern in eine VCF-Verwaltungsdomäne	30
Bereitstellungsworkflow zum Konvertieren von vCenter-Serverinstanzen in VCF-Verwaltungsdomänen	
mit NFS-Datenspeichern	32
Bereitstellungsworkflow zum Konvertieren von vCenter-Serverinstanzen in VCF-Verwaltungsdomänen	
mit Fibre Channel-Datenspeichern	32
Bereitstellen von VCF mit Hauptspeicher	33
Stellen Sie eine VCF-Umgebung mit ONTAP als primäre Speicherlösung bereit	33
Verwenden Sie einen FC-basierten VMFS-Datenspeicher auf ONTAP als Hauptspeicher für die VCF-	
Verwaltungsdomäne	33
Verwenden Sie einen NFS-Datenspeicher auf ONTAP als Hauptspeicher für die VCF-	
Verwaltungsdomäne	34
Verwenden Sie einen FC-basierten VMFS-Datenspeicher auf ONTAP als Hauptspeicher für eine VI-	

Workload-Domäne	36
Verwenden Sie einen NFS-Datenspeicher auf ONTAP als Hauptspeicher für eine VI-Workloaddomäne	38
Erweitern Sie VCF mit zusätzlichem Speicher	59
Erfahren Sie mehr über die Speichererweiterung für eine VCF-Umgebung mithilfe von zusätzlichem Speicher	59
Erweitern Sie Verwaltungsdomänen mit iSCSI	61
Fügen Sie mithilfe von ONTAP tools for VMware vSphere einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher für eine Verwaltungsdomäne hinzu	83
Erweitern Sie VI-Workload-Domänen mit vVols iSCSI	84
Erweitern Sie VI-Workload-Domänen mit vVols NFS	112
Erweitern Sie VI-Workloaddomänen mit NVMe/TCP	138
Fügen Sie einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher zu einer VI-Workload-Domäne hinzu	160
Schützen Sie VCF mit SnapCenter	161
Erfahren Sie mehr über den Schutz von VCF-Workload-Domänen mit dem SnapCenter -Plug-in für VMware vSphere	161
Schützen Sie eine VCF-Workloaddomäne mit dem SnapCenter -Plug-in für VMware vSphere	161
Schützen Sie VCF-Verwaltungs- und Workloaddomänen mit dem SnapCenter -Plug-in für VMware vSphere	197
Schützen Sie VCF-Workload-Domänen mit NVMe über TCP-Speicher und SnapCenter -Plug-in für VMware vSphere	210
Schützen Sie Workloads mit vSphere Metro Storage Cluster	218
Erfahren Sie mehr über die Integration der hohen Verfügbarkeit von ONTAP mit VMware vSphere Metro Storage Cluster (vMSC)	218
Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne mit MetroCluster	219
Konfigurieren eines Stretch-Clusters für eine VI-Workloaddomäne mit MetroCluster	230
Konfigurieren eines Stretch-Clusters für eine VCF-Verwaltungsdomäne mit SnapMirror Active Sync ..	242
Konfigurieren eines Stretch-Clusters für eine VI-Workloaddomäne mit SnapMirror Active Sync	244
Migrieren Sie VMs von VMware vSphere zu ONTAP -Datenspeichern	246
Netzwerkanforderungen	247
VM-Migrationsszenarien	249
Szenarien für die Migration von VM-Vorlagen	274
Anwendungsfälle	282
Weitere Ressourcen	283
Autonomer Ransomware-Schutz für NFS-Speicher	283
Überwachen Sie den lokalen Speicher mit Data Infrastructure Insights	293
Überwachung des lokalen Speichers mit Data Infrastructure Insights	293
Übersicht über die Lösungsbereitstellung	293
Voraussetzungen	294
Lösungsbereitstellung	294
Abschluss	311
Weitere Informationen	311

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

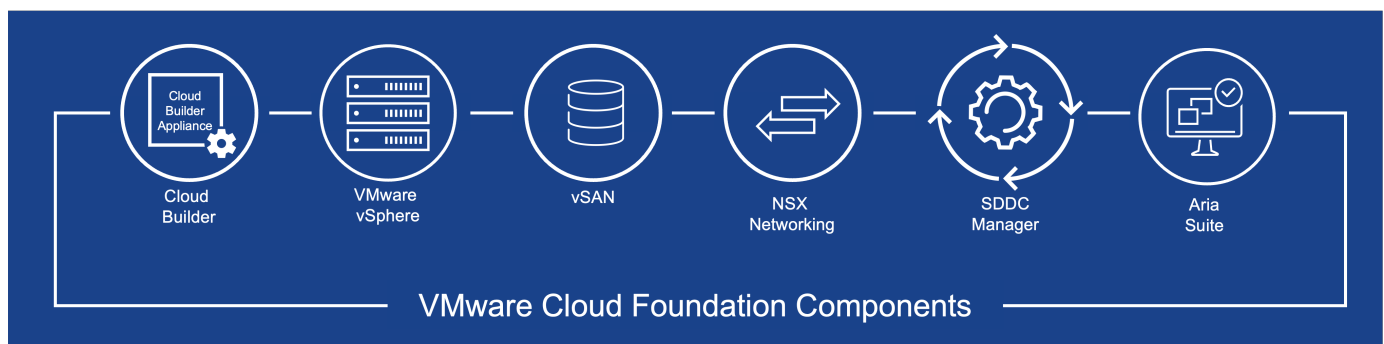
Die Verwendung von NetApp mit VCF verbessert die Datenverwaltung und Speichereffizienz durch die erweiterten Funktionen von NetApp wie Deduplizierung, Komprimierung und Snapshots. Diese Kombination bietet nahtlose Integration, hohe Leistung und Skalierbarkeit für virtualisierte Umgebungen. Darüber hinaus 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.

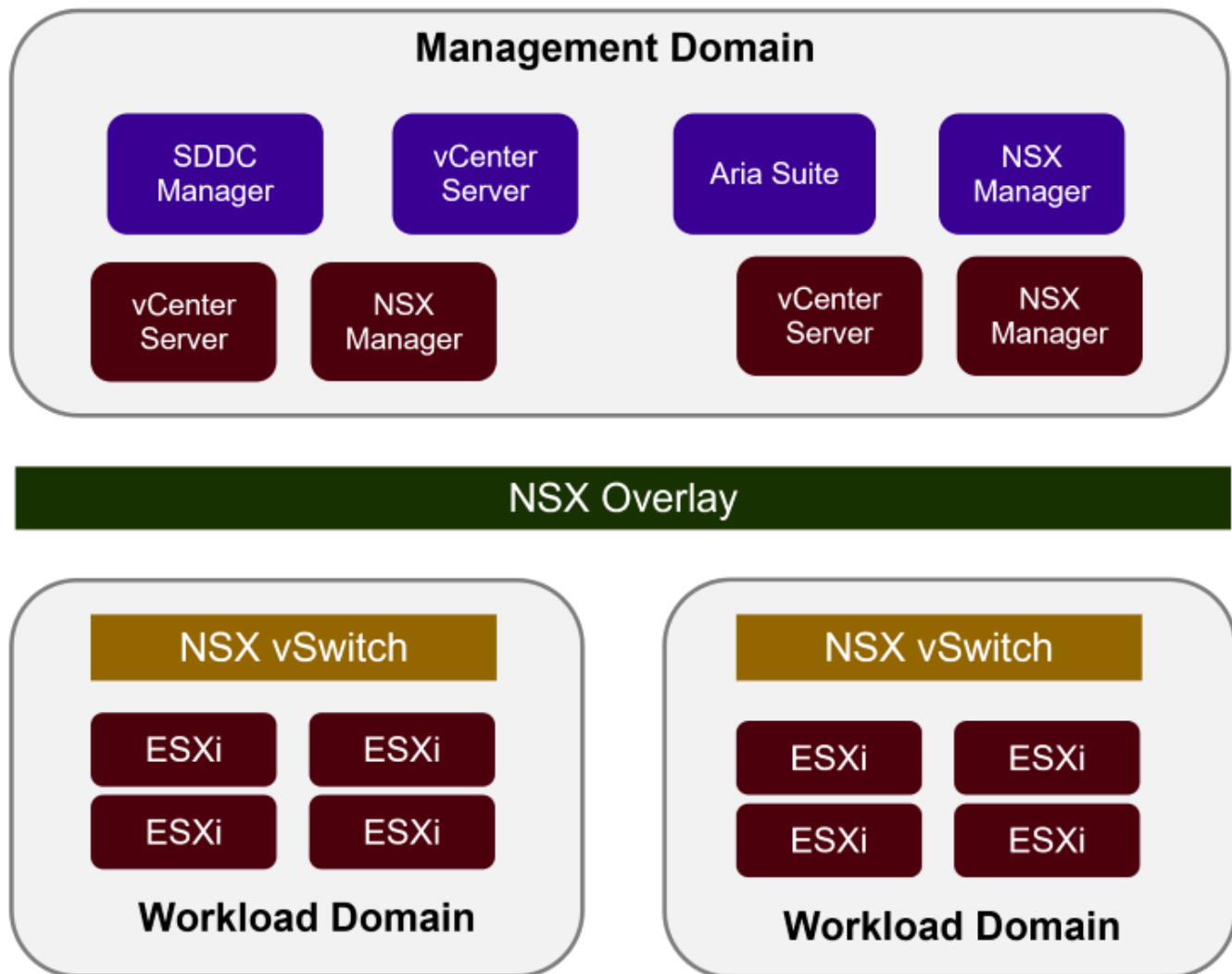
Einführung in VMware Cloud Foundation

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



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.

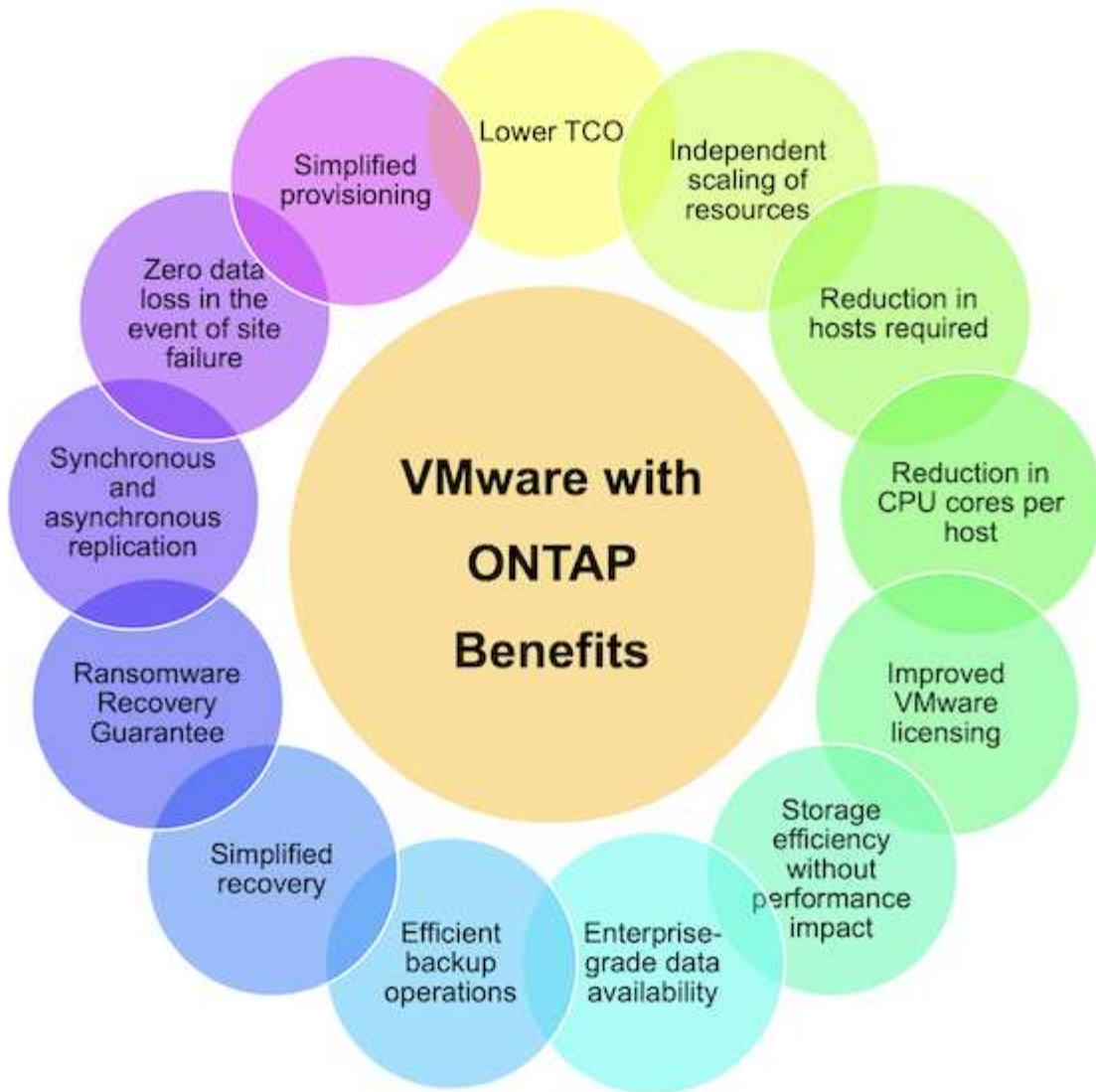
Unterstützt VCF-Speichertypen

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"](#)
- ["NetApp Disaster Recovery"](#)
- ["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

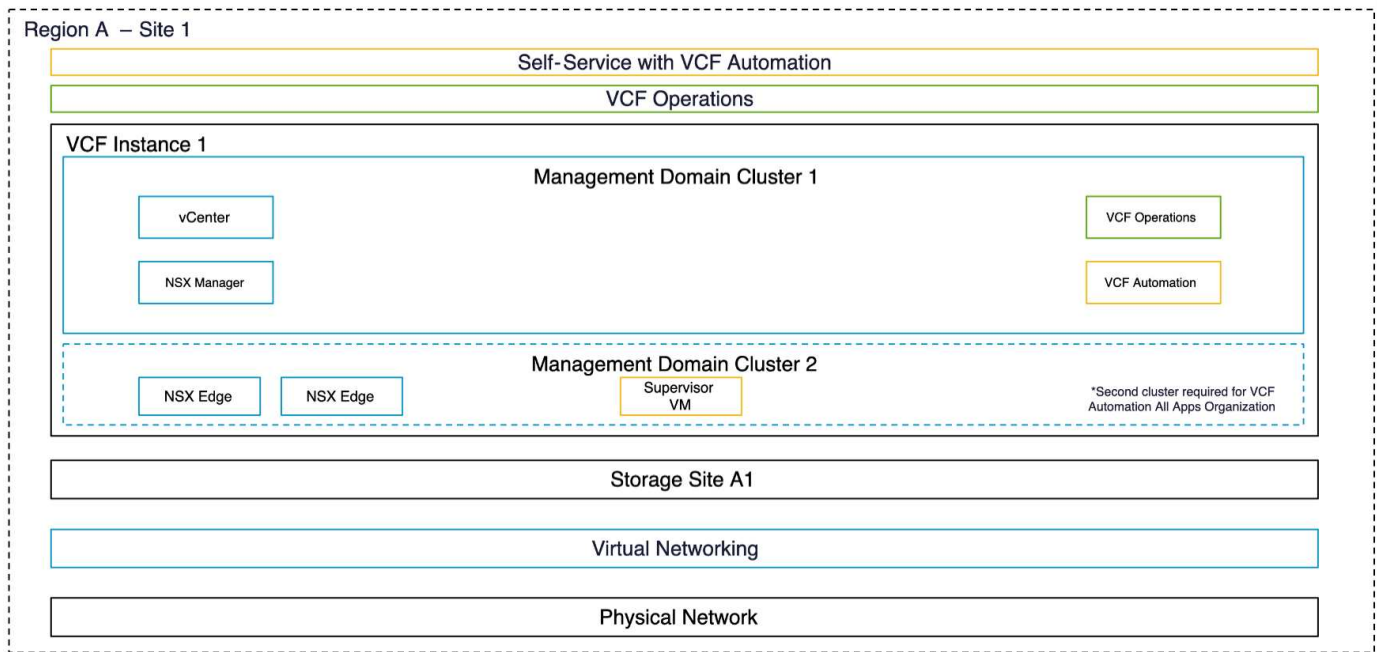
Blaupausen

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"](#).

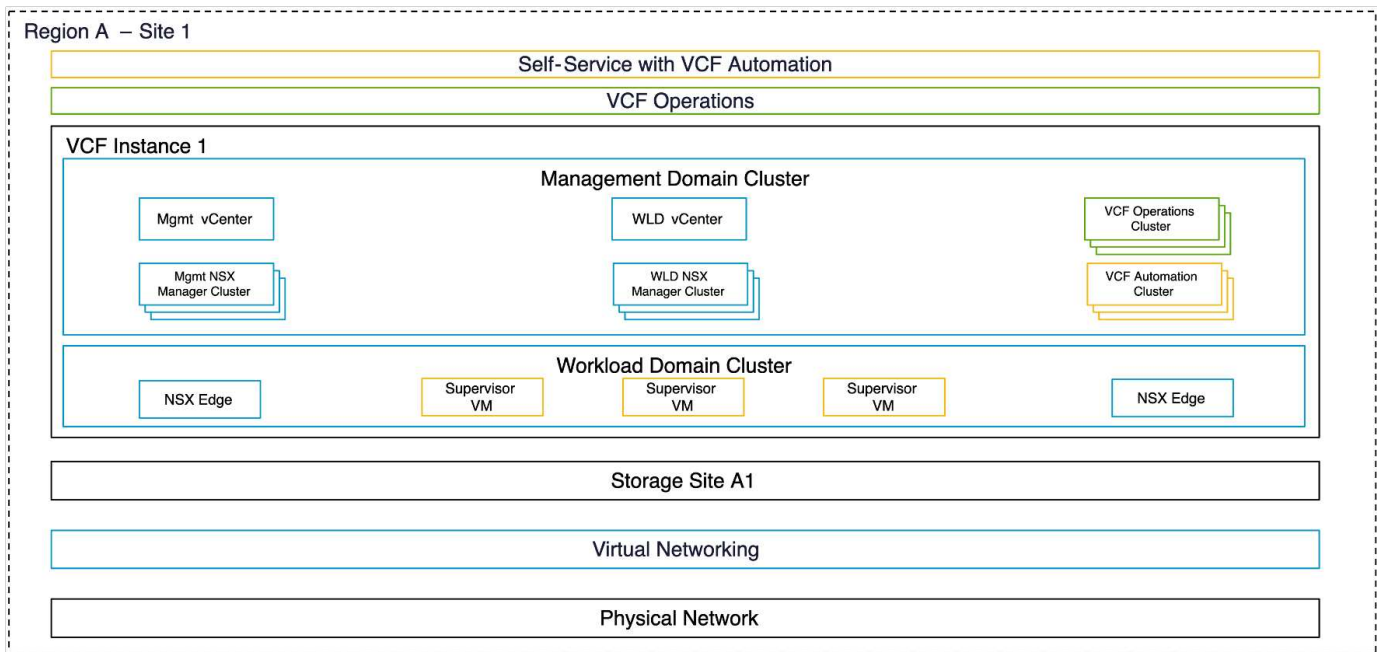
VCF-Flotte an einem einzigen Standort

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"](#).

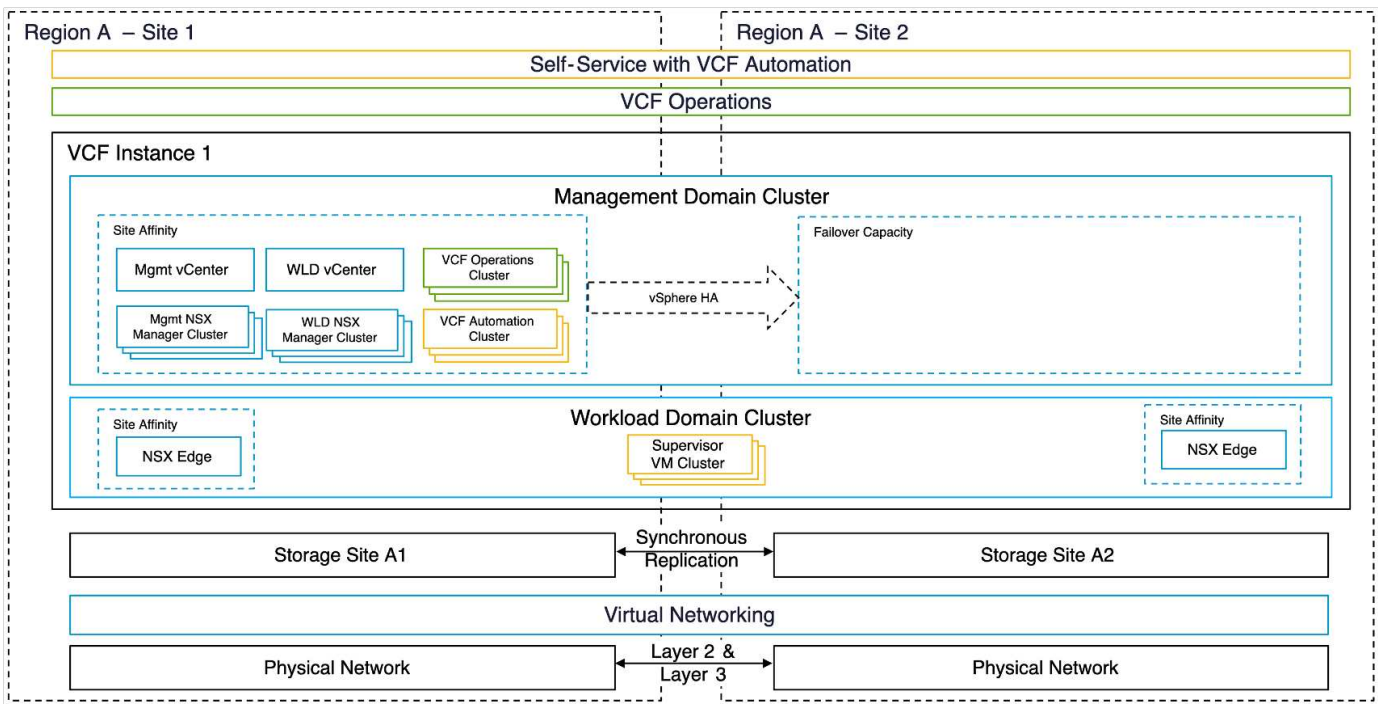
VCF-Flotte mit mehreren Standorten in einer einzigen Region

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 der NetApp Console 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-Backup-Richtlinien mit NetApp Backup and Recovery for VMs über SnapMirror und SnapMirror to Cloud implementieren. Sie können Wiederherstellungen von jedem der drei Standorte aus durchführen.

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

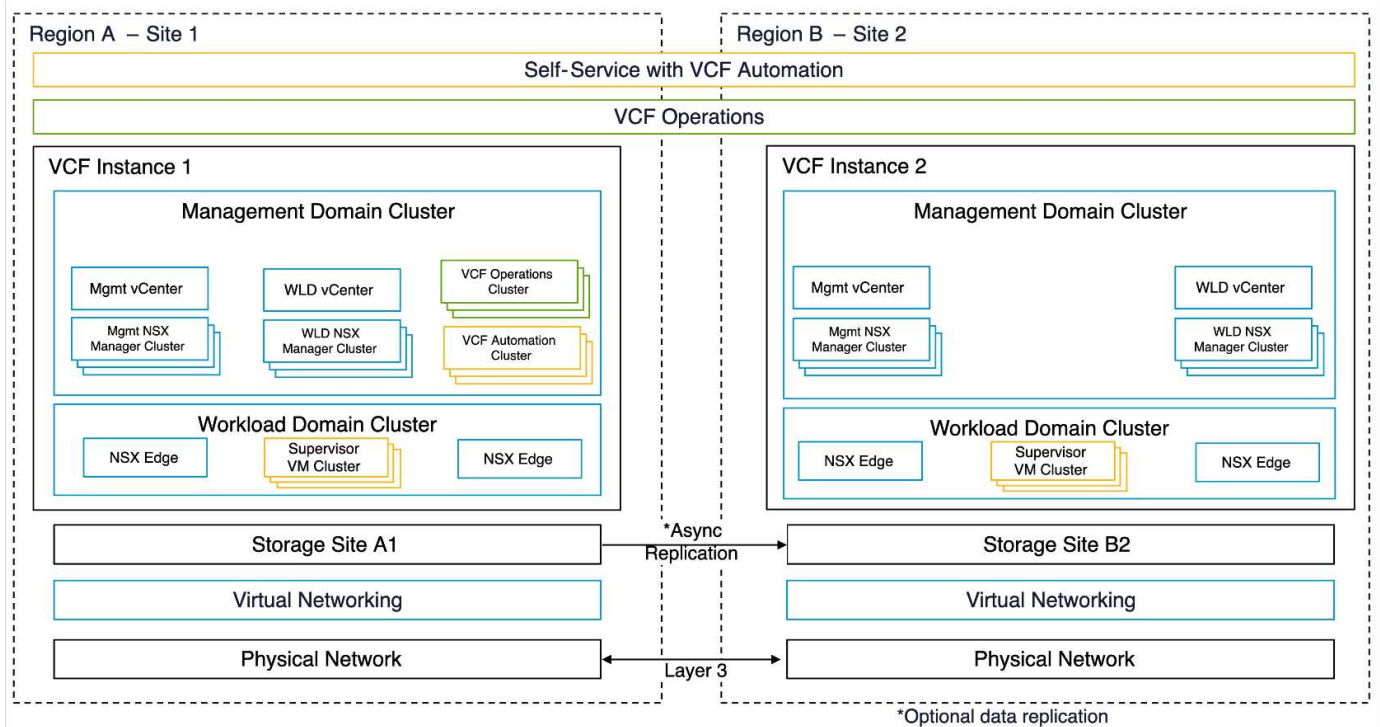
Weitere Informationen finden Sie im ["Technische Dokumentation von Broadcom zur VCF-Flotte mit mehreren Standorten in einer einzigen Region"](#).

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.

Die Notfallwiederherstellung für VMs kann mit VMware Live Site Recovery oder NetApp Disaster Recovery verwaltet werden. 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



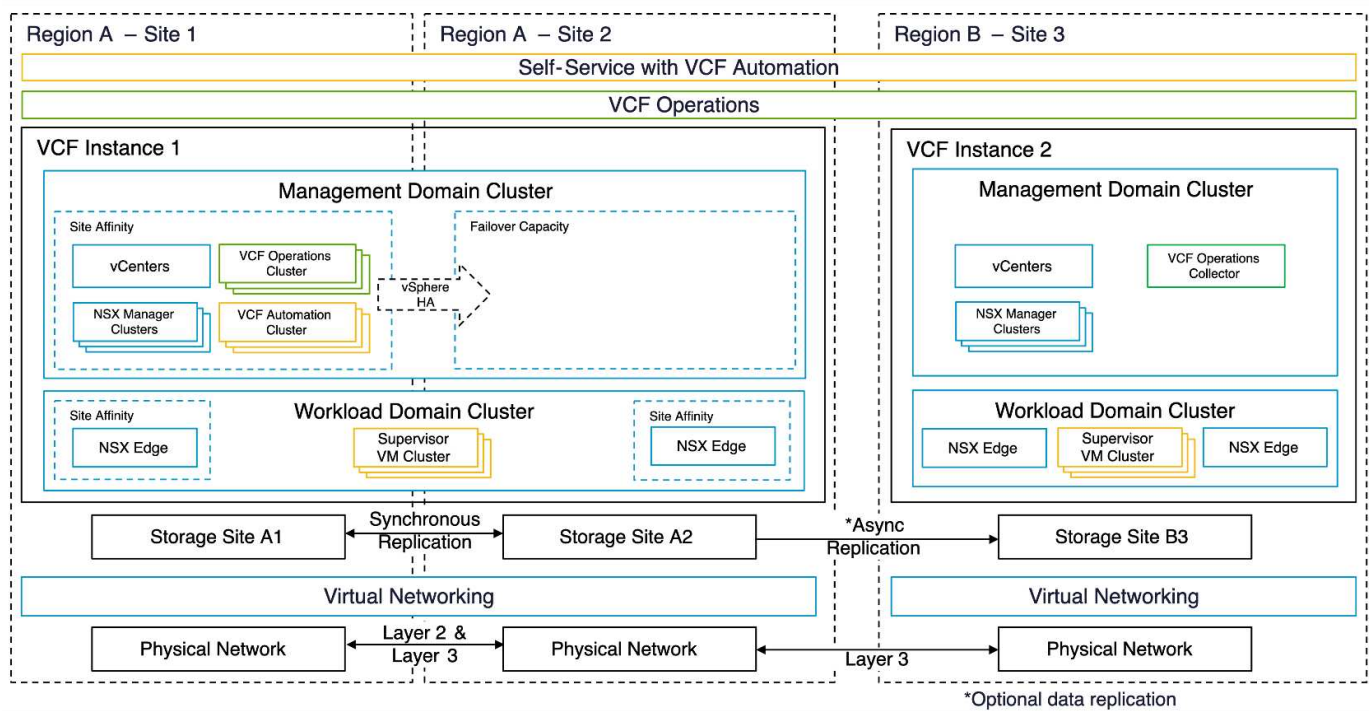
ONTAP -Tools bieten eine Benutzeroberfläche für die Einrichtung der Datenspeicherreplikation. Die NetApp Console kann auch zur Replikation zwischen Speicherarrays verwendet werden. Das SnapCenter Plug-in for VMware vSphere nutzt vorhandene SnapMirror -Beziehungen für Snapshots.

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 die NetApp Console 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-Bereitstellungsschritten"](#).
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 NetApp Console Agenten bereit.
- ["Prüfen Sie, was Sie ohne Console-Agent tun können."](#)Die
 - ["Agentenbereitstellungsmodi"](#)Die
- d. Verwenden Sie NetApp Backup and Recovery
- ["Schützen Sie VM -Workloads"](#)Die
 - ["Schützen Sie VKS -Workloads"](#)Die
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 NetApp Backup and Recovery
- ["Schützen Sie VM -Workloads"](#)Die
 - ["Schützen Sie VKS -Workloads"](#)Die

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 der Notfallwiederherstellung mit NetApp Disaster Recovery

VCF-Notfallwiederherstellungslösung für NFS-Datenspeicher mit NetApp SnapMirror und NetApp Disaster Recovery

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.

Weitere Informationen finden Sie im Folgenden. ["NetApp Disaster Recovery -Dokumentation"](#) Die

Dieser Abschnitt beschreibt die Konfiguration von NetApp Disaster Recovery zur Einrichtung von Disaster Recovery für lokale VMware-VMs.

Das Setup umfasst:

- Erstellen eines NetApp Console Kontos und Bereitstellen eines Agenten.
- Hinzufügen von ONTAP Arrays zur NetApp Console zu den unter Verwaltung stehenden Systemen, 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.

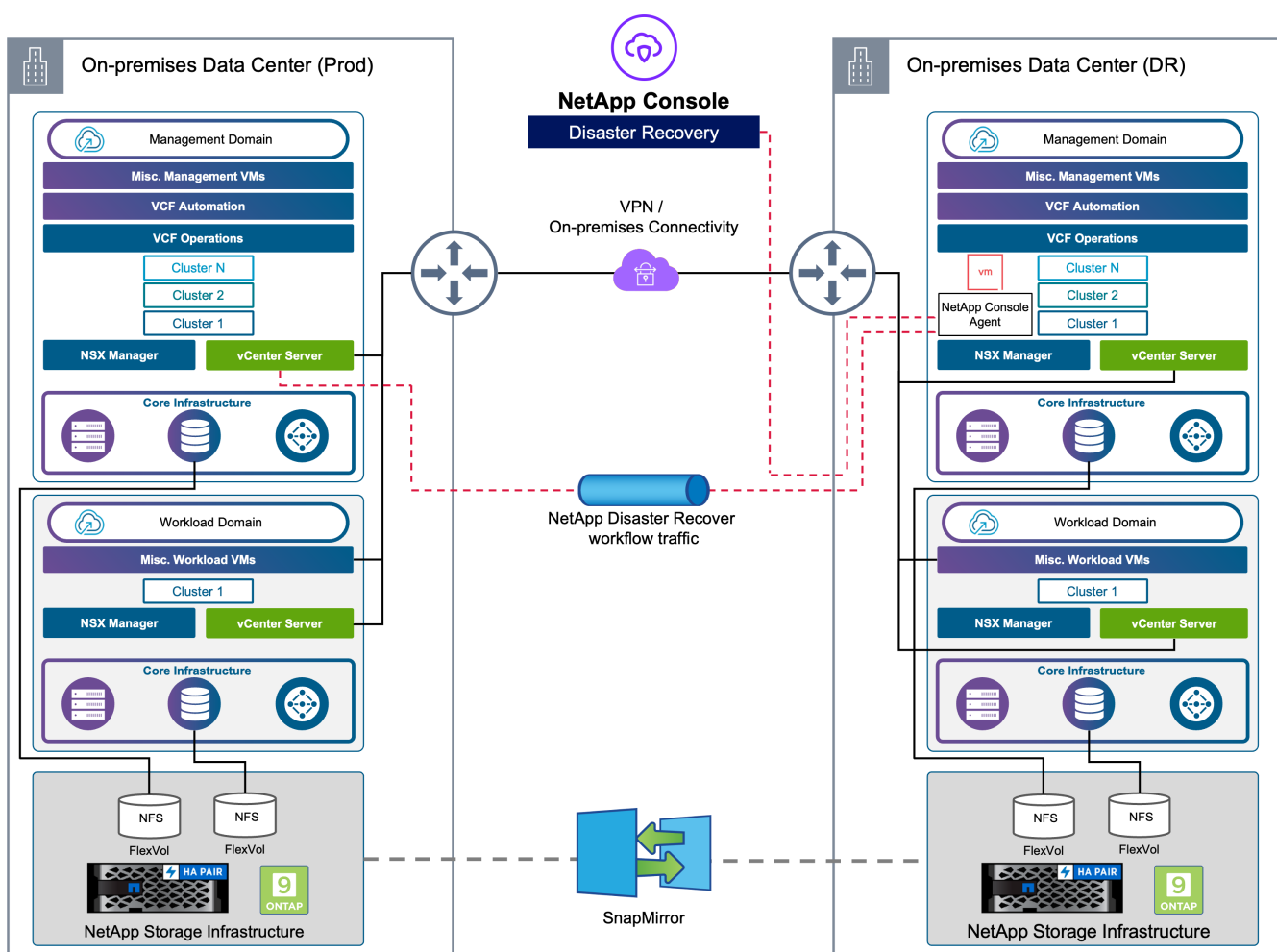
NetApp Disaster Recovery ist in die NetApp Console integriert und ermöglicht es Unternehmen, ihre lokalen VMware vCenter- und ONTAP Speichersysteme nahtlos zu erkennen. Nach der Erkennung können Administratoren Ressourcengruppierungen definieren, Notfallwiederherstellungspläne erstellen, diese mit den

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.

NetApp Disaster Recovery 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 die NetApp Console den Wiederherstellungsprozess und stellt geschützte virtuelle Maschinen am festgelegten DR-Standort mit minimalem Benutzereingriff automatisch wieder her. 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.

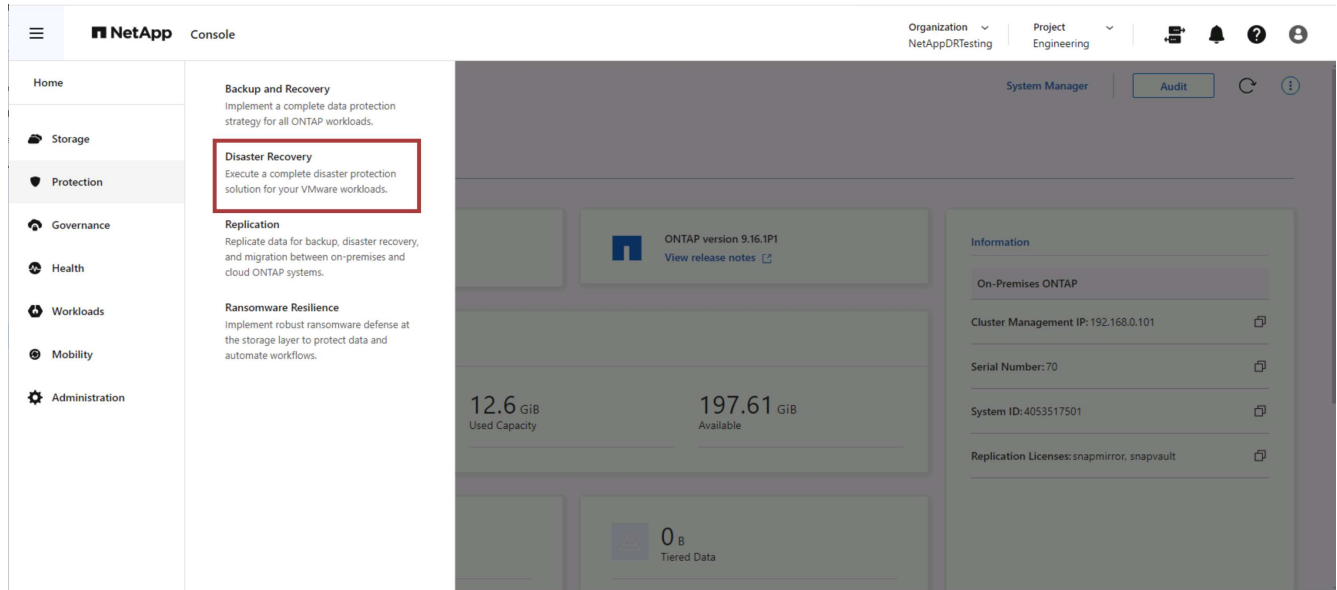
Alle diese Funktionen werden im Vergleich zu herkömmlichen Disaster-Recovery-Lösungen zu deutlich geringeren Kosten bereitgestellt.



Erste Schritte

Um mit NetApp Disaster Recovery zu beginnen, verwenden Sie die NetApp Console und greifen Sie dann auf den Dienst zu.

1. Melden Sie sich bei der NetApp Console an.
2. Wählen Sie in der linken Navigationsleiste der NetApp Console „Schutz“ > „Notfallwiederherstellung“.
3. Das NetApp Disaster Recovery Dashboard wird angezeigt.



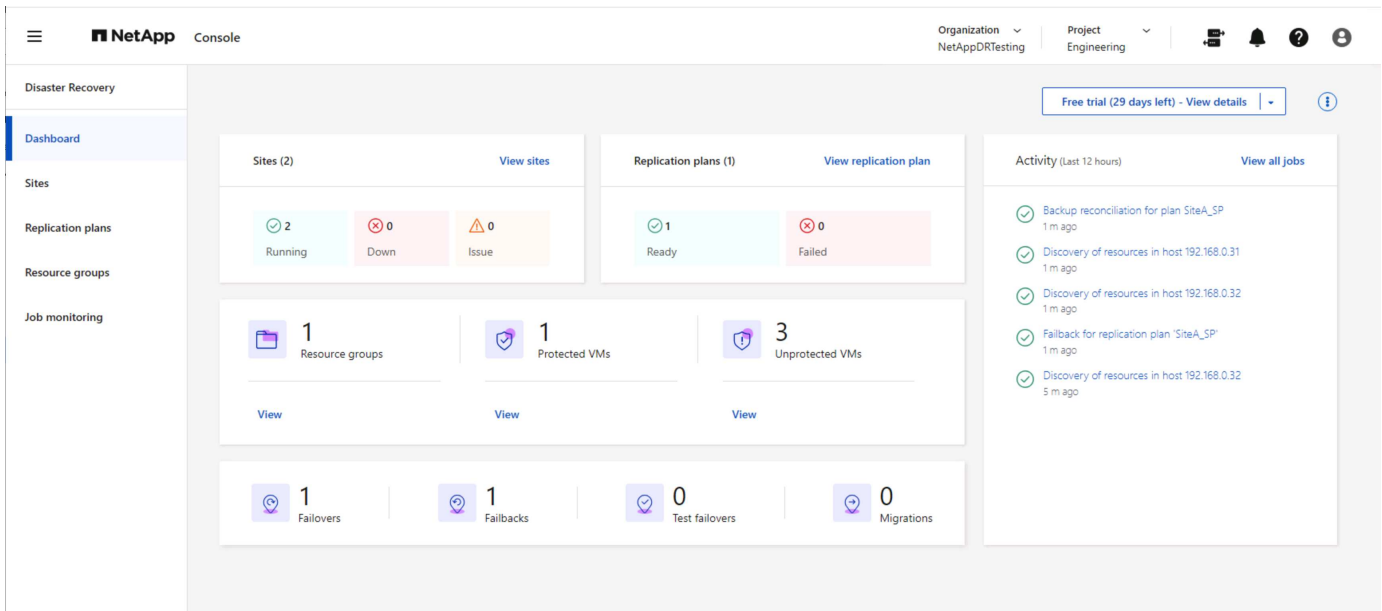
Bevor Sie den Notfallwiederherstellungsplan konfigurieren, stellen Sie Folgendes sicher: **"Voraussetzungen"** werden erfüllt:

- Der Console-Agent ist in der NetApp Console eingerichtet.
- Die Agenteninstanz verfügt über Verbindungen zum Quell- und Ziel-Workload-Domänen-vCenter und zu den Speichersystemen.
- NetApp Data ONTAP Cluster zur Bereitstellung von NFS- oder VMFS-Datenspeichern.
- In der NetApp Console 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 Datenspeichervolumen 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 Console-Agenten am Zielstandort oder an einem dritten Standort bereitzustellen, damit der Agent 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.



NetApp Disaster Recovery -Konfiguration

Der erste Schritt bei der Vorbereitung auf die Notfallwiederherstellung besteht darin, die Quell-vCenter- und Speicherressourcen zu ermitteln und zu NetApp Disaster Recovery hinzuzufügen.

Öffnen Sie die NetApp Console und wählen Sie im linken Navigationsmenü „Schutz“ > „Notfallwiederherstellung“. Wählen Sie „Standorte“ und anschließend „Hinzufügen“. Geben Sie einen Namen für die neue Quellseite und deren Standorte ein. Wiederholen Sie den Schritt, um das Zielgelände und den Standort hinzuzufügen.

Add site

A site is a collection of vCenter servers, either on-premises or in the cloud.

Site

Location

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 ermöglicht die 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. NetApp Disaster Recovery erstellt außerdem die SnapMirror Beziehung, vorausgesetzt, Cluster- und SVM-Peering sind vorher konfiguriert.

Für Fälle, in denen der primäre Speicher nicht vollständig verloren geht, bietet SnapMirror eine effiziente Möglichkeit zur Resynchronisierung des primären Speichers und des DR-Standorts. SnapMirror kann die beiden Standorte neu synchronisieren, indem es lediglich geänderte oder neue Daten vom DR-Standort zurück zum primären Standort überträgt, indem es die SnapMirror Beziehungen umkehrt. Dies bedeutet, dass Replikationspläne in NetApp Disaster Recovery nach einem Failover in beide Richtungen resynchronisiert werden können, ohne dass das gesamte Volume neu kopiert werden muss. Wird eine Beziehung in umgekehrter Richtung resynchronisiert, werden nur neue Daten, die seit der letzten erfolgreichen Synchronisierung der Snapshot-Kopie geschrieben wurden, an das Ziel zurückgesendet.



Wenn die SnapMirror Beziehung für das Volume bereits über die CLI oder den System Manager konfiguriert ist, erkennt NetApp Disaster Recovery die Beziehung und fährt mit den übrigen Workflow-Operationen fort.

So richten Sie Replikationsbeziehungen für NetApp Disaster Recovery ein

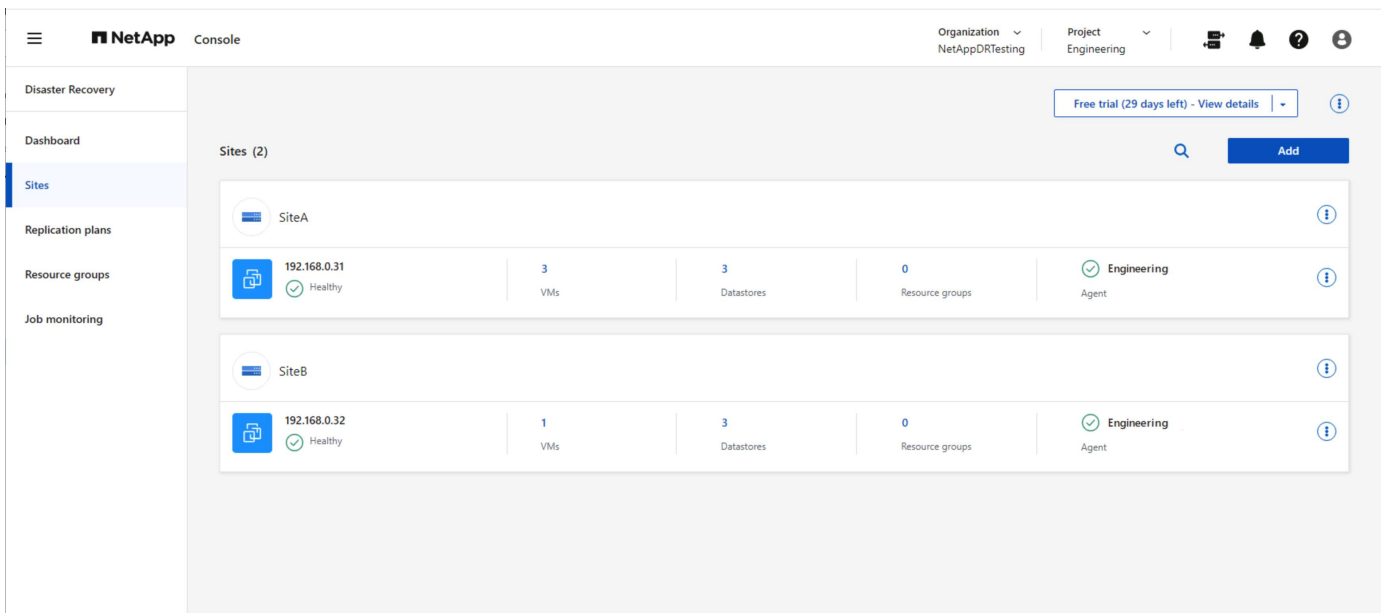
Der zugrunde liegende Prozess zur Erstellung der SnapMirror Replikation bleibt für jede Anwendung derselbe. Am einfachsten lässt sich dies durch die Nutzung von NetApp Disaster Recovery realisieren, das den Replikationsworkflow automatisiert, sofern die folgenden beiden Kriterien erfüllt sind: Der Prozess kann manuell oder automatisiert erfolgen. Am einfachsten ist es, NetApp Disaster Recovery zu nutzen, mit dem der Replizierungs-Workflow automatisiert wird, sofern die folgenden zwei Kriterien erfüllt sind:

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

Die NetApp Console bietet außerdem eine alternative Möglichkeit zur Konfiguration der SnapMirror Replikation, indem das Quell ONTAP -System in der Umgebung einfach per Drag & Drop auf das Zielsystem gezogen wird, um den Assistenten auszulösen, der durch den restlichen Prozess führt.

Was kann NetApp Disaster Recovery für Sie tun?

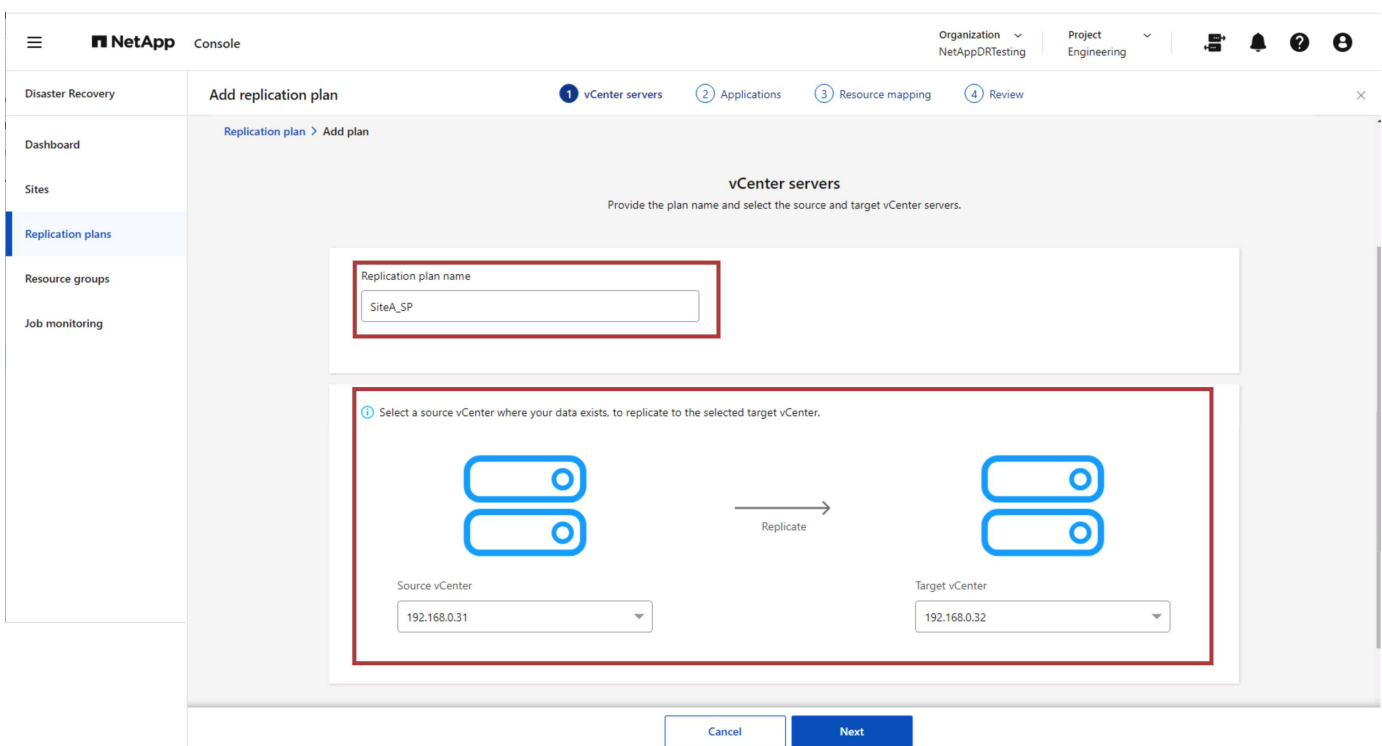
Nach dem Hinzufügen der Quell- und Zielstandorte führt NetApp Disaster Recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. NetApp Disaster Recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und trägt diese ein.



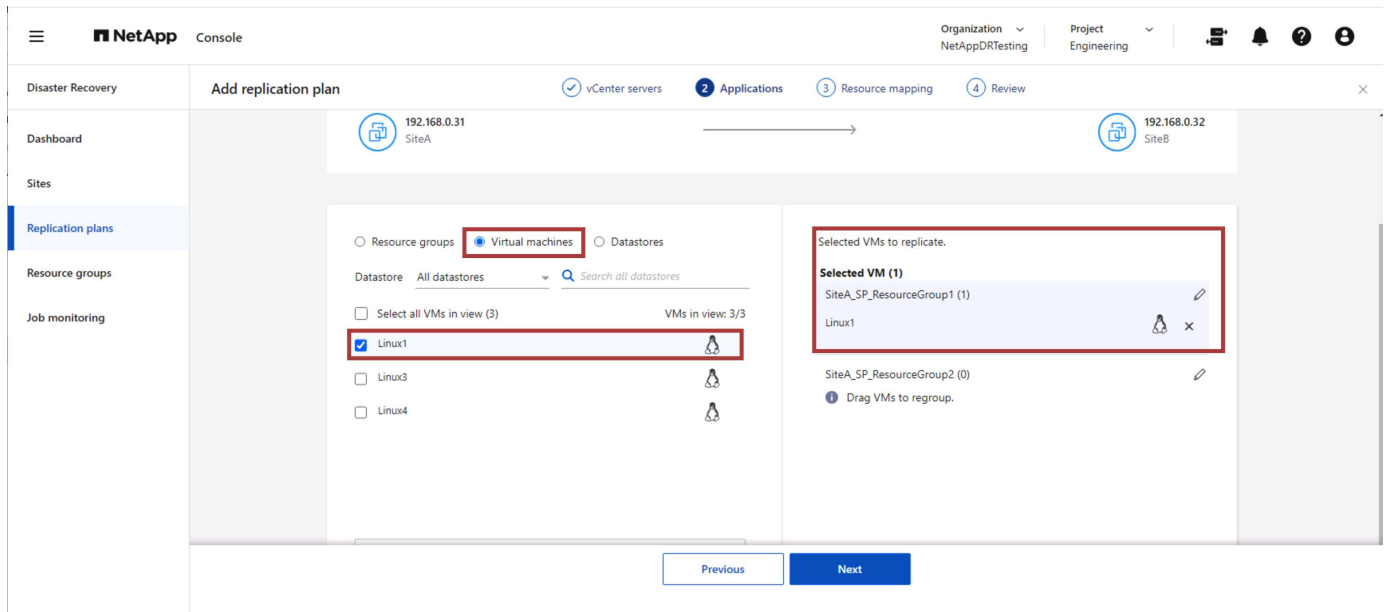
Nachdem die Standorte hinzugefügt wurden, konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen auswählen und die Ressourcengruppen festlegen, die in den Plan aufgenommen werden sollen, sowie die Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und die Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationspläne** und klicken Sie auf **Hinzufügen**.

In diesem Schritt können die VMs in Ressourcengruppen gruppiert werden. Mit NetApp Disaster Recovery -Ressourcengruppen können Sie eine Reihe abhängiger VMs in logische Gruppen zusammenfassen, die deren Startreihenfolge und Startverzögerungen enthalten, die bei der Wiederherstellung ausgeführt werden können. Ressourcengruppen können während der Erstellung des Replikationsplans oder über die Registerkarte „Ressourcengruppe“ in der linken Navigationsleiste erstellt werden.

Zuerst benennen Sie den Replikationsplan und wählen das Quell-vCenter und das Ziel-vCenter aus.



Im nächsten Schritt müssen Sie entscheiden, ob Sie einen Replikationsplan mit Ressourcengruppen, virtuellen Maschinen oder Datenspeichern erstellen möchten. Wählen Sie eine vorhandene Ressourcengruppe aus. Falls keine Ressourcengruppen erstellt wurden, hilft Ihnen der Assistent dabei, die benötigten virtuellen Maschinen anhand der Wiederherstellungsziele zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Reihenfolge der Wiederherstellung von virtuellen Anwendungsmaschinen festzulegen.



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 sind, besteht der nächste Schritt darin, die Zuordnung zu erstellen, um virtuelle Maschinen und Anwendungen im Katastrophenfall wiederherstellen zu können. In diesem Schritt legen Sie fest, wie die Ressourcen aus der Quellumgebung der Zielumgebung zugeordnet werden. Dazu gehören Rechenressourcen, virtuelle Netzwerke, IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Anwendungskonsistenz und so weiter. Für detaillierte Informationen siehe ["Erstellen eines Replikationsplans"](#). Wie bereits in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie anhand des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des Replikationsplans angegeben wurden.

Hinweis: Standardmäßig werden für Test- und Failover-Operationen die gleichen Mapping-Parameter 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. Sobald die Ressourcenzuordnung abgeschlossen ist, klicken Sie auf Weiter.

NetApp Console

Organization: NetAppDRTesting | Project: Engineering

Free trial (29 days left) - View details

Disaster Recovery

Dashboard

Sites

Replication plans

Resource groups

Job monitoring

Replication plans (1)

Create report Add

Name	Compliance status	Plan status	Protected site	Resource groups	Fallover site	
SiteA_SP	Healthy	Ready	SiteA	SiteA_SP_ResourceGroup1	SiteB	...

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

NetApp Console

Organization: NetAppDRTesting | Project: Engineering

Last updated: November 4, 2025, 6:45 PM

Disaster Recovery

Dashboard

Sites

Replication plans

Resource groups

Job monitoring

Last 12 hours

9 Jobs

9 Success View jobs

0 In progress View jobs

0 Queued View jobs

0 Canceled View jobs

0 Warning View jobs

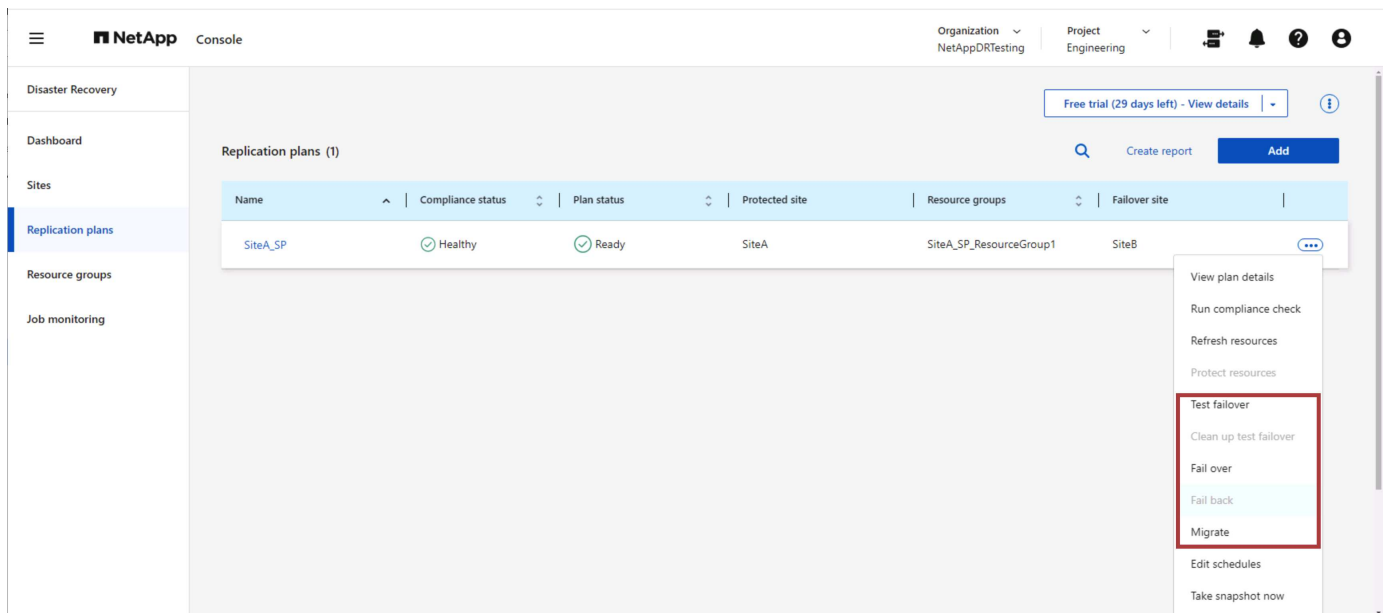
0 Failed View jobs

Jobs (9)

ID	Status	Workload	Name	Start time	End time	Action
018d8b44-c951-4113-a91c-	Success	Compliance	Compliance check for replication plan 'SiteA_SP'	11/04/2025, 06:44:33 PM	11/04/2025, 06:44:36 PM	
d79b74c1-c4ea-4473-bf22-	Success	Compliance	Initialize Compliance of SiteA_SP for every 180 mi...	11/04/2025, 06:44:32 PM	11/04/2025, 06:44:33 PM	
bfc453ac-83f7-4669-a821-9	Success	DRCleanupSecond:	Initialize DRCleanupSecondaryBackups of Cleanu...	11/04/2025, 06:44:30 PM	11/04/2025, 06:44:31 PM	
b654a09f-6b1a-41d0-9885-	Success	DRReplicationPlan	Replication plan modification for 'SiteA_SP'	11/04/2025, 06:44:28 PM	11/04/2025, 06:44:31 PM	
85e9e7d7-67eb-4e48-88ca-	Success	Discovery	Discovery of resources in host 192.168.0.32	11/04/2025, 06:34:37 PM	11/04/2025, 06:34:44 PM	

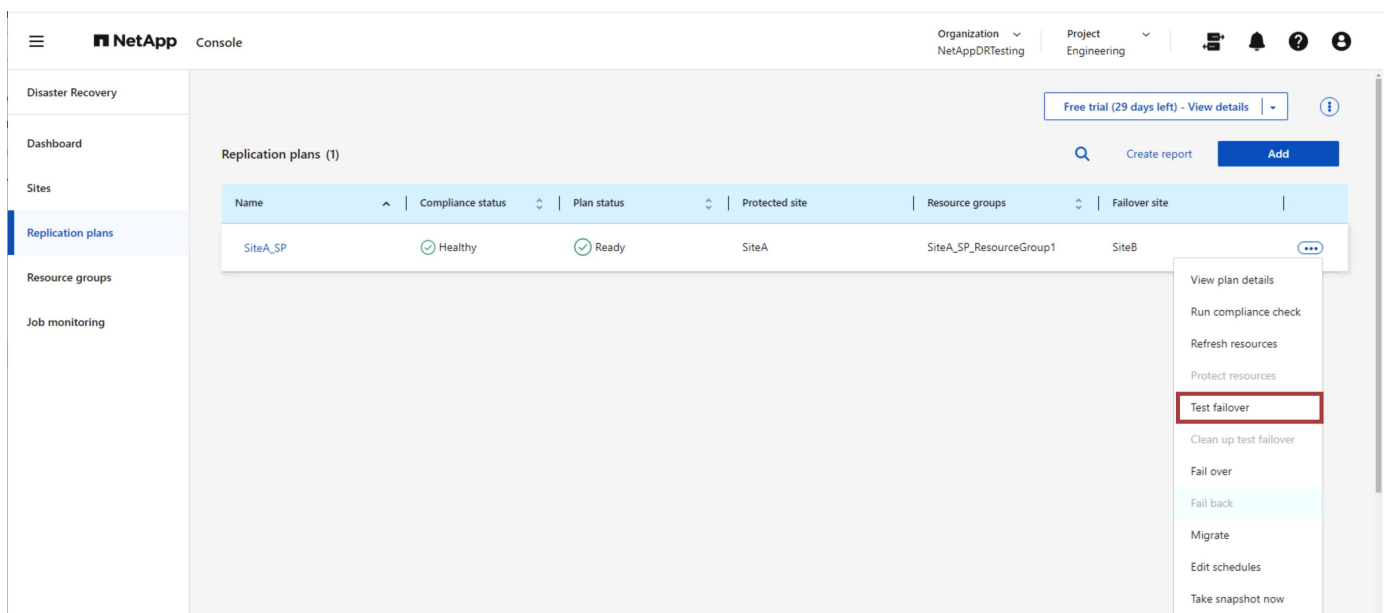
NetApp Disaster Recovery umfasst die folgenden Arbeitsabläufe:

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

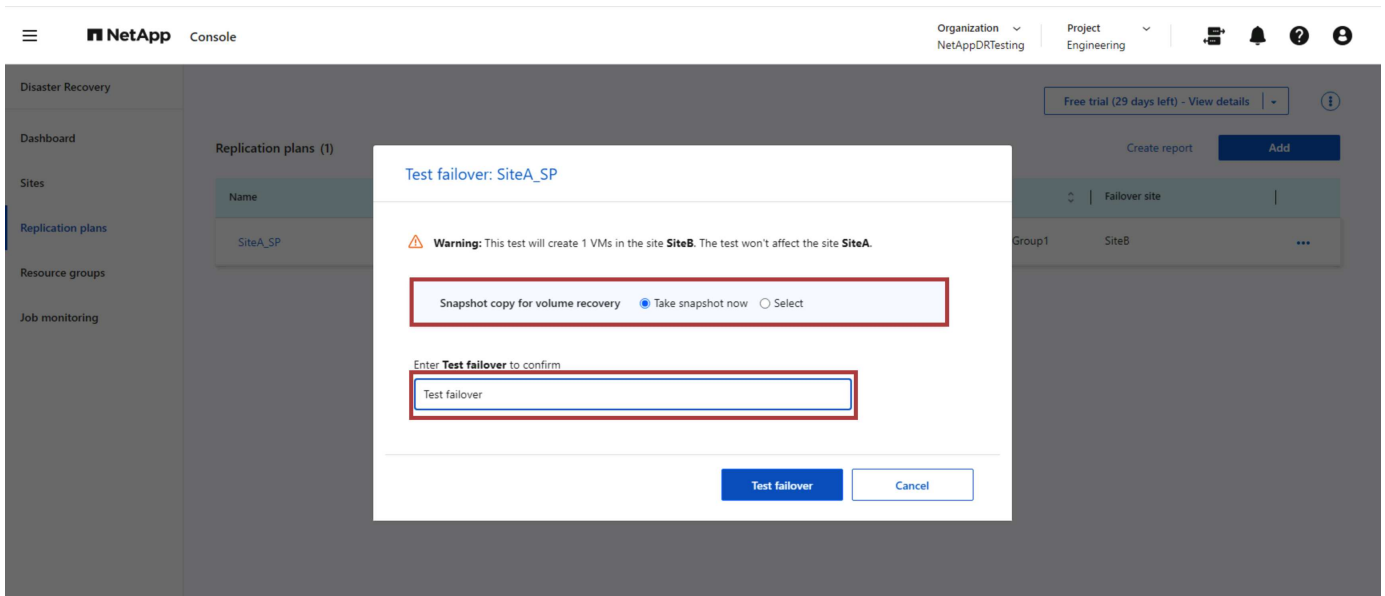


Testen des Failovers

Das Test-Failover in NetApp Disaster Recovery ist ein Betriebsverfahren, das es VMware-Administratoren ermöglicht, ihre Wiederherstellungspläne vollständig zu validieren, ohne ihre Produktionsumgebungen zu unterbrechen.

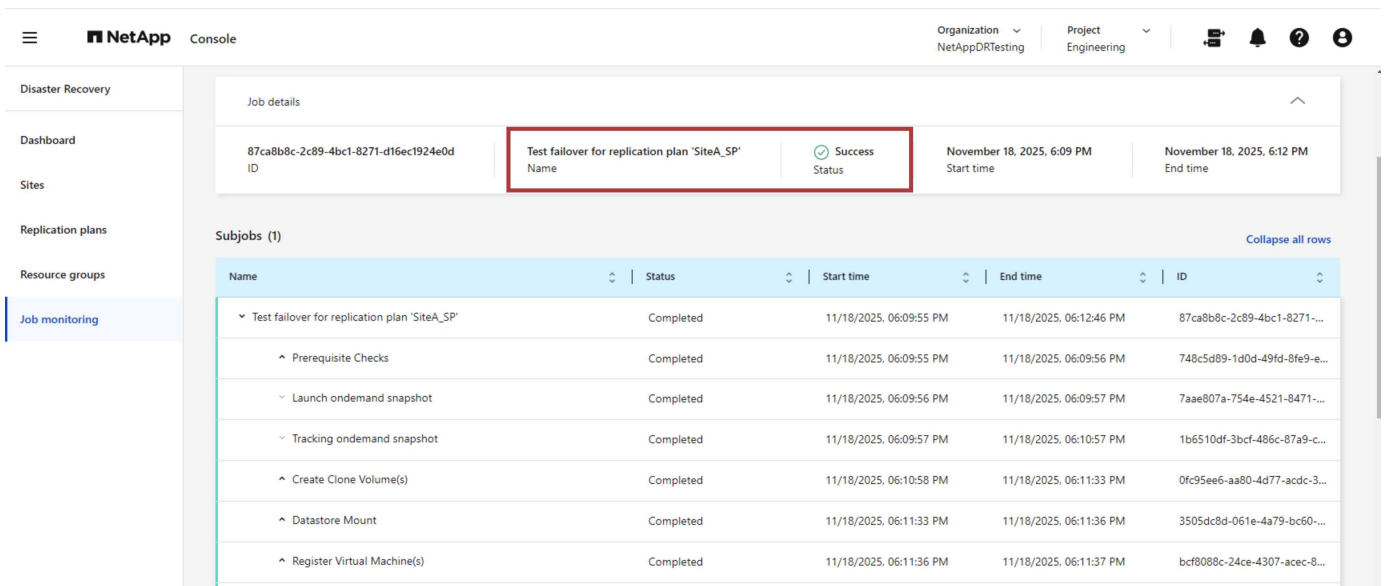


NetApp Disaster Recovery bietet die Möglichkeit, den Snapshot als optionale Funktion im Test-Failover-Vorgang auszuwählen. Diese Funktion ermöglicht es dem VMware-Administrator zu überprüfen, ob alle kürzlich in der Umgebung vorgenommenen Änderungen auf den Zielstandort repliziert wurden und somit während des Tests vorhanden sind. Zu diesen Änderungen gehören Patches für das VM-Gastbetriebssystem.



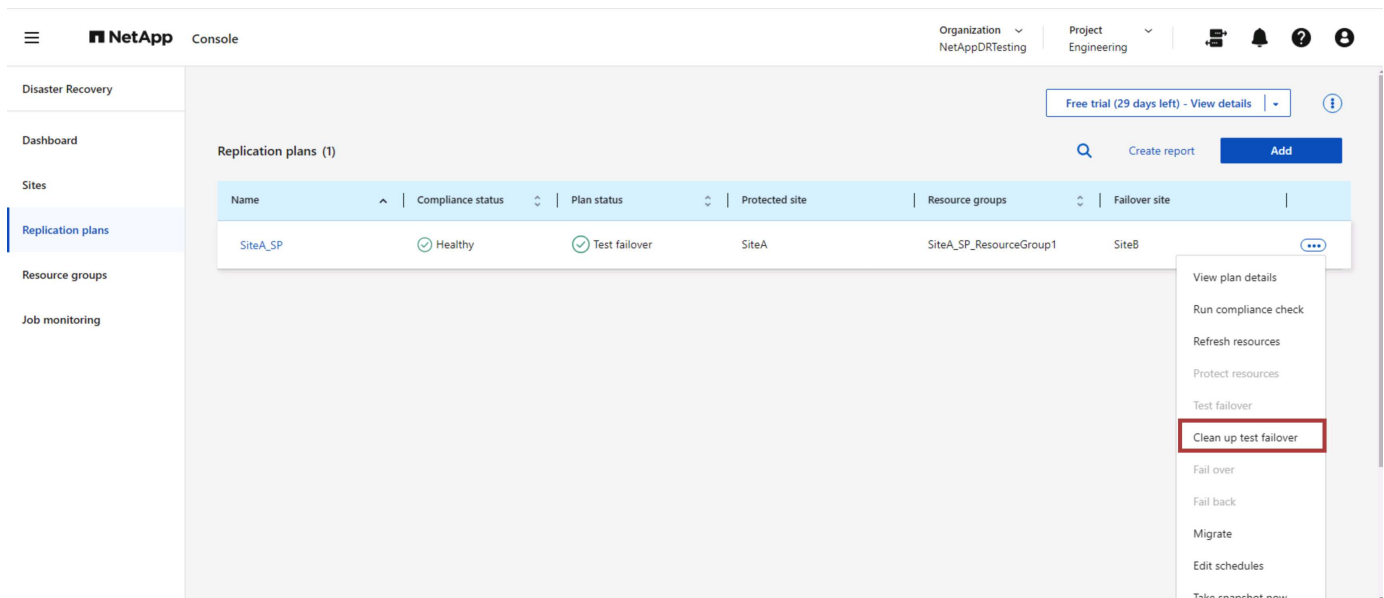
Wenn der VMware-Administrator einen Test-Failover durchführt, automatisiert NetApp Disaster Recovery die folgenden Aufgaben:

- 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.

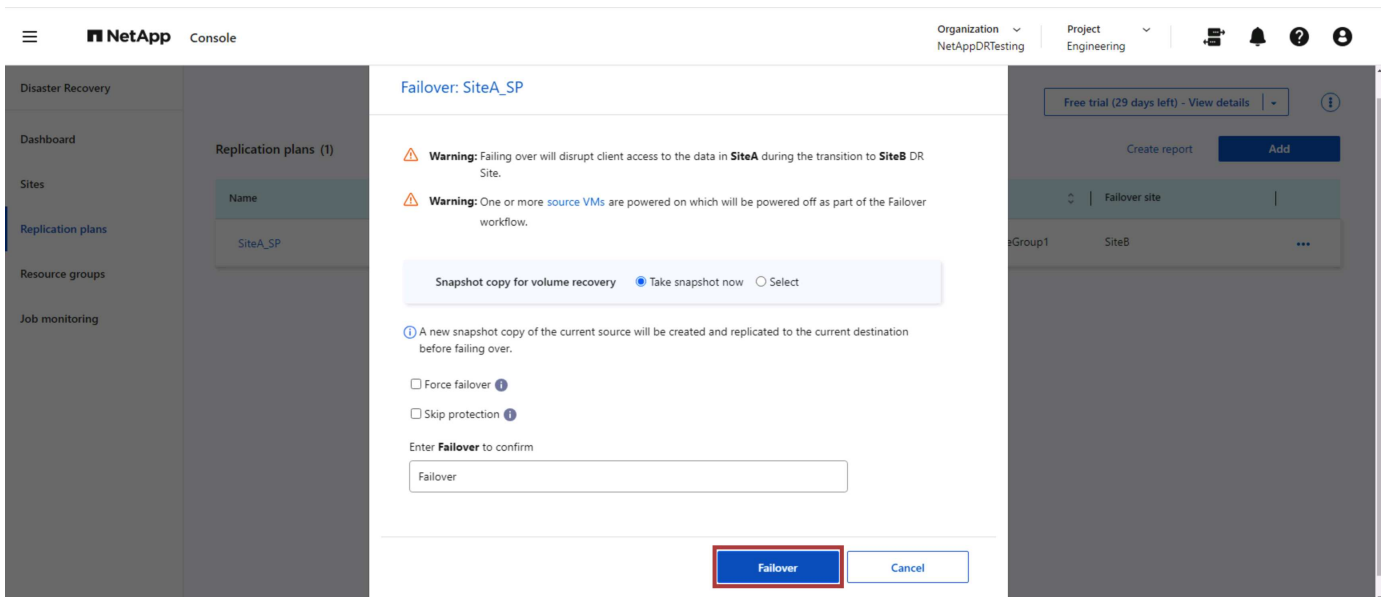
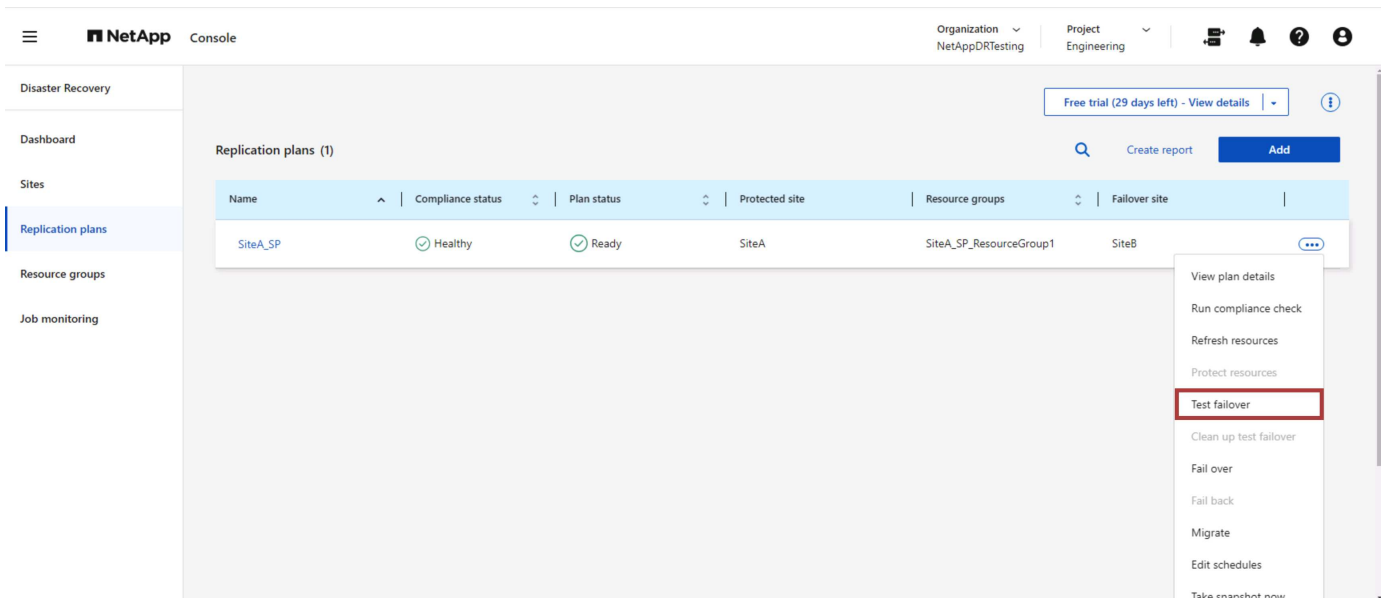


Diese Aktion setzt die virtuellen Maschinen (VMs) und den Status des Replikationsplans auf den Status „Bereit“ zurück. Wenn der VMware-Administrator eine Wiederherstellungsoperation durchführt, schließt NetApp Disaster Recovery den folgenden Prozess ab:

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

NetApp Disaster Recovery bietet zwei Methoden zur Durchführung eines echten Failovers: geplante Migration und Failover. Die erste Methode, die geplante Migration, beinhaltet das Herunterfahren der VMs und die Synchronisierung der Speicherreplikation in den Prozess, um die VMs wiederherzustellen oder effektiv an den Zielstandort zu verschieben. Für die geplante Migration ist der Zugriff auf den Quellstandort 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. Je nach dem in der Lösung festgelegten RPO (Recovery Point Objective) ist im DR-Szenario mit einem gewissen Datenverlust zu rechnen.



Wenn der VMware-Administrator einen Failover durchführt, automatisiert NetApp Disaster Recovery 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.

Recent Tasks

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time	Server
Power On virtual machine	Linux1	Completed	Powering on the new Virtual Machine	DEMO.LOCAL\Administrator	6 ms	11/18/2025, 7:32:46 P M	11/18/2025, 7:32:51 P M	vc2.demo.netapp.com

Failback

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

Replication plans (1)

Name	Compliance status	Plan status	Protected site	Resource groups	Failover site
SiteA_SP	Healthy	Failed over	SiteA	SiteA_SP_ResourceGroup1	SiteB

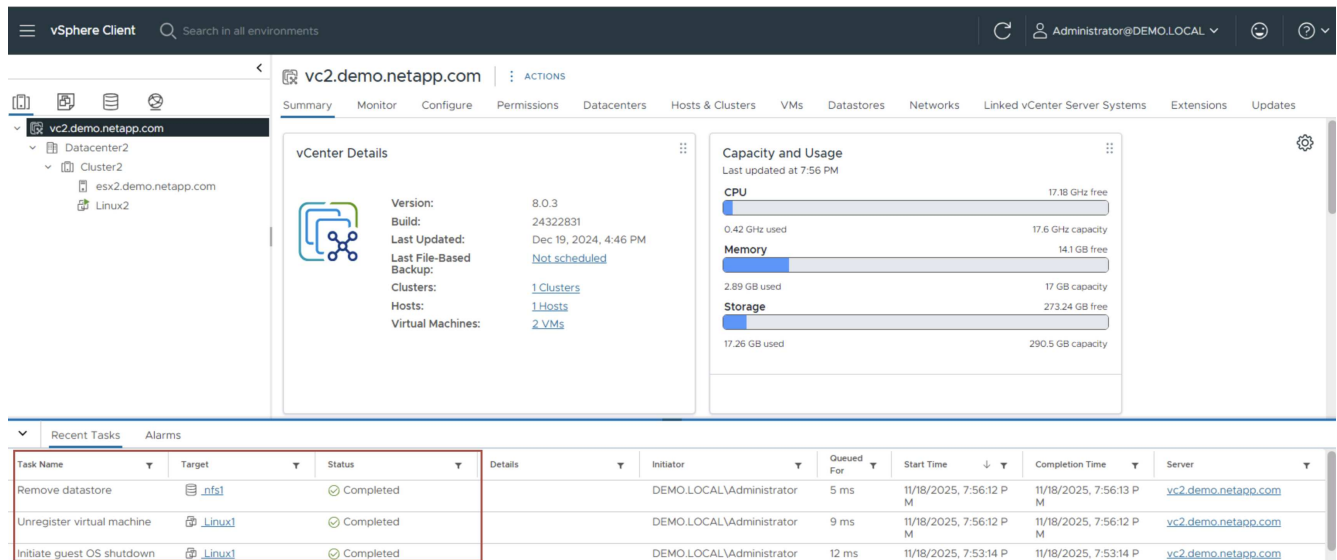
VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie bereit sind, die Dienste auf der ursprünglichen Quellsite wiederherzustellen.



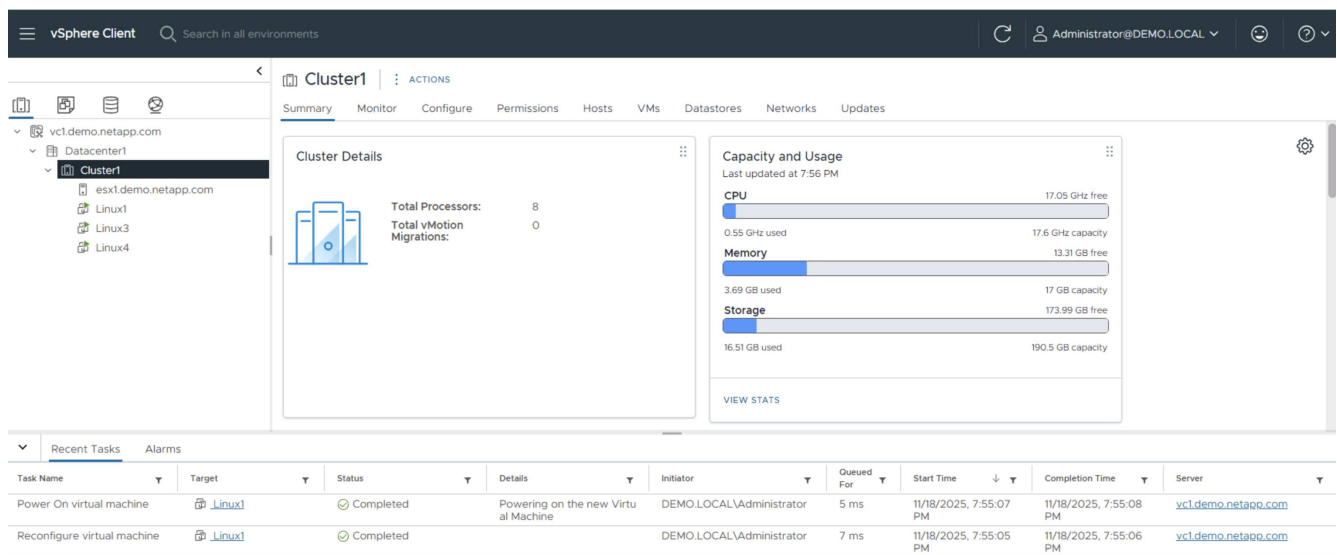
NetApp Disaster Recovery repliziert (resynchronisiert) alle Änderungen zurück auf die ursprüngliche virtuelle Quellmaschine, bevor die Replikationsrichtung umgekehrt wird.

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.



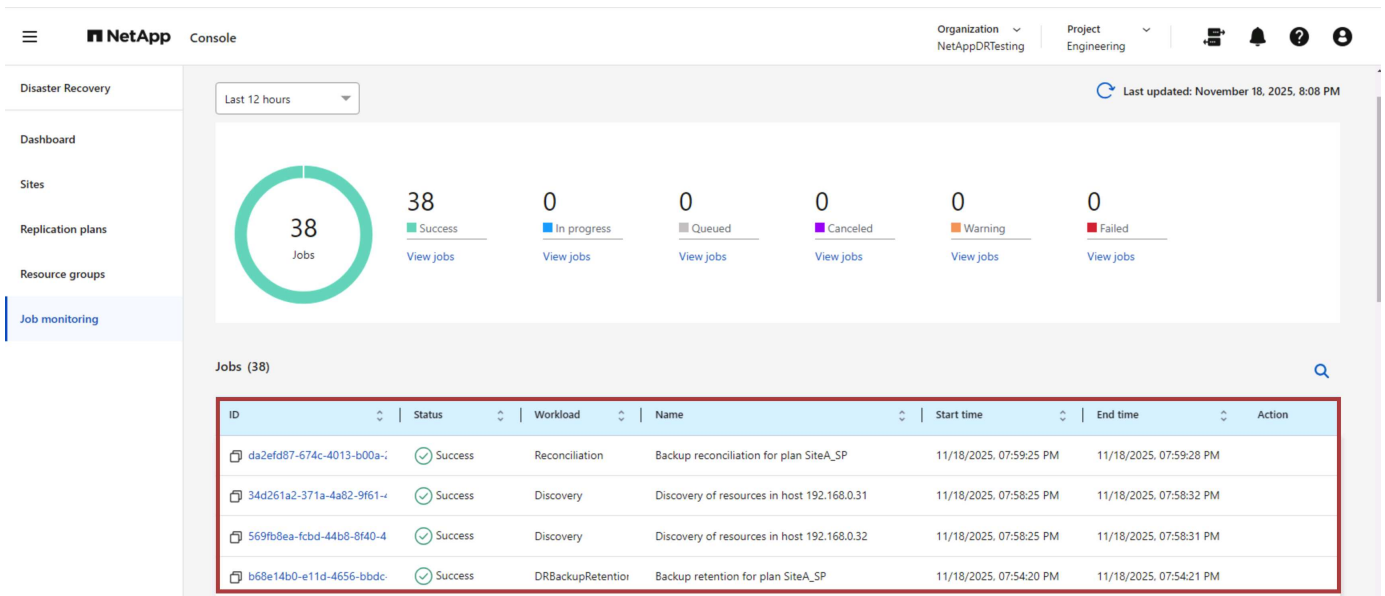
- Unterbrechen Sie die SnapMirror -Beziehung zur Originalquelle, um Lese-/Schreibzugriff zu ermöglichen.
- Synchronisieren Sie die SnapMirror -Beziehung erneut, um die Replikation umzukehren.
- Mounten Sie das Volume auf der Quelle, schalten Sie die virtuellen Quellmaschinen ein und registrieren Sie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



Weitere Informationen zum Zugriff auf und zur Konfiguration von NetApp Disaster Recovery finden Sie unter ["Erfahren Sie mehr über NetApp Disaster Recovery für VMware"](#) Die

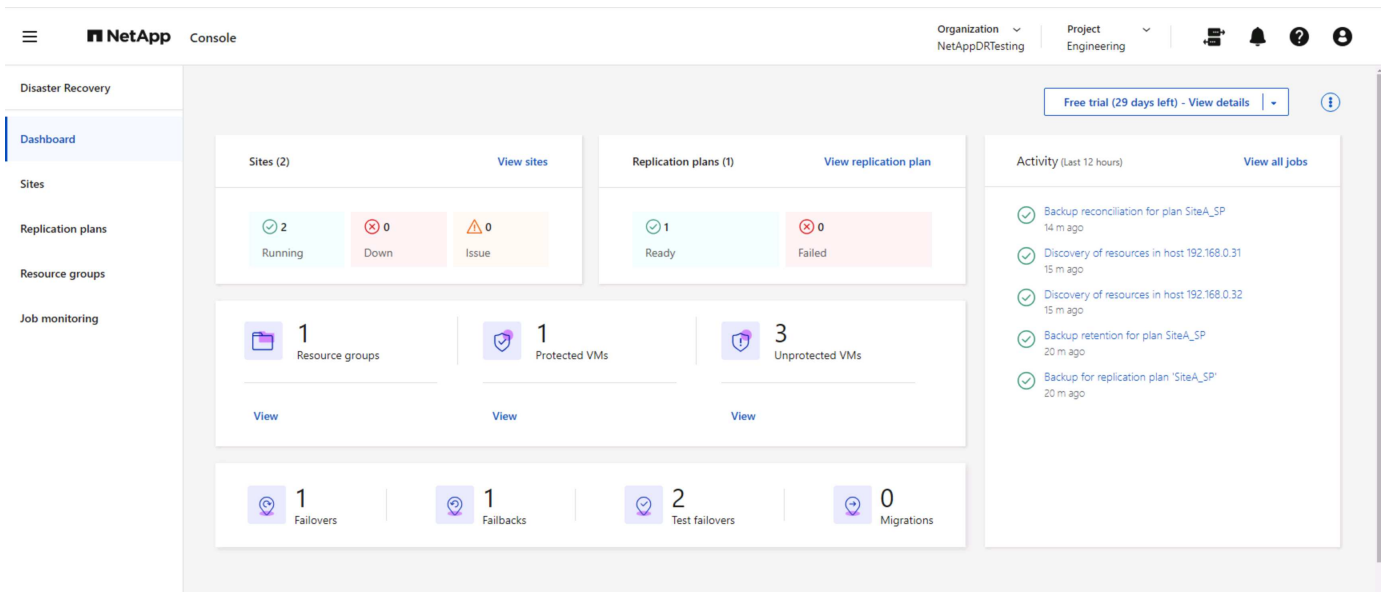
Überwachung und Dashboard

Über NetApp Disaster Recovery oder die ONTAP CLI können Sie den Replikationsstatus der entsprechenden Datenspeichervolumes überwachen, und der Status eines Failovers oder Test-Failovers kann über die Jobüberwachung verfolgt werden.



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 NetApp Disaster Recovery Dashboard können Sie den Status von Disaster-Recovery-Standorten und Replikationsplänen zuverlässig beurteilen. Dies ermöglicht es Administratoren, intakte, nicht verbundene oder beeinträchtigte Standorte und Pläne schnell zu 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 eine VCF-Verwaltungsdomäne

Die Konvertierung einer vSphere-Umgebung mit vorhandenen Fibre Channel- oder NFS-Datenspeichern auf ONTAP beinhaltet die Integration der aktuellen Infrastruktur in eine moderne Private Cloud-Architektur.

Lösungsübersicht

Diese Lösung zeigt, wie vorhandene FC- oder NFS-Datenspeicher in vSphere zum Hauptspeicher werden, wenn der Cluster in eine VCF-Verwaltungsdomäne konvertiert wird.

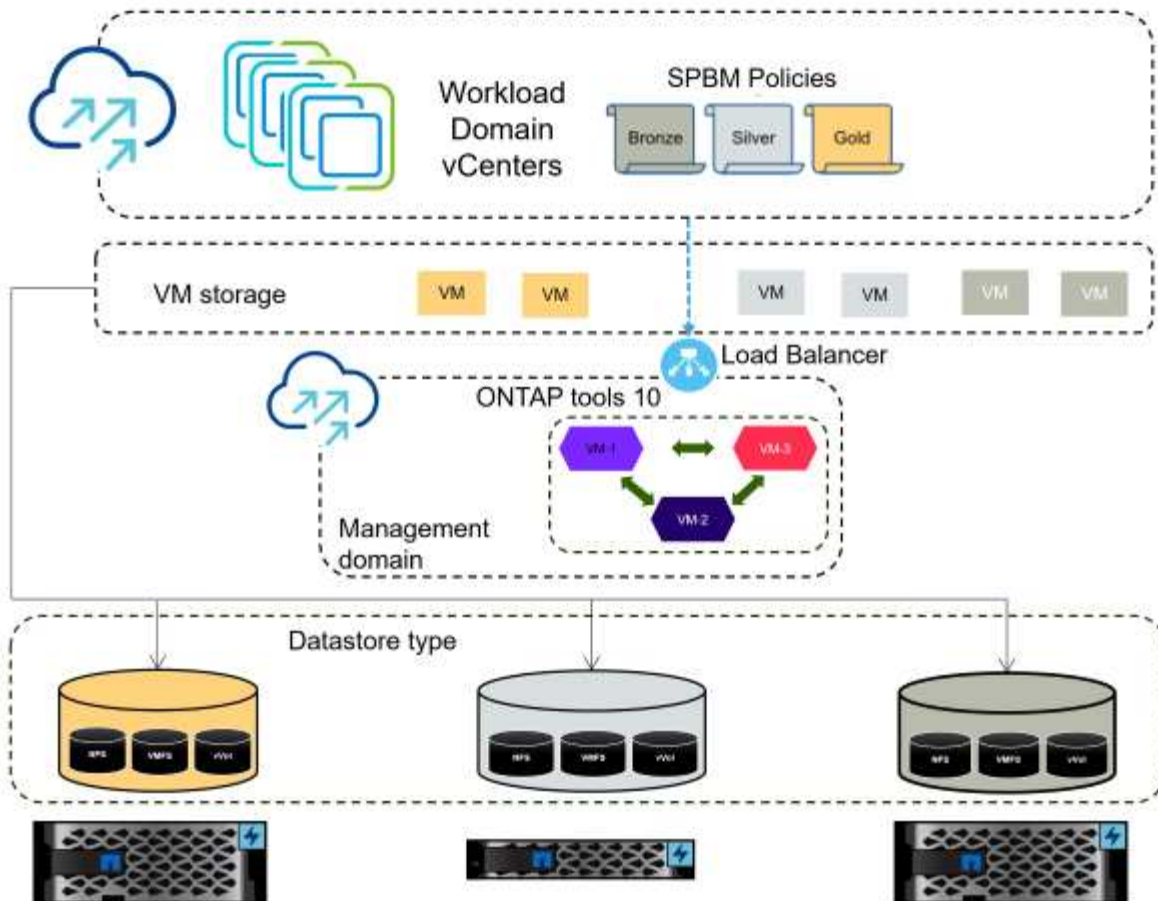
Dieser Prozess profitiert von der Robustheit und Flexibilität des ONTAP Speichers, um einen nahtlosen Datenzugriff und eine nahtlose Datenverwaltung zu gewährleisten. Nachdem durch den Konvertierungsprozess eine VCF-Verwaltungsdomäne eingerichtet wurde, können Administratoren zusätzliche vSphere-Umgebungen, einschließlich solcher, die sowohl FC- als auch 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.

Architekturübersicht

Die Architektur der ONTAP -Tools lässt sich nahtlos in VMware-Umgebungen integrieren und nutzt ein modulares und skalierbares Framework, das die ONTAP -Tool-Dienste, das vSphere-Plug-in und REST-APIs umfasst, um eine effiziente Speicherverwaltung, Automatisierung und Datensicherung zu ermöglichen.

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



Unterstützte Lösungen zum Konvertieren einer vSphere-Umgebung

Die technischen Details zum Konvertieren einer vCenter-Instanz finden Sie in den folgenden Lösungen.

- ["Konvertieren einer vCenter-Instanz in die VCF-Verwaltungsdomäne \(NFS-Datenspeicher\)"](#)
- ["Konvertieren Sie die vCenter-Instanz in die VCF-Verwaltungsdomäne \(FC-Datenspeicher\)."](#)

Weitere Informationen

- Videodemos dieser Lösungen finden Sie unter ["Bereitstellung von VMware-Datenspeichern mit ONTAP"](#) .
- Eine Übersicht über den Konvertierungsprozess finden Sie im ["Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workloaddomäne in VMware Cloud Foundation"](#) .
- Informationen zur Konfiguration von ONTAP -Speichersystemen finden Sie unter ["ONTAP 9 Dokumentation"](#) .
- Informationen zur Konfiguration von VCF finden Sie unter ["VMware Cloud Foundation-Dokumentation"](#) .
- 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"](#) .

Bereitstellungsworkflow zum Konvertieren von vCenter-Serverinstanzen in VCF-Verwaltungsdomänen mit NFS-Datenspeichern

Konvertieren Sie einen vorhandenen vSphere 8-Cluster mit NetApp ONTAP NFS-Datenspeichern in eine VMware Cloud Foundation-Verwaltungsdomäne. Sie überprüfen die Konfigurationsanforderungen, stellen ONTAP Tools bereit, stellen NFS-Datenspeicher bereit und verwenden das VCF-Importtool zum Validieren und Konvertieren des Clusters.

Eine Übersicht über den Konvertierungsprozess finden Sie in der VMware-Dokumentation: ["Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workloadomäne in VMware Cloud Foundation"](#) .

1

"Überprüfen der Konfigurationsanforderungen"

Überprüfen Sie die wichtigsten Anforderungen für die Konvertierung von vCenter-Serverinstanzen in VCF-Verwaltungsdomänen mithilfe von NFS-Datenspeichern.

2

"Bereitstellen von ONTAP -Tools und Bereitstellen eines NFS-Datenspeichers"

Stellen Sie ONTAP tools for VMware vSphere bereit und stellen Sie einen NFS-Datenspeicher bereit.

3

"Konvertieren Sie den vSphere-Cluster in eine VCF-Verwaltungsdomäne"

Verwenden Sie das VCF-Importtool, um vSphere 8 zu validieren und in die VCF-Verwaltungsdomäne zu konvertieren.

Bereitstellungsworkflow zum Konvertieren von vCenter-Serverinstanzen in VCF-Verwaltungsdomänen mit Fibre Channel-Datenspeichern

Konvertieren Sie einen vorhandenen vSphere 8-Cluster mit NetApp ONTAP Fibre Channel (FC)-Datenspeichern in eine VMware Cloud Foundation-Verwaltungsdomäne. Sie überprüfen die Konfigurationsanforderungen, stellen ONTAP Tools und FC-Datenspeicher bereit und verwenden das VCF-Importtool zum Validieren und Konvertieren des Clusters.

Eine Übersicht über den Konvertierungsprozess finden Sie in der VMware-Dokumentation: ["Konvertieren Sie eine vSphere-Umgebung in eine Verwaltungsdomäne oder importieren Sie eine vSphere-Umgebung als VI-Workloadomäne in VMware Cloud Foundation"](#) .

1

"Überprüfen der Konfigurationsanforderungen"

Überprüfen Sie die wichtigsten Anforderungen für die Konvertierung von vCenter-Serverinstanzen in VCF-Verwaltungsdomänen mithilfe von FC-Datenspeichern.

2

"Bereitstellen von ONTAP -Tools und Bereitstellen eines FC-Datenspeichers"

Stellen Sie ONTAP tools for VMware vSphere bereit und stellen Sie einen FC-Datenspeicher bereit.

"Konvertieren Sie den vSphere-Cluster in eine VCF-Verwaltungsdomäne"

Verwenden Sie das VCF-Importtool, um den vSphere 8-Cluster zu validieren und in die VCF-Verwaltungsdomäne zu konvertieren.

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-Workloadaddomänen 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-lokaliserten 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)-Workload-Domäne. 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-Traffic
- 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-Volumen zu gewähren.
- Erstellen Sie ein NFS-Volumen 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.

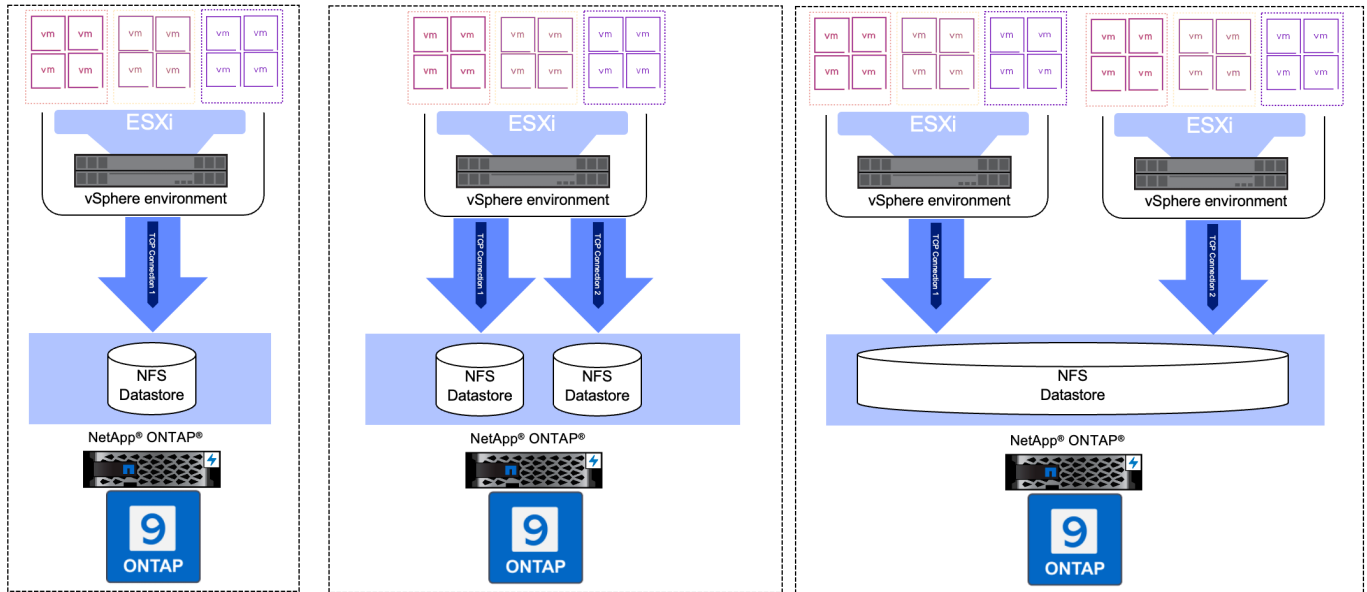


Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass entweder 1) das Verwaltungsnetzwerk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



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.

The screenshot shows the ONTAP System Manager interface. The left sidebar has a menu with 'STORAGE' expanded, showing 'Storage VMs' selected. The main area shows a list of Storage VMs with 'EHC_NFS' selected. On the right, the 'Overview' tab is active, showing 'NETWORK IP INTERFACES' for 'NFS' with a count of 7. A dropdown menu is open, showing a list of IP addresses, with '172.21.118.163' and '172.21.118.164' highlighted.

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>
```

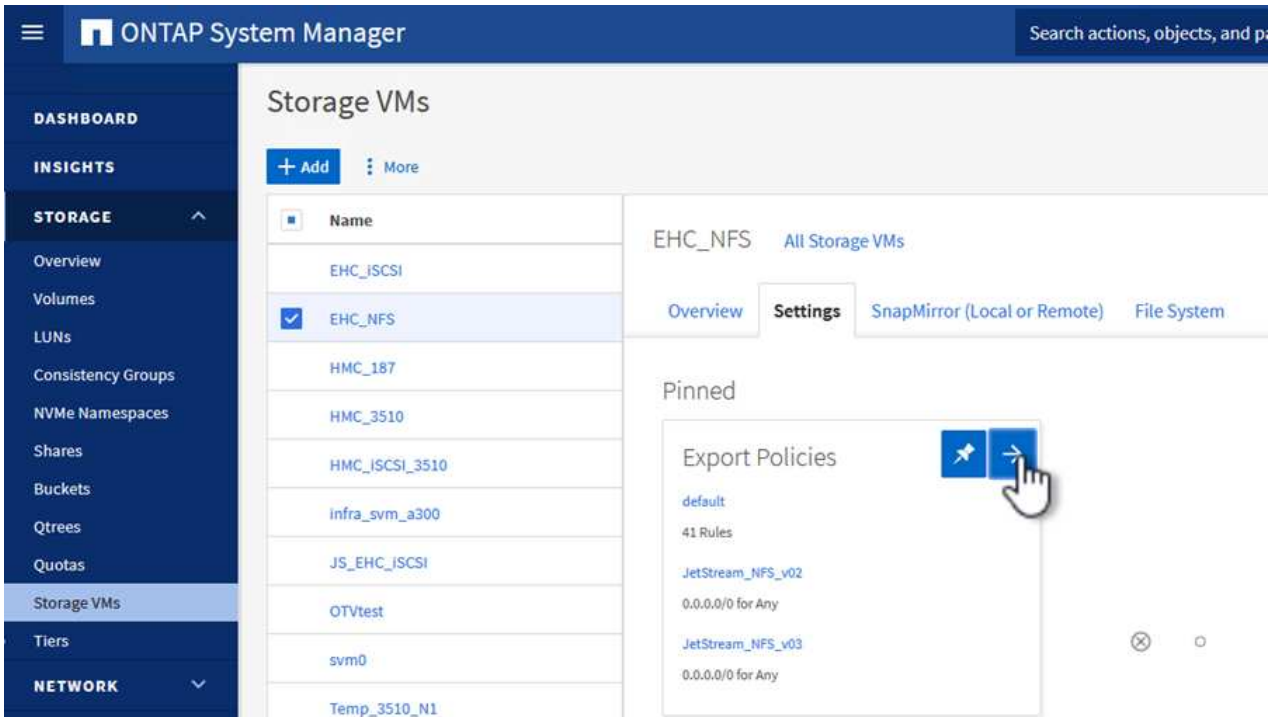



Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass entweder 1) das Verwaltungsnetzwerk 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.

New export policy

NAME

WKLD_DM01

☒ Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. Geben Sie die IP-Adressen, den IP-Adressbereich oder das Netzwerk ein, 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.

New Rule



CLIENT SPECIFICATION

172.21.166.0/24


ACCESS PROTOCOLS

☐ SMB/CIFS

☐ FlexCache

☒ NFS ☒ NFSv3 ☒ NFSv4

ACCESS DETAILS

Type	Read-only Access	Read/Write Access	Superuser Access
All	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
All (As anonymous user) 	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
UNIX	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Kerberos 5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5i	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Kerberos 5p	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
NTLM	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Cancel

Save



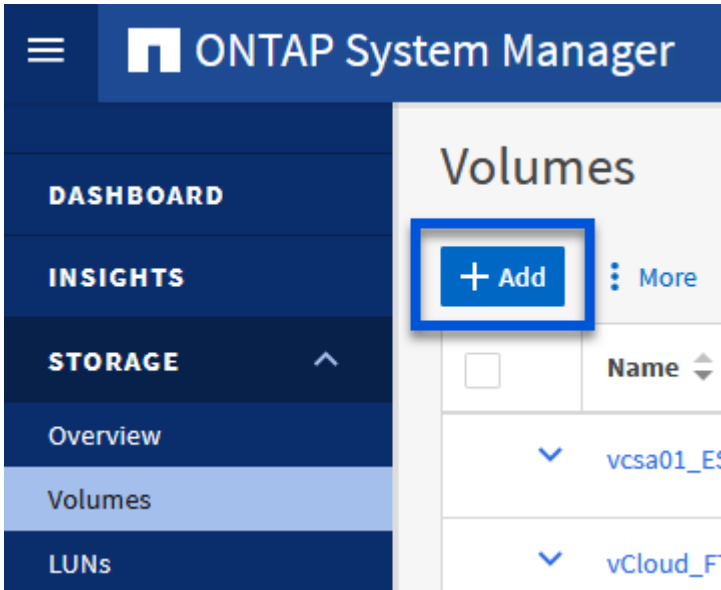
Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass die Exportrichtlinie das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

- Nachdem alle Regeln eingegeben wurden, klicken Sie auf die Schaltfläche **Speichern**, um die neue Exportrichtlinie zu speichern.
- 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.

Add Volume



NAME

VCF_WKLD_01

CAPACITY

5



TiB



STORAGE VM

EHC_NFS



Export via NFS

More Options

Cancel

Save

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

Access Permissions

☒ Export via NFS

GRANT ACCESS TO HOST

default

JetStream_NFS_v04

Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01

3 rules

NFSmountTestReno01

Clients : 0.0.0.0/0 | Access protocols : Any

PerfTestVols

Clients : 172.21.253.0/24 | Access protocols : NFSv3, NFSv4, NFS

TestEnv_VPN

Clients : 172.21.254.0/24 | Access protocols : Any

VCF_WKLD

2 rules

WKLD_DM01

2 rules

Wkld01_NFS

Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.252.208

+



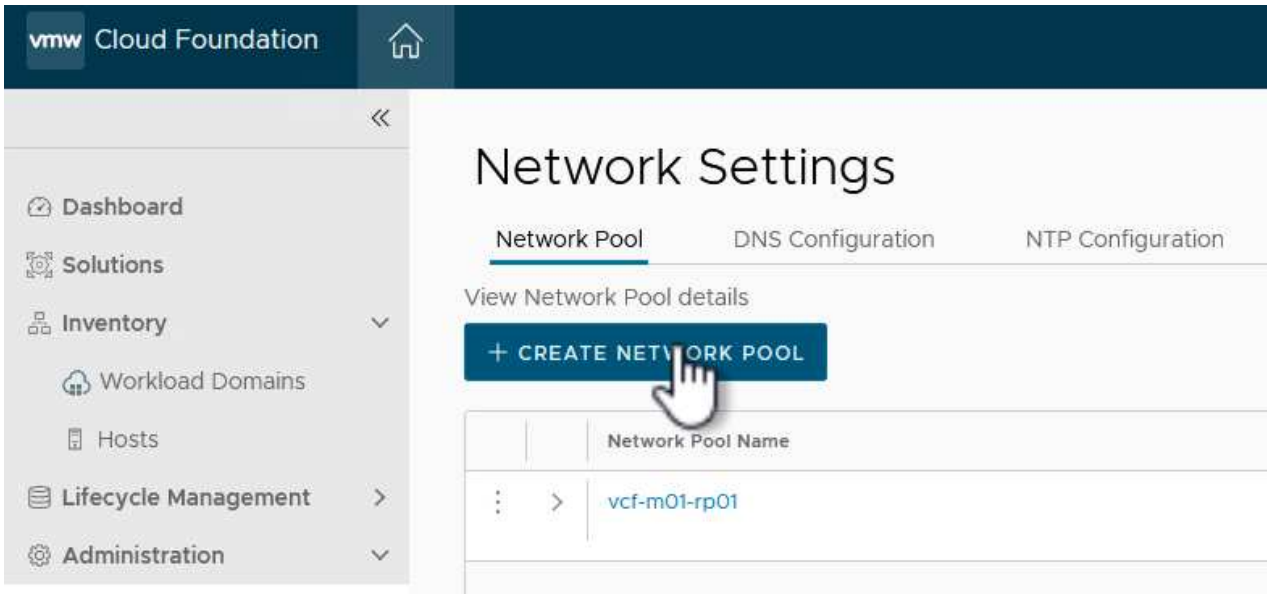
Beim Bereitstellen einer VI-Workload-Domäne validiert VCF die Konnektivität zum NFS-Server. Dies erfolgt mithilfe des Verwaltungsadapters auf den ESXi-Hosts, bevor ein zusätzlicher VMkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass entweder 1) das Verwaltungsnetzwerk 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.

vmw Cloud Foundation

Dashboard

Solutions

Inventory

Workload Domains

Hosts

Lifecycle Management

Administration

Network Settings

Storage Settings

Licensing

Single Sign On

Proxy Settings

Online Depot

Composable Infrastructure

VMware Aria Suite

Backup

VMware CEP

Security

Password Management

Certificate Authority

Developer Center

Network Settings

Network Pool

DNS Configuration

NTP Configuration

Create Network Pool

Ensure that all required networks are selected based on their usage for workload domains.

Network Pool Name

NFS_NP01

Network Type

☐ vSAN

☒ NFS

☐ iSCSI

☒ vMotion

NFS Network Information

VLAN ID

3374

MTU

9000

Network

172.21.118.0

Subnet Mask

255.255.255.0

Default Gateway

172.21.118.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.118.145

To

172.21.118.148

REMOVE

xxx.xxx.xxx.xxx

To

xxx.xxx.xxx.xxx

ADD

vMotion Network Information

VLAN ID

3423

MTU

9000

Network

172.21.167.0

Subnet Mask

255.255.255.0

Default Gateway

172.21.167.1

Included IP Address Ranges

Once a network pool has been created, you are not able to edit or remove IP ranges from that pool.

172.21.167.121

To

172.21.167.124

REMOVE

xxx.xxx.xxx.xxx

To

xxx.xxx.xxx.xxx

ADD

CANCEL

SAVE

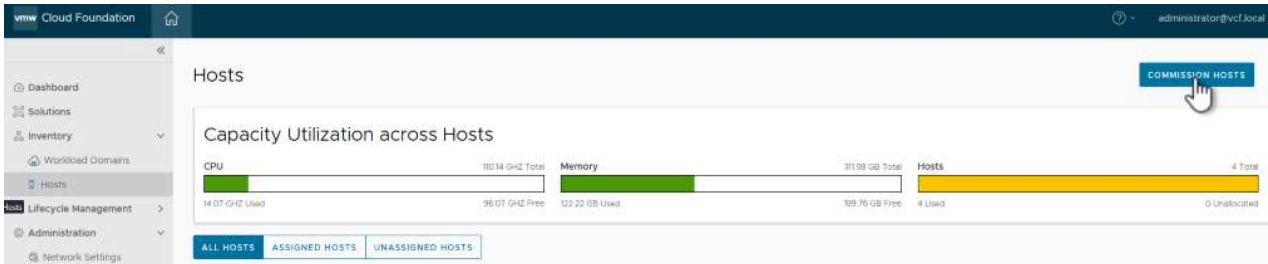
3. Klicken Sie auf die Schaltfläche **Speichern**, um die Erstellung des Netzwerkpools abzuschließen.

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.

Checklist

Commissioning a host adds it to the VMware Cloud Foundation inventory. The host you want to commission must meet the checklist criterion below.

- ☒ **Select All**
- ☒ Host for vSAN/vSAN ESA workload domain should be vSAN/vSAN ESA compliant and certified per the VMware Hardware Compatibility Guide. BIOS, HBA, SSD, HDD, etc. must match the VMware Hardware Compatibility Guide.
- ☒ Host has a standard switch with two NIC ports with a minimum 10 Gbps speed.
- ☒ Host has the drivers and firmware versions specified in the VMware Compatibility Guide.
- ☒ Host has ESXi installed on it. The host must be preinstalled with supported versions (8.0.2-22380479)
- ☒ Host is configured with DNS server for forward and reverse lookup and FQDN.
- ☒ Hostname should be same as the FQDN.
- ☒ Management IP is configured to first NIC port.
- ☒ Ensure that the host has a standard switch and the default uplinks with 10Gb speed are configured starting with traditional numbering (e.g., vmnic0) and increasing sequentially.
- ☒ Host hardware health status is healthy without any errors.
- ☒ All disk partitions on HDD / SSD are deleted.
- ☒ Ensure required network pool is created and available before host commissioning.
- ☒ Ensure hosts to be used for VSAN workload domain are associated with VSAN enabled network pool.
- ☒ Ensure hosts to be used for NFS workload domain are associated with NFS enabled network pool.
- ☒ Ensure hosts to be used for VMFS on FC workload domain are associated with NFS or VMOTION only enabled network pool.
- ☒ Ensure hosts to be used for vVol FC workload domain are associated with NFS or VMOTION only enabled network pool.
- ☒ Ensure hosts to be used for vVol NFS workload domain are associated with NFS and VMOTION only enabled network pool.
- ☒ Ensure hosts to be used for vVol iSCSI workload domain are associated with iSCSI and VMOTION only enabled network pool.
- ☒ For hosts with a DPU device, enable SR-IOV in the BIOS and in the vSphere Client (if required by your DPU vendor).

CANCEL

PROCEED

3. 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.

Commission Hosts

1 Host Addition and Validation

2 Review

Host Addition and Validation

✓ Add Hosts

You can either choose to add host one at a time or download [JSON](#) template and perform bulk commission.

☒ Add new ☐ Import

Host FQDN

Storage Type ☐ vSAN ☒ NFS ☐ VMFS on FC ☐ vVol

Network Pool Name ⓘ

User Name

Password ⓘ

ADD

Hosts Added

✓ Hosts added successfully. Add more or confirm fingerprint and validate host

REMOVE

☐ Confirm all Finger Prints ⓘ

VALIDATE ALL

<input checked="" type="checkbox"/>	FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status ⓘ
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.135	<input checked="" type="checkbox"/> SHA256:CKbsinf EOG+Hz/ lpFUoFDI2tLuY FZ47WicVdp6v EQM	⊖ Not Validated

1 hosts

CANCEL

NEXT

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

Hosts Added

✓ Host Validated Successfully.

REMOVE



Confirm all Finger Prints ⓘ

VALIDATE ALL

✓		FQDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
✓	⋮	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.138	✓ SHA256:9Kg+9 nQaE4SQkOMs QPON/ k5gZB9zyKN+6 CBPmXsvLBc	✓ Valid
✓	⋮	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.137	✓ SHA256:nPX4/ mei/ 2zmLJHfmPwbk 6zhapoUxV2IO wZDPFH+zo	✓ Valid
✓	⋮	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.136	✓ SHA256:AMhyR 60OpTQ1YYq0 DJhqVbj/M/ GvrQaqUy7Ce+ M4IWY	✓ Valid
✓	⋮	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 ⓘ	172.21.166.135	✓ SHA256:CKbsinf EOG+!+z/ lpFUoFDI2tLuY FZ47WicVDp6v EQM	✓ Valid

CANCEL

NEXT

- 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

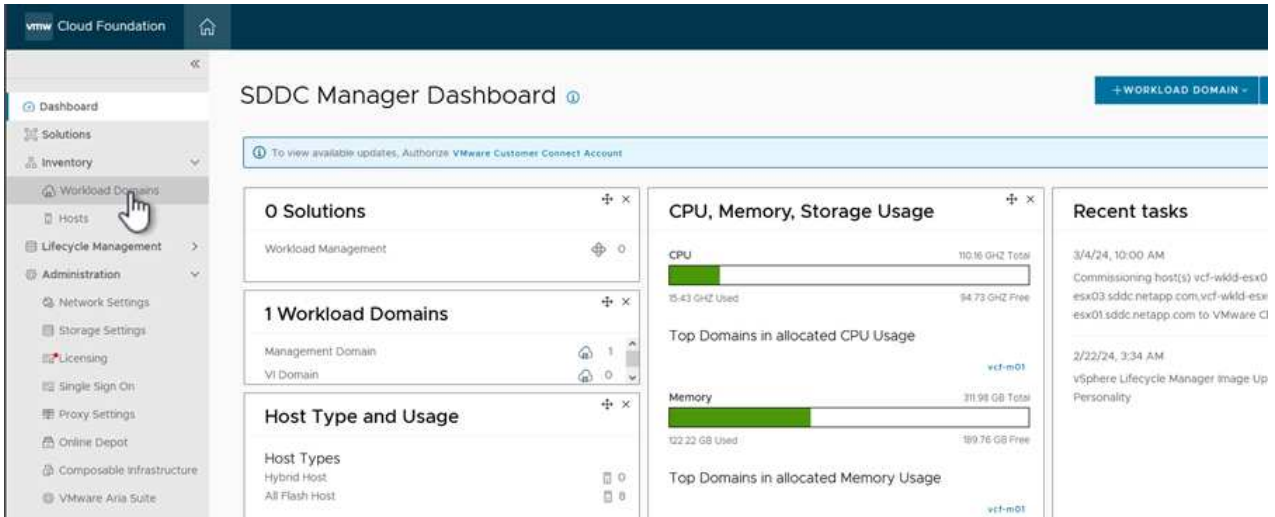


Bereitstellen der VI-Workloaddomäne

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](#)".

VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

7 Switch Configuration

8 License

9 Review

+

1. 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.

VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

NFS Storage

NFS Share Details

Datastore Name ⓘ

VCF_WKLD_01

Folder ⓘ

/VCF_WKLD_01

NFS Server IP Address ⓘ

172.21.118.163

2. Führen Sie im VI-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.

VI Configuration

- General Info
- Cluster
- Compute
- Networking
- Host Selection
- NFS Storage
- Switch Configuration
- License
- Review**

Review

General

Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain

Cluster

Cluster Name	IT-INF-WKLD-01
--------------	----------------

Compute

vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1

Networking

NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxcl01.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL

BACK

FINISH

- 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 leistungstärkere 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 Workloadomänen der virtuellen Infrastruktur (VI).

Die ONTAP tools for 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.

Unterstützte Protokolle zur Speichererweiterung

VCF-Umgebungen können mithilfe mehrerer Speicherprotokolle erweitert werden, die jeweils einzigartige Vorteile und Anwendungsfälle bieten.

Sie können die folgenden Protokolle verwenden, um den Speicher in VCF-Verwaltungsdomänen und VI-Workloadomänen zu erweitern. Wählen Sie die beste Option für Ihre Umgebung, um zusätzlichen Speicher nahtlos in Ihre VCF-Bereitstellung zu integrieren.

iSCSI

Blockbasiertes Protokoll, das Standard-Ethernet-Netzwerke verwendet. Ideal für Umgebungen, die hohe Leistung, Flexibilität und kostengünstige Skalierung erfordern.

iSCSI wird häufig für VMFS-Datenspeicher verwendet und unterstützt erweiterte ONTAP -Funktionen wie Snapshots und Klonen.

- **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:** Verwendet die vorhandene Ethernet-Infrastruktur, wodurch der Bedarf an Spezialhardware reduziert wird und Unternehmen zuverlässige und skalierbare Speicherlösungen erreichen können.

Weitere Informationen zur Verwendung von iSCSI mit NetApp -Speichersystemen finden Sie unter ["SAN-Bereitstellung mit iSCSI"](#) .

Fibre Channel (FC)

Hochgeschwindigkeitsprotokoll mit geringer Latenz, das dedizierte FC-Netzwerke verwendet. FC wird für unternehmenskritische Workloads bevorzugt, die Zuverlässigkeit, dedizierte Bandbreite und robuste Fehlerkorrektur erfordern. Es wird häufig für VMFS-Datenspeicher in Unternehmensumgebungen verwendet.

- **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"](#) .

NFS (Network File System)

Dateibasiertes Protokoll, das die einfache gemeinsame Nutzung und Verwaltung von Dateien zwischen Hosts ermöglicht. NFS lässt sich einfach einrichten und effizient skalieren, sodass es sich für virtualisierte Workloads und Umgebungen eignet, die einen flexiblen Dateizugriff erfordern.

NFS-Datenspeicher werden von ONTAP und vSphere sowohl für Verwaltungs- als auch für Workload-Domänen unterstützt.

- **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"](#) .

NVMe/TCP

Modernes Protokoll, das über TCP/IP hohe Leistung und geringe Latenz über Standard-Ethernet-Netzwerke bietet. NVMe/TCP ist ideal für anspruchsvolle Anwendungen und umfangreiche Datenvorgänge und bietet Skalierbarkeit und Kosteneffizienz ohne spezielle Hardware.

- **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?"](#) .

Anwendungsfälle für das Hinzufügen von zusätzlichem Speicher

Die folgenden Anwendungsfälle zeigen, wie mithilfe verschiedener Protokolle und Konfigurationen zusätzlicher Speicher zu VCF-Verwaltungsdomänen und Virtual Infrastructure (VI)-Workloaddomänen hinzugefügt wird.

- ["Verwaltungsdomäne mit iSCSI"](#)
- ["Managementdomäne mit FC"](#)

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

Erweitern Sie Verwaltungsdomänen mit iSCSI

Bereitstellungsworkflow zum Hinzufügen eines iSCSI-Datenspeichers als zusätzlichen Speicher in einer VCF-Verwaltungsdomäne

Beginnen Sie mit dem Hinzufügen eines iSCSI-Datenspeichers als zusätzlichen Speicher für eine VMware Cloud Foundation (VCF)-Verwaltungsdomäne. Sie richten eine Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI ein, konfigurieren iSCSI-Netzwerke auf ESXi-Hosts, stellen ONTAP tools for VMware vSphere bereit und erstellen einen VMFS-Datenspeicher.

1

"Überprüfen der Bereitstellungsanforderungen"

Überprüfen Sie die Anforderungen zum Hinzufügen von iSCSI-Datenspeichern als zusätzlichen Speicher zur VCF-Verwaltungsdomäne.

2

"Erstellen Sie die SVM und LIFs"

Erstellen Sie eine SVM mit mehreren LIFs für iSCSI-Verkehr.

3

"Konfigurieren des Netzwerks"

Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein.

4

"Konfigurieren des Speichers"

Stellen Sie ONTAP -Tools bereit und verwenden Sie sie, um den Speicher zu konfigurieren.

Bereitstellungsanforderungen für das Hinzufügen eines iSCSI-Datenspeichers zu einer VCF-Verwaltungsdomäne

Überprüfen Sie die Anforderungen für das Hinzufügen von iSCSI-Datenspeichern als zusätzlichen Speicher zu einer VMware Cloud Foundation (VCF)-Verwaltungsdomäne.

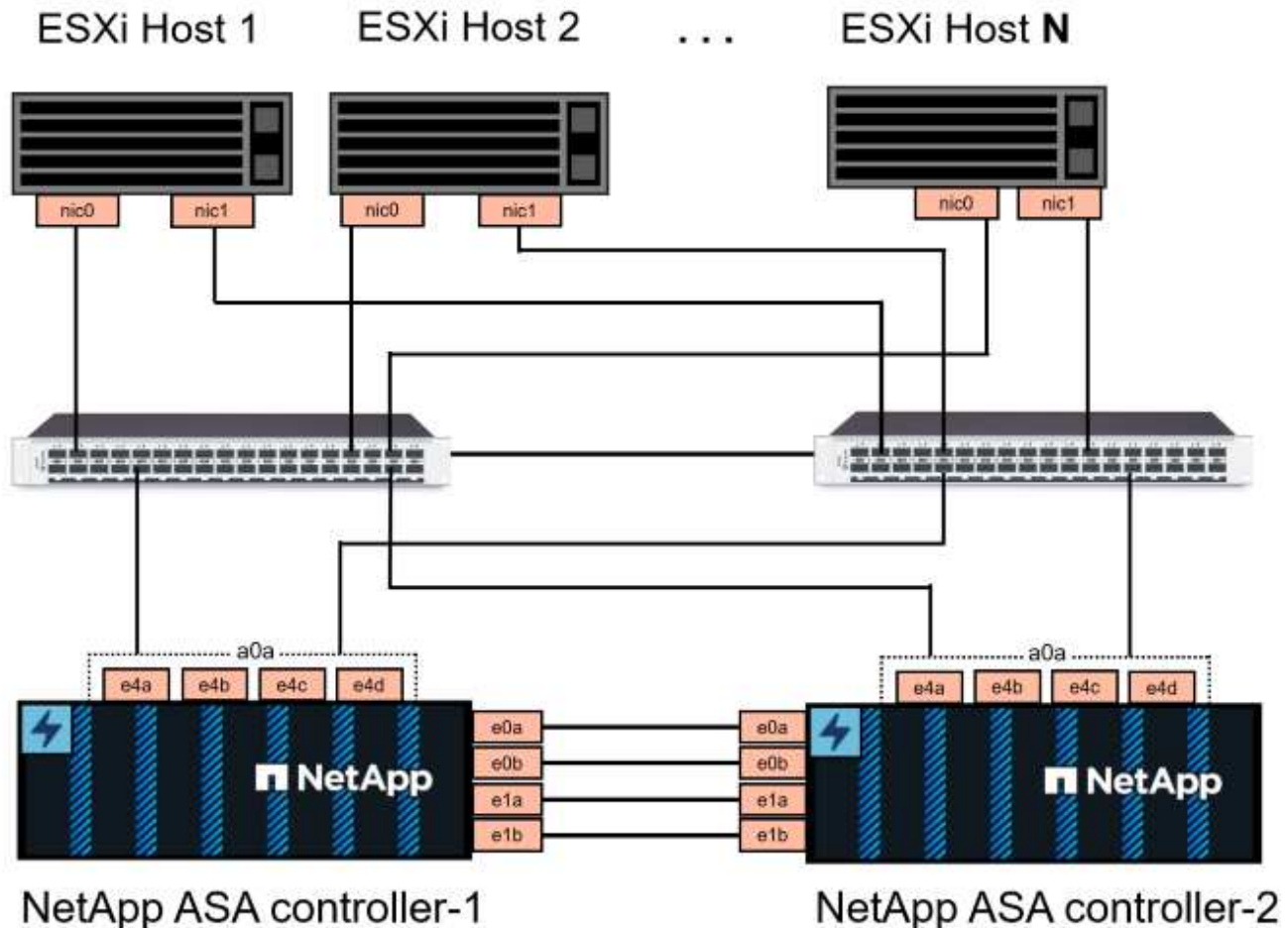
Infrastrukturanforderungen

Stellen Sie sicher, dass die folgenden Komponenten und Konfigurationen vorhanden sind.

- 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.

Empfohlenes iSCSI-Netzwerkdesign

Sie sollten vollständig redundante Netzwerkdesigns für iSCSI konfigurieren. 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.



Erstellen Sie für Multipathing und Failover über mehrere Pfade mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken für alle SVMs in iSCSI-Konfigurationen.



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"](#).

Wie geht es weiter?

Nach der Überprüfung der Bereitstellungsanforderungen, ["Erstellen Sie die SVM und LIFs"](#).

Erstellen Sie SVM und LIFs für iSCSI-Datenspeicher in einer VCF-Verwaltungsdomäne

Erstellen Sie eine Storage Virtual Machine (SVM) mit mehreren logischen Schnittstellen (LIFs), um iSCSI-Konnektivität für VMware Cloud Foundation-Verwaltungsdomänen

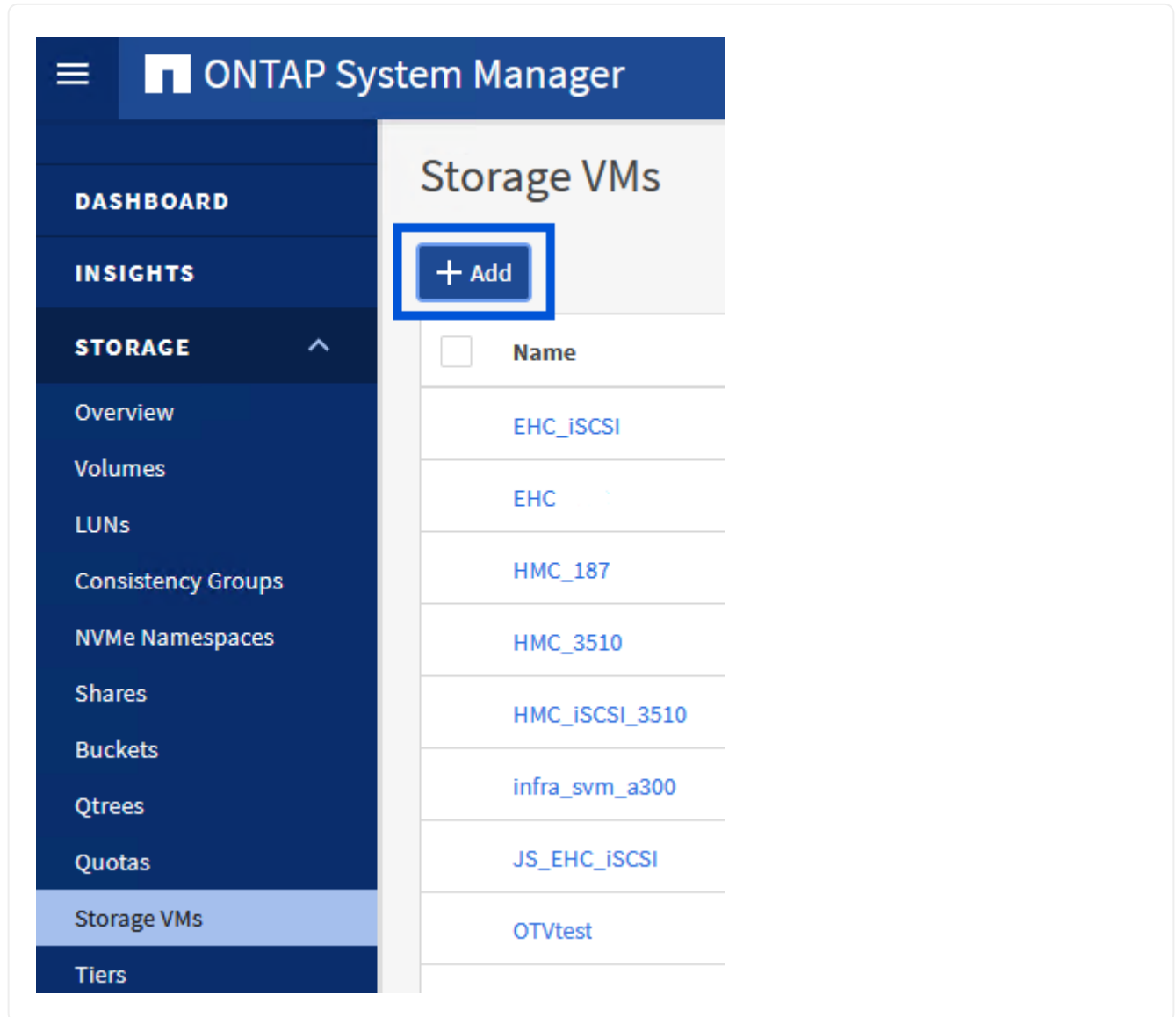
bereitzustellen. Sie konfigurieren die SVM mit iSCSI-Protokollunterstützung und richten mehrere LIFs über separate Ethernet-Netzwerke ein, um Multipathing und Failover für optimale Leistung und Verfügbarkeit zu ermöglichen.

Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie in der ONTAP Dokumentation: ["Erstellen Sie ONTAP LIFs"](#) .

Schritte

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

Beispiel anzeigen



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**.

Beispiel anzeigen

Add Storage VM ×

STORAGE VM NAME

IPSPACE

Default ▼

Access Protocol

SMB/CIFS, NFS, S3 ✓ iSCSI FC NVMe

☒ Enable iSCSI

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



Erstellen Sie für Multipathing und Failover über mehrere Pfade mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken für alle SVMs in iSCSI-Konfigurationen.

Beispiel anzeigen

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
<input type="text" value="172.21.118.179"/>	<input type="text" value="24"/>	Add optional gateway	<input type="text" value="NFS_iSCSI"/>

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

IP ADDRESS	PORT
<input type="text" value="172.21.119.179"/>	<input type="text" value="a0a-3375"/>

ntaphci-a300-02

IP ADDRESS	PORT
<input type="text" value="172.21.118.180"/>	<input type="text" value="a0a-3374"/>

IP ADDRESS	PORT
<input type="text" value="172.21.119.180"/>	<input type="text" value="a0a-3375"/>

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

Beispiel anzeigen

Storage VM Administration

☐ Manage administrator account

[Cancel](#)

Wie geht es weiter?

Nachdem Sie die SVM und LIFs erstellt haben, "[Konfigurieren des Netzwerks für iSCSI auf ESXi-Hosts](#)".

Konfigurieren Sie das Netzwerk für iSCSI auf ESXi-Hosts in einer VCF-Verwaltungsdomäne

Konfigurieren Sie iSCSI-Netzwerke auf ESXi-Hosts in VMware Cloud Foundation-Verwaltungsdomänen, um die Konnektivität zu ONTAP -Speichersystemen zu ermöglichen. Sie erstellen verteilte Portgruppen mit VLAN-Trennung, konfigurieren Uplink-Teaming für Redundanz und richten VMkernel-Adapter auf jedem ESXi-Host ein, um dedizierte iSCSI-Pfade für Failover-Funktionen einzurichten.

Führen Sie diese Schritte mithilfe des vSphere-Clients auf dem VCF-Verwaltungsdomänencluster aus.

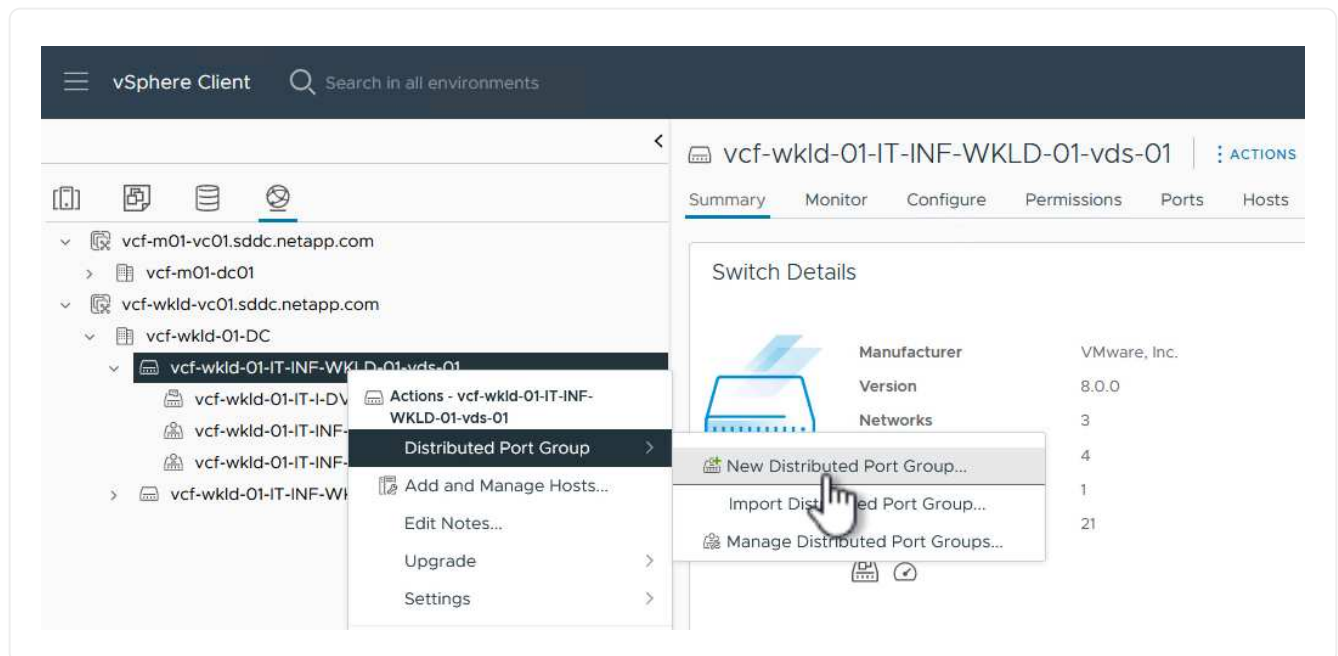
Schritt 1: Erstellen Sie verteilte Portgruppen für iSCSI-Datenverkehr

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

Schritte

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 **Distributed Port Group**....

Beispiel anzeigen



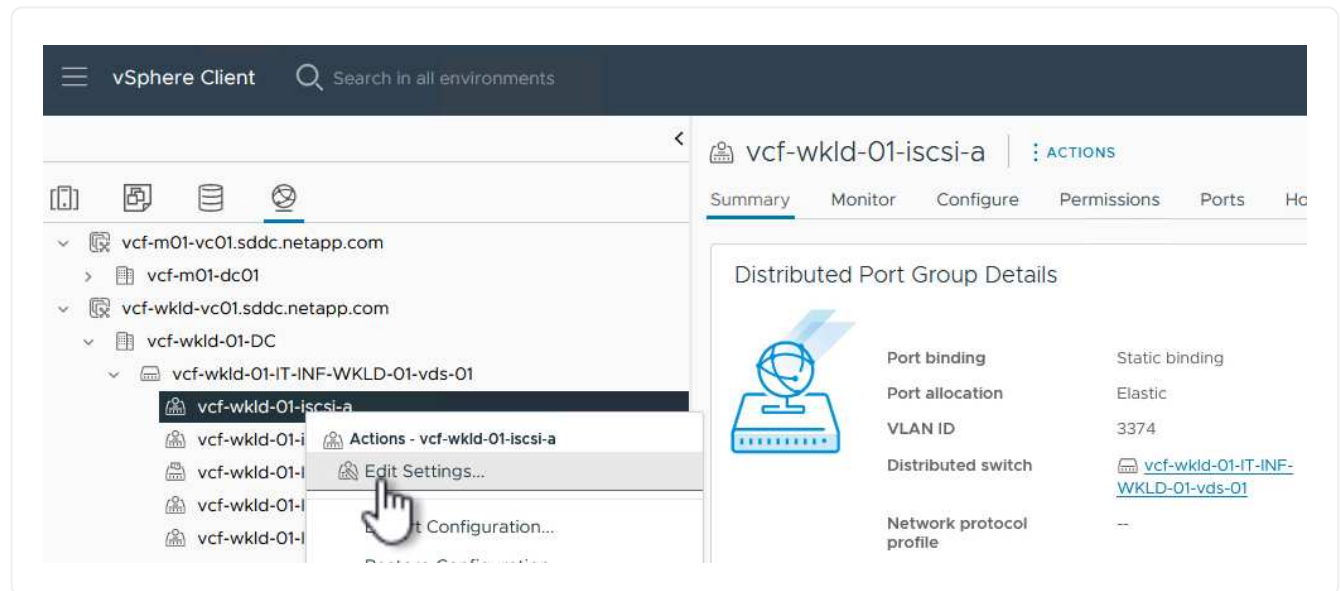
2. Geben Sie im Assistenten **Neue verteilte Portgruppe** einen Namen für die neue Portgruppe ein und klicken Sie dann auf **Weiter**, um fortzufahren.
3. Füllen Sie auf der Seite **Einstellungen konfigurieren** alle Einstellungen aus. Wenn VLANs verwendet werden, stellen Sie sicher, dass Sie die richtige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

Beispiel anzeigen

The screenshot shows a configuration window titled 'New Distributed Port Group' with a sidebar on the left containing three steps: '1 Name and location', '2 Configure settings' (which is highlighted), and '3 Ready to complete'. The main area is titled 'Configure settings' and includes a sub-header 'Set general properties of the new port group.' Below this, there are several configuration fields: 'Port binding' set to 'Static binding', 'Port allocation' set to 'Elastic' with an information icon, 'Number of ports' set to '8', and 'Network resource pool' set to '(default)'. Under the 'VLAN' section, 'VLAN type' is set to 'VLAN' and 'VLAN ID' is set to '3374'. An 'Advanced' section at the bottom has a checkbox for 'Customize default policies configuration' which is currently unchecked. At the bottom right of the window are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking on the 'NEXT' button.

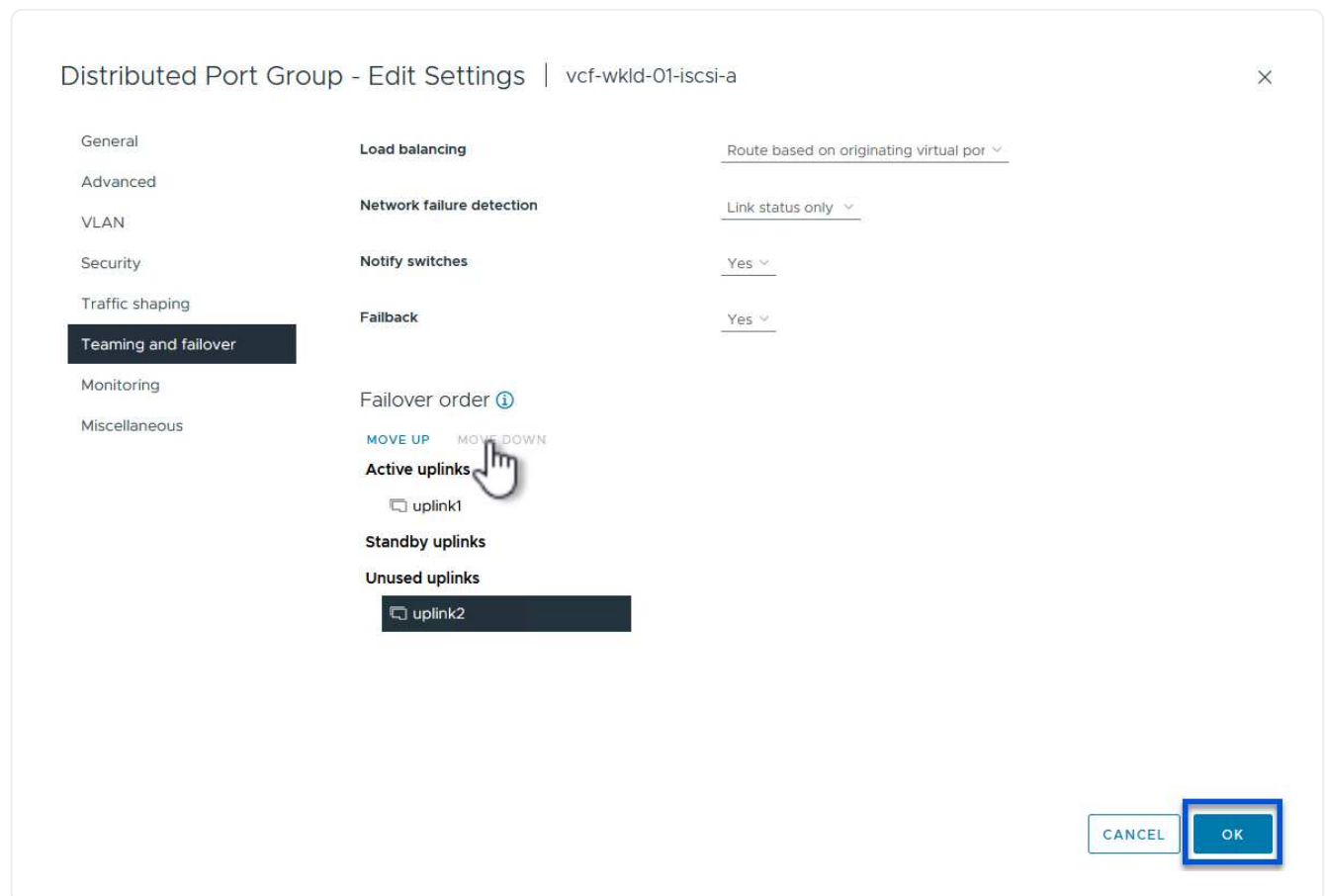
4. Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Änderungen und klicken Sie auf **Fertig**, um die neue verteilte Portgruppe zu erstellen.
5. Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen, und stellen Sie sicher, dass 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.

Beispiel anzeigen



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.

Beispiel anzeigen



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

Beispiel anzeigen

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Failback

Failover order ⓘ

Active uplinks

Standby uplinks

Unused uplinks

Route based on originating virtual port

Link status only

Yes

Yes

MOVE UP MOVE DOWN

uplink2

uplink1

Schritt 2: Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host in der Verwaltungsdomäne.

Schritte

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....**

Beispiel anzeigen

vSphere Client

vcf-wkld-esx01.sddc.netapp.com

Summary

Monitor

Configure

Permissions

VMs

Datastores

Networks

Updates

Storage

Networking

VMkernel adapters

ADD NETWORKING...

REFRESH

		Network Label
vmk0		vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt
vmk1		vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion
vmk2		vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs
vmk10		--

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

Beispiel anzeigen

The screenshot shows the 'Add Networking' window with the 'Select connection type' step selected in the left sidebar. The main area has the title 'Select connection type' and a subtitle 'Select a connection type to create.' There are three radio button options:

- ☒ **VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.
- ☐ **Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- ☐ **Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

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

Beispiel anzeigen

The screenshot shows the 'Add Networking' window with the 'Select target device' step selected in the left sidebar. The main area has the title 'Select target device' and a subtitle 'Select a target device for the new connection.' There are three radio button options:

- ☒ **Select an existing network**
- ☐ **Select an existing standard switch**
- ☐ **New standard switch**

Below the options is a 'Quick Filter' section with a text input field labeled 'Enter value'. Below that is a table with 5 items:

	Name	NSX Port Group ID	Distributed Switch
<input checked="" type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

At the bottom right of the window are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking the 'NEXT' button.

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU

Get MTU from switch

9000

TCP/IP stack

Default

Available services

Enabled services

☒ vMotion

☐ vSphere Replication NFC

☐ NVMe over RDMA

☐ Provisioning

☐ vSAN

☐ Fault Tolerance logging

☐ vSAN Witness

☐ Management

☐ vSphere Backup NFC

☐ vSphere Replication

☐ NVMe over TCP

5. Geben Sie auf der Seite **IPv4-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.

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically

☒ Use static IPv4 settings

IPv4 address

172.21.118.127

Subnet mask

255.255.255.0

Default gateway

☐ Override default gateway for this adapter

172.21.166.1

DNS server addresses

10.61.185.231

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

Distributed port groupvcf-wkld-01-iscsi-a

Distributed switchvcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ Port properties

New port groupvcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU9000

vMotionDisabled

ProvisioningDisabled

Fault Tolerance loggingDisabled

ManagementDisabled

vSphere ReplicationDisabled

vSphere Replication NFCDisabled

vSANDisabled

vSAN WitnessDisabled

vSphere Backup NFCDisabled

NVMe over TCPDisabled

NVMe over RDMADisabled

▼ IPv4 settings

IPv4 address172.21.118.127 (static)

Subnet mask255.255.255.0

CANCEL

BACK

FINISH

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

Wie geht es weiter?

Nachdem Sie das Netzwerk für iSCSI auf allen ESXi-Hosts in der Workloaddomäne konfiguriert haben, "[Konfigurieren des Speichers für iSCSI auf ESXi-Hosts](#)".

Konfigurieren Sie iSCSI-Speicher in einer VCF-Verwaltungsdomäne mit ONTAP -Tools

Richten Sie zusätzlichen iSCSI-Speicher ein, um die Verwaltungsdomänen von VMware Cloud Foundation zu erweitern. Sie stellen ONTAP -Tools bereit, konfigurieren einen iSCSI-Datenspeicher in der Verwaltungsdomäne und migrieren Verwaltungs-VMs in den neuen Datenspeicher.

Führen Sie die folgenden Schritte auf dem VCF-Verwaltungsdomänencluster mithilfe des vSphere-Clients aus.

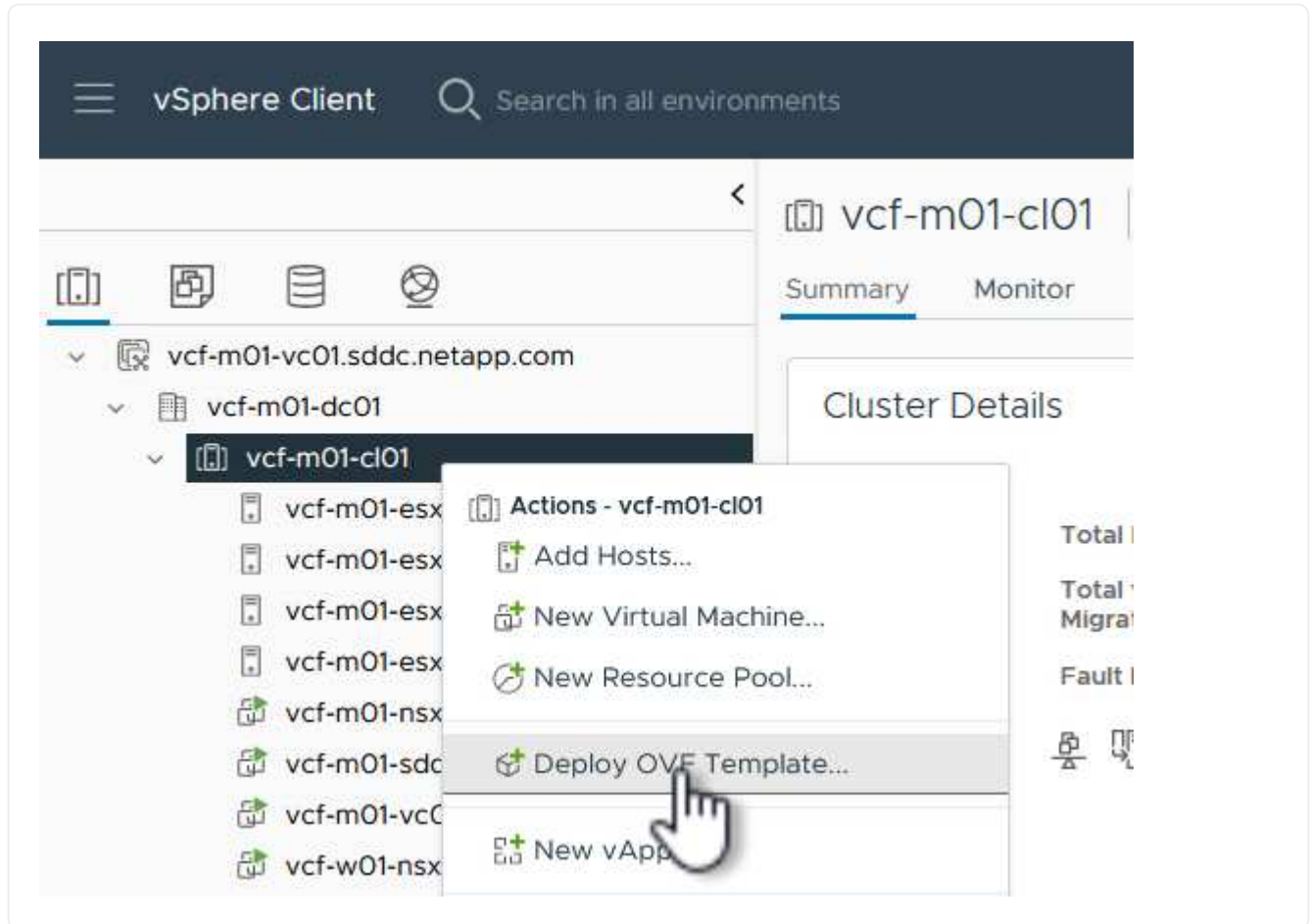
Schritt 1: ONTAP tools for VMware vSphere bereitstellen

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

Schritte

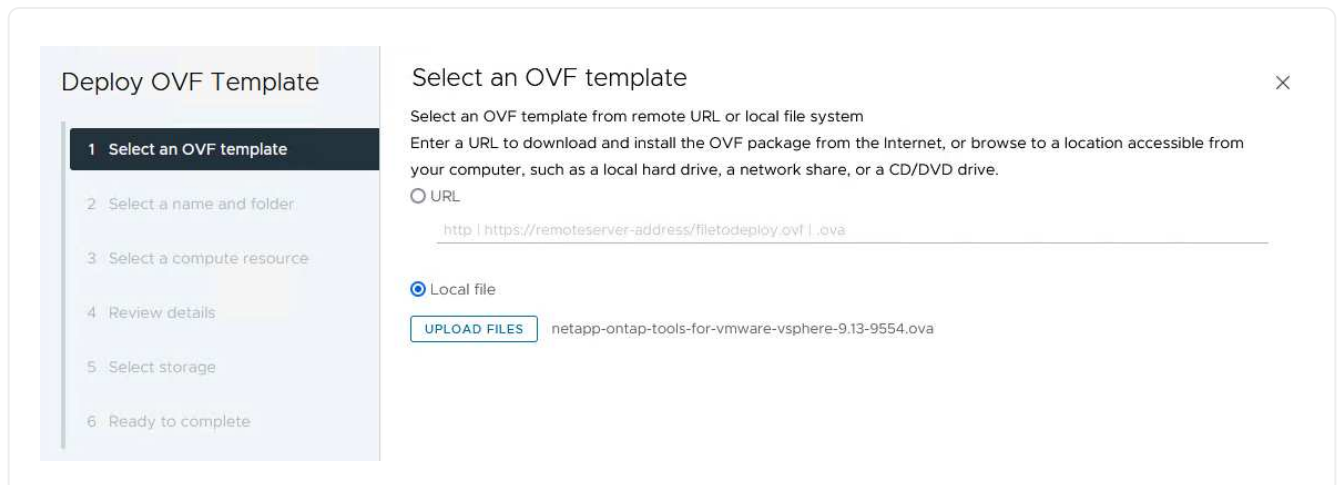
1. Beziehen Sie das OVA-Image der ONTAP -Tools von der "[NetApp Support-Site](#)" und laden Sie es in einen lokalen Ordner herunter.
2. Melden Sie sich bei der vCenter-Appliance für die VCF-Verwaltungsdomäne an.
3. Klicken Sie in der vCenter-Appliance-Schnittstelle mit der rechten Maustaste auf den Verwaltungscluster und wählen Sie **OVF-Vorlage bereitstellen...**

Beispiel anzeigen



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

Beispiel anzeigen



- Wählen Sie in den Schritten 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.
- Wählen Sie als Speicherort der Konfigurations- und Datenträgerdateien den vSAN-Datenspeicher des VCF-Managementdomänenclusters aus.

Beispiel anzeigen

Name	Storage Compatibility	Capacity	Provisioned	Free	
vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	<input checked="" type="radio"/>
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	<input type="radio"/>
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	<input type="radio"/>
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	<input type="radio"/>
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	<input type="radio"/>

- Wählen Sie auf der Seite **Netzwerk auswählen** das für den Verkehrsverkehr verwendete Netzwerk aus.

Beispiel anzeigen

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

- 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 Wartungskonto der ONTAP -Tools.

- 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**
- Erforderliche Netzwerkeigenschaften.

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

Beispiel anzeigen

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration

4 settings

Application User Password (*)

Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password

Confirm Password

NTP Servers

A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

172.21.166.1

Maintenance User Password (*)

Password to assign to maint user account.

Password

Confirm Password

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Customize template

Configure vCenter or Enable VCF

5 settings

Enable VMware Cloud Foundation (VCF)

vCenter server and user details are ignored when VCF is enabled.

vCenter Server Address (*)

Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*)

Specify the HTTPS port of an existing vCenter to register to.

443

Username (*)

Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*)

Specify the password of an existing vCenter to register to.

Password

Confirm Password

Network Properties

8 settings

Host Name

Specify the hostname for the appliance. (Leave blank if DHCP is desired)

vcf-w01-otv9

IP Address

Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL

BACK

NEXT

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

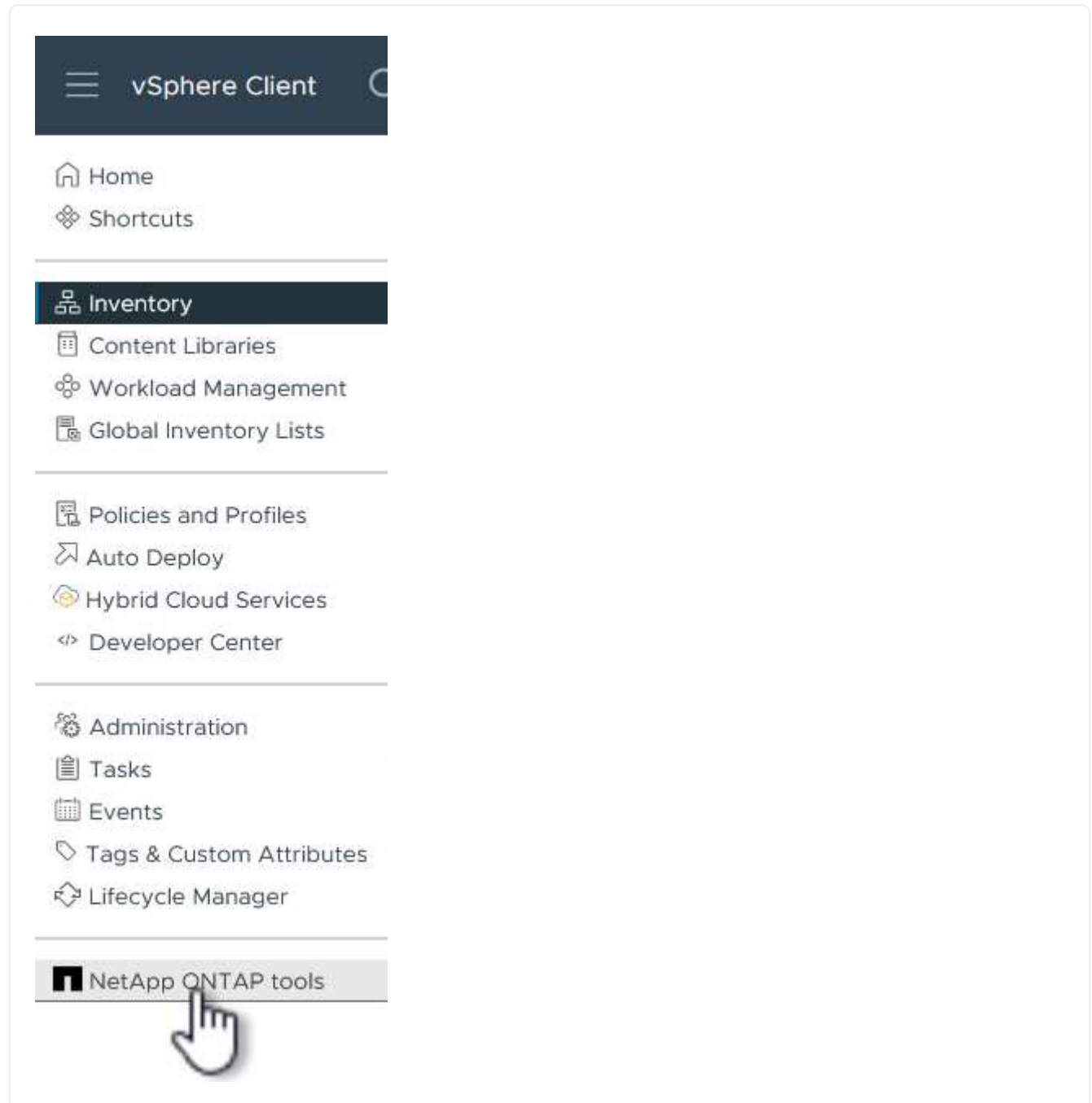
Schritt 2: Ein Speichersystem hinzufügen

Führen Sie die folgenden Schritte aus, um mithilfe von ONTAP -Tools ein Speichersystem hinzuzufügen.

Schritte

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

Beispiel anzeigen




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

Beispiel anzeigen

The screenshot displays the vSphere Client interface for ONTAP tools. The top navigation bar shows 'vSphere Client' and a search bar. The left sidebar contains a menu with 'Overview' (selected), 'Storage Systems', 'Storage capability profile', 'Storage Mapping', 'Settings', and 'Reports'. The main content area is titled 'ONTAP tools for VMware vSphere' and includes tabs for 'Getting Started', 'Traditional Dashboard', and 'vVols Dashboard'. A descriptive paragraph states: 'ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.' Below this, there are two main sections: 'Add Storage System' with an 'ADD' button (highlighted by a red box) and 'Provision Datastore' with a 'PROVISION' button. To the right, the 'Next Steps' section includes 'View Dashboard' and 'Settings' links. At the bottom, there are 'What's new?' and 'Resources' sections with links to documentation and user guides.


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

Add Storage System

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

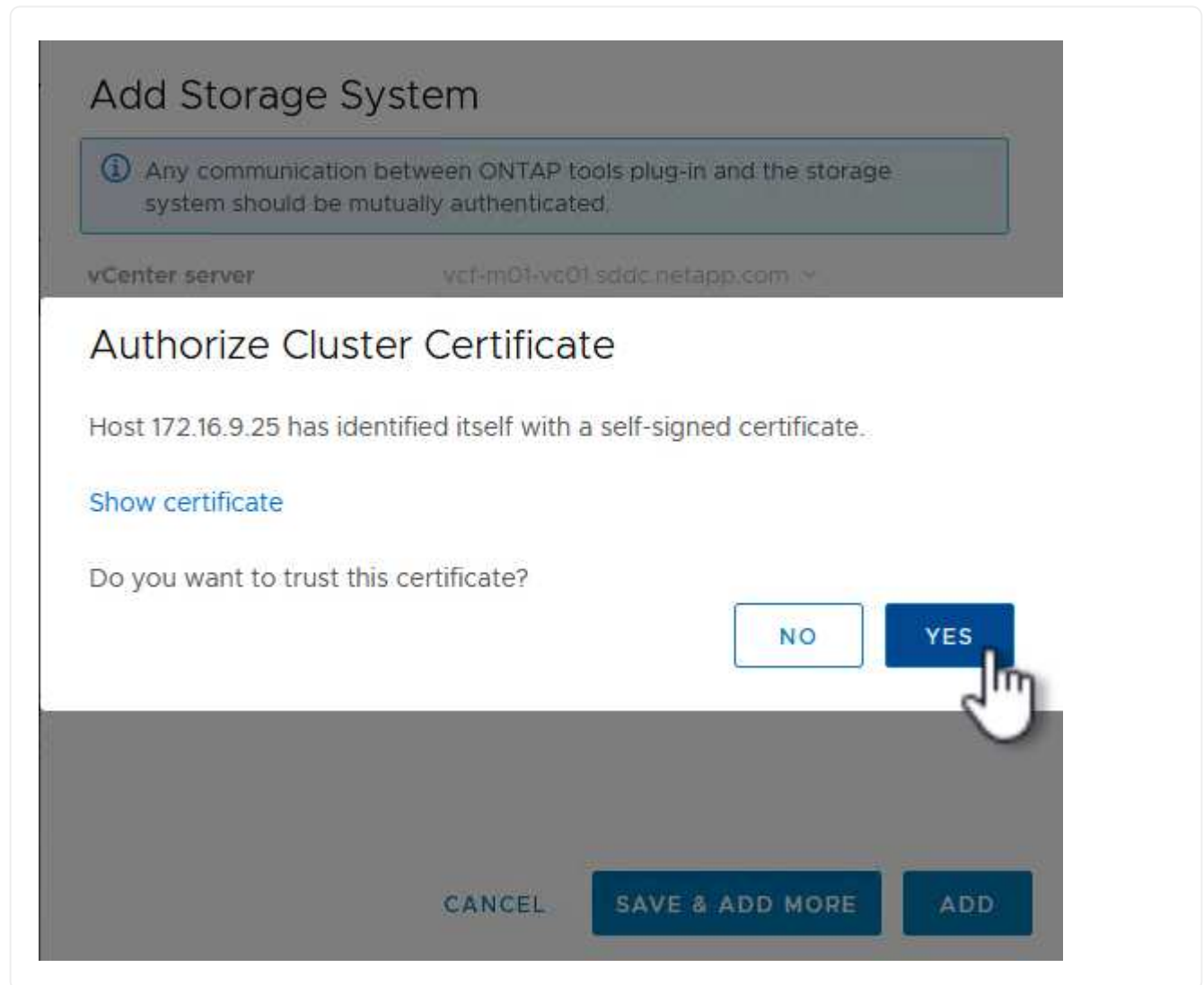
vCenter server	vcf-m01-vc01.sddc.netapp.com
Name or IP address:	172.16.9.25
Username:	admin
Password:	••••••••
Port:	443
Advanced options	>

[CANCEL](#) [SAVE & ADD MORE](#) [ADD](#)



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

Beispiel anzeigen



Optional: Migrieren Sie Management-VMs in den iSCSI-Datenspeicher

In Fällen, in denen Sie zum Schutz der VCF-Verwaltungs-VMs lieber ONTAP Speicher verwenden möchten, migrieren Sie die VMs mit vMotion in den neu erstellten iSCSI-Datenspeicher.

Schritte

1. Navigieren Sie im 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...**

Beispiel anzeigen

The screenshot shows the vSphere Client interface. On the left, a tree view shows the hierarchy of virtual machines under 'vcf-m01-ci01'. The main pane displays a table of virtual machines. A context menu is open over the 'vcf-m01-nsx01a' VM, with the 'Migrate' option highlighted by a mouse cursor.

Name	State	Status	Provisioned Space	Used Space	Host CPU	Host Mem
vcf-m01-nsx01a	Powered On	✓ Normal	616.52 GB	97.88 GB	5 GHz	31.63 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	106.33 GB	19.33 GB	2.52 GHz	6.77 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	1.79 TB	237.82 GB	344 MHz	15.98 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	1.16 TB	143.81 GB	757 MHz	13.98 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	600.35 GB	90.61 GB	7.99 GHz	48.11 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	600.39 GB	94.6 GB	6.06 GHz	48.1 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	600.45 GB	95.14 GB	7.16 GHz	48.14 GB
vcf-m01-nsx01a	✓ Normal	✓ Normal	1.82 TB	126.69 GB	780 MHz	28.02 GB

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

Beispiel anzeigen

The screenshot shows the '8 Virtual Machines - Migrate' wizard. The 'Select a migration type' step is active, and the 'Change storage only' option is selected by a mouse cursor.

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- ☐ Change compute resource only
Migrate the virtual machines to another host or cluster.
- ☒ Change storage only
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- ☐ Change both compute resource and storage
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- ☐ Cross vCenter Server export
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

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

Beispiel anzeigen

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Same format as source

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
	mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	⌵
	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB	⌵

Manage Columns

Items per page: 10 2 items

Compatibility

✓ Compatibility checks succeeded.

















CANCEL

BACK

NEXT

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

Beispiel anzeigen

Recent Tasks					Alarms
Task Name	Target	Status			Details
Relocate virtual machine	 vcf-w01-nsx03	<div><div></div></div> 38% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-wkld-vc01	<div><div></div></div> 42% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-m01-otv9	<div><div></div></div> 36% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-m01-nsx01a	<div><div></div></div> 49% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-w01-nsx02	<div><div></div></div> 47% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-m01-sddcm01	<div><div></div></div> 39% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-w01-nsx01	<div><div></div></div> 42% 			Migrating Virtual Machine active state
Relocate virtual machine	 vcf-m01-vc01	<div><div></div></div> 44% 			Migrating Virtual Machine active state

Weitere Informationen

- Informationen zur Konfiguration von ONTAP -Speichersystemen finden Sie unter ["ONTAP 9 Dokumentation"](#) .
- Informationen zur Konfiguration von VCF finden Sie unter ["VMware Cloud Foundation-Dokumentation"](#) .
- Informationen zur Verwendung von VMFS iSCSI-Datenspeichern mit VMware finden Sie unter ["vSphere VMFS-Datenspeicher – iSCSI-Speicher-Backend mit ONTAP"](#) .
- Videodemos dieser Lösung finden Sie unter ["Bereitstellung von VMware-Datenspeichern"](#) .

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, wie ein VMFS-Datenspeicher über Fibre Channel (FC) als zusätzlicher Speicher für die Verwaltungsdomäne von VMware Cloud Foundation (VCF) konfiguriert wird. Dieses Verfahren fasst die Schritte zum Bereitstellen von ONTAP Tools in der Verwaltungsdomäne, zum Hinzufügen eines Speicher-Backends und zum Bereitstellen des Datenspeichers zusammen.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Komponenten und Konfigurationen vorhanden sind.

- Ein ONTAP Speichersystem mit FC-Ports, die mit FC-Switches verbunden sind.
- Mit FC-LIFs erstellte SVM.
- 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.
- Verwenden Sie Multipath für FC-LUNs.

Schritte

1. Stellen Sie ONTAP -Tools in der Verwaltungsdomäne bereit, indem Sie den Anweisungen in der Dokumentation zu den ONTAP tools for VMware vSphere folgen: "[Stellen Sie ONTAP -Tools in der Verwaltungsdomäne bereit](#)".

Die ONTAP tools for VMware vSphere Appliance werden als kleiner Einzelknoten mit Kerndiensten zur Unterstützung von NFS- und VMFS-Datenspeichern bereitgestellt.

2. Fügen Sie mithilfe der vSphere-Clientschnittstelle ein Speicher-Backend hinzu, indem Sie den Anweisungen in der Dokumentation zu den ONTAP tools for VMware vSphere folgen: "[Definieren Sie das Speicher-Backend mithilfe der vSphere-Clientschnittstelle](#)".

Durch Hinzufügen eines Speicher-Backends können Sie einen ONTAP Cluster integrieren.

3. Stellen Sie VMFS auf FC bereit, indem Sie den Anweisungen in der Dokumentation zu den ONTAP tools for VMware vSphere folgen: "[Bereitstellen von VMFS auf FC](#)".

Weitere Informationen

- Informationen zum Konfigurieren von ONTAP Speichersystemen finden Sie unter "[ONTAP 9 Dokumentation](#)".
- Informationen zur Konfiguration von VCF finden Sie im "[VMware Cloud Foundation-Dokumentation](#)".
- Informationen zur Konfiguration von Fibre Channel auf ONTAP Speichersystemen finden Sie in der ONTAP 9-Dokumentation. "[SAN-Speicherverwaltung](#)".
- Weitere Informationen zur Verwendung von VMFS mit ONTAP Speichersystemen finden Sie im "[Bereitstellungshandbuch für VMFS](#)".
- Videodemos dieser Lösung finden Sie unter "[Bereitstellung von VMware-Datenspeichern](#)".

Erweitern Sie VI-Workload-Domänen mit vVols iSCSI

Bereitstellungsworkflow zum Hinzufügen eines iSCSI vVols Datenspeichers als zusätzlichen Speicher in einer VI-Workloaddomäne

Beginnen Sie mit der Konfiguration eines iSCSI vVols -Datenspeichers als zusätzlichen Speicher in einer VMware Cloud Foundation (VCF) Virtual Infrastructure (VI)-Workloaddomäne. Sie erstellen die SVM und LIFs, richten das iSCSI-Netzwerk ein, stellen ONTAP tools for VMware vSphere bereit und konfigurieren den Speicher.



"Überprüfen der Bereitstellungsanforderungen"

Überprüfen Sie die Anforderungen zum Bereitstellen von iSCSI vVols in einer VMware Cloud Foundation VI-Workloaddomäne.

2**"Erstellen Sie die SVM und LIFs"**

Erstellen Sie eine SVM mit mehreren LIFs für iSCSI-Verkehr.

3**"Konfigurieren des Netzwerks"**

Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein.

4**"Konfigurieren des Speichers"**

Stellen Sie ONTAP -Tools bereit und verwenden Sie sie, um den Speicher zu konfigurieren.

Bereitstellungsanforderungen für iSCSI- vVols in einer VI-Workloaddomäne

Überprüfen Sie das empfohlene Netzwerkdesign und die Infrastrukturanforderungen zum Bereitstellen von iSCSI vVols in einer VMware Cloud Foundation VI-Workloaddomäne. Sie benötigen ein vollständig konfiguriertes ONTAP AFF oder ASA Speichersystem, eine vollständige VCF-Verwaltungsdomäne und eine vorhandene VI-Workloaddomäne.

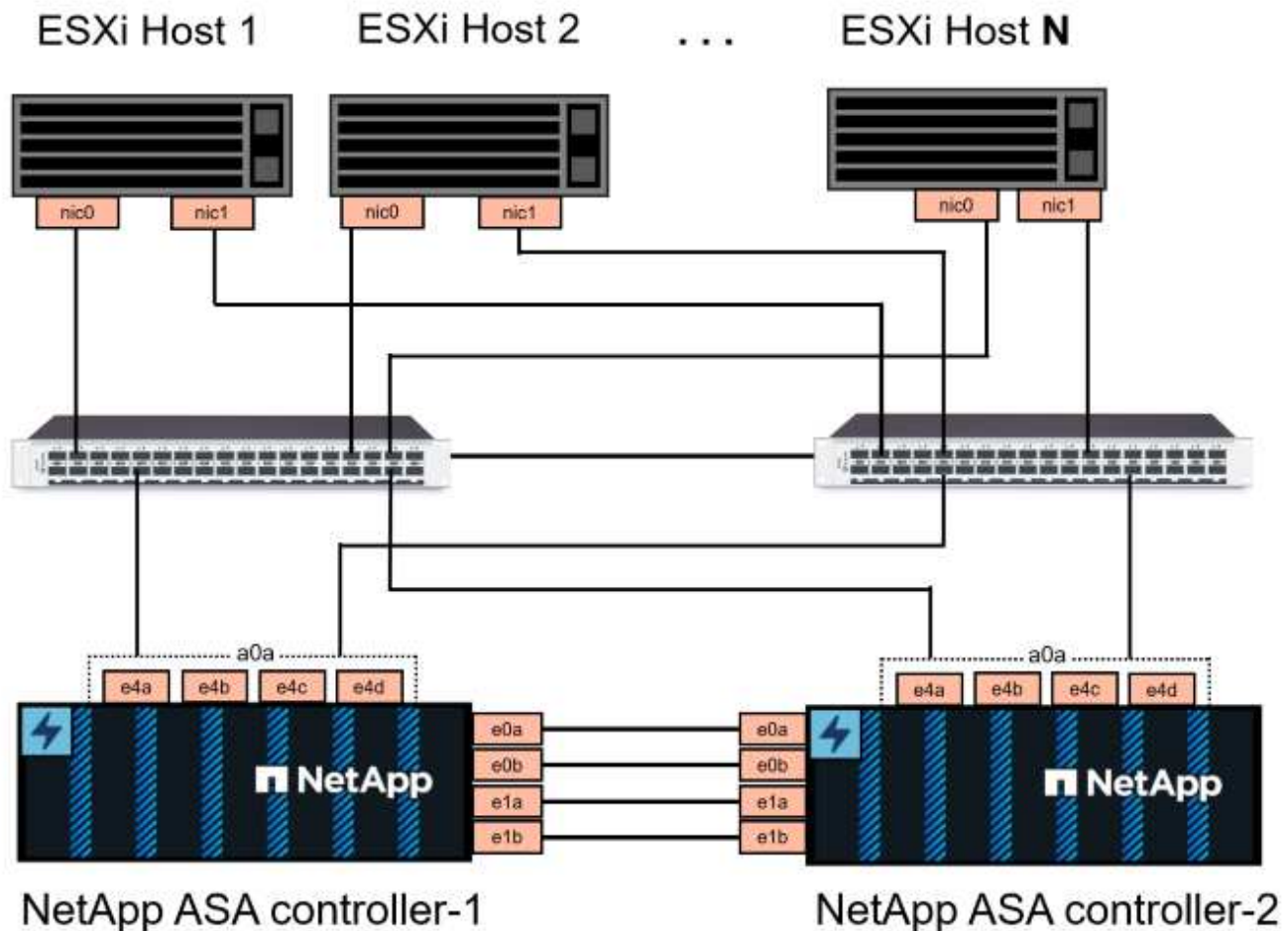
Infrastrukturanforderungen

Stellen Sie sicher, dass die folgenden Komponenten und Konfigurationen vorhanden sind.

- 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.

Empfohlenes iSCSI-Netzwerkdesign

Sie sollten vollständig redundante Netzwerkdesigns für iSCSI konfigurieren. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration. Es bietet Fehlertoleranz für Speichersysteme, Switches, Netzwerkadapter und Hostsysteme. Weitere Informationen finden Sie in der NetApp ["SAN-Konfigurationsreferenz"](#) .



Erstellen Sie für Multipathing und Failover über mehrere Pfade mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken für alle SVMs in iSCSI-Konfigurationen.



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

Wie geht es weiter?

Nach der Überprüfung der Bereitstellungsanforderungen, "[Erstellen Sie die SVM und LIFs](#)".

Erstellen Sie SVM und LIFs für iSCSI vVols Datenspeicher in einer VCF VI-Workloaddomäne

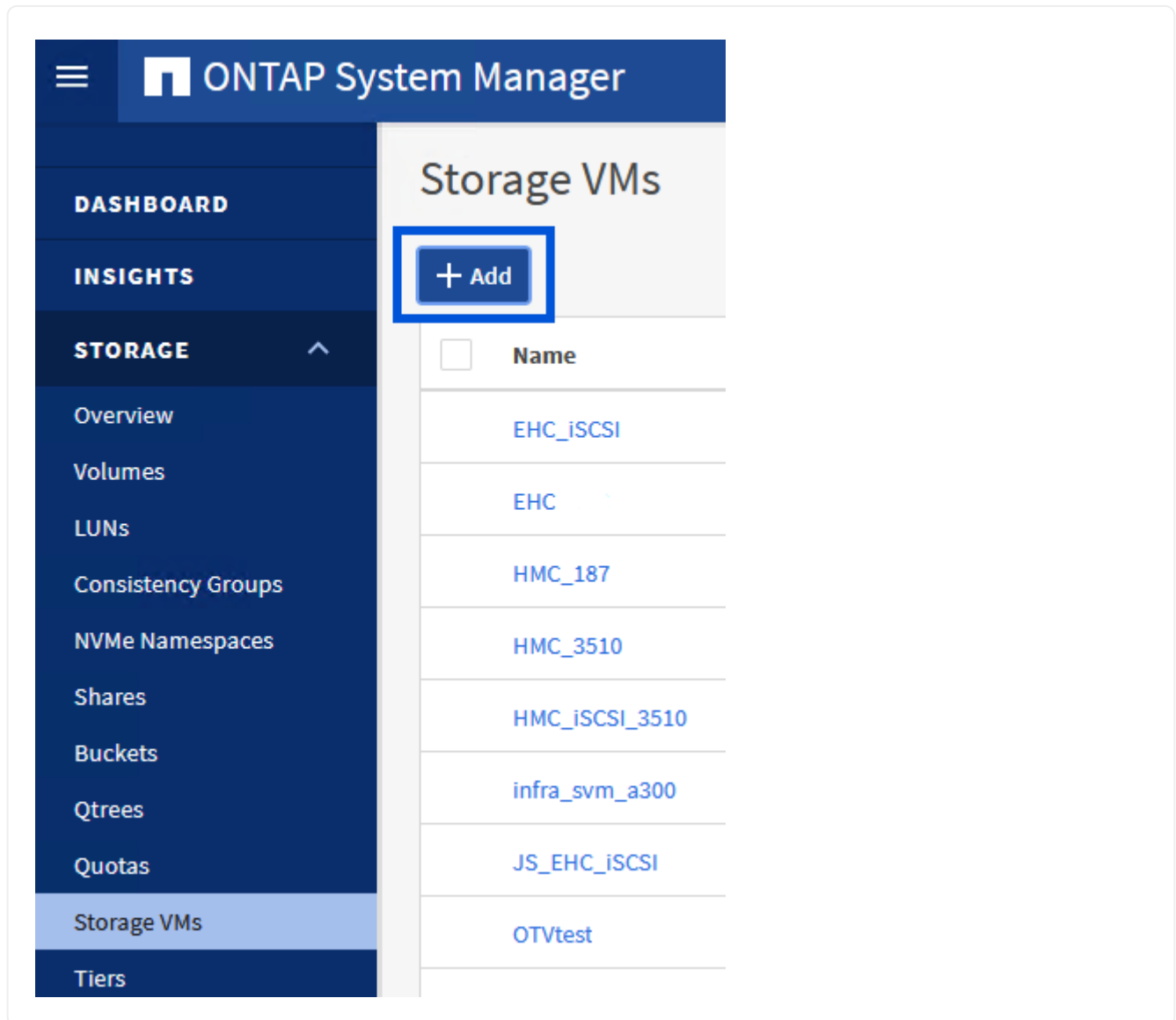
Erstellen Sie eine Storage Virtual Machine (SVM) und mehrere logische Schnittstellen (LIFs) auf einem ONTAP -System, um iSCSI-Datenverkehr für vVols Datenspeicher in einer VMware Cloud Foundation VI-Workloaddomäne zu unterstützen. Sie fügen eine neue SVM hinzu, aktivieren iSCSI, konfigurieren LIFs und aktivieren optional das Storage VM-Administrationskonto.

Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie in der ONTAP

Schritte

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

Beispiel anzeigen



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**.

Beispiel anzeigen

Add Storage VM ×

STORAGE VM NAME

IPSPACE

Default ▼

Access Protocol

SMB/CIFS, NFS, S3 ✓ iSCSI FC NVMe

☒ Enable iSCSI

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



Erstellen Sie für Multipathing und Failover über mehrere Pfade mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken für alle SVMs in iSCSI-Konfigurationen.

Beispiel anzeigen

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS	SUBNET MASK	GATEWAY	BROADCAST DOMAIN AND PORT
<input type="text" value="172.21.118.179"/>	<input type="text" value="24"/>	Add optional gateway	<input type="text" value="NFS_iSCSI"/>

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

IP ADDRESS	PORT
<input type="text" value="172.21.119.179"/>	<input type="text" value="a0a-3375"/>

ntaphci-a300-02

IP ADDRESS	PORT
<input type="text" value="172.21.118.180"/>	<input type="text" value="a0a-3374"/>

IP ADDRESS	PORT
<input type="text" value="172.21.119.180"/>	<input type="text" value="a0a-3375"/>

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

Beispiel anzeigen

Storage VM Administration

☐ Manage administrator account

Wie geht es weiter?

Nachdem Sie die SVM und LIFs erstellt haben, "[Konfigurieren des Netzwerks für iSCSI auf ESXi-Hosts](#)".

Konfigurieren Sie das Netzwerk für iSCSI auf ESXi-Hosts in einer VCF VI-Workloaddomäne

Konfigurieren Sie die Vernetzung für iSCSI-Speicher auf ESXi-Hosts in einer VI-Workloaddomäne. Sie erstellen verteilte Portgruppen für iSCSI-Verkehr und richten VMkernel-Adapter mithilfe des vSphere-Clients ein, um zuverlässige Konnektivität und Multipathing zu ermöglichen.

Verwenden Sie den vSphere-Client mit vCenter Single Sign-On, um diese Schritte auf dem VI Workload Domain-Cluster auszuführen. Derselbe vSphere-Client verwaltet sowohl die Verwaltungs- als auch die Workload-Domänen.

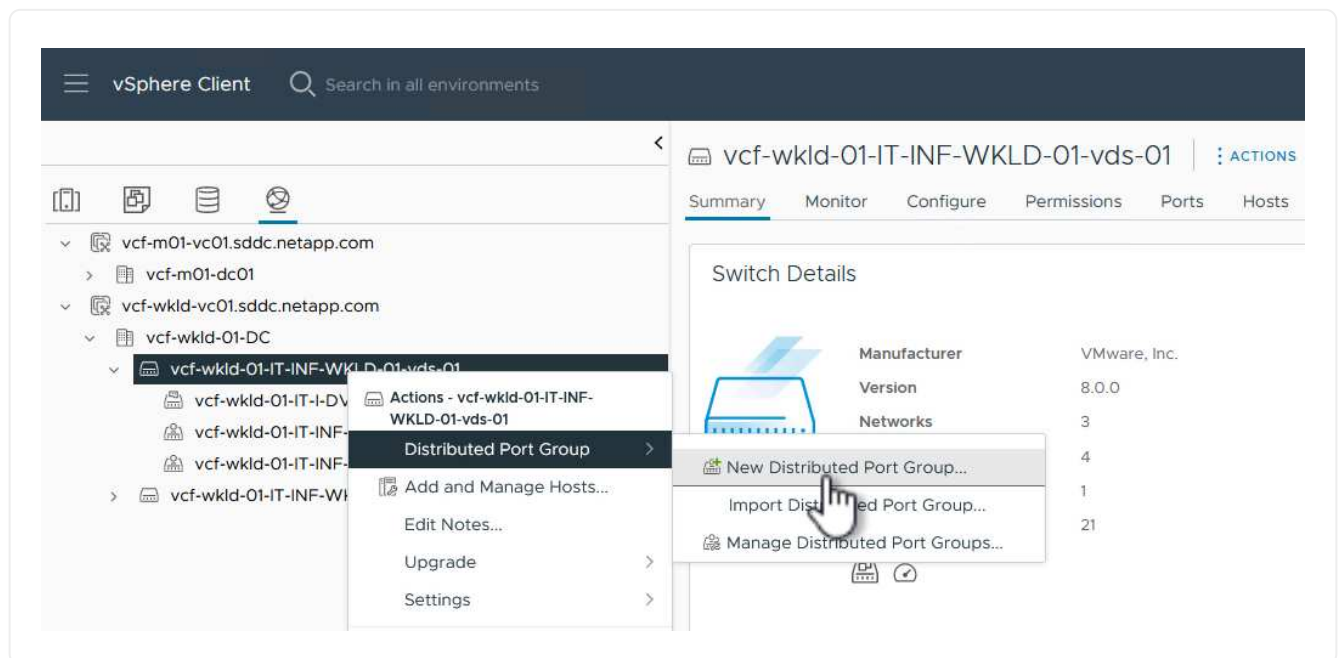
Schritt 1: Erstellen Sie verteilte Portgruppen für iSCSI-Datenverkehr

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

Schritte

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 **Distributed Port Group**....

Beispiel anzeigen



2. Geben Sie im Assistenten **Neue verteilte Portgruppe** einen Namen für die neue Portgruppe ein und klicken Sie dann 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.

Beispiel anzeigen

New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

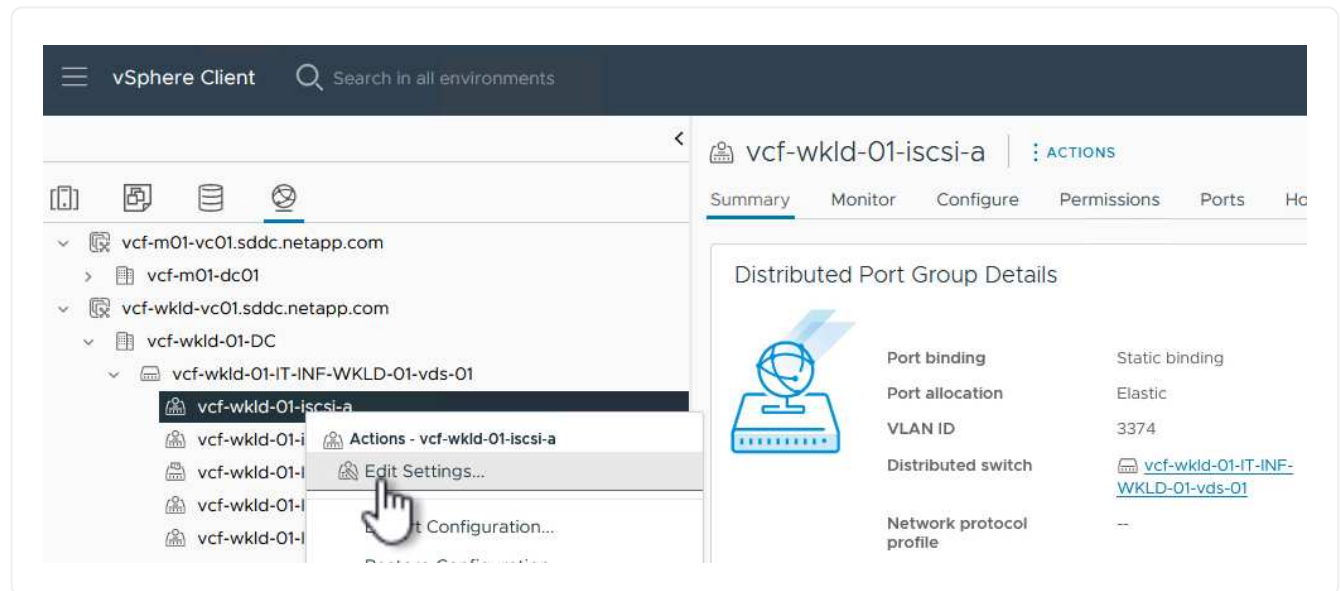
CANCEL

BACK

NEXT

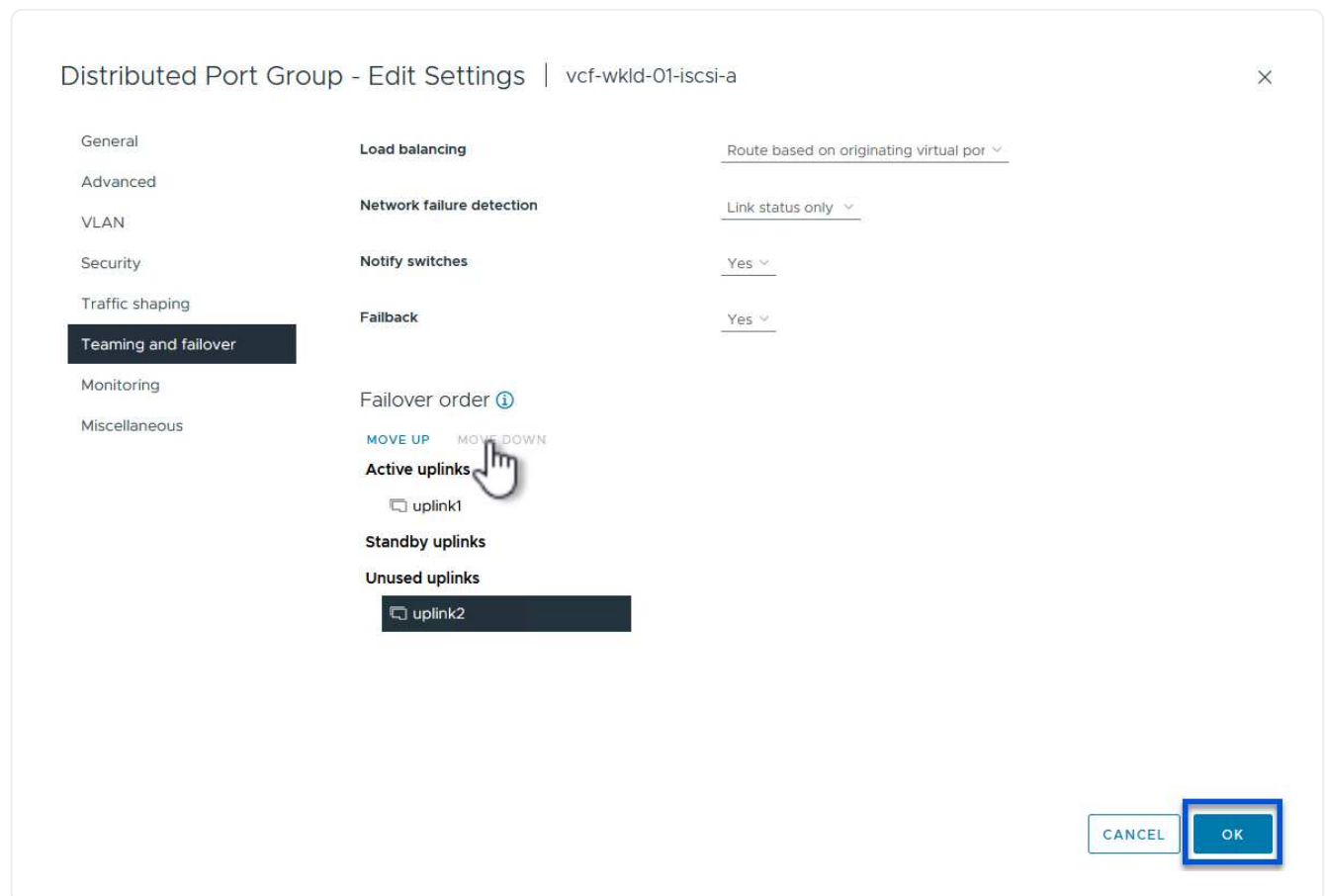
- Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Änderungen und klicken Sie auf **Fertig**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen, und stellen Sie sicher, dass Sie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

Beispiel anzeigen



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.

Beispiel anzeigen



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

Beispiel anzeigen

Distributed Port Group - Edit Settings | vcf-wkld-01-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Failback

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

Unused uplinks

uplink1

Route based on originating virtual port

Link status only

Yes

Yes

Schritt 2: Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

Führen Sie die folgenden Schritte auf jedem ESXi-Host in der Workload-Domäne mithilfe des vSphere-Clients aus.

Schritte

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....**

Beispiel anzeigen

vSphere Client

Search in all environments

vcf-m01-vc01.sddc.netapp.com

vcf-m01-dc01

vcf-m01-cl01

vcf-wkld-vc01.sddc.netapp.com

vcf-wkld-01-DC

IT-INF-WKLD-01

vcf-wkld-esx01.sddc.netapp.com

vcf-wkld-esx02.sddc.netapp.com

vcf-wkld-esx03.sddc.netapp.com

vcf-wkld-esx04.sddc.netapp.com

vcf-w01-otv9

vcf-wkld-esx01.sddc.netapp.com

Summary

Monitor

Configure

Permissions

VMs

Datastores

Networks

Updates

Storage

Storage Adapters

Storage Devices

Host Cache Configuration

Protocol Endpoints

I/O Filters

Networking

Virtual switches

VMkernel adapters

Physical adapters

TCP/IP configuration

VMkernel adapters

ADD NETWORKING... REFRESH

		Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt	
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion	
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs	
vmk10	--	

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

Beispiel anzeigen

The screenshot shows the 'Add Networking' window with the 'Select connection type' step selected in the left sidebar. The main area has the title 'Select connection type' and a subtitle 'Select a connection type to create.' There are three radio button options:

- ☒ **VMkernel Network Adapter**
The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.
- ☐ **Virtual Machine Port Group for a Standard Switch**
A port group handles the virtual machine traffic on standard switch.
- ☐ **Physical Network Adapter**
A physical network adapter handles the network traffic to other hosts on the network.

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

Beispiel anzeigen

The screenshot shows the 'Add Networking' window with the 'Select target device' step selected in the left sidebar. The main area has the title 'Select target device' and a subtitle 'Select a target device for the new connection.' There are three radio button options:

- ☒ **Select an existing network**
- ☐ **Select an existing standard switch**
- ☐ **New standard switch**

Below the options is a 'Quick Filter' section with a text input 'Enter value'. Below that is a table with 5 items:

	Name	NSX Port Group ID	Distributed Switch
<input checked="" type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

At the bottom right of the window are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking the 'NEXT' button.

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU

Get MTU from switch

9000

TCP/IP stack

Default

Available services

Enabled services

☒ vMotion

☐ Provisioning

☐ Fault Tolerance logging

☐ Management

☐ vSphere Replication

☐ vSphere Replication NFC

☐ vSAN

☐ vSAN Witness

☐ vSphere Backup NFC

☐ NVMe over TCP

☐ NVMe over RDMA

5. Geben Sie auf der Seite **IPv4-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.

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically

☒ Use static IPv4 settings

IPv4 address

172.21.118.127

Subnet mask

255.255.255.0

Default gateway

☐ Override default gateway for this adapter

172.21.166.1

DNS server addresses

10.61.185.231

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

Distributed port group	vcf-wkld-01-iscsi-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ Port properties

New port group	vcf-wkld-01-iscsi-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

▼ IPv4 settings

IPv4 address	172.21.118.127 (static)
Subnet mask	255.255.255.0

CANCEL BACK FINISH

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

Wie geht es weiter?

Nachdem Sie das Netzwerk für iSCSI auf allen ESXi-Hosts in der Workloaddomäne konfiguriert haben, "[Speicher für iSCSI vVols konfigurieren](#)".

Konfigurieren Sie den iSCSI vVols Speicher in einer VCF VI-Workloaddomäne mit ONTAP -Tools

Konfigurieren Sie den iSCSI vVols Speicher in einer VI-Workload-Domäne mithilfe von ONTAP Tools. Sie stellen ONTAP tools for VMware vSphere bereit, registrieren ein Speichersystem, erstellen ein Speicherfähigkeitsprofil und stellen einen vVols Datenspeicher im vSphere-Client bereit.

Schritt 1: ONTAP tools for VMware vSphere bereitstellen

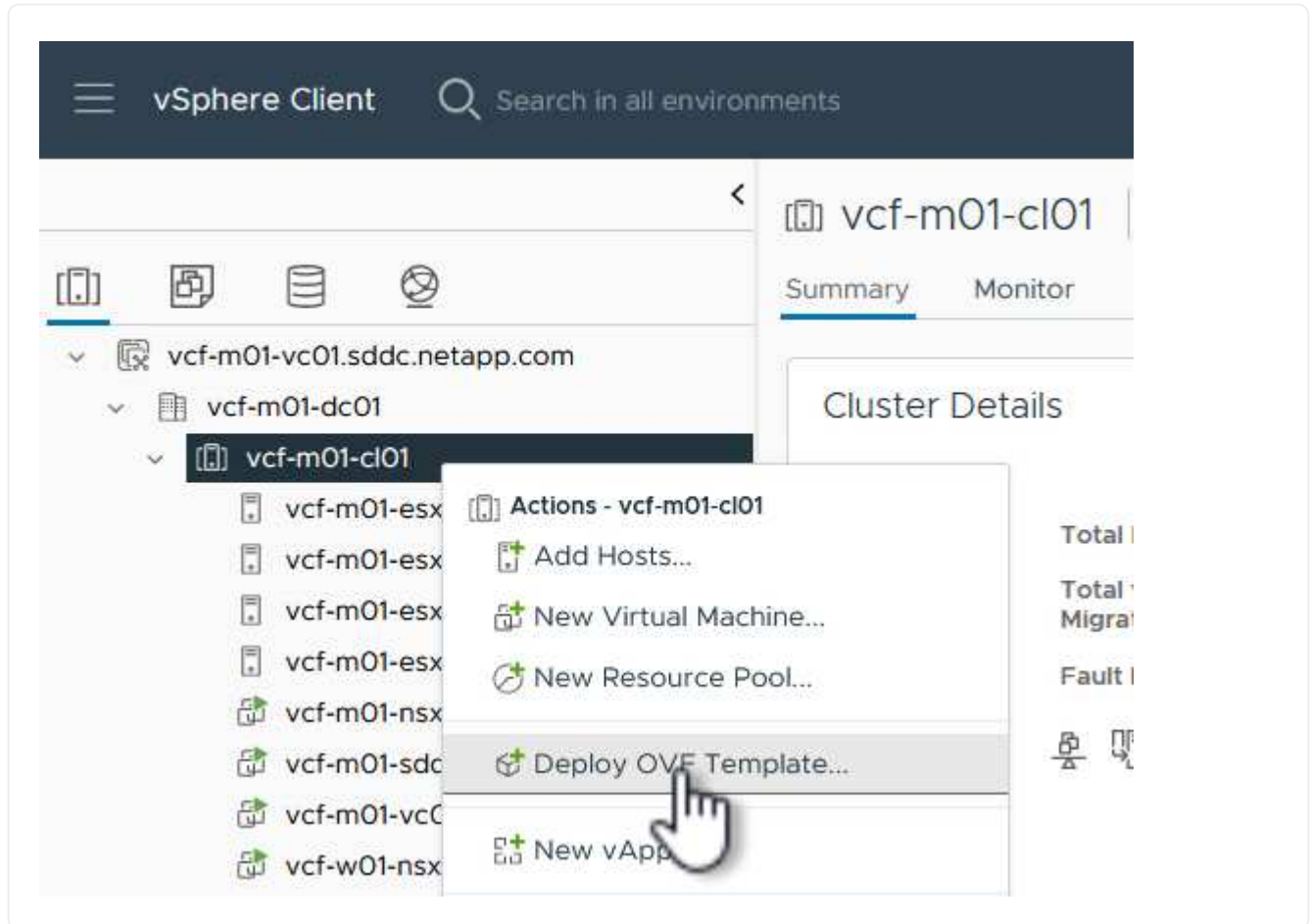
Für VI-Workloaddomänen werden ONTAP Tools im VCF-Verwaltungscluster installiert, aber beim vCenter registriert, das der VI-Workloaddomäne zugeordnet ist.

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

Schritte

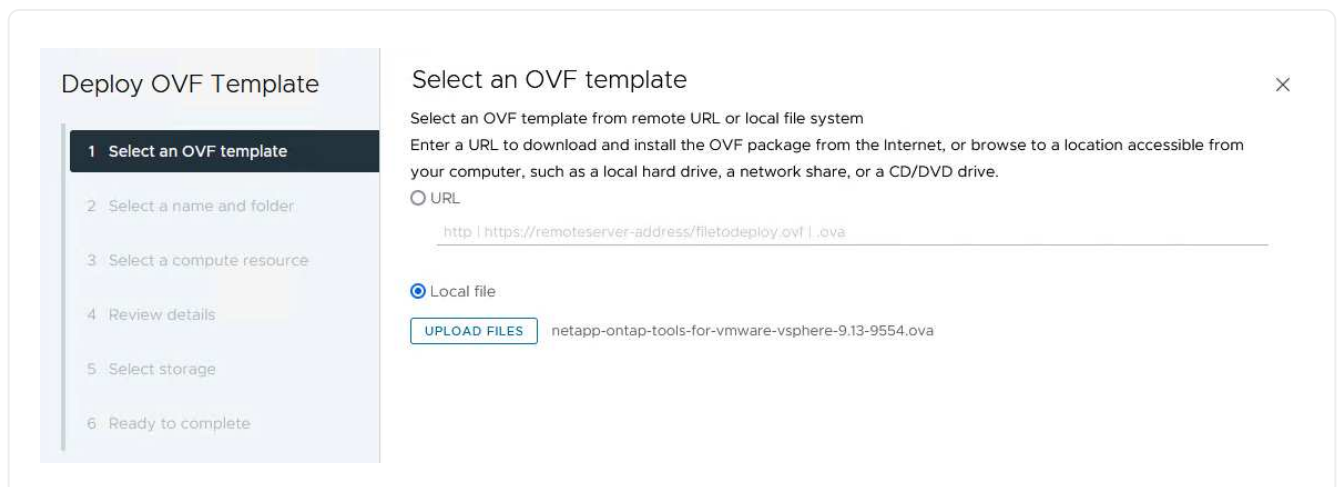
1. Beziehen Sie das OVA-Image der ONTAP -Tools von der "[NetApp Support-Site](#)" und laden Sie es in einen lokalen Ordner herunter.
2. Melden Sie sich bei der vCenter-Appliance für die VCF-Verwaltungsdomäne an.
3. Klicken Sie in der vCenter-Appliance-Schnittstelle mit der rechten Maustaste auf den Verwaltungscluster und wählen Sie **OVF-Vorlage bereitstellen...**

Beispiel anzeigen



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

Beispiel anzeigen



- Wählen Sie in den Schritten 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.
- Wählen Sie als Speicherort der Konfigurations- und Datenträgerdateien den vSAN-Datenspeicher des VCF-Managementdomänenclusters aus.

Beispiel anzeigen

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage**
- Select networks
- Customize template
- Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine ⓘ

Select virtual disk format: As defined in the VM storage policy ▾

VM Storage Policy: **Datastore Default** ▾

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns | Items per page: 10 | 5 items

- Wählen Sie auf der Seite **Netzwerk auswählen** das für den Verwaltungsverkehr verwendete Netzwerk aus.

Beispiel anzeigen

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks**

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan ▾

Manage Columns | 1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4 ▾

vcf-m01-cl01-vds01-pg-vsan
SDDC-DPortGroup-VM-Mgmt
Browse ...

- 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 Wartungskonto der ONTAP -Tools.

- 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**
- Erforderliche Netzwerkeigenschaften.

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

Beispiel anzeigen

Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration	4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.
	Password <input type="password"/>
	Confirm Password <input type="password"/>
NTP Servers	A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used. 172.21.166.1
Maintenance User Password (*)	Password to assign to maint user account.
	Password <input type="password"/>
	Confirm Password <input type="password"/>

Deploy OVF Template

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

Customize template

5 settings

Configure vCenter or Enable VCF	5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>
Port (*)	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
Username (*)	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
Password (*)	Specify the password of an existing vCenter to register to.
	Password <input type="password"/>
	Confirm Password <input type="password"/>

Network Properties 8 settings

Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-w01-otv9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL BACK NEXT

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

Schritt 2: Ein Speichersystem hinzufügen

Führen Sie die folgenden Schritte aus, um mithilfe von ONTAP -Tools ein Speichersystem hinzuzufügen.

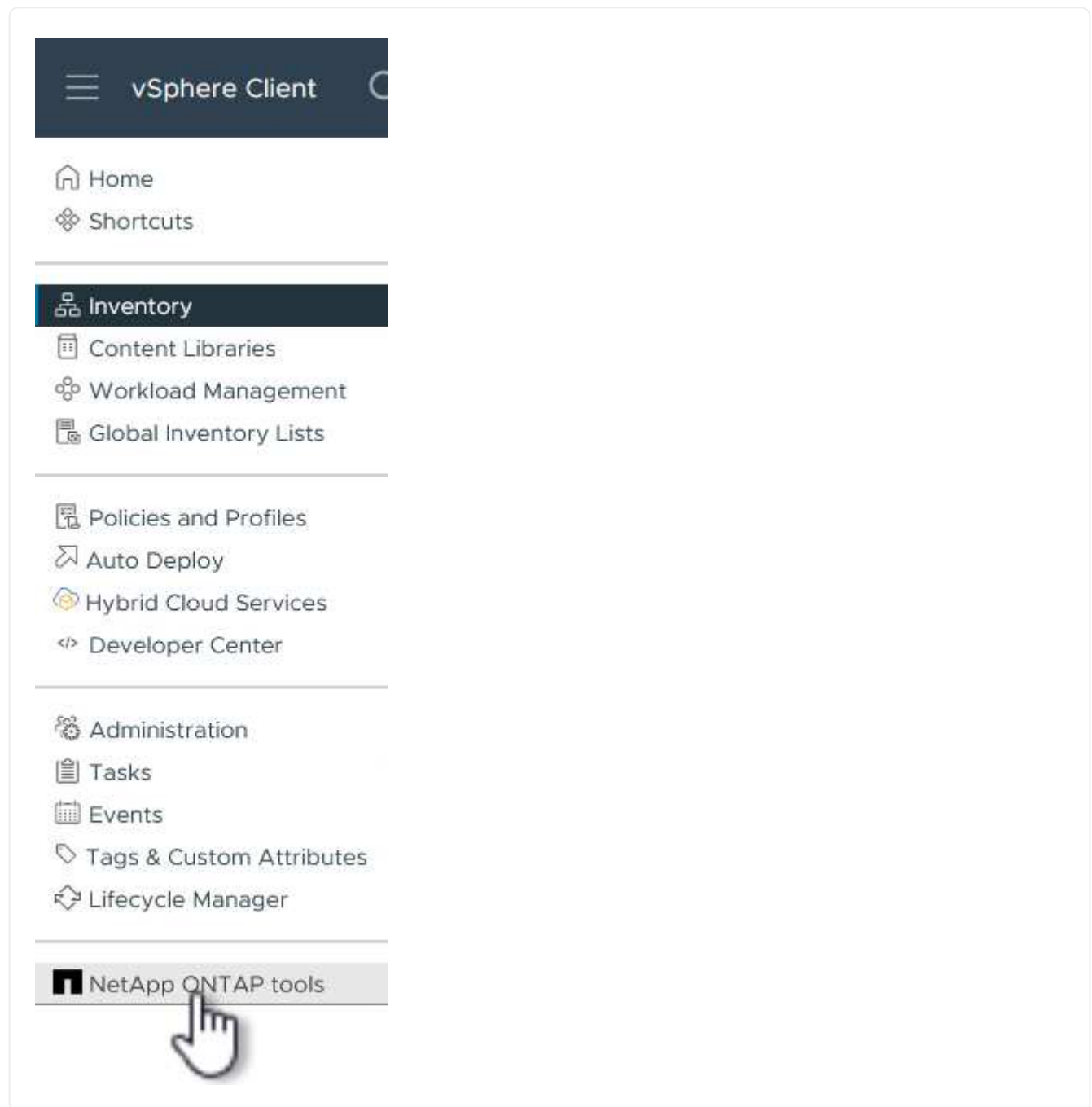


vVol erfordert ONTAP Cluster-Anmeldeinformationen anstelle von SVM-Anmeldeinformationen. Weitere Informationen finden Sie in der Dokumentation zu den ONTAP tools for VMware vSphere : "[Speichersysteme hinzufügen](#)".

Schritte

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

Beispiel anzeigen



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

Beispiel anzeigen

The screenshot displays the vSphere Client interface for the ONTAP tools. The top navigation bar shows 'vSphere Client' and a search bar. The left sidebar contains a menu with 'Overview' (selected), 'Storage Systems', 'Storage capability profile', 'Storage Mapping', 'Settings', and 'Reports'. The main content area is titled 'ONTAP tools for VMware vSphere' and includes tabs for 'Getting Started', 'Traditional Dashboard', and 'vVols Dashboard'. Below the tabs, a description states: 'ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.' The dashboard is divided into two main columns. The left column, 'Add Storage System', features a storage icon and a green 'ADD' button with a hand cursor, which is highlighted by a red rectangular box. The right column, 'Provision Datastore', features a server icon and a green 'PROVISION' button. To the right of these columns is a 'Next Steps' section with a clock icon and links to 'View Dashboard' and 'Settings'. At the bottom, there are two sections: 'What's new?' with a date of September 4, 2023, and 'Resources' with links to documentation and user guides.

NetApp ONTAP tools **INSTANCE 172.21.166.139:8443**

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings


▼ Reports

- Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report
- Log Integrity Report

ONTAP tools for VMware vSphere


Getting Started Traditional Dashboard vVols Dashboard


ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.



Add Storage System


Add storage systems to ONTAP tools for VMware vSphere.






Provision Datastore

Create traditional or vVols datastores.




Next Steps



[View Dashboard](#)

View and monitor the datastores in ONTAP tools for VMware vSphere.



[Settings](#)

Configure administrative settings such as credentials, alarm thresholds.

What's new?

September 4, 2023


- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management

Resources

- [ONTAP tools for VMware vSphere Documentation Resources](#)
- [RBAC User Creator for Data ONTAP](#)
- [ONTAP tools for VMware vSphere REST API Documentation](#)


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

Add Storage System

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

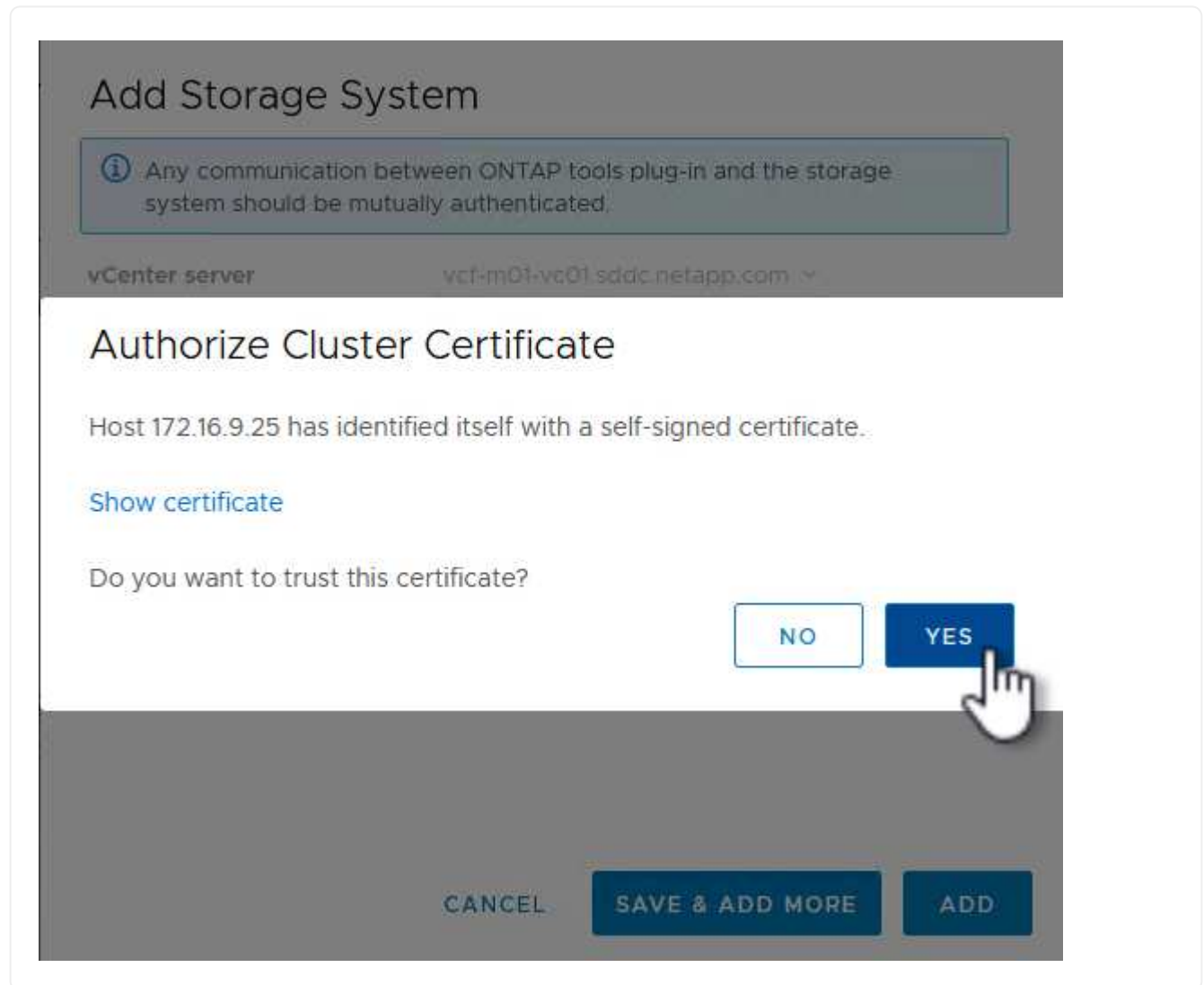
vCenter server	vcf-m01-vc01.sddc.netapp.com
Name or IP address:	172.16.9.25
Username:	admin
Password:	••••••••
Port:	443
Advanced options	>

[CANCEL](#) [SAVE & ADD MORE](#) [ADD](#)



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

Beispiel anzeigen



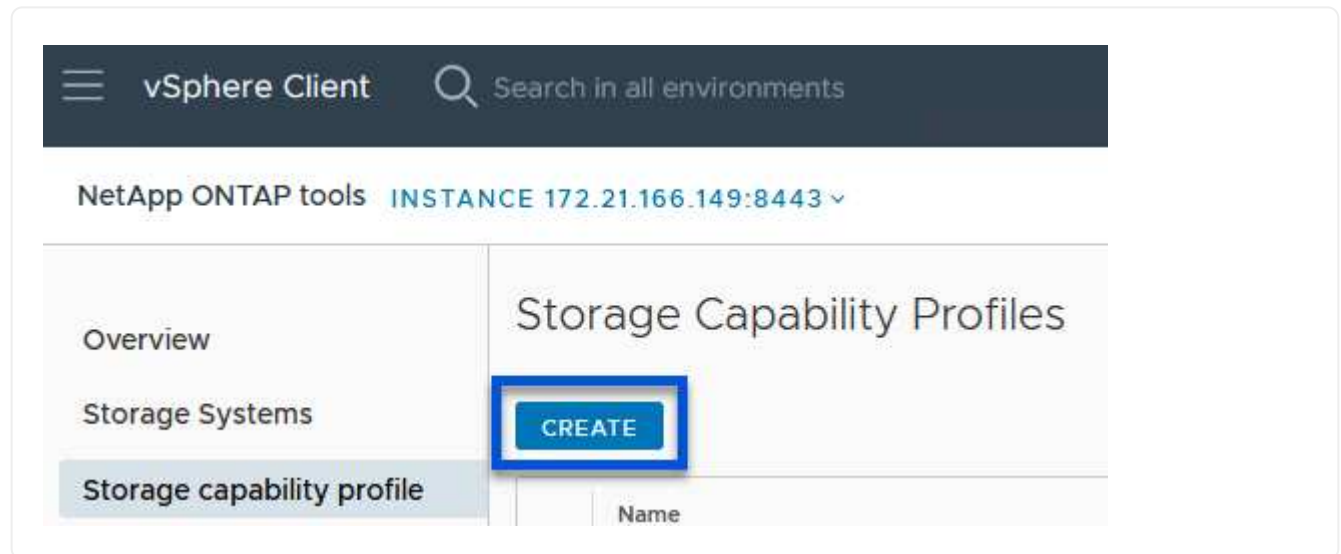
Schritt 3: Erstellen Sie ein Speicherkapazitätsprofil in ONTAP -Tools

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.

Schritte

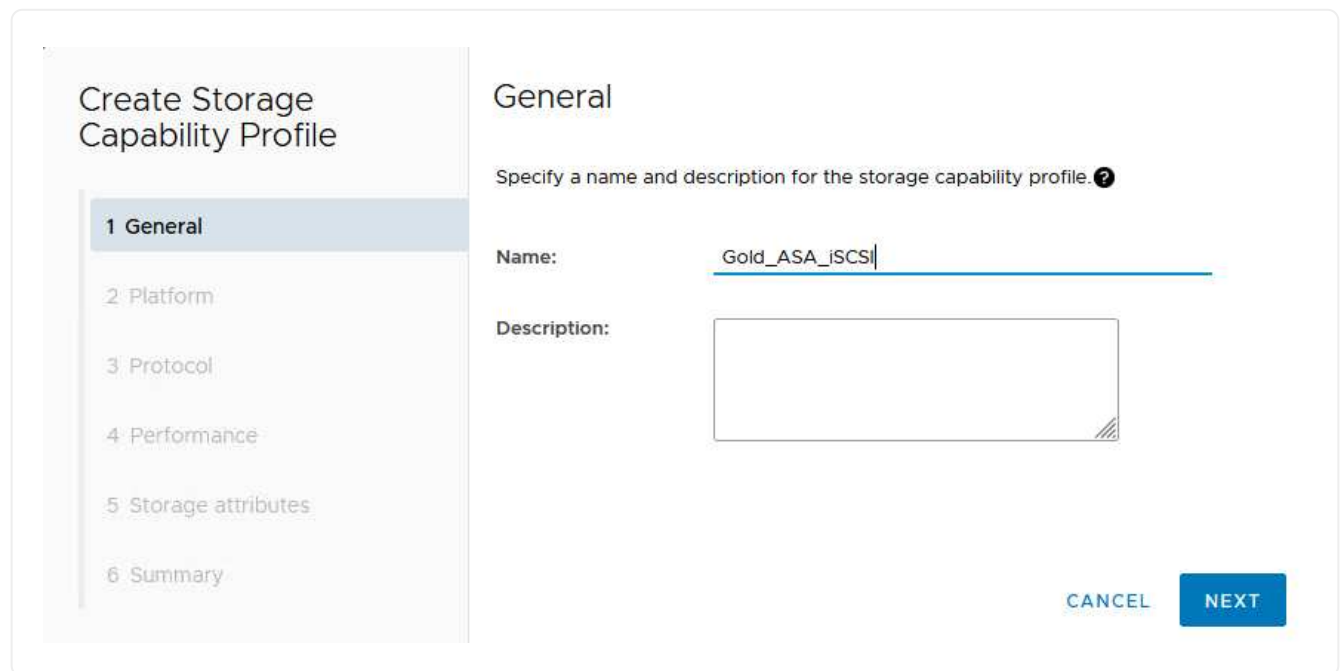
1. Wählen Sie in den ONTAP -Tools im linken Menü **Storage Capability Profile** aus und drücken Sie dann **Create**.

Beispiel anzeigen



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

Beispiel anzeigen



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

Beispiel anzeigen

The screenshot shows the 'Create Storage Capability Profile' wizard at step 2, 'Platform'. On the left, a sidebar lists six steps: 1 General, 2 Platform (highlighted), 3 Protocol, 4 Performance, 5 Storage attributes, and 6 Summary. The main area is titled 'Platform' and contains two settings: 'Platform:' with a dropdown menu set to 'Performance', and 'Asymmetric:' with a toggle switch that is currently turned off. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

4. Wählen Sie das gewünschte Protokoll aus oder wählen Sie **Beliebig**, um alle möglichen Protokolle zuzulassen.
5. Klicken Sie auf **Weiter**, um fortzufahren.

Beispiel anzeigen

The screenshot shows the 'Create Storage Capability Profile' wizard at step 3, 'Protocol'. The sidebar on the left highlights step 3, 'Protocol'. The main area is titled 'Protocol' and features a 'Protocol:' dropdown menu. The dropdown is open, showing a list of options: 'Any', 'FCP', 'iSCSI', and 'NVMe/FC'. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'.

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

Beispiel anzeigen

Create Storage Capability Profile

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

Performance

☐ None ⓘ

☒ QoS policy group ⓘ

Min IOPS: _____

Max IOPS: 6000

☐ Unlimited

CANCEL BACK NEXT

7. Füllen Sie die Seite **Speicherattribute** aus, indem Sie Speichereffizienz, Speicherplatzreservierung, Verschlüsselung und ggf. Tiering-Richtlinien auswählen.

Beispiel anzeigen

Create Storage Capability Profile

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

Storage attributes

Deduplication: Yes ▼

Compression: Yes ▼

Space reserve: Thin ▼

Encryption: No ▼

Tiering policy (FabricPool): None ▼

CANCEL BACK NEXT

8. Überprüfen Sie die Zusammenfassung und klicken Sie auf **Fertig**, um das Profil zu erstellen.

Beispiel anzeigen

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

Schritt 4: Erstellen Sie einen vVols -Datenspeicher in ONTAP -Tools

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

Schritte

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

Beispiel anzeigen

☰ vSphere Client

🔍 Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.149:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings


▼ Reports

- Datastore Report
- Virtual Machine Report
- vVols Datastore Report
- vVols Virtual Machine Report
- Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started Traditional Dashboard vVols Dashboard


ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware envi



Add Storage System

Add storage systems to ONTAP tools for VMware vSphere.

ADD



Provision Datastore

Create traditional or vVols datastores.

PROVISION

109

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

Beispiel anzeigen

The screenshot shows the 'New Datastore' wizard in vSphere. The left sidebar has four tabs: '1 General' (selected), '2 Storage system', '3 Storage attributes', and '4 Summary'. The main area is titled 'General' and contains the following fields:

- Provisioning destination:** A text field containing 'IT-INF-WKLD-01' and a 'BROWSE' button to its right.
- Type:** Three radio buttons: 'NFS', 'VMFS', and 'vVols' (which is selected).
- Name:** A text field containing 'VCF_WKLD_02_VVOLS'.
- Description:** An empty text area.
- Protocol:** Four radio buttons: 'NFS', 'iSCSI' (selected), 'FC / FCoE', and 'NVMe/FC'.

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

5. Wählen Sie auf der Seite **Speichersystem** ein Speicherfähigkeitsprofil, das Speichersystem und die VM aus.
6. Klicken Sie auf **Weiter**, um fortzufahren.

Beispiel anzeigen

The screenshot shows the 'New Datastore' wizard in vSphere, specifically the 'Storage system' tab. The left sidebar has four tabs: '1 General', '2 Storage system' (selected), '3 Storage attributes', and '4 Summary'. The main area is titled 'Storage system' and contains the following fields:

- Storage capability profiles:** A list box showing several profiles: 'AFF_Encrypted_Min50_ASA_A', 'FAS_Default', 'FAS_Max20', 'Custom profiles', and 'ASA_Gold_iSCSI' (which is selected).
- Storage system:** A dropdown menu showing 'ntaphci-a300e9u25 (172.16.9.25)'.
- Storage VM:** A dropdown menu showing 'VCF_iSCSI'.

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

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

Beispiel anzeigen

New Datastore


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

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ☒ Create new volumes ☐ Select volumes

Create new volumes

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

Name	Size(GB) ^①	Storage capability profile	Aggregates	Space reserve
f_wkld_02_vvols	3000	ASA_Gold_iSCSI	EHCaggr02 - (27053.3 GE	Thin

CANCEL
BACK
ADD
NEXT

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

Beispiel anzeigen

New Datastore

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

Summary

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: ASA_Gold_iSCSI

Storage system details

Storage system: ntaphci-a300e9u25

SVM: VCF_iSCSI

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile
vcf_wkld_02_vvols	3000 GB	EHCaggr02	ASA_Gold_iSCSI

Click 'Finish' to provision this datastore.

CANCEL
BACK
FINISH

Weitere Informationen

- Informationen zur Konfiguration von ONTAP -Speichersystemen finden Sie unter ["ONTAP 9](#)

[Dokumentation](#)" .

- Informationen zur Konfiguration von VCF finden Sie unter "[VMware Cloud Foundation-Dokumentation](#)" .
- Informationen zur Verwendung von VMFS iSCSI-Datenspeichern mit VMware finden Sie unter "[vSphere VMFS-Datenspeicher – iSCSI-Speicher-Backend mit ONTAP](#)" .
- Videodemos dieser Lösung finden Sie unter "[Bereitstellung von VMware-Datenspeichern](#)" .

Erweitern Sie VI-Workload-Domänen mit vVols NFS

Bereitstellungsworkflow zum Hinzufügen von NFS vVols Datenspeichern als zusätzlicher Speicher in einer VI-Workloaddomäne

Beginnen Sie mit dem Hinzufügen von NFS vVols Datenspeichern als zusätzlichen Speicher in VI-Workloaddomänen mithilfe von ONTAP tools for VMware vSphere. Sie überprüfen die Bereitstellungsanforderungen, stellen ONTAP tools for VMware vSphere bereit, konfigurieren die SVM mit logischen Schnittstellen und konfigurieren den Speicher.

1

"Überprüfen der Bereitstellungsanforderungen"

Überprüfen Sie die Anforderungen zum Bereitstellen von NFS- vVols in einer VMware Cloud Foundation-Verwaltungsdomäne.

2

"Erstellen Sie die SVM und LIFs"

Erstellen Sie eine SVM mit mehreren LIFs für NFS-Verkehr.

3

"Konfigurieren des Netzwerks"

Richten Sie das Netzwerk für NFS auf ESXi-Hosts ein.

4

"Konfigurieren des Speichers"

Stellen Sie ONTAP -Tools bereit und verwenden Sie sie, um den Speicher zu konfigurieren.

Bereitstellungsanforderungen für das Hinzufügen von NFS- vVols in einer VI-Workloaddomäne

Überprüfen Sie das empfohlene Netzwerkdesign und die Infrastrukturanforderungen zum Bereitstellen von NFS vVols in einer VMware Cloud Foundation VI-Workloaddomäne. Sie benötigen ein vollständig konfiguriertes ONTAP AFF oder ASA Speichersystem, eine vollständige VCF-Verwaltungsdomäne und eine vorhandene VI-Workloaddomäne.

Infrastrukturanforderungen

Stellen Sie sicher, dass die folgenden Komponenten und Konfigurationen vorhanden sind.

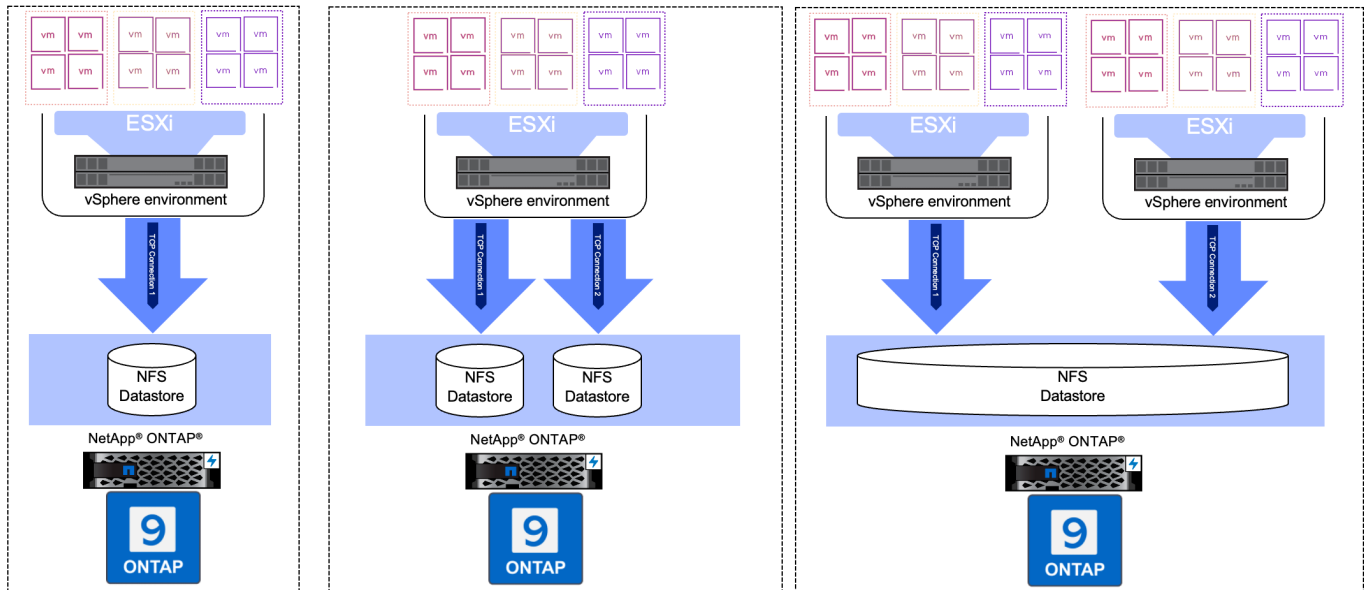
- Ein ONTAP AFF oder FAS Speichersystem mit physischen Datenports auf Ethernet-Switches, die für den Speicherverkehr vorgesehen sind.
- Die Bereitstellung der VCF-Verwaltungsdomäne ist abgeschlossen und auf den vSphere-Client kann

zugegriffen werden.

- Zuvor wurde eine VI-Workloaddomäne bereitgestellt.

Empfohlenes NFS-Netzwerkdesign

Konfigurieren Sie redundante Netzwerkdesigns für NFS, um Fehlertoleranz für Speichersysteme, Switches, Netzwerkadapter und Hostsysteme bereitzustellen. Es ist üblich, NFS je nach den Architektur Anforderungen mit einem einzelnen Subnetz oder mehreren Subnetzen bereitzustellen.



Weitere Informationen

- Ausführliche Informationen speziell zu VMware vSphere finden Sie unter ["Best Practices für die Ausführung von NFS mit VMware vSphere"](#).
- Netzwerkinweise zur Verwendung von ONTAP mit VMware vSphere finden Sie im ["Netzwerkconfiguration – 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"](#).

Wie geht es weiter?

Nach Prüfung der Anforderungen ["Erstellen Sie die SVM und LIFs"](#).

Erstellen Sie SVM und LIFs für NFS vVols Datenspeicher in einer VCF VI-Workloaddomäne

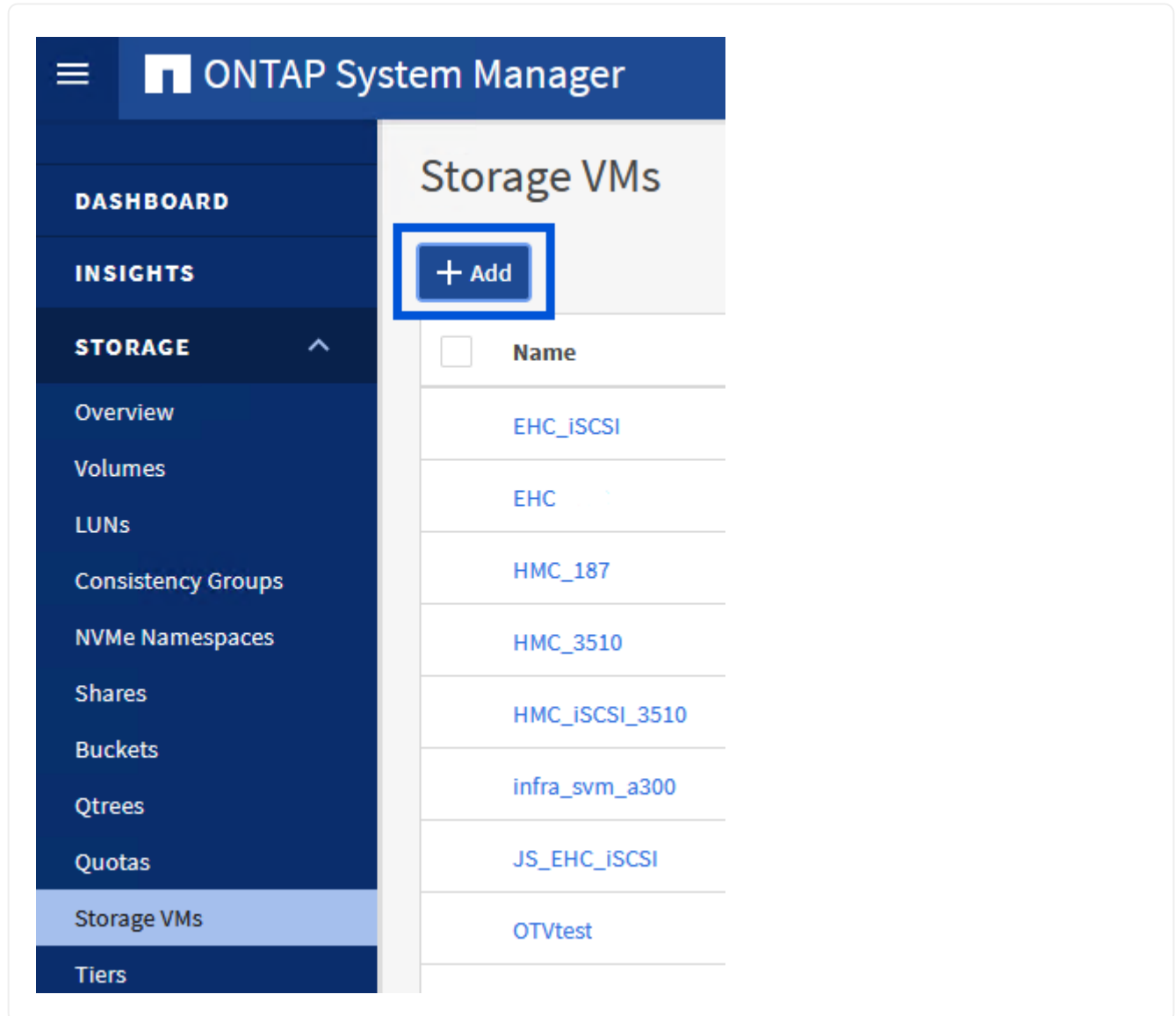
Erstellen Sie eine Storage Virtual Machine (SVM) und mehrere logische Schnittstellen (LIFs) auf einem ONTAP -System, um NFS-Datenverkehr für vVols Datenspeicher in einer VMware Cloud Foundation VI-Workloaddomäne zu unterstützen.

Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie in der ONTAP Dokumentation: ["Erstellen Sie ONTAP LIFs"](#) .

Schritte

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

Beispiel anzeigen



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**.

Beispiel anzeigen

Add Storage VM ×

STORAGE VM NAME

IPSPACE

Default ▼

Access Protocol

✓ SMB/CIFS, NFS, S3

iSCSI

FC

NVMe

☐ Enable SMB/CIFS

☒ Enable NFS

☐ Allow NFS client access

⚠ Add at least one rule to allow NFS clients to access volumes in this storage VM. ?

EXPORT POLICY

Default

☐ Enable S3

DEFAULT LANGUAGE ?

c.utf_8 ▼



Sie müssen das Kontrollkästchen **NFS-Clientzugriff zulassen** nicht aktivieren. ONTAP tools for VMware vSphere werden verwendet, um den Datastore-Bereitstellungsprozess zu automatisieren, was auch die Bereitstellung des Clientzugriffs für die ESXi-Hosts umfasst.

- Geben Sie im Abschnitt **Netzwerkschnittstelle** die **IP-Adresse**, **Subnetzmaske** und **Broadcast-Domäne und -Port** für das erste LIF ein. Für nachfolgende LIFs können Sie entweder individuelle Einstellungen verwenden oder das Kontrollkästchen aktivieren, um gemeinsame Einstellungen für alle verbleibenden LIFs zu verwenden.

Beispiel anzeigen

NETWORK INTERFACE

Use multiple network interfaces when client traffic is high.

ntaphci-a300-01

SUBNET

Without a subnet

IP ADDRESS

172.21.118.119

SUBNET MASK

24

GATEWAY

Add optional gateway

BROADCAST DOMAIN AND PORT

NFS_iSCSI

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

ntaphci-a300-02

SUBNET

Without a subnet

IP ADDRESS

172.21.118.120

PORT

a0a-3374

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

Beispiel anzeigen

Storage VM Administration

☐ Manage administrator account

Save Cancel

Wie geht es weiter?

Nach dem Erstellen der SVM und LIFs "[Konfigurieren des Netzwerks für NFS auf ESXi-Hosts](#)".

Konfigurieren Sie das Netzwerk für NFS auf ESXi-Hosts in einer VCF VI-Workloaddomäne

Konfigurieren Sie NFS-Netzwerke auf ESXi-Hosts in VMware Cloud Foundation-Verwaltungsdomänen, um die Konnektivität mit ONTAP -Speichersystemen zu

ermöglichen. Sie erstellen verteilte Portgruppen mit VLAN-Trennung, konfigurieren Uplink-Teaming für Redundanz und richten VMkernel-Adapter auf jedem ESXi-Host ein, um dedizierte NFS-Pfade für Failover-Funktionen einzurichten.

Führen Sie die folgenden Schritte auf dem VI Workload Domain-Cluster mithilfe des vSphere-Clients aus. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client in allen Verwaltungs- und Workloadomänen gleich ist.

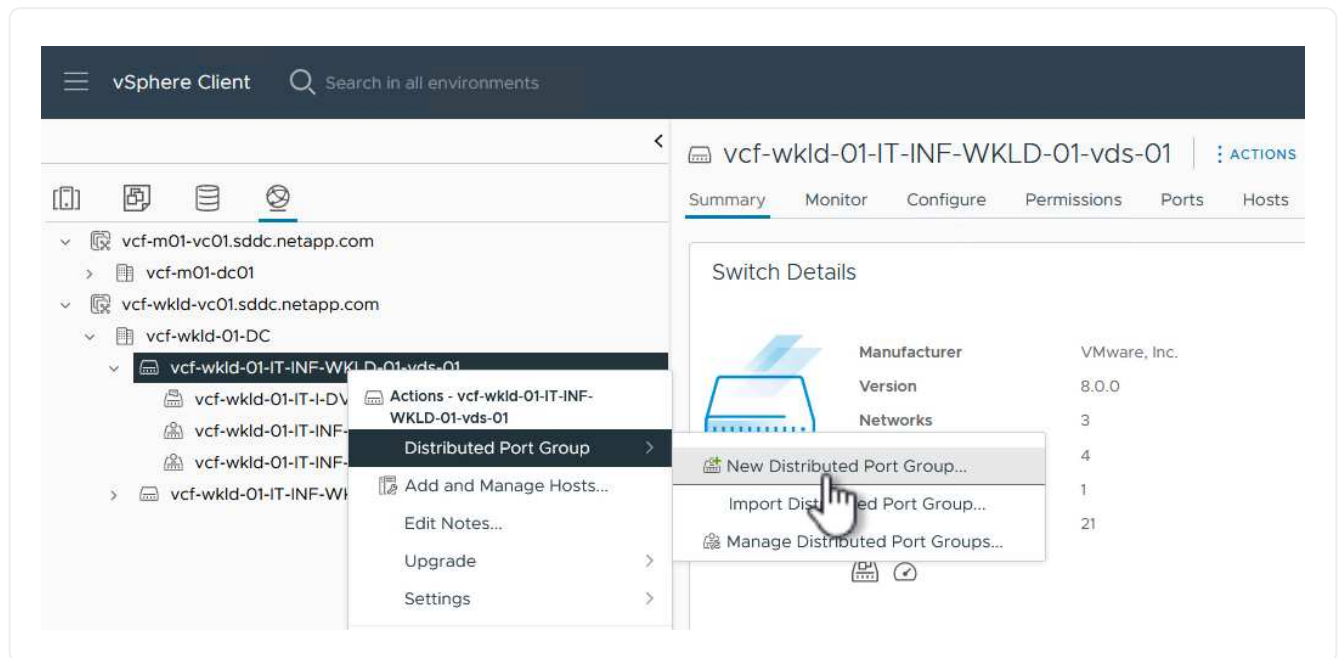
Schritt 1: Erstellen einer verteilten Portgruppe für NFS-Verkehr

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

Schritte

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

Beispiel anzeigen



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.

Beispiel anzeigen

New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

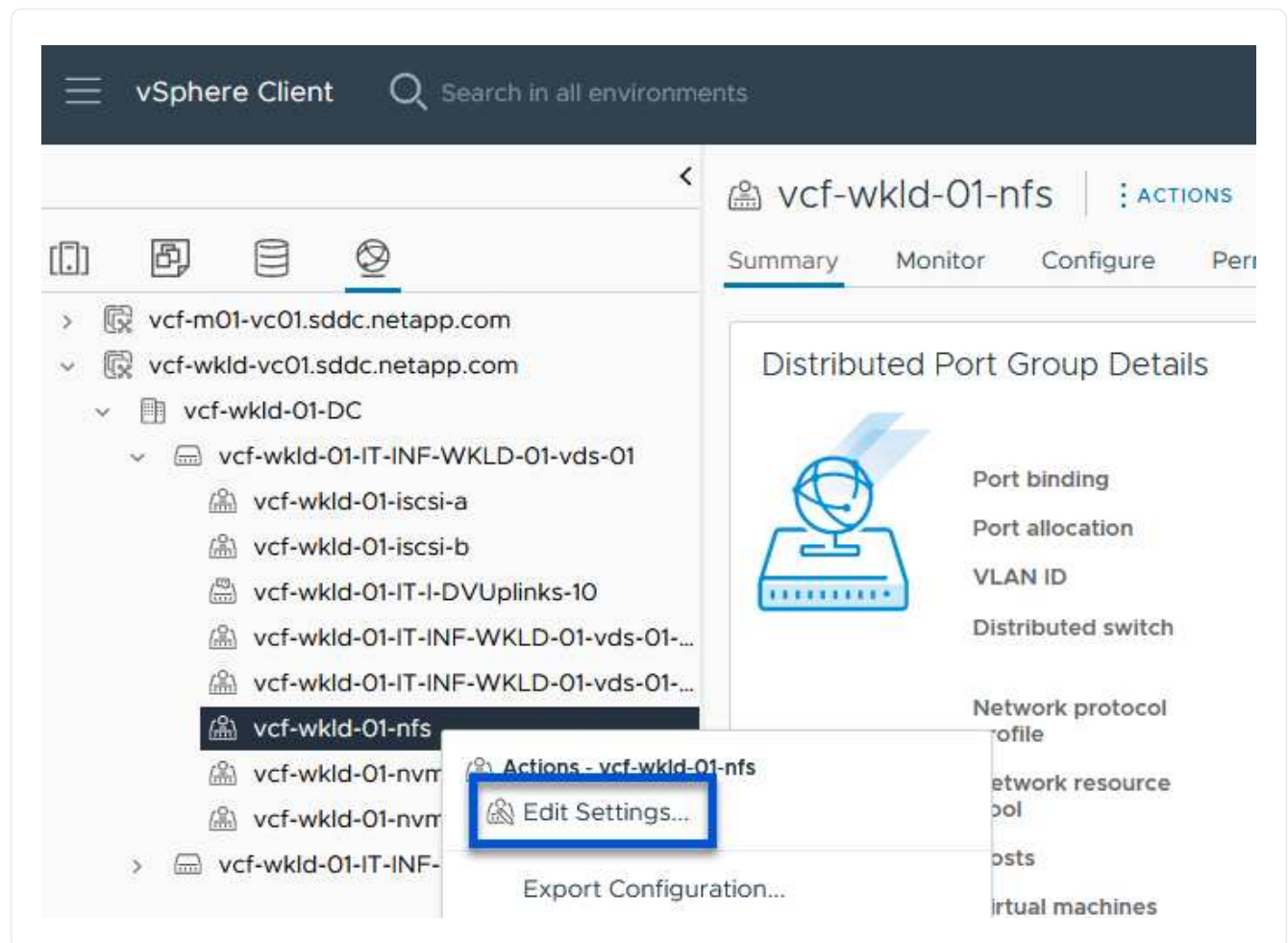
CANCEL

BACK

NEXT

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

Beispiel anzeigen



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**.

Beispiel anzeigen

Distributed Port Group - Edit Settings | vcf-wkld-01-nfs

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Failback

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

uplink1

Standby uplinks

Unused uplinks

Route based on originating virtual port

Link status only

Yes

Yes

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

Schritt 2: Erstellen Sie auf jedem ESXi-Host einen VMkernel-Adapter

Erstellen Sie auf jedem ESXi-Host in der Workload-Domäne einen VMkernel-Adapter.

Schritte

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....**

Beispiel anzeigen

vSphere Client Search in all environments

vcf-wkld-esx01.sddc.netapp.com ACTIONS

Summary Monitor Configure Permissions VMs Datastores Networks Updates

Storage

Storage Adapters

Storage Devices

Host Cache Configuration

Protocol Endpoints

I/O Filters

Networking

Virtual switches

VMkernel adapters

Physical adapters

TCP/IP configuration

VMkernel adapters

ADD NETWORKING... REFRESH

		Network Label
:	>>	vmk0 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt
:	>>	vmk1 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion
:	>>	vmk2 vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs
:	>>	vmk10 --

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select connection type

Select a connection type to create.

☒ VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

☐ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

☐ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

☒ Select an existing network

☐ Select an existing standard switch

☐ New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns 8 items

CANCEL

BACK

NEXT

4. Behalten Sie auf der Seite **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.

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically

☒ Use static IPv4 settings

IPv4 address

172.21.118.145

Subnet mask

255.255.255.0

Default gateway

☐ Override default gateway for this adapter

172.21.166.1

DNS server addresses

10.61.185.231

CANCEL

BACK

NEXT

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

Distributed port group

vcf-wkld-01-nfs

Distributed switch

vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ Port properties

New port group

vcf-wkld-01-nfs (vcf-wkld-01-IT-INF-WKLD-01-vds-01)

MTU

9000

vMotion

Disabled

Provisioning

Disabled

Fault Tolerance logging

Disabled

Management

Disabled

vSphere Replication

Disabled

vSphere Replication NFC

Disabled

vSAN

Disabled

vSAN Witness

Disabled

vSphere Backup NFC

Disabled

NVMe over TCP

Disabled

CANCEL

BACK

FINISH

Wie geht es weiter?

Nachdem Sie die Netzwerkkonfiguration für NFS auf allen ESXi-Hosts in der Workloaddomäne durchgeführt haben, "[Speicher für NFS vVols konfigurieren](#)".

Konfigurieren Sie NFS vVols Speicher in einer VCF VI-Workloaddomäne mit ONTAP -Tools

Konfigurieren Sie NFS- vVols Speicher in einer VI-Workloaddomäne. Nachdem Sie ONTAP tools for VMware vSphere bereitgestellt haben, verwenden Sie die vSphere-Clientschnittstelle, um das Speichersystem hinzuzufügen, ein Speicherfunktionsprofil zu erstellen und einen vVols Datenspeicher bereitzustellen.

Schritt 1: ONTAP tools for VMware vSphere bereitstellen

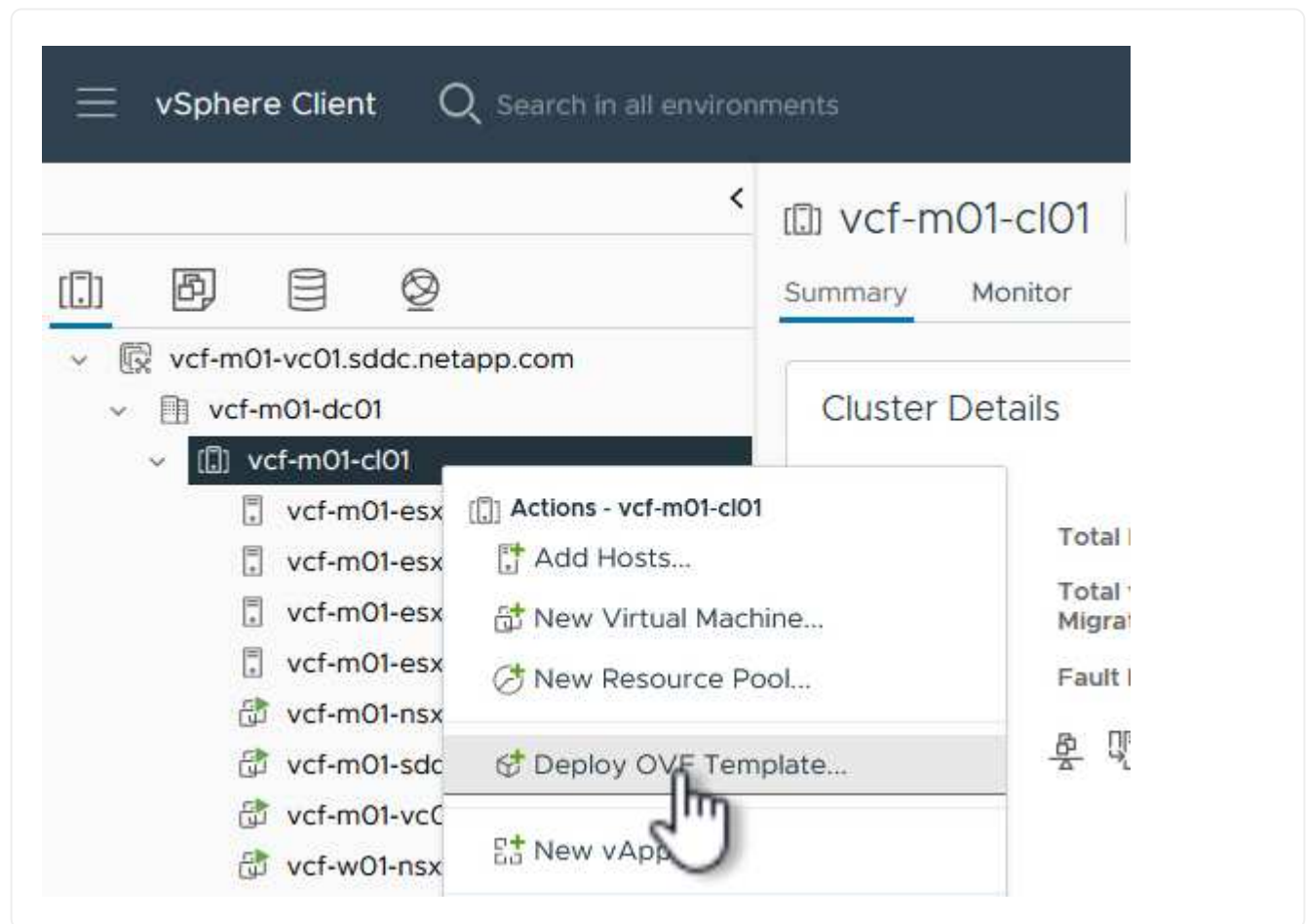
Für VI-Workloaddomänen werden ONTAP Tools im VCF-Verwaltungscluster installiert, aber beim vCenter registriert, das der VI-Workloaddomäne zugeordnet ist.

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

Schritte

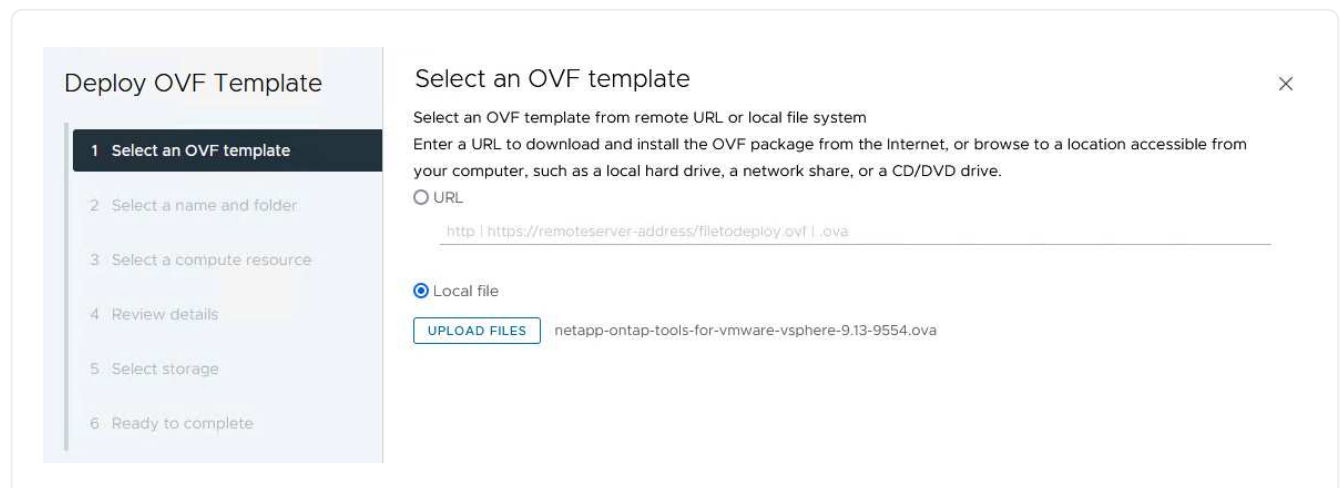
1. Beziehen Sie das OVA-Image der ONTAP -Tools von der "[NetApp Support-Site](#)" und laden Sie es in einen lokalen Ordner herunter.
2. Melden Sie sich bei der vCenter-Appliance für die VCF-Verwaltungsdomäne an.
3. Klicken Sie in der vCenter-Appliance-Schnittstelle mit der rechten Maustaste auf den Verwaltungscluster und wählen Sie **OVF-Vorlage bereitstellen...**

Beispiel anzeigen



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

Beispiel anzeigen



5. Wählen Sie in den Schritten 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.

Beispiel anzeigen

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage**
- Select networks
- Customize template
- Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine ⓘ

Select virtual disk format As defined in the VM storage policy ▾

VM Storage Policy **Datastore Default** ▾

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 5 items

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

Beispiel anzeigen

Deploy OVF Template

- Select an OVF template
- Select a name and folder
- Select a compute resource
- Review details
- License agreements
- Select storage
- Select networks**

Select networks

Select a destination network for each source network.

Source Network	Destination Network
nat	vcf-m01-cl01-vds01-pg-vsan

Manage Columns 1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4 ▾

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 Wartungskonto der ONTAP -Tools.
 - 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**

- Erforderliche Netzwerkeigenschaften.

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

Beispiel anzeigen

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration

4 settings

Application User Password (*)

Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character.

Password

Confirm Password

NTP Servers

A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.

172.21.166.1

Maintenance User Password (*)

Password to assign to maint user account.

Password

Confirm Password

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Customize template

Configure vCenter or Enable VCF

5 settings

Enable VMware Cloud Foundation (VCF)

vCenter server and user details are ignored when VCF is enabled.

vCenter Server Address (*)

Specify the IP address/hostname of an existing vCenter to register to.

cf-wkld-vc01.sddc.netapp.com

Port (*)

Specify the HTTPS port of an existing vCenter to register to.

443

Username (*)

Specify the username of an existing vCenter to register to.

administrator@vsphere.local

Password (*)

Specify the password of an existing vCenter to register to.

Password

Confirm Password

Network Properties

8 settings

Host Name

Specify the hostname for the appliance. (Leave blank if DHCP is desired)

vcf-w01-otv9

IP Address

Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL

BACK

NEXT

10. Überprüfen Sie alle Informationen auf der Seite **Bereit zum Abschließen** und klicken Sie dann auf **Fertig**, um mit der Bereitstellung der ONTAP -Tools-Appliance zu beginnen.

Schritt 2: Ein Speichersystem hinzufügen

Führen Sie die folgenden Schritte aus, um mithilfe von ONTAP -Tools ein Speichersystem hinzuzufügen.

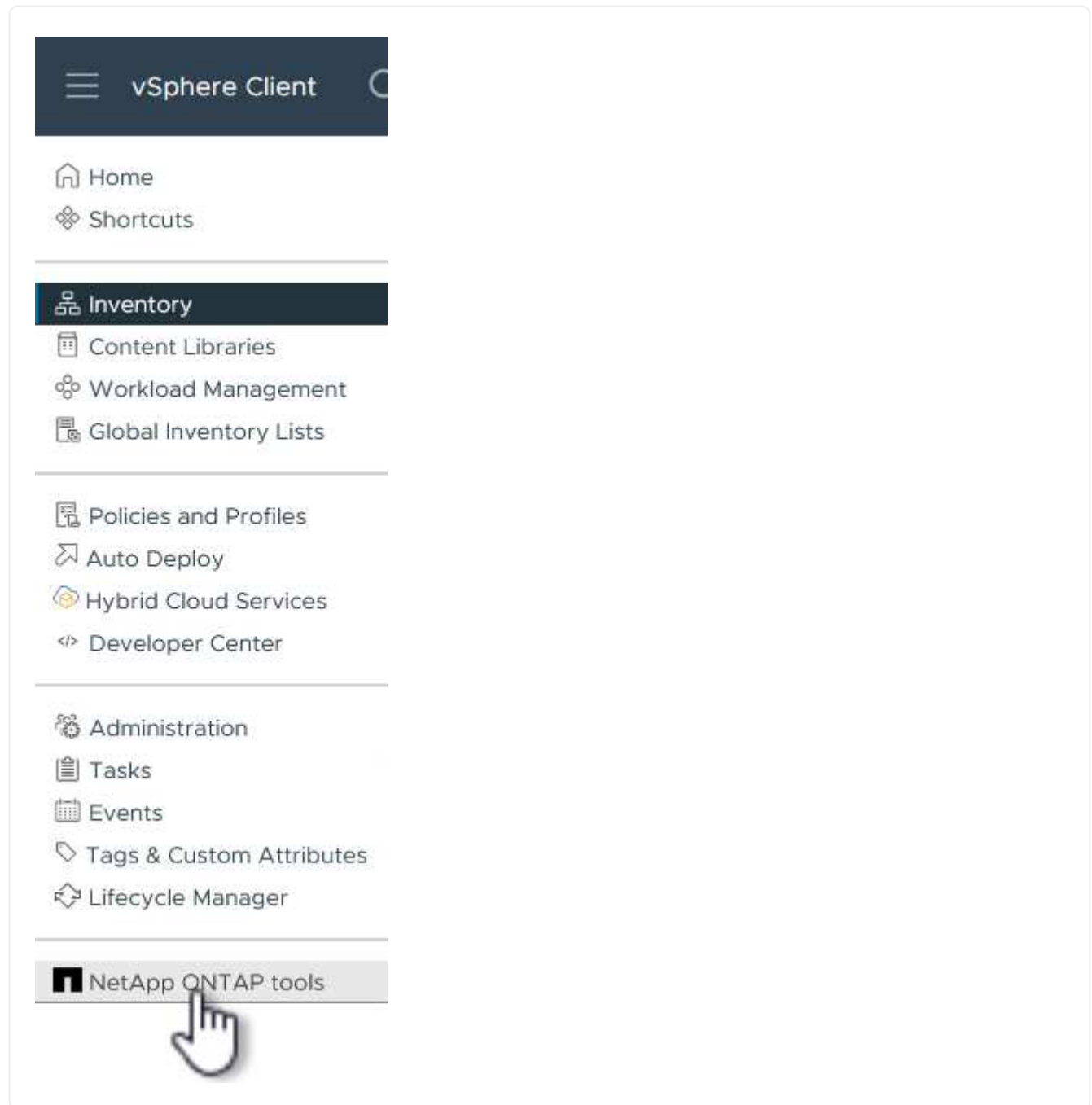


vVol erfordert ONTAP Cluster-Anmeldeinformationen anstelle von SVM-Anmeldeinformationen. Weitere Informationen finden Sie in der Dokumentation zu den ONTAP tools for VMware vSphere : "[Speichersysteme hinzufügen](#)".

Schritte

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

Beispiel anzeigen



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

Beispiel anzeigen

vSphere Client

Search in all environments

Ac

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings

▼ Reports

Datastore Report

Virtual Machine Report

vVols Datastore Report

vVols Virtual Machine Report

Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started

Traditional Dashboard

vVols Dashboard

ONTAP tools for VMware vSphere is a vCenter Server plug-in that provides end-to-end lifecycle management for virtual machines in VMware environments using NetApp storage systems.

Add Storage System

Provision Datastore

Add storage systems to ONTAP tools for VMware vSphere.

ADD

Create traditional or vVols datastores.

PROVISION

Next Steps

View Dashboard

View and monitor the datastores in ONTAP tools for VMware vSphere.

Settings

Configure administrative settings such as credentials, alarm thresholds.

What's new?

September 4, 2023

- Qualified and supported with ONTAP 9.13.1
- Supports and interoperates with VMware vSphere 8.x releases
- Includes newer enhanced SCPs that efficiently map workloads to the newer All SAN Array platforms through policy based management


Resources

- ONTAP tools for VMware vSphere Documentation Resources
- RBAC User Creator for Data ONTAP
- ONTAP tools for VMware vSphere REST API Documentation

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


130

Add Storage System

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

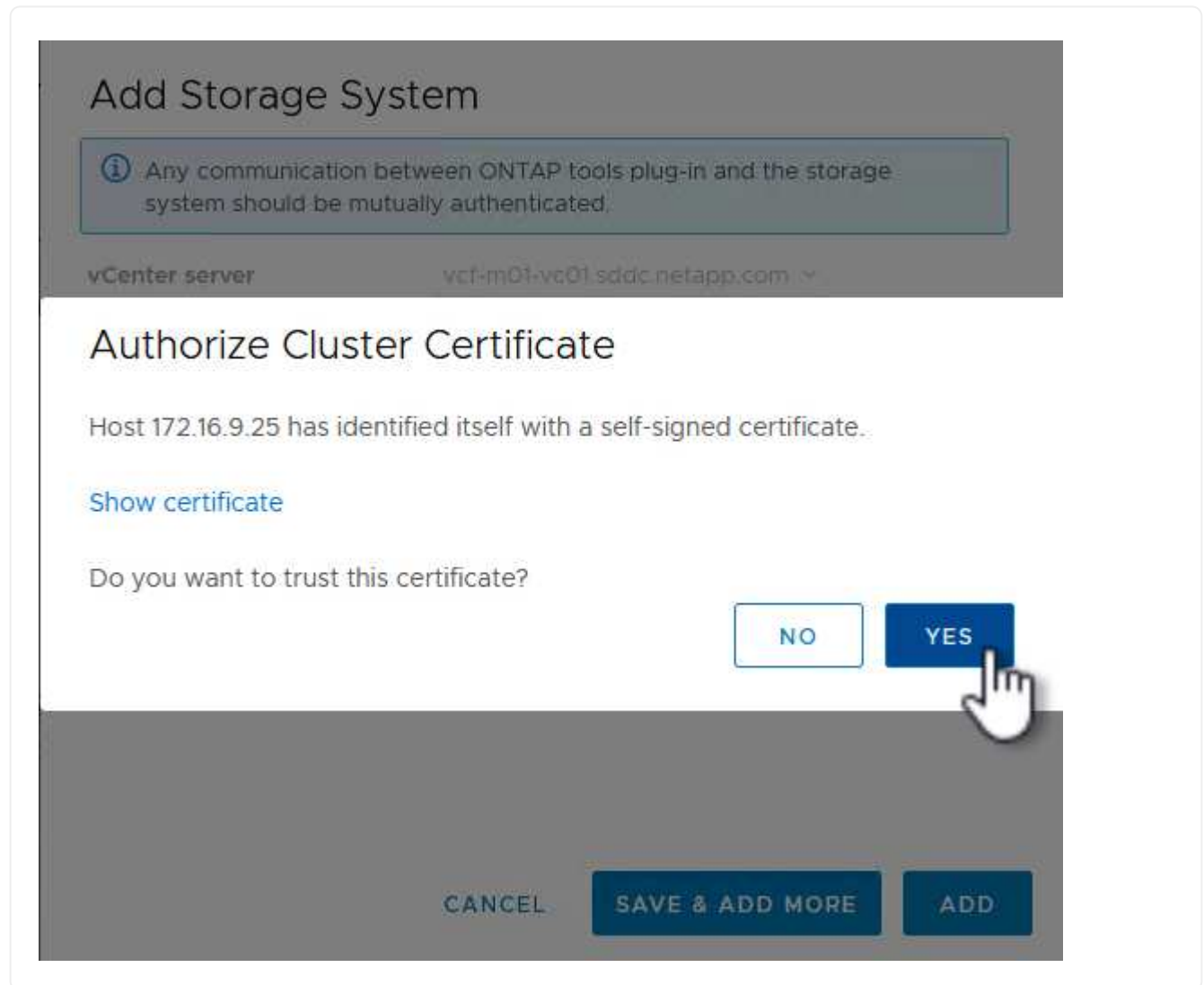
vCenter server	vcf-m01-vc01.sddc.netapp.com
Name or IP address:	172.16.9.25
Username:	admin
Password:	••••••••
Port:	443
Advanced options	>

[CANCEL](#) [SAVE & ADD MORE](#) [ADD](#)



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

Beispiel anzeigen



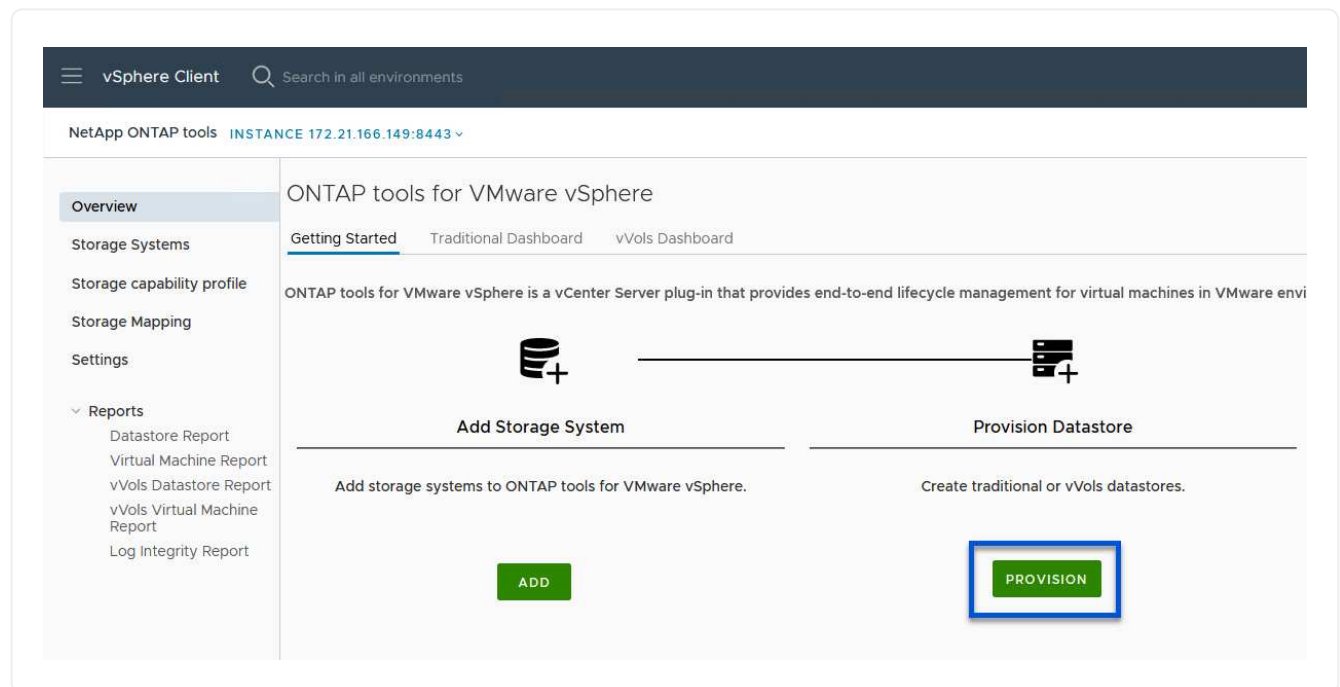
Schritt 3: Erstellen Sie einen NFS-Datenspeicher in ONTAP -Tools

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

Schritte

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

Beispiel anzeigen



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



Wenn Sie „Datastore-Daten über den Cluster verteilen“ auswählen, wird das zugrunde liegende Volume als FlexGroup -Volume erstellt, was die Verwendung von Storage Capability Profiles ausschließt. Siehe "[Unterstützte und nicht unterstützte Konfigurationen für FlexGroup -Volumes](#)" Weitere Informationen zur Verwendung von FlexGroup -Volumes.

Beispiel anzeigen

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

General

Specify the details of the datastore to provision. ⓘ

Provisioning destination:

vcf-wkld-01-DC

BROWSE

Type:

☒ NFS ☐ VMFS ☐ vVols

Name:

VCF_WKLD_05_NFS

Size:

2

TB

▼

Protocol:

☒ NFS 3 ☐ NFS 4.1

☐ Distribute datastore data across the ONTAP cluster.

☒ Use storage capability profile for provisioning

Advanced options

>

CANCEL

NEXT

6. Wählen Sie auf der Seite **Speichersystem** ein Speicherfunktionsprofil, das Speichersystem und die SVM aus. Klicken Sie auf **Weiter**, um fortzufahren.

Beispiel anzeigen

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profile:

Platinum_AFF_A

▼

Storage system:

ntaphci-a300e9u25 (172.16.9.25)

▼

Storage VM:

VCF_NFS

▼

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

Beispiel anzeigen

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Aggregate:

EHCAGgr02 - (25350.17 GB Free)

Volumes:

Automatically creates a new volume.

Advanced options

>

8. Überprüfen Sie die **Zusammenfassung** und klicken Sie auf **Fertig**, um mit der Erstellung des NFS-Datenspeichers zu beginnen.

Beispiel anzeigen

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Summary

General

vCenter server:

vcf-wkld-vc01.sddc.netapp.com

Provisioning destination:

vcf-wkld-01-DC

Datastore name:

VCF_WKLD_05_NFS

Datastore size:

2 TB

Datastore type:

NFS

Protocol:

NFS 3

Datastore cluster:

None

Storage capability profile:

Platinum_AFF_A

Storage system details

Storage system:

ntaphci-a300e9u25

SVM:

VCF_NFS

Storage attributes

Aggregate:

EHCAGgr02

CANCEL

BACK

FINISH

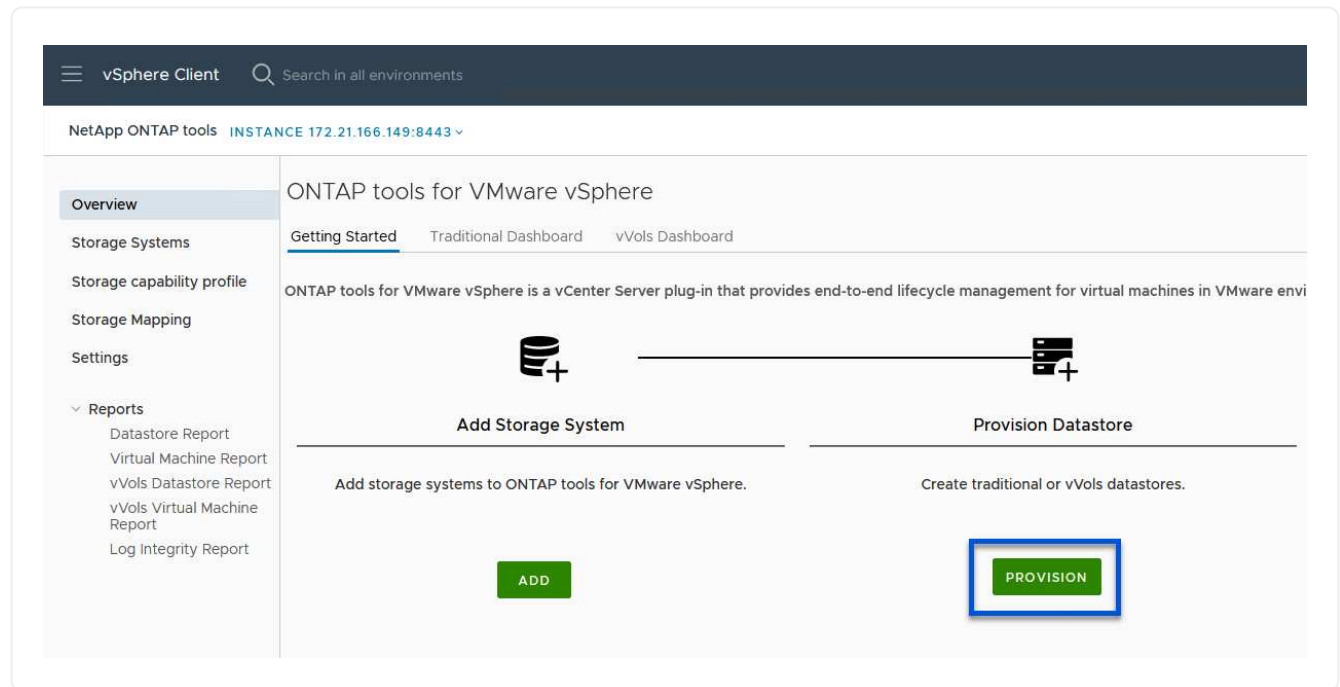
Schritt 4: Erstellen Sie einen vVols -Datenspeicher in ONTAP -Tools

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

Schritte

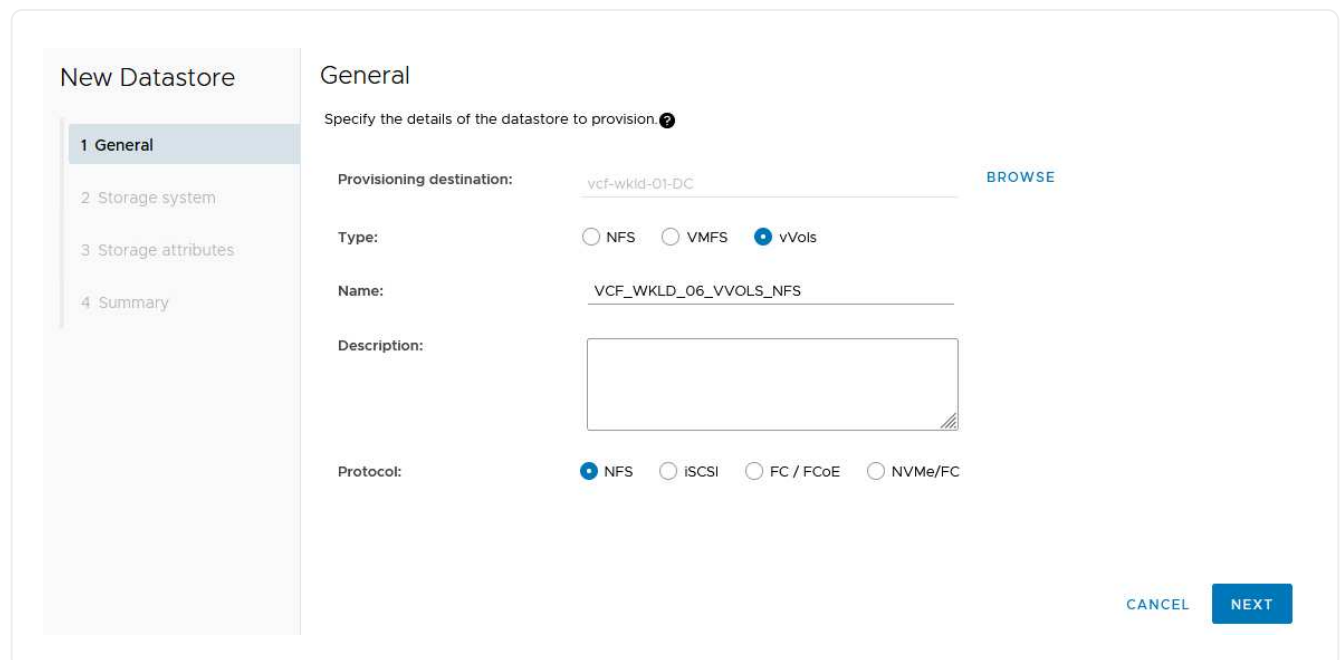
1. Wählen Sie in den ONTAP -Tools **Übersicht** aus und klicken Sie auf der Registerkarte **Erste Schritte** auf **Bereitstellung**, um den Assistenten zu starten.

Beispiel anzeigen



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

Beispiel anzeigen



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

Beispiel anzeigen

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profile:

Platinum_AFF_A

▼

Storage system:

ntaphci-a300e9u25 (172.16.9.25)

▼

Storage VM:

VCF_NFS

▼

7. Wählen Sie auf der Seite **Speicherattribute** die Option **Neues Volume erstellen** aus und geben Sie die Speicherattribute des zu erstellenden Volumes ein.

Beispiel anzeigen

Name	Size(GB) ⓘ	Storage capability profile	Aggregates	Space reserve
vcf_wkld_06_vvr	2000	Platinum_AFF_A ▼	EHCaggr02 - (25404 GB) ▼	Thin

ADD

8. Klicken Sie auf **Hinzufügen**, um das Volume zu erstellen, und dann auf **Weiter**, um fortzufahren.

Beispiel anzeigen

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ☒ Create new volumes ☐ Select volumes

Create new volumes

Name	Size	Storage Capability Profile	Aggregate
vcf_wkld_06_vvols	2000 GB	Platinum_AFF_A	EHCaggr02

1 - 1 of 1 Item

Name

Size(GB) ⓘ

Storage capability profile

Aggregates

Space reserve

Platinum_AFF_A ▼

EHCaggr02 - (25407.15 G) ▼

Thin

ADD

Default storage capability profile: Platinum_AFF_A ▼

CANCEL BACK NEXT

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

Beispiel anzeigen

New Datastore

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

Summary

General

vCenter server: vcf-wkld-vc01.sddc.netapp.com
Provisioning destination: vcf-wkld-01-DC
Datastore name: VCF_WKLD_06_VVOLS_NFS
Datastore type: vVols
Protocol: NFS
Storage capability profile: Platinum_AFF_A

Storage system details

Storage system: ntaphci-a300e9u25
SVM: EHC_NFS

Storage attributes

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL BACK FINISH

Weitere Informationen

- Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im ["ONTAP 9 Dokumentation"](#) .
- Informationen zur Konfiguration von VCF finden Sie im ["VMware Cloud Foundation-Dokumentation"](#) .
- Informationen zum Bereitstellen und Verwenden von ONTAP -Tools in mehreren vCenter-Umgebungen finden Sie im ["Voraussetzungen für die Registrierung von ONTAP Tools in mehreren vCenter-Serverumgebungen"](#) .
- Videodemos dieser Lösung finden Sie unter ["Bereitstellung von VMware-Datenspeichern"](#) .

Erweitern Sie VI-Workloaddomänen mit NVMe/TCP

Bereitstellungsworkflow zum Hinzufügen von vVols NVMe-Datenspeichern als zusätzlicher Speicher in einer VI-Workloaddomäne

Beginnen Sie mit dem Hinzufügen von NVMe/TCP vVols -Datenspeichern als zusätzlichen Speicher für eine VMware Cloud Foundation (VCF) Virtual Infrastructure (VI)-Workloaddomäne. Sie überprüfen die Bereitstellungsanforderungen, richten NVMe/TCP-fähige SVMs und LIFs ein, konfigurieren das ESXi-Host-Netzwerk und stellen den NVMe/TCP-Datenspeicher bereit.

1

"Überprüfen der Bereitstellungsanforderungen"

Überprüfen Sie die Anforderungen zum Bereitstellen eines NVMe/TCP-Datenspeichers in einer VMware Cloud Foundation VI-Workloaddomäne.

2

"Erstellen Sie die SVM und LIFs sowie den NVMe-Namespace"

Erstellen Sie eine virtuelle Speichermaschine mit logischen Schnittstellen und dem NVMe-Namespace für

3

"Konfigurieren des Netzwerks"

Erstellen Sie verteilte Portgruppen und VMkernel-Adapter auf den ESXi-Hosts für die VI-Workloaddomäne.

4

"Konfigurieren des Speichers"

Stellen Sie den NVMe/TCP-Datenspeicher bereit.

Bereitstellungsanforderungen für NVMe vVols in einer VI-Workloaddomäne

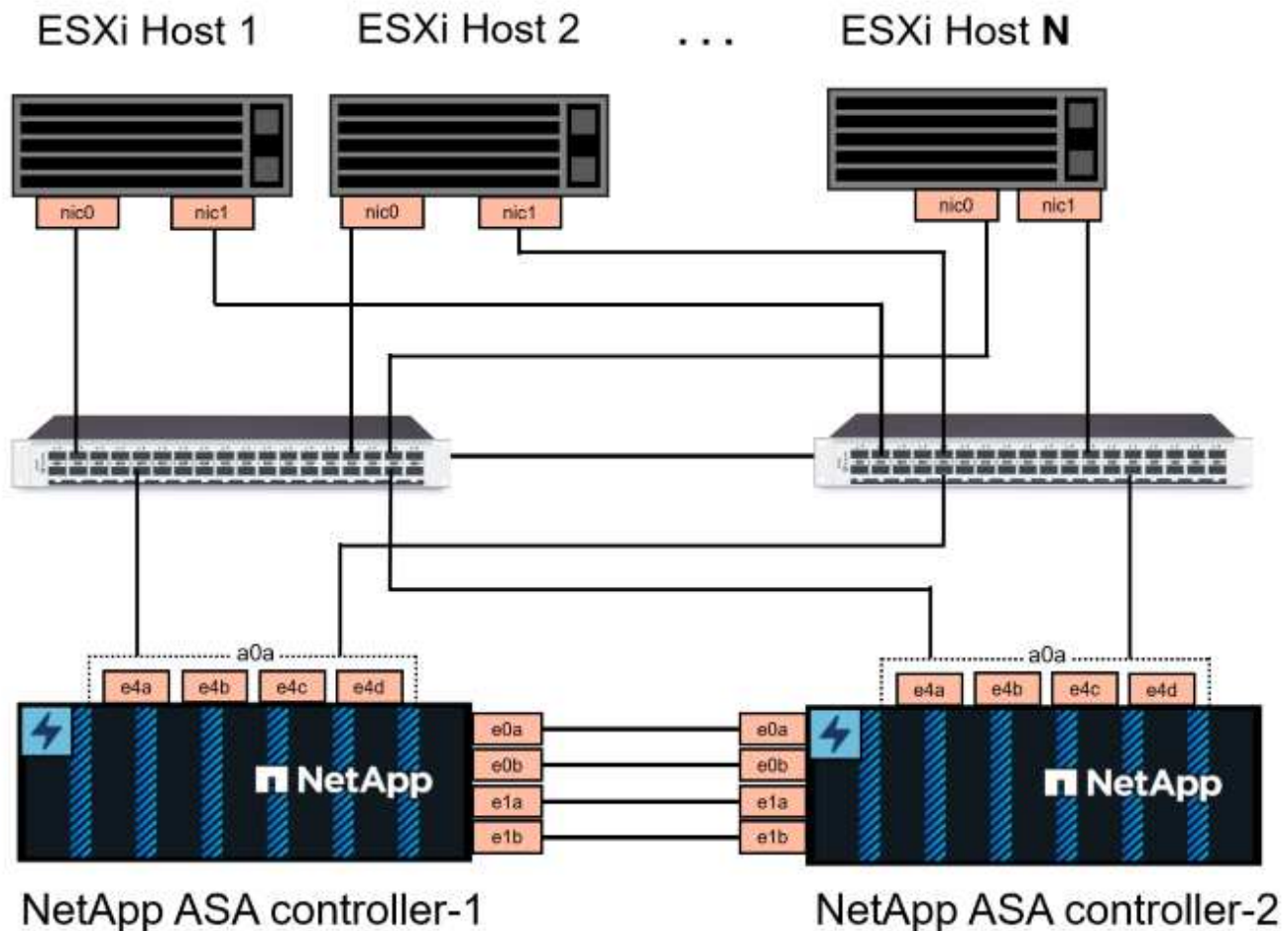
Überprüfen Sie das empfohlene Netzwerkdesign und die Infrastrukturanforderungen zum Bereitstellen von NVMe vVols in einer VMware Cloud Foundation VI-Workloaddomäne. Sie benötigen ein vollständig konfiguriertes ONTAP AFF oder ASA Speichersystem, eine bereitgestellte VCF-Verwaltungsdomäne und eine vorhandene VI-Workloaddomäne.

Infrastrukturanforderungen

- 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.

Empfohlenes NVMe/TCP-Netzwerkdesign

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.



Konfigurieren Sie für Multipathing und Failover über mehrere Pfade mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken für alle SVMs in NVMe/TCP-Konfigurationen.

Wie geht es weiter?

Nach der Überprüfung der Bereitstellungsanforderungen, ["Erstellen Sie die SVM und LIFs"](#) .

Erstellen Sie SVM und LIFs und den NVMe-Namespace für NVMe/TCP vVols Datenspeicher in einer VCF VI-Workloaddomäne

Erstellen Sie eine Storage Virtual Machine (SVM) mit mehreren logischen Schnittstellen (LIFs), um NVMe-Konnektivität für VMware Cloud Foundation-Workloaddomänen bereitzustellen. Dieses Verfahren fasst die Einrichtung eines NVMe/TCP-fähigen SVM und LIFs sowie die Erstellung der NVMe-Namespace zusammen.

Schritt 1: Erstellen der SVMs und LIFs

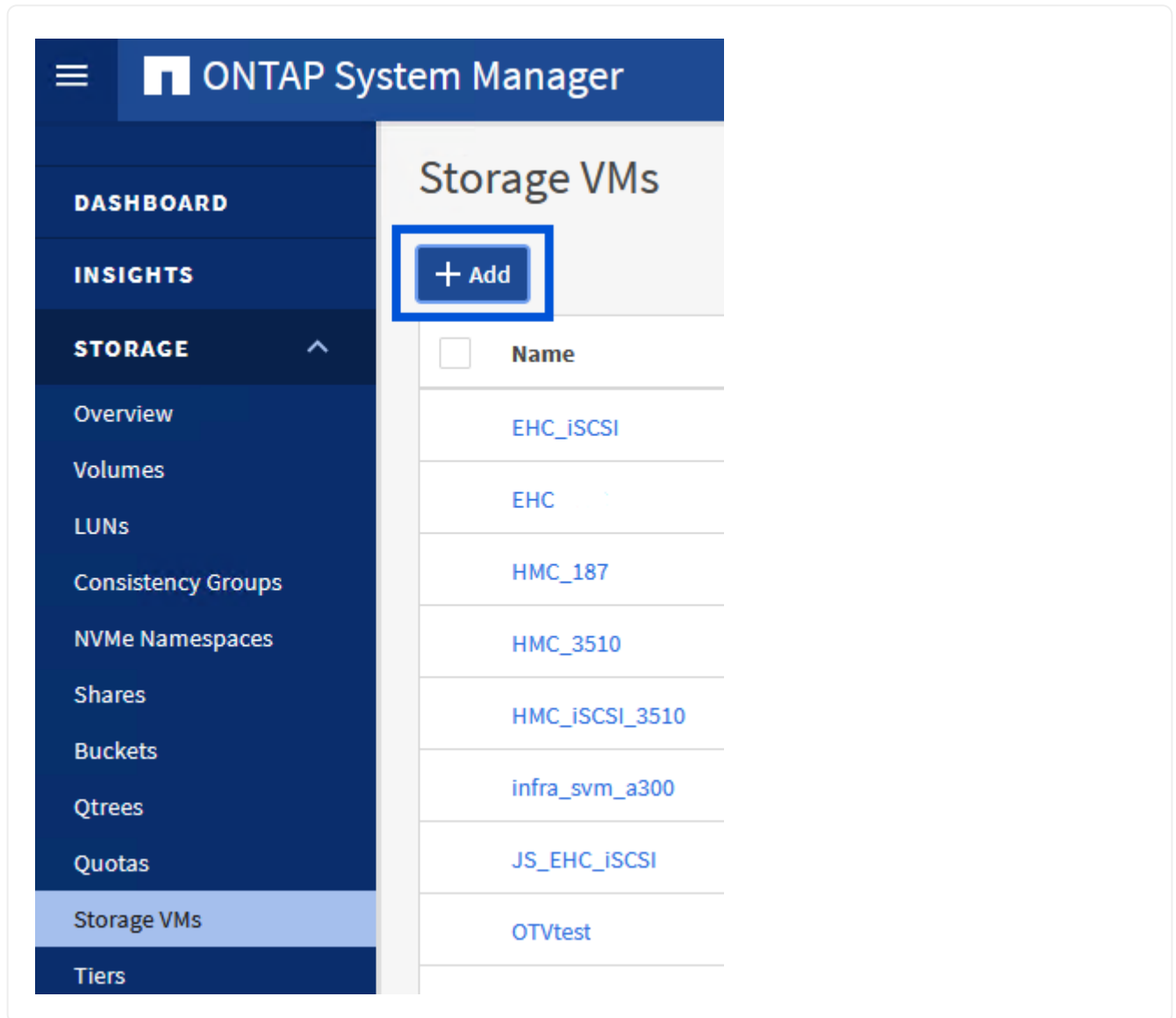
Führen Sie die folgenden Schritte aus, um eine SVM mit mehreren LIFs für NVMe/TCP-Verkehr zu erstellen.

Informationen zum Hinzufügen neuer LIFs zu einem vorhandenen SVM finden Sie in der ONTAP Dokumentation: ["Erstellen Sie ONTAP LIFs"](#) .

Schritte

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

Beispiel anzeigen



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**.

Beispiel anzeigen

Add Storage VM ×

STORAGE VM NAME

IPSPACE

Default ▼

Access Protocol

SMB/CIFS, NFS, S3 iSCSI FC ✓ NVMe

☐ Enable NVMe/FC

☒ Enable NVMe/TCP

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



Erstellen Sie für Multipathing und Failover über mehrere Pfade mindestens zwei LIFs pro Speicherknoten in separaten Ethernet-Netzwerken für alle SVMs in NVMe/TCP-Konfigurationen.

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.

Beispiel anzeigen

Storage VM Administration

☐ Manage administrator account

Save

Cancel

Schritt 2: Erstellen des NVMe-Namespace

NVMe-Namespace sind analog zu LUNs für iSCSi oder FC. Sie müssen den NVMe-Namespace erstellen, bevor ein VMFS-Datenspeicher vom vSphere-Client bereitgestellt werden kann.

Um den NVMe-Namespace zu erstellen, rufen Sie den NVMe Qualified Name (NQN) von jedem ESXi-Host im Cluster ab. ONTAP verwendet den NQN, um die Zugriffskontrolle für den Namespace bereitzustellen.

Schritte

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:

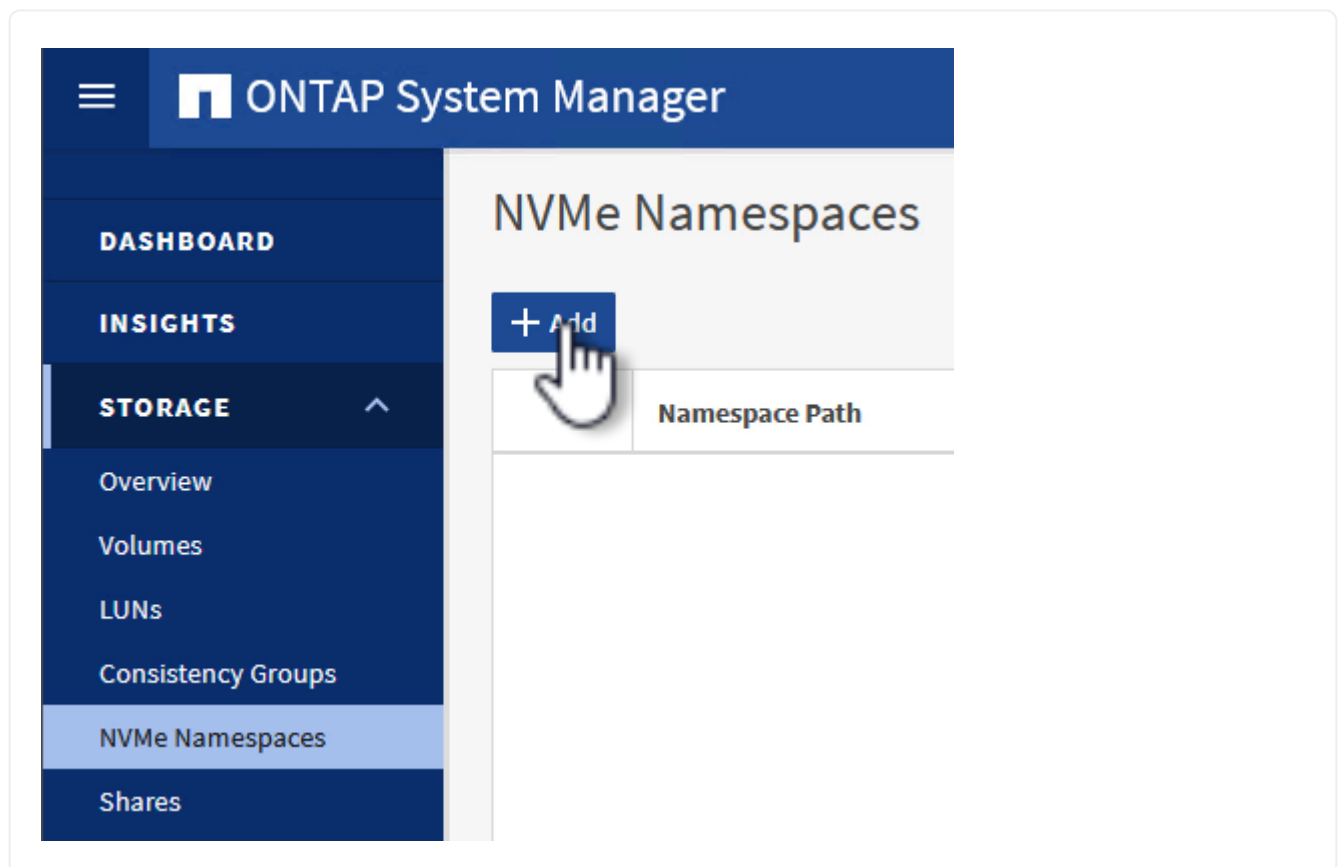
```
esxcli nvme info get
```

Es sollte eine Ausgabe ähnlich dem folgenden Beispiel 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-Namespace** und klicken Sie zum Starten auf **+ Hinzufügen**.

Beispiel anzeigen

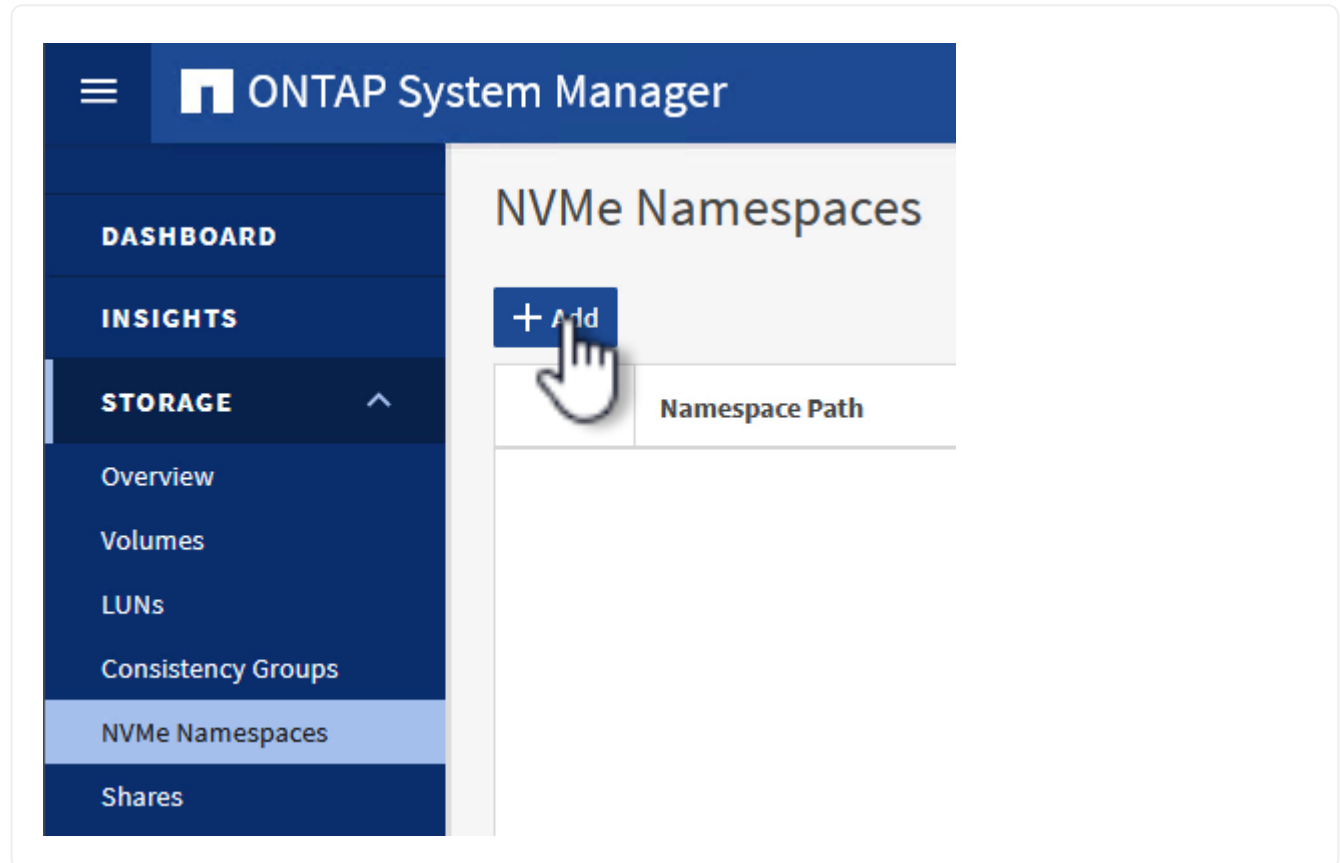


4. Geben Sie auf der Seite **NVMe-Namespace hinzufügen** ein Namenspräfix, die Anzahl der zu erstellenden

Namespaces, die Größe des Namespaces und das Host-Betriebssystem ein, das auf den Namespace zugreifen wird.

5. Erstellen Sie im Abschnitt **Host-NQN** eine durch Kommas getrennte Liste der NQNs, die zuvor von den ESXi-Hosts erfasst wurden, die auf die Namespaces zugreifen werden.
6. Klicken Sie auf **Weitere Optionen**, um zusätzliche Elemente zu konfigurieren, beispielsweise die Snapshot-Schutzrichtlinie.
7. Klicken Sie abschließend auf **Speichern**, um den NVMe-Namespace zu erstellen.

Beispiel anzeigen



Wie geht es weiter?

Nach dem Erstellen der SVM und LIFs "[Konfigurieren Sie das Netzwerk für NVMe/TCP \(NVMe/TCP\) vVols](#)".

Konfigurieren Sie das Netzwerk für NVMe/TCP auf ESXi-Hosts in einer VCF VI-Workloaddomäne

Konfigurieren Sie die Vernetzung für NVMe over TCP (NVMe/TCP)-Speicher auf ESXi-Hosts in einer VI-Workloaddomäne. Sie erstellen verteilte Portgruppen für NVMe-Verkehr, richten VMkernel-Adapter auf jedem ESXi-Host ein und fügen einen NVMe/TCP-Adapter hinzu, um zuverlässige Konnektivität und Multipathing zu ermöglichen.

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

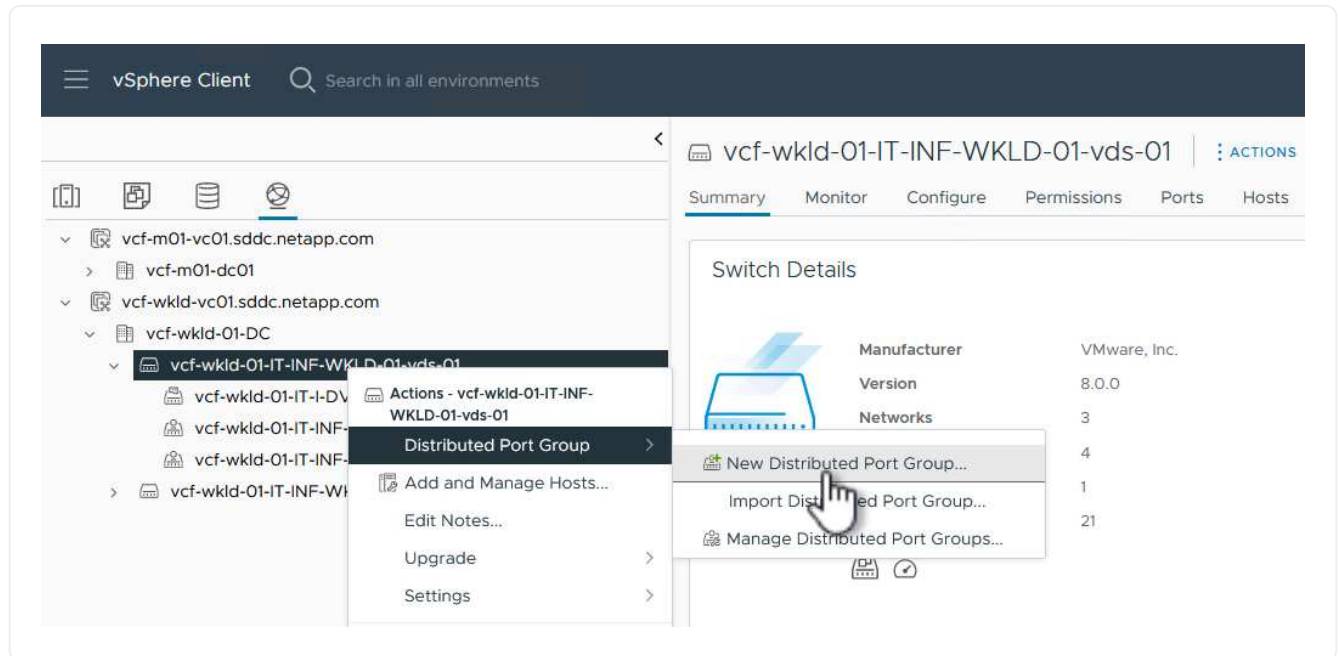
Schritt 1: Erstellen Sie verteilte Portgruppen für NVME/TCP-Verkehr

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

Schritte

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...**

Beispiel anzeigen



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.

Beispiel anzeigen

New Distributed Port Group

1 Name and location

2 Configure settings

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

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

Beispiel anzeigen

The screenshot displays the vSphere Client interface. The top navigation bar shows 'vSphere Client' and a search bar. The left sidebar contains a tree view of the environment, with 'vcf-wkld-01-nvme-a' selected. The right pane shows the 'Distributed Port Group Details' for 'vcf-wkld-01-nvme-a'. The details include a summary table and a list of actions.

Distributed Port Group Details	
Port binding	Static
Port allocation	Elastic
VLAN ID	3374
Distributed switch	VC WKLD
Network protocol profile	--
Network resource pool	--
Hosts	4
Virtual machines	0

Actions for vcf-wkld-01-nvme-a:

- Actions - vcf-wkld-01-nvme-a
- Edit Settings...
- Export Configuration...
- Restore Configuration...

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.

Beispiel anzeigen

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-a

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

uplink1

Standby uplinks

Unused uplinks

uplink2

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

Beispiel anzeigen

Distributed Port Group - Edit Settings | vcf-wkld-01-nvme-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Network failure detection

Notify switches

Failback

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

Unused uplinks

uplink1

Route based on originating virtual port

Link status only

Yes

Yes

Schritt 2: Erstellen Sie die VMkernel-Adapter auf jedem ESXi-Host

Erstellen Sie die VMkernel-Adapter auf jedem ESXi-Host in der Workload-Domäne.

Schritte

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....**

Beispiel anzeigen

vSphere Client

vcf-wkld-esx01.sddc.netapp.com

Summary

Monitor

Configure

Permissions

VMs

Datastores

Networks

Updates

vcf-m01-vc01.sddc.netapp.com

vcf-m01-dc01

vcf-wkld-vc01.sddc.netapp.com

vcf-wkld-01-DC

IT-INF-WKLD-01

vcf-wkld-esx01.sddc.netapp.com

vcf-wkld-esx02.sddc.netapp.com

vcf-wkld-esx03.sddc.netapp.com

vcf-wkld-esx04.sddc.netapp.com

vcf-w01-otv9

Storage

Storage Adapters

Storage Devices

Host Cache Configuration

Protocol Endpoints

I/O Filters

Networking

Virtual switches

VMkernel adapters

Physical adapters

TCP/IP configuration

VMkernel adapters

ADD NETWORKING... REFRESH

		Network Label
vmk0	vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-mgmt	
vmk1	vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-vmotion	
vmk2	vcf-wkld-01-IT-INF-WKLD-01-vd s-01-pg-nfs	
vmk10	--	

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select connection type

Select a connection type to create.

☒ VMkernel Network Adapter

The VMkernel TCP/IP stack handles traffic for ESXi services such as vSphere vMotion, iSCSI, NFS, FCoE, Fault Tolerance, vSAN, host management and etc.

☐ Virtual Machine Port Group for a Standard Switch

A port group handles the virtual machine traffic on standard switch.

☐ Physical Network Adapter

A physical network adapter handles the network traffic to other hosts on the network.

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

☒ Select an existing network

☐ Select an existing standard switch

☐ New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01

Manage Columns

7 items

CANCEL

BACK

NEXT

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

Beispiel anzeigen

The screenshot shows the 'Add Networking' wizard with five steps: 1. Select connection type, 2. Select target device, 3. Port properties (active), 4. IPv4 settings, and 5. Ready to complete. The 'Port properties' section is titled 'Specify VMkernel port settings.' and includes the following fields: 'Network label' (vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)), 'MTU' (Get MTU from switch, 9000), and 'TCP/IP stack' (Default). Below these is the 'Available services' section with a list of services: vMotion, Provisioning, Fault Tolerance logging, Management, vSphere Replication, vSphere Replication NFC, vSAN, vSAN Witness, vSphere Backup NFC, NVMe over RDMA, and NVMe over TCP. The 'NVMe over TCP' checkbox is checked. At the bottom right, there are three buttons: 'CANCEL', 'BACK', and 'NEXT'. A mouse cursor is clicking the 'NEXT' button.

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.

Beispiel anzeigen

The screenshot shows the 'Add Networking' wizard with five steps: 1. Select connection type, 2. Select target device, 3. Port properties, 4. IPv4 settings (active), and 5. Ready to complete. The 'IPv4 settings' section is titled 'Specify VMkernel IPv4 settings.' and includes the following options: 'Obtain IPv4 settings automatically' (radio button), 'Use static IPv4 settings' (radio button, selected), 'IPv4 address' (172.21.118.191), 'Subnet mask' (255.255.255.0), 'Default gateway' (checkbox 'Override default gateway for this adapter' is unchecked, and the IP address 172.21.166.1 is entered), and 'DNS server addresses' (10.61.185.231).

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

Beispiel anzeigen

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 **Ready to complete**

Ready to complete ×

Review your selections before finishing the wizard

▼ **Select target device**

Distributed port group	vcf-wkld-01-nvme-a
Distributed switch	vcf-wkld-01-IT-INF-WKLD-01-vds-01

▼ **Port properties**

New port group	vcf-wkld-01-nvme-a (vcf-wkld-01-IT-INF-WKLD-01-vds-01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Enabled
NVMe over RDMA	Disabled

▼ **IPv4 settings**

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

CANCEL BACK **FINISH**

Packages

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

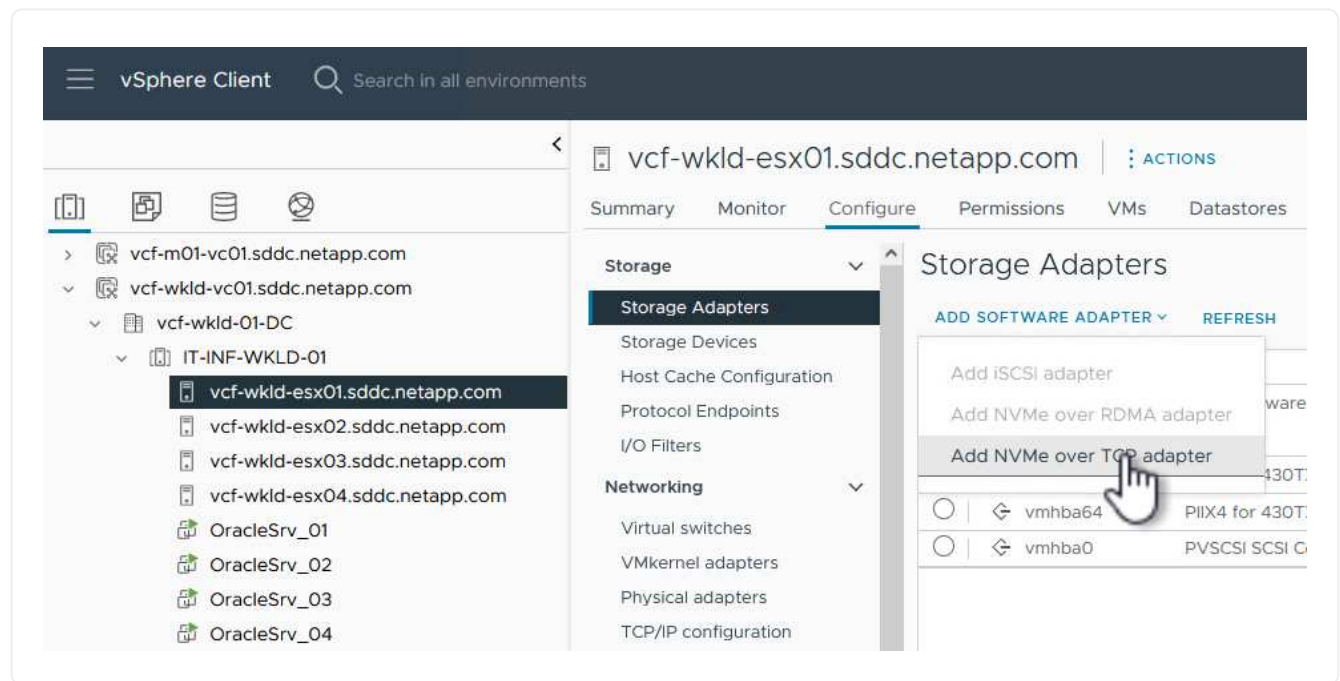
Schritt 3: NVMe/TCP-Adapter hinzufügen

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

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

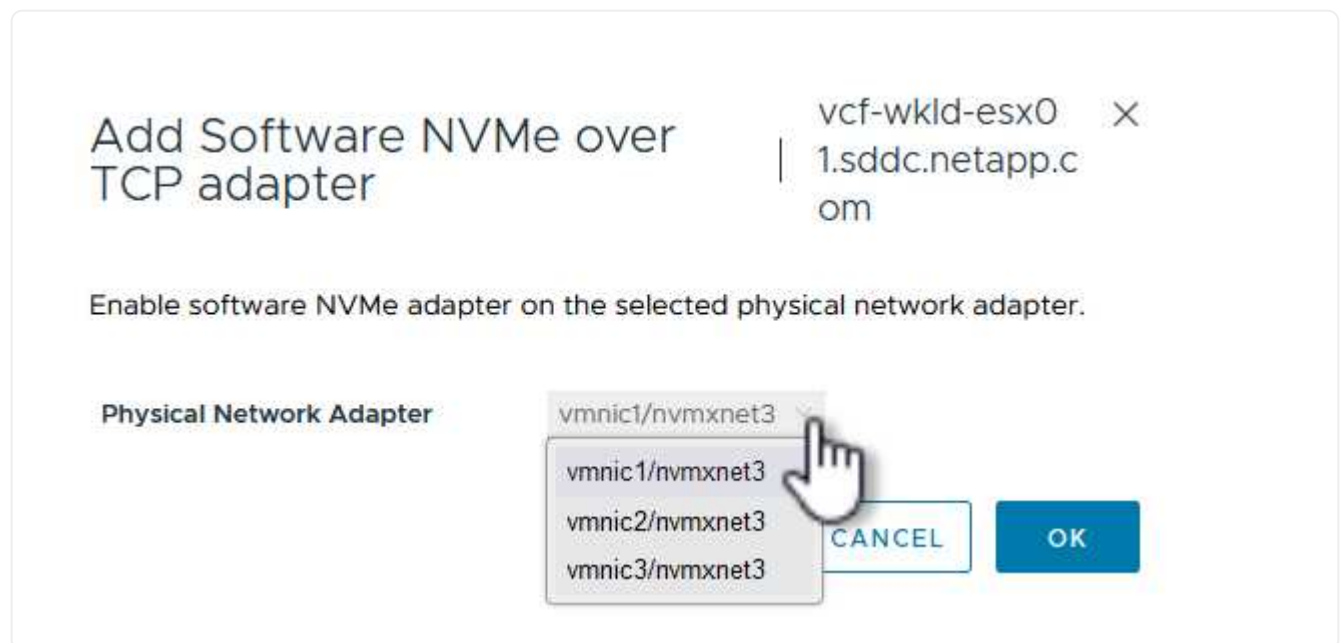
1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Klicken Sie auf der Registerkarte **Konfigurieren** im Menü auf **Speicheradapter**.
2. Wählen Sie im Dropdown-Menü **Softwareadapter hinzufügen** die Option **NVMe over TCP-Adapter hinzufügen**.

Beispiel anzeigen



3. 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.

Beispiel anzeigen



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

Beispiel anzeigen

The screenshot shows the vSphere Client interface. The left-hand navigation pane displays a tree view of the environment, with the host **vcf-wkld-esx01.sddc.netapp.com** selected. The main pane shows the configuration for this host, with the **Storage** tab selected. Under **Storage**, the **Storage Adapters** sub-tab is active. A table lists the storage adapters:

Adapter	Model	Type
vmhba65	iSCSI Software Adapter	iSCSI
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI
vmhba0	PVSCSI SCSI Controller	SCSI
vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP
vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP

Below the table, the **ADD CONTROLLER** button is highlighted with a mouse cursor. The interface also shows a top navigation bar with tabs for Summary, Monitor, Configure, Permissions, VMs, Datastores, Networks, and Updates.

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

Beispiel anzeigen

Add controller | vmhba68

Automatically | Manually

Host NQN

nqn.2014-08.com.netapp.sddc:nvme:vcf-wkld-...

COPY

IP

172.21.118.189

Enter IPv4 / IPv6 address

☐ Central discovery controller

Port Number

Range more from 0

Digest parameter

☐ Header digest

☐ Data digest

DISCOVER CONTROLLERS

Select which controller to connect

<input type="checkbox"/>	Id	Subsystem NQN	Transport Type	IP	Port Number
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF_WKLD_04_NVMe_VCF_WKLD_04_NVMe	nvm	172.21.118.189	4420
<input checked="" type="checkbox"/>	65535	nqn.1992-08.com.netapp:sn.64df3069fb6411eea55100a098b46a21:subsystem.VCF	nvm	172.21.118.190	4420

Manage Columns

4 items

OK

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

Beispiel anzeigen

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

	Adapter ▾	Model ▾	Type ▾	Status ▾	Identifier ▾	Targets ▾	Devices ▾	Paths ▾
<input type="radio"/>	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(ign.1998-01.com.vmw:warevcf-wkld-esx01.sddc.net:app.com:794177624:65)	4	2	8
<input type="radio"/>	vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
<input type="radio"/>	vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
<input type="radio"/>	vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
<input checked="" type="radio"/>	vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
<input type="radio"/>	vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

Manage Columns Export ▾ 6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

<input type="checkbox"/>	Name ▾	LUN ▾	Type ▾	Capacity ▾	Datastore ▾	Operational State ▾	Hardware Acceleration ▾	Drive Type ▾	Transport
<input type="checkbox"/>	NVMe TCP Disk (uuid:929a6a90457647849146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTNAN RT

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

Wie geht es weiter?

Nach der Netzwerkkonfiguration "[Speicher für NVMe vVols konfigurieren](#)".

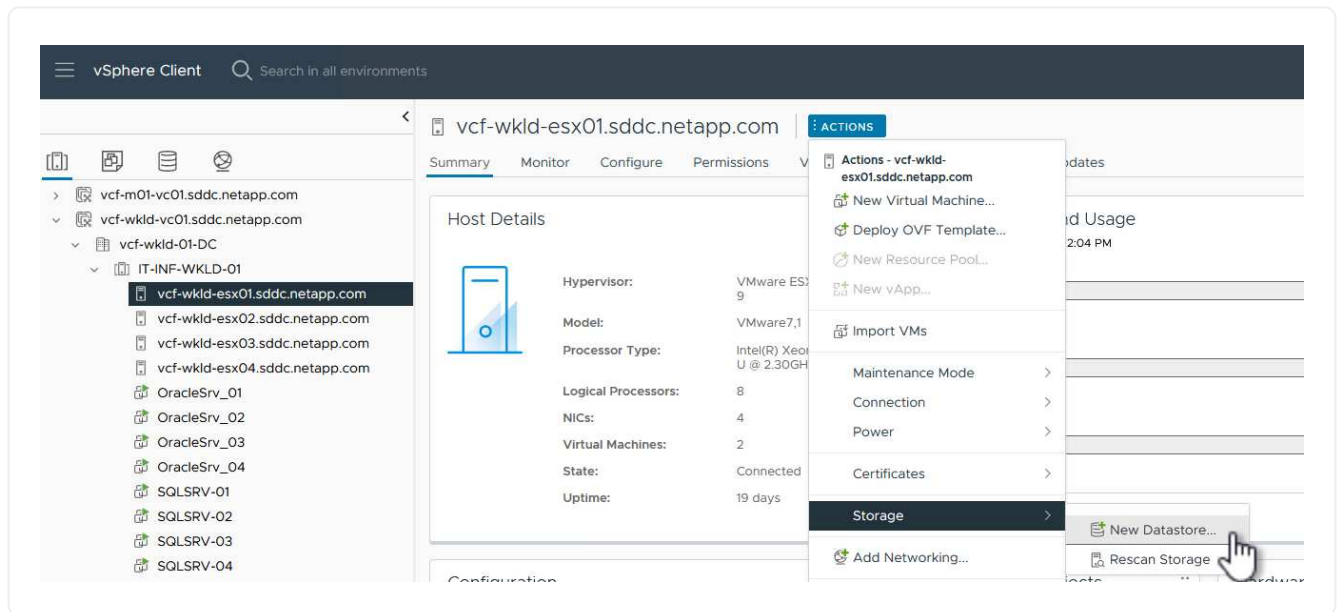
Konfigurieren Sie den NVMe/TCP vVols -Speicher in einer VCF VI-Workloaddomäne

Konfigurieren Sie NVMe/TCP vVols -Speicher in einer VMware Cloud Foundation VI-Workloaddomäne. Sie stellen ONTAP Tools bereit, registrieren ein Speichersystem, erstellen ein Speicherfähigkeitsprofil und stellen einen vVols Datenspeicher im vSphere-Client bereit.

Schritte

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

Beispiel anzeigen



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.

Beispiel anzeigen

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection

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

Name

VCF_WKLD_04_NVMe

	Name	LUN	Capacity	Hardware Acceleration	Drive Type	Sector Format	Cl V St
<input checked="" type="radio"/>	NVMe TCP Disk (uuid.929a6a90457647849146e09d6e55b076)	0	3.00 TB	Supported	Flash	512e	N
<input type="radio"/>	Local VMware Disk (naa.6000c29f83dcf1e42d230340deb66036)	0	4.00 GB	Not supported	Flash	512n	N
<input type="radio"/>	Local VMware Disk (naa.6000c291464644a835bc23d384813ac0)	0	75.00 GB	Not supported	Flash	512n	N

Manage Columns

Export

3 items

CANCEL

BACK

NEXT

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

Beispiel anzeigen

New Datastore

- 1 Type
- 2 Name and device selection
- 3 VMFS version
- 4 Partition configuration**
- 5 Ready to complete

Partition configuration

Review the disk layout and specify partition configuration details.

Partition Configuration Use all available partitions ▾

Datastore Size 3072 GB

Block size 1 MB ▾

Space Reclamation Granularity 1 MB ▾

Space Reclamation Priority Low ▾

Empty: 3.0 TB

Free Space: 3TB
Usage on selected partition: 3TB

CANCEL BACK **NEXT**

- Überprüfen Sie auf der Seite **Bereit zum Abschließen** die Zusammenfassung und klicken Sie auf **Fertig**, um den Datenspeicher zu erstellen.
- 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.

Beispiel anzeigen

vSphere Client

Search in all environments

Administrator@VCF.LOCAL

VCF_WKLD_04_NVMe

ACTIONS

Summary Monitor Configure Permissions Files **Hosts** VMs

Quick Filter Enter value

	Name	State	Status	Cluster	Consumed CPU %	Consumed Memory %	HA State	Uptime
<input type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-Q 1	15%	13%	✓ Connected (Secondary)	19 days
<input type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-Q 1	9%	15%	✓ Running (Primary)	19 days
<input type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-Q 1	9%	21%	✓ Connected (Secondary)	19 days
<input type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-Q 1	11%	4%	✓ Connected (Secondary)	19 days

Weitere Informationen

- Weitere Informationen zur Konfiguration von SAN für Redundanz finden Sie im ["NetApp SAN-Konfigurationsreferenz"](#) .
- Weitere Informationen zu NVMe-Designüberlegungen für ONTAP Speichersysteme finden Sie unter ["NVMe-Konfiguration, -Unterstützung und -Einschränkungen"](#) .
- Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im ["ONTAP 9 Dokumentation"](#) .
- Informationen zur Konfiguration von VCF finden Sie im ["VMware Cloud Foundation-Dokumentation"](#) .

Fügen Sie einen FC-basierten VMFS-Datenspeicher als zusätzlichen Speicher zu einer VI-Workload-Domäne 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)-Workload-Domäne. 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.

Bevor Sie beginnen

Stellen Sie sicher, dass die folgenden Komponenten und Konfigurationen vorhanden sind.

- Ein ONTAP AFF oder ASA Speichersystem mit FC-Ports, die mit FC-Switches verbunden sind.
- Mit FC-LIFs erstellte SVM.
- 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.
- Verwenden Sie Multipath für FC-LUNs.

Schritte

1. Registrieren Sie das VI-Workload-vCenter, indem Sie den Anweisungen in der Dokumentation zu den ONTAP tools for VMware vSphere folgen: ["VI-Workload vCenter registrieren"](#) .

Durch die Registrierung des VI-Workload-vCenter wird das vCenter-Plugin aktiviert.

2. Fügen Sie mithilfe der vSphere-Clientschnittstelle ein Speicher-Backend hinzu, indem Sie den Anweisungen in der Dokumentation zu den ONTAP tools for VMware vSphere folgen: ["Definieren Sie das Speicher-Backend mithilfe der vSphere-Clientschnittstelle"](#) .

Durch Hinzufügen eines Speicher-Backends können Sie einen ONTAP Cluster integrieren.

3. Stellen Sie VMFS auf Fibre Channel (FC) bereit, indem Sie den Anweisungen in der Dokumentation zu den ONTAP tools for VMware vSphere folgen: ["Bereitstellen von VMFS auf FC"](#) .

Weitere Informationen

- Informationen zur Konfiguration von ONTAP Speichersystemen finden Sie im ["ONTAP 9 Dokumentation"](#) .

- Informationen zur Konfiguration von VCF finden Sie im ["VMware Cloud Foundation-Dokumentation"](#) .
- Informationen zur Konfiguration von Fibre Channel auf ONTAP Speichersystemen finden Sie im ["SAN-Speicherverwaltung"](#) in der ONTAP 9-Dokumentation.
- Informationen zur Verwendung von VMFS mit ONTAP Speichersystemen finden Sie im ["Bereitstellungshandbuch für VMFS"](#) .
- Videodemos dieser Lösung finden Sie unter ["Bereitstellung von VMware-Datenspeichern"](#) .

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"](#)

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

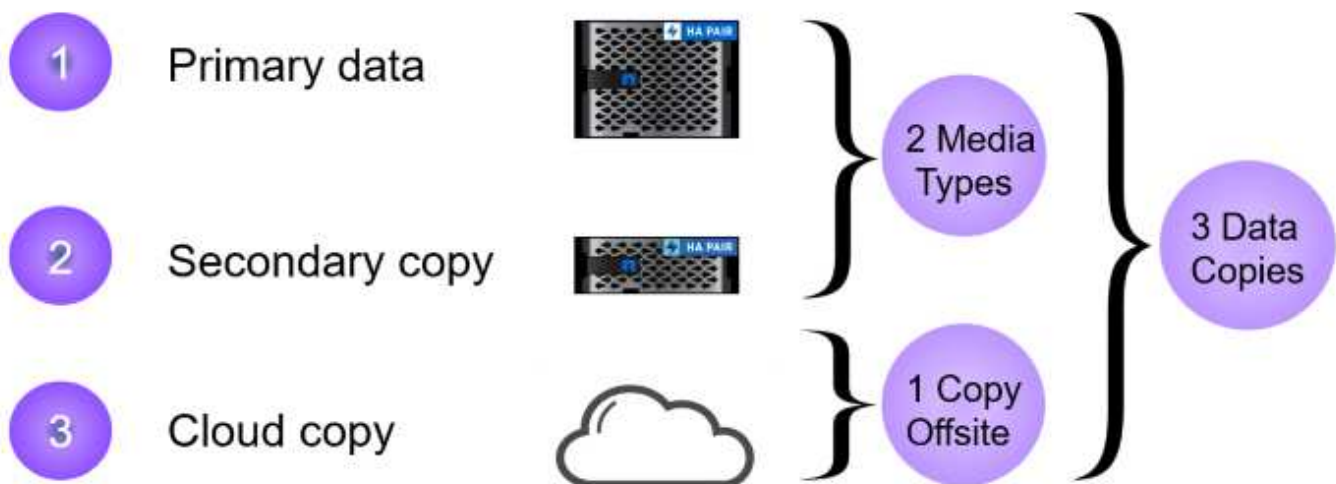
Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- 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 Sekundärspeicher können mit NetApp Backup and Recovery for VMs auch Offsite-Kopien von Daten auf Objektspeicher bei einem der drei (3) führenden Cloud-Anbieter erstellt werden. Weitere Informationen finden Sie in diesem Angebot. ["NetApp Backup and Recovery"](#) Die



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

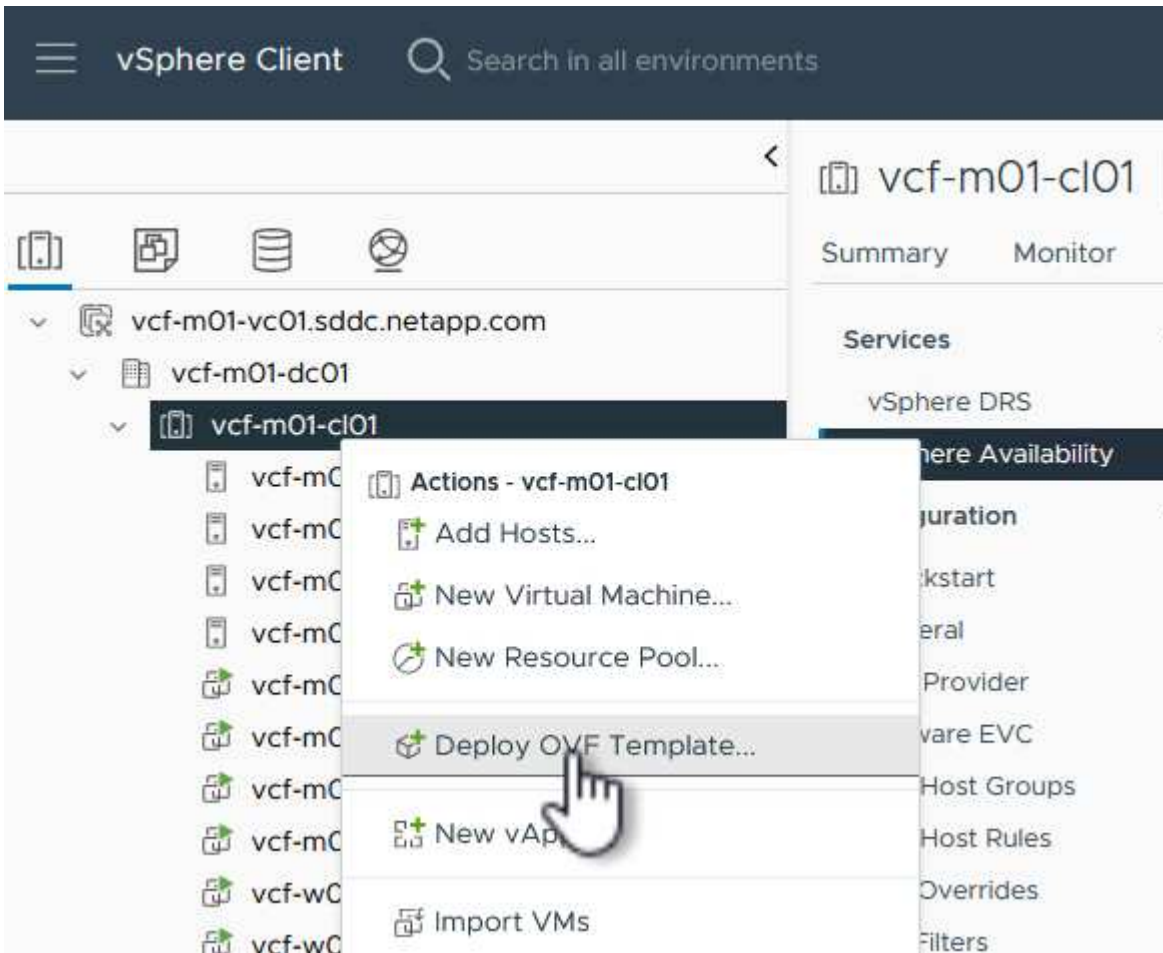
Führen Sie die folgenden Schritte aus, um SCV bereitzustellen, zu konfigurieren und zum Schutz von Daten in einer VI-Workloaddomäne zu verwenden:

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.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

http | https://remoteserver-address/filetoinstall.ovf | .ova

☒ Local file

UPLOAD FILES

scv-5.0P2-240310_1514.ova

- 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.
- 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.
- Überprüfen Sie die Informationen zur OVF-Vorlage auf der Seite **Details überprüfen** und stimmen Sie den Lizenzbedingungen auf der Seite **Lizenzvereinbarungen** zu.
- 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.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine ⓘ

Select virtual disk format

Thin Provision

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	V
<input type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	49.16 GB	957.54 GB	V
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	V

Compatibility

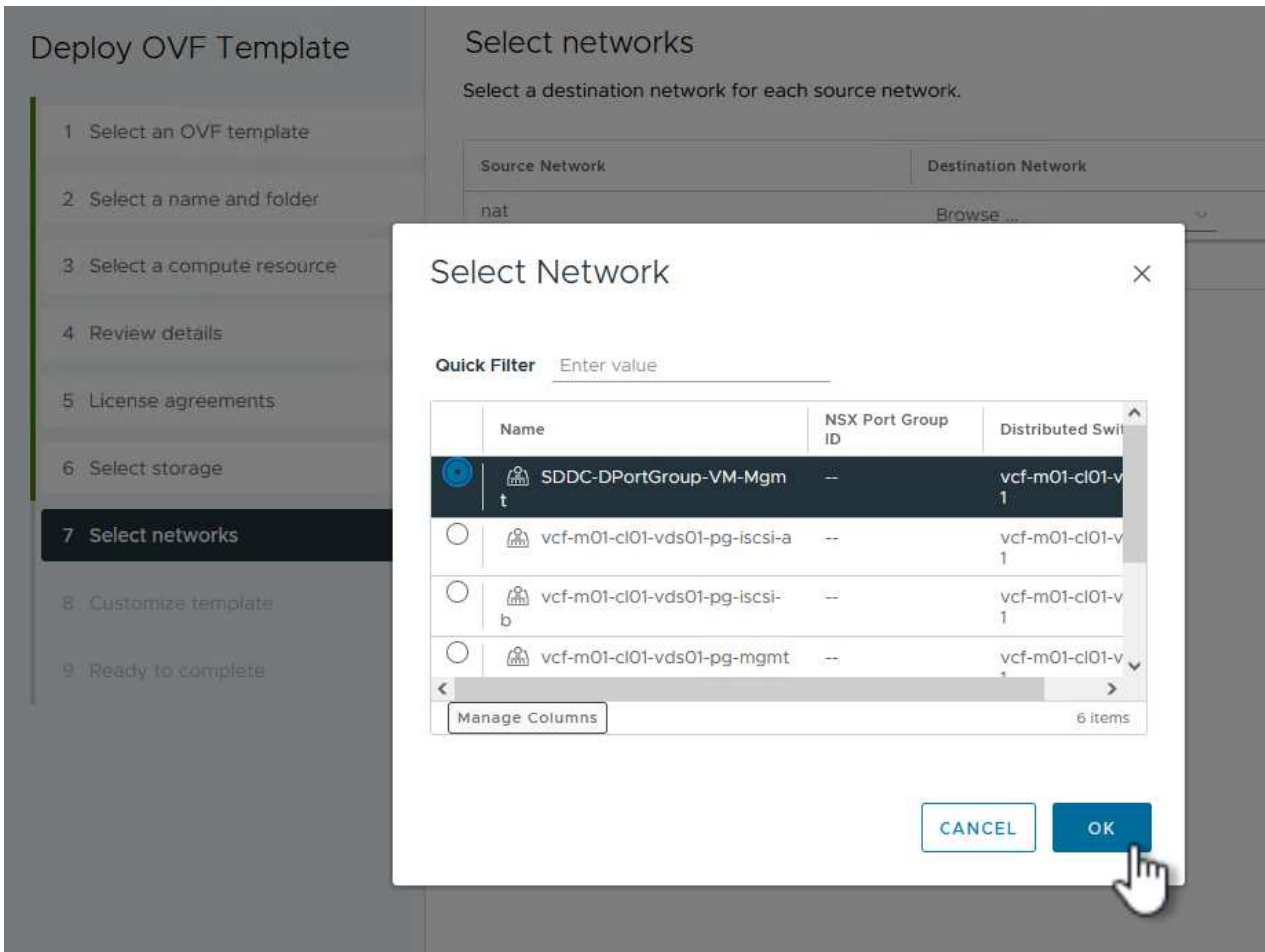
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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 Workloadaddomäne.
- 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.

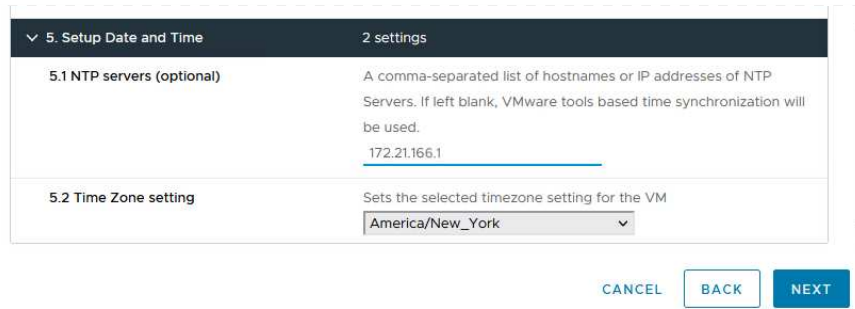
1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com	
1.2 vCenter username	administrator@vcf.local	
1.3 vCenter password	Password
	Confirm Password
1.4 vCenter port	443	
2. Create SCV Credentials		2 settings
2.1 Username	admin	
2.2 Password	Password
	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	
4.3 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)	



5. Setup Date and Time 2 settings

5.1 NTP servers (optional) A comma-separated list of hostnames or IP addresses of NTP Servers. If left blank, VMware tools based time synchronization will be used.
172.21.166.1

5.2 Time Zone setting Sets the selected timezone setting for the VM
America/New_York

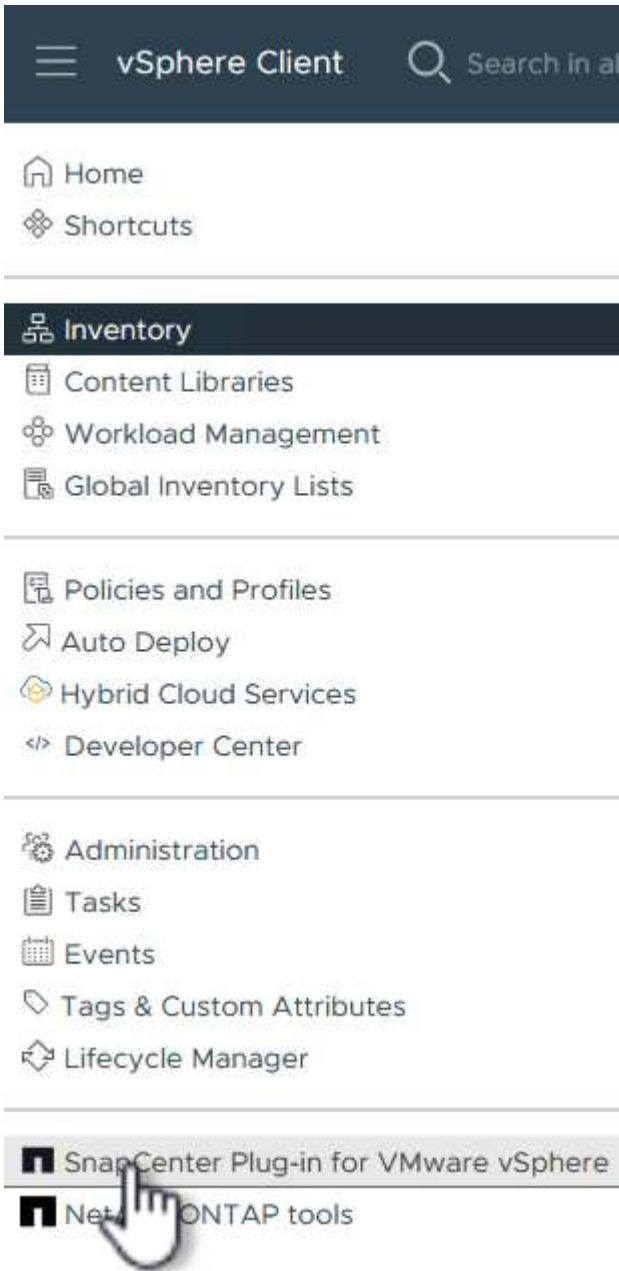
CANCEL BACK NEXT

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

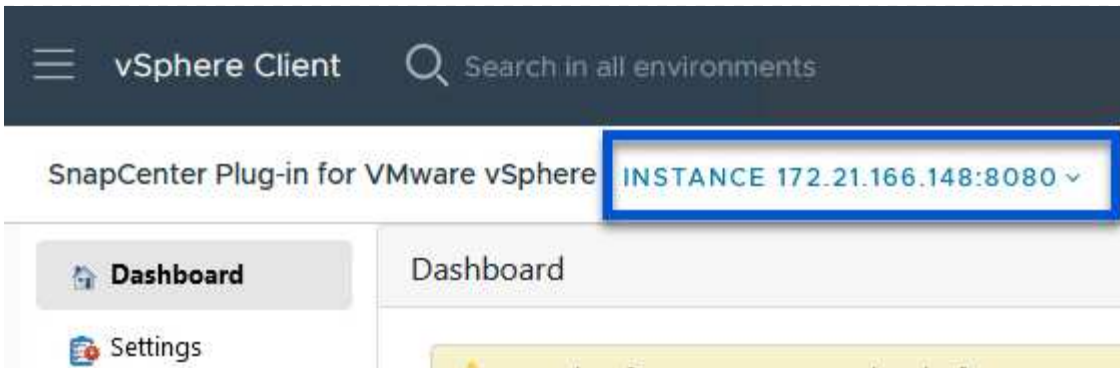
Speichersysteme zu SCV hinzufügen

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

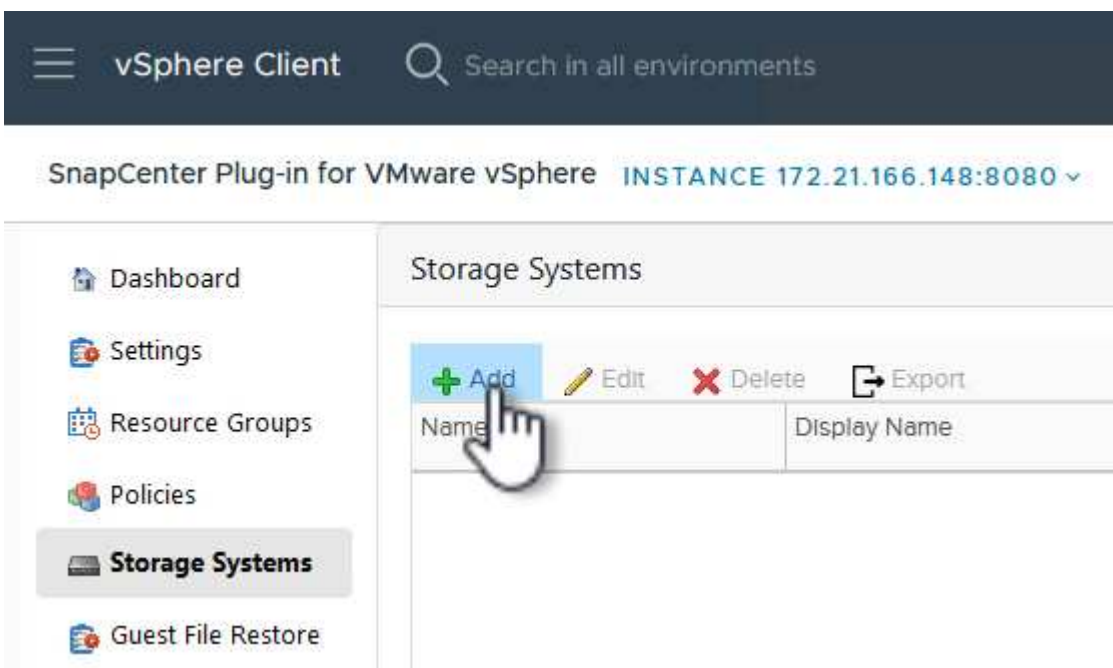
1. Auf SCV kann über das Hauptmenü im vSphere-Client zugegriffen werden.



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.

Add Storage System



Storage System	<input type="text" value="172.16.9.25"/>
Authentication Method	<input checked="" type="radio"/> Credentials <input type="radio"/> Certificate
Username	<input type="text" value="admin"/>
Password	<input type="password" value="••••••••"/>
Protocol	<input type="text" value="HTTPS"/>
Port	<input type="text" value="443"/>
Timeout	<input type="text" value="60"/> Seconds
<input type="checkbox"/> Preferred IP	<input type="text" value="Preferred IP"/>

Event Management System(EMS) & AutoSupport Setting

☐ Log Snapcenter server events to syslog

☐ Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



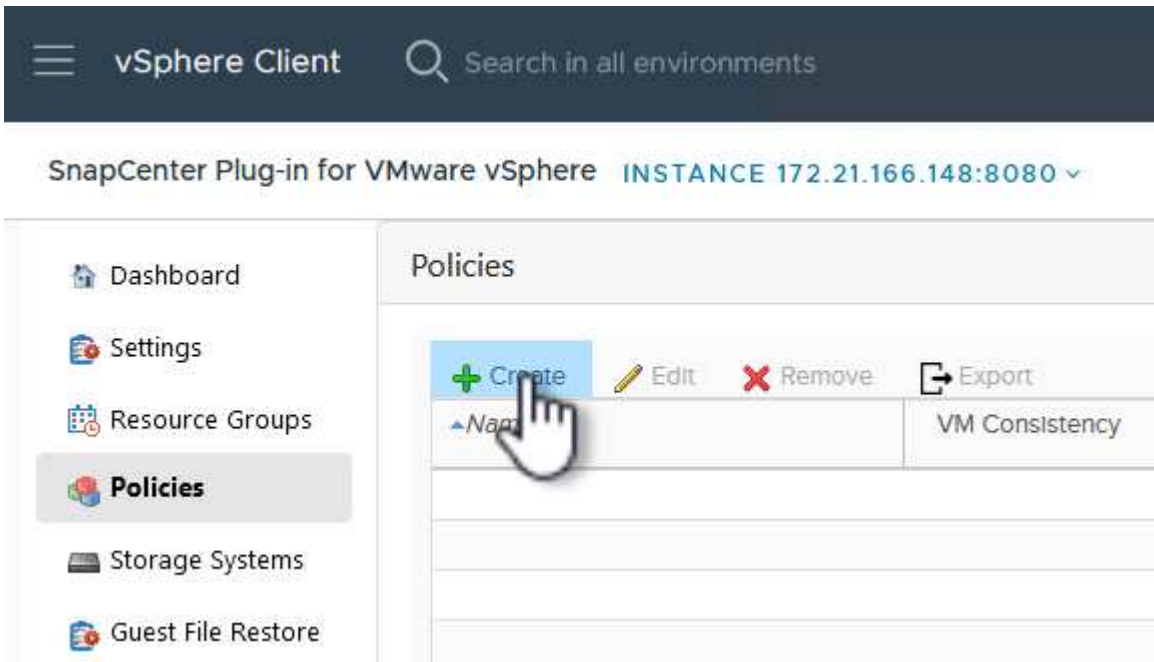
5. Wiederholen Sie diesen Vorgang für alle weiteren zu verwaltenden Speichersysteme, einschließlich aller Systeme, die als sekundäre Sicherungsziele verwendet werden sollen.

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.

New Backup Policy



Name	<input type="text" value="Daily_Snapmirror"/>
Description	<input type="text" value="description"/>
Frequency	<input type="text" value="Daily"/>
Locking Period	<input type="checkbox"/> Enable Snapshot Locking ⓘ
Retention	<input type="text" value="Days to keep"/> <input type="text" value="15"/> ⓘ
Replication	<input checked="" type="checkbox"/> Update SnapMirror after backup ⓘ <input type="checkbox"/> Update SnapVault after backup ⓘ
	Snapshot label <input type="text"/>
Advanced ▾	<input type="checkbox"/> VM consistency ⓘ <input type="checkbox"/> Include datastores with independent disks
	Scripts ⓘ <div><input type="text" value="Enter script path"/></div>

CANCEL

ADD

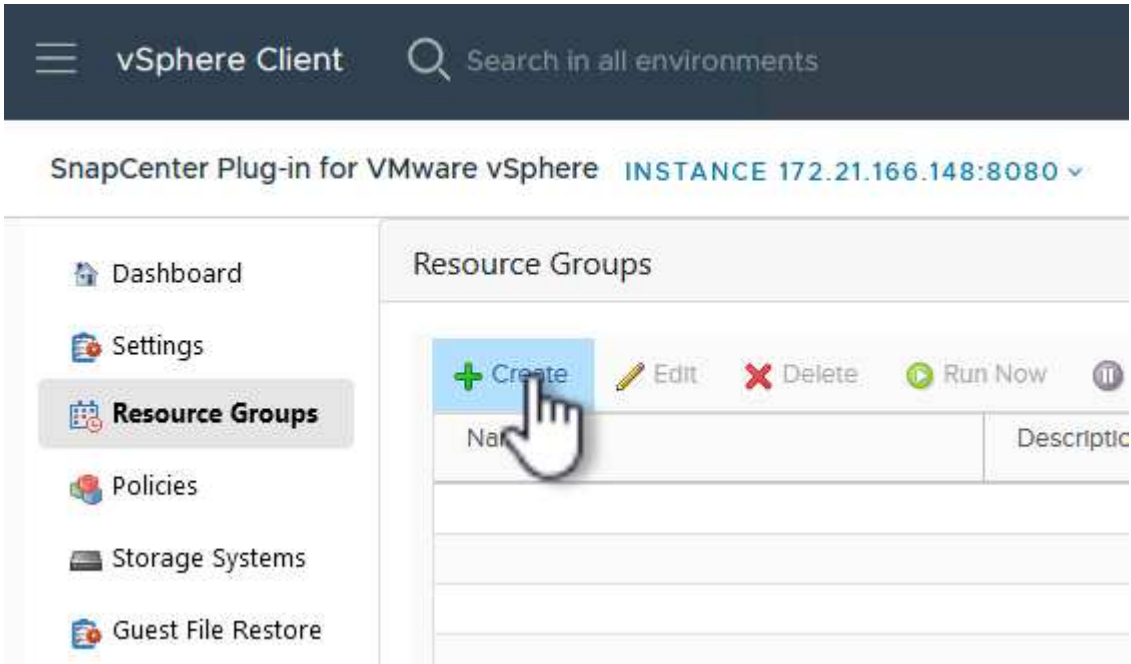


Erstellen von Ressourcengruppen in SCV

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.

Create Resource Group

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities

OracleSrv_01
OracleSrv_02
OracleSrv_03
OracleSrv_04

Selected entities

SQLSRV-01
SQLSRV-02
SQLSRV-03
SQLSRV-04

BACK

NEXT

FINISH

CANCEL

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

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

☐ Always exclude all spanning datastores

This means that only the datastores directly added to the resource group and the primary datastore of VMs directly added to the resource group will be backed up

☒ Always include all spanning datastores

All datastores spanned by all included VMs are included in this backup

☐ Manually select the spanning datastores to be included ⓘ

You will need to modify the list every time new VMs are added

There are no spanned entities in the selected virtual entities list.

BACK

NEXT

FINISH

CANCEL

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

Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- 4. Policies**
- 5. Schedules
- 6. Summary

[+ Create](#)

[illegible]

BACK NEXT FINISH CANCEL

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.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily_Snapmi... ▼

Type

Daily

Every

1

Day(s)

Starting

04/04/2024



At

04



45



PM



BACK

NEXT

FINISH

CANCEL

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

Create Resource Group

- ✓ 1. General info & notification
- ✓ 2. Resource
- ✓ 3. Spanning disks
- ✓ 4. Policies
- ✓ 5. Schedules
- ✓ 6. Summary

Name	SQL_Servers		
Description			
Send email	Never		
Latest Snapshot name	None ⓘ		
Custom snapshot format	None ⓘ		
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04		
Spanning	False		
Policies	Name	Frequency	Snapshot Locking Period
	Daily_Snapmir...	Daily	-

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

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

☰

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

»

Resource Groups

+

 Create

Edit

Delete

Run Now

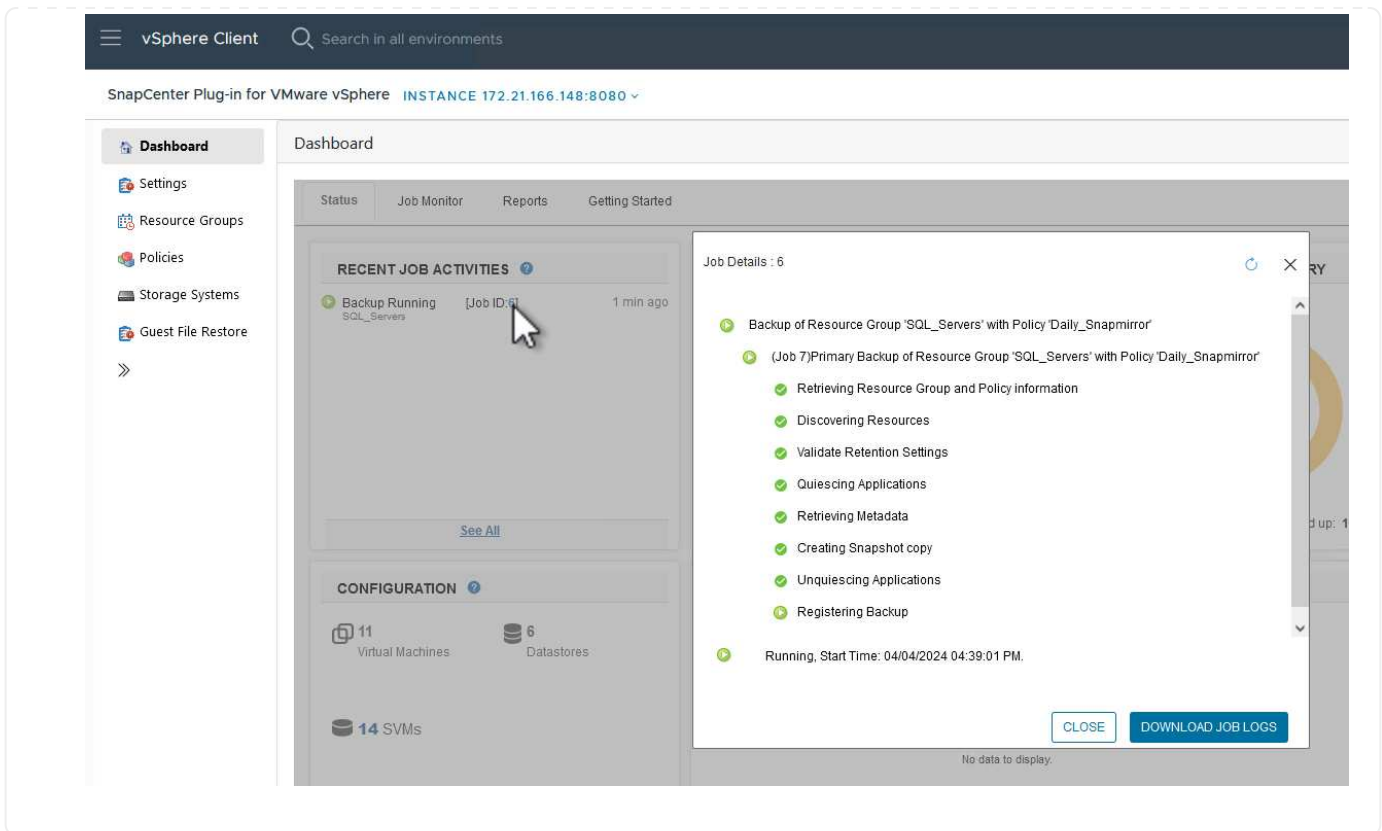
Suspend

Resume

Export

Name	Description	Polik
SQL_Servers		Daily_

9. Navigieren Sie zum **Dashboard** und klicken Sie unter **Letzte Jobaktivitäten** auf die 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

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

vcf-wkl

OracleS

OracleS

OracleS

OracleS

SQLSR

SQLSR

SQLSR

SQLSR

Win20

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

Recent Tasks

Task Name

Manage Columns

Run

OracleSrv_04

Summary

Monitor

Configure

Permissions

Guest OS

Virtual Mac

4 CPU(s), 22 MHz used

32 GB, 0 GB memory active

100 GB | Thin Provision

VCF_WKLD_03_ISCSI

vcf-wkld-01-IT-INF-WKLD-01-vc

(connected) | 00:50:56:83:02:f

Disconnected

ESXi 7.0 U2 and later (VM vers

Create Resource Group

Add to Resource Group

Attach Virtual Disk(s)

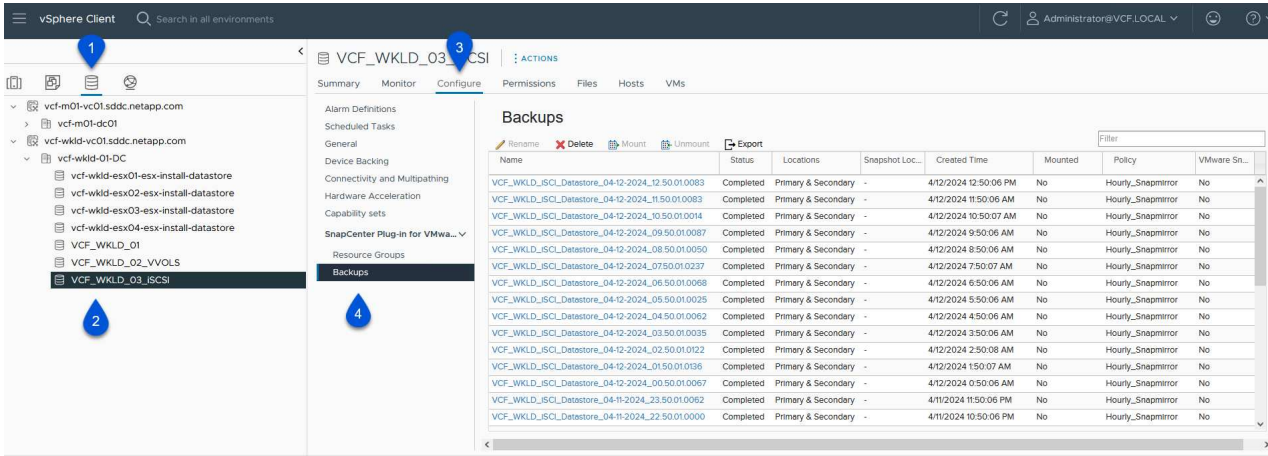
Detach Virtual Disk(s)

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.

Restore



1. Select backup

2. Select scope

3. Select location

4. Summary

Search a backup



Available backups

(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_ISCI_...	4/4/2024 4:50:0...	No	Hourly_Snapmirror	No
VCF_WKLD_ISCI_...	4/4/2024 4:45:1...	No	Hourly_Snapmirror	No

[BACK](#)[NEXT](#)[FINISH](#)[CANCEL](#)[VCF_WKLD_03_ISCI](#)

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:**

Restore

1. Select backup
2. Select scope
3. Select location
4. Summary

Restore scope: Entire virtual machine

Restart VM: ☐

Restore Location: ☐ Original Location
(This will restore the entire VM to the original Hypervisor with the original settings. Existing VM will be unregistered and replaced with this VM.)
☒ Alternate Location
(This will create a new VM on selected vCenter and Hypervisor with the customized settings.)

Destination vCenter Server: 172.21.166.143

Destination ESXi host: vcf-wkld-esx04.sddc.netapp.com

Network: vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-

VM name after restore: OracleSrv_04_restored

Select Datastore: VCF_WKLD_03_ISCSI

BACK NEXT FINISH CANCEL

VCF_WKLD_03_ISCSI

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

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

Restore

✓ 1. Select backup

✓ 2. Select scope

3. Select location

4. Summary

Destination datastore	Locations
VCF_WKLD_03_iSCSI	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Primary) VCF_iSCSI:VCF_WKLD_03_iSCSI
	(Secondary) svm_iscsi:VCF_WKLD_03_iSCSI_dest
	< >

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

Restore

✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

Virtual machine to be restored	OracleSrv_04
Backup name	VCF_WKLD_iSCI_Datastore_04-04-2024_16.50.00.0940
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.143
ESXi host to be used to mount the backup	vcf-wkld-esx04.sddc.netapp.com
VM Network	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt
Destination datastore	VCF_WKLD_03_iSCSI
VM name after restore	OracleSrv_04_restored



Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

FINISH

CANCEL

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

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

>>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago
VCF_WKLD_ISCI_Datastore_04-04-20...
- Backup Successful [Job ID:15] 8 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:12] 13 min ago
VCF_WKLD_ISCI_Datastore
- Backup Successful [Job ID:9] 13 min ago
SQL_Servers
- Backup Successful [Job ID:6] 19 min ago
SQL_Servers

[See All](#)

CONFIGURATION

- 11 Virtual Machines
- 6 Datastores
- 14 SVMs
- 2 Resource Groups
- 2 Backup Policies

Job Details : 18

- Restoring backup with name: VCF_WKLD_ISCI_Datastore_04-04-2024_16:50:00.0940
 - Preparing for Restore: Retrieving Backup metadata from Repository.
 - Pre Restore
 - Restore

Running, Start Time: 04/04/2024 04:58:24 PM.

CLOSE

DOWNLOAD JOB LOGS

No data to display.

Recent Tasks

Task Name	Target	Status	Details	Initiator	Queued For	Start Time
NetApp Mount Datastore	vcf-wkld-esx04.sdd c.netapp.com	35%	Mount operation completed successfully.	VCF.LOCAL\Administrator	6 ms	04/04/2024, 4:58:27 PM
NetApp Restore	vcf-wkld-esx04.sdd c.netapp.com	2%	Restore operation started.	VCF.LOCAL\Administrator	10 ms	04/04/2024, 4:58:27 PM

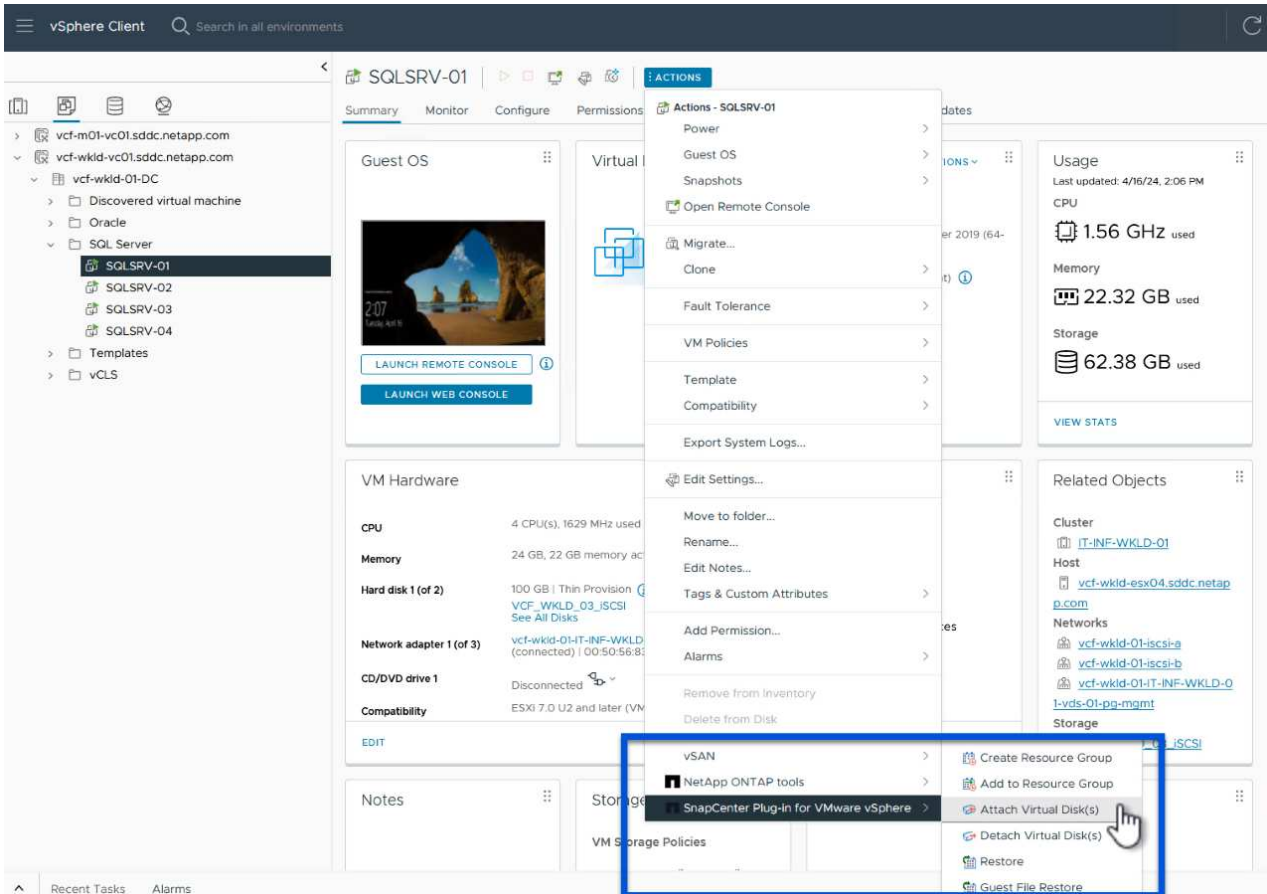
Manage Columns Running [More Tasks](#)

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.

Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

Backup

Search for Backups



(This list shows primary backups. **1** modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_ISCI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_ISCI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

Select disks

<input type="checkbox"/> Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_ISCI_Datastore_04-17-2024_09.50.01.0218
<input checked="" type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01_1.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_ISCI_Datastore_04-17-2024_09.50.01.0218

2

3

CANCEL

ATTACH



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

Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

Backup

Search for Backups



(This list shows primary backups.)

Name
VCF_WKLD_ISCI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_ISCI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_ISCI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_ISCI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_ISCI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_ISCI_Datastore_04-17-2024_04.50.01.0231

Select disks

<input type="checkbox"/> Virtual disk
<input type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01.vmdk
<input checked="" type="checkbox"/> [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01_1.vmdk

Time range

From

Hour Minute Second

To

Hour Minute Second

VMware snapshot

Mounted

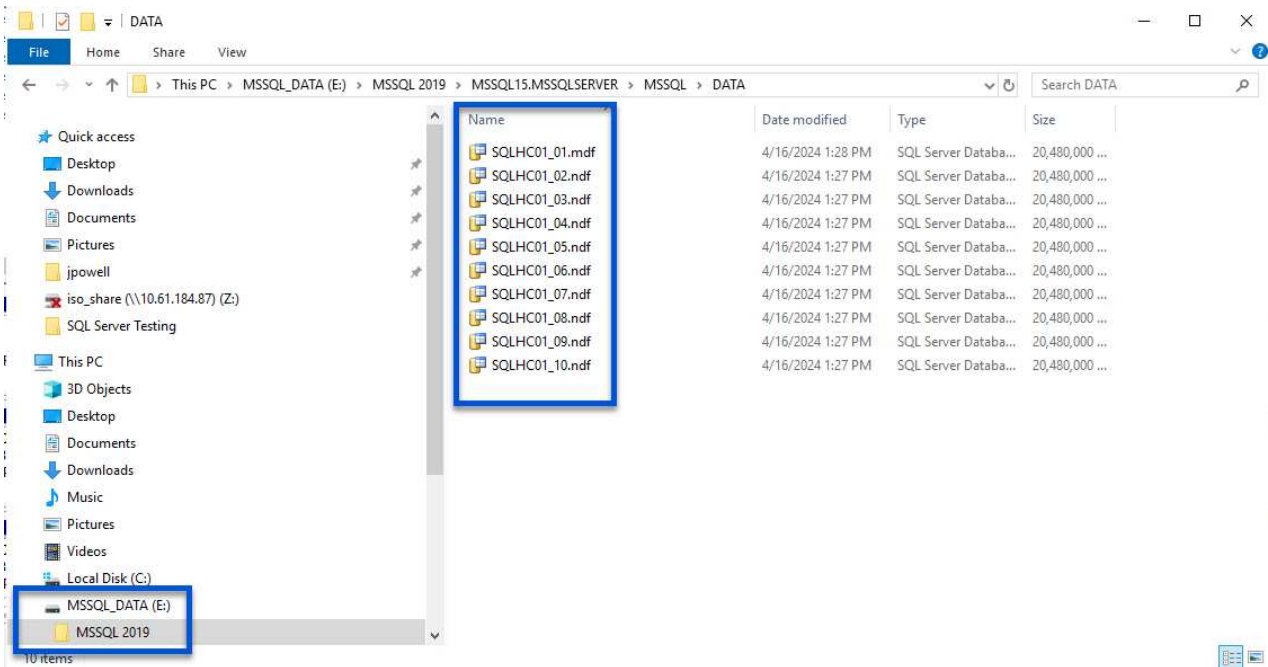
Location

CLEAR OK

CANCEL

ATTACH

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.



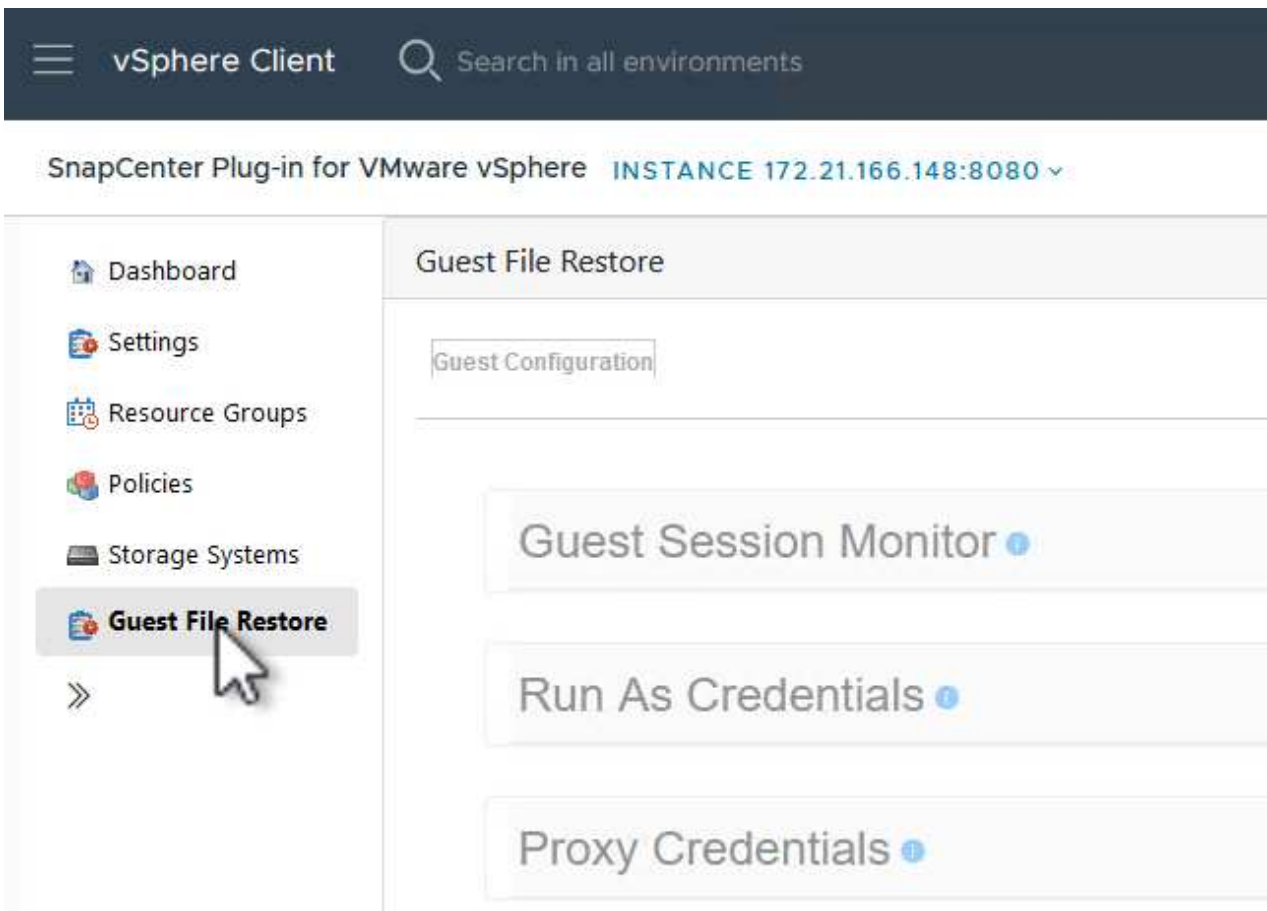
Wiederherstellung des Gastdateisystems mit dem SnapCenter -Plug-in

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

Run As Credentials



Run As Name	<input type="text" value="Administrator"/>	
Username	<input type="text" value="administrator"/>	
Password	<input type="password" value="••••••••"/>	
Authentication Mode	<input type="text" value="Windows"/>	
VM Name	<input type="text"/>	

Select VM



CANCEL

SAVE

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**.

Proxy VM



VM Name

SQLSRV-01

☒ Search by ESXi Host

ESXi Host

vcf-wkld-esx04.sddc.netapp.com

Virtual Machine

SQLSRV-01

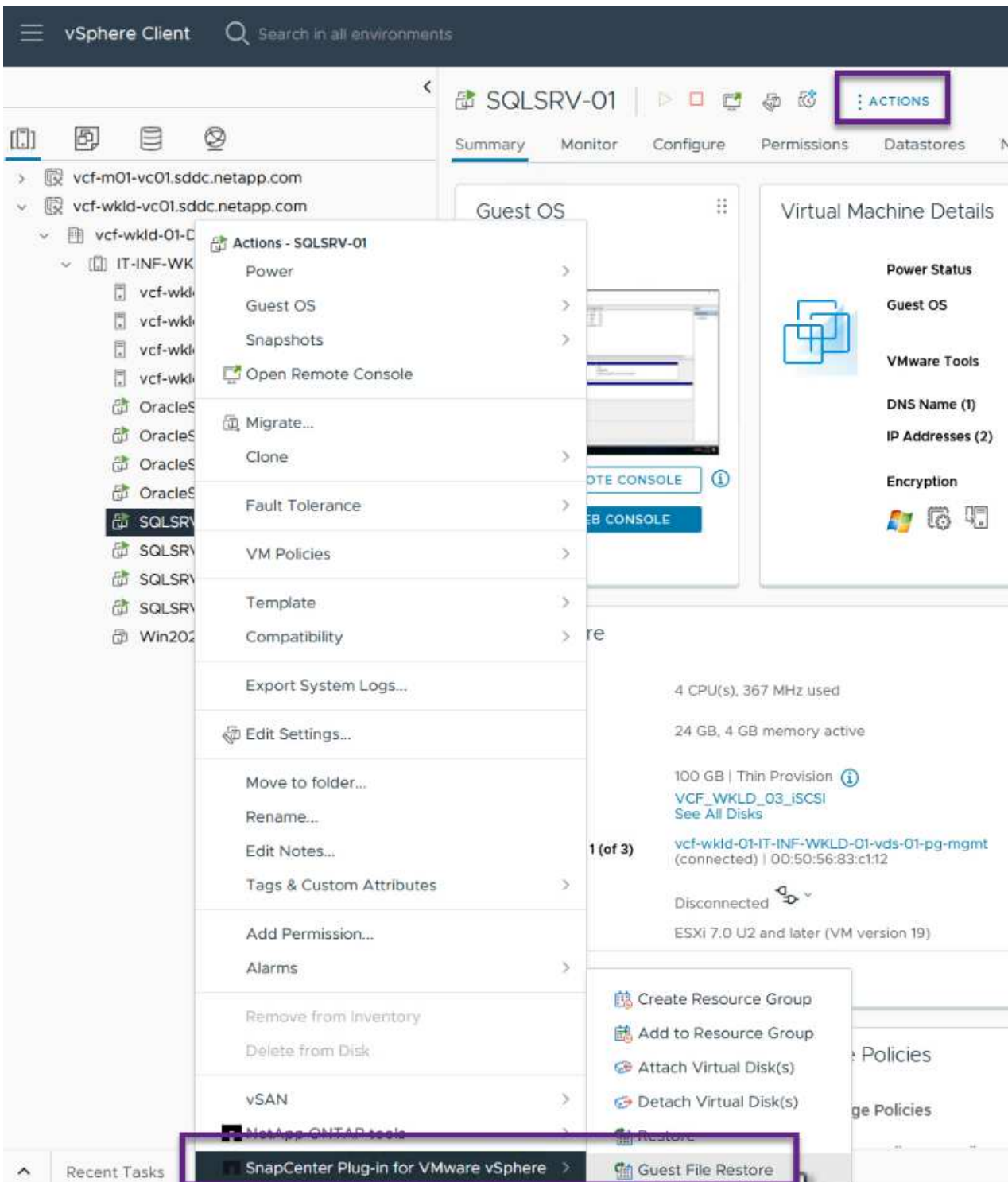
☐ Search by Virtual Machine name

CANCEL

SAVE



5. Klicken Sie im Fenster **Run As Credentials** erneut auf **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.



- 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.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iSCSI_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iSCSI_dest:SQL_Servers_04-16-2024_13.52.34.0329

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

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

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

Use Guest File Restore proxy VM

☐ Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

- Überprüfen Sie abschließend die Seite **Zusammenfassung** und klicken Sie auf **Fertig**, um die Sitzung zur Wiederherstellung des Gastdateisystems zu starten.
- 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.

The screenshot shows the vSphere Client interface with the SnapCenter Plug-in for VMware vSphere. The left sidebar contains navigation options: Dashboard, Settings, Resource Groups, Policies, Storage Systems, and Guest File Restore. The main area displays the Guest File Restore configuration, including the Guest Configuration section and the Guest Session Monitor table.

Backup Name	Source VM	Disk Path	Guest Mount Path	Time To Expire	Browse Files
SQL_Servers_04-16-2024_13:52:34.0329	SQLSRV-01	[VCF_WKLD_03_SCSI(sc-202404161419...	E:\	23h:58m	

Below the table, there are sections for Run As Credentials and Proxy Credentials, each with a dropdown arrow.

- 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	
<input type="checkbox"/>	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

☐ IPv6

Either Files to Restore or Restore Location is not selected!

CANCEL

RESTORE

Select Restore Location

Select address family for UNC path:

☒ IPv4

☐ IPv6

Restore to path:

Provide UNC path to the guest where files will be restored. eg: \\10.60.136.65\\c\$
Run As Credentials while triggering the Guest File Restore workflow will be used to connect to the UNC path

If original file(s) exist:

☒ Always overwrite

☐ Always skip

☒ Disconnect Guest Session after successful restore

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 Workloadomänen 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 Sicherheitsrichtlinien und das Durchführen von Wiederherstellungsvorgängen.

Mithilfe von VMware Cloud Foundation (VCF)-Workloadomänen 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.

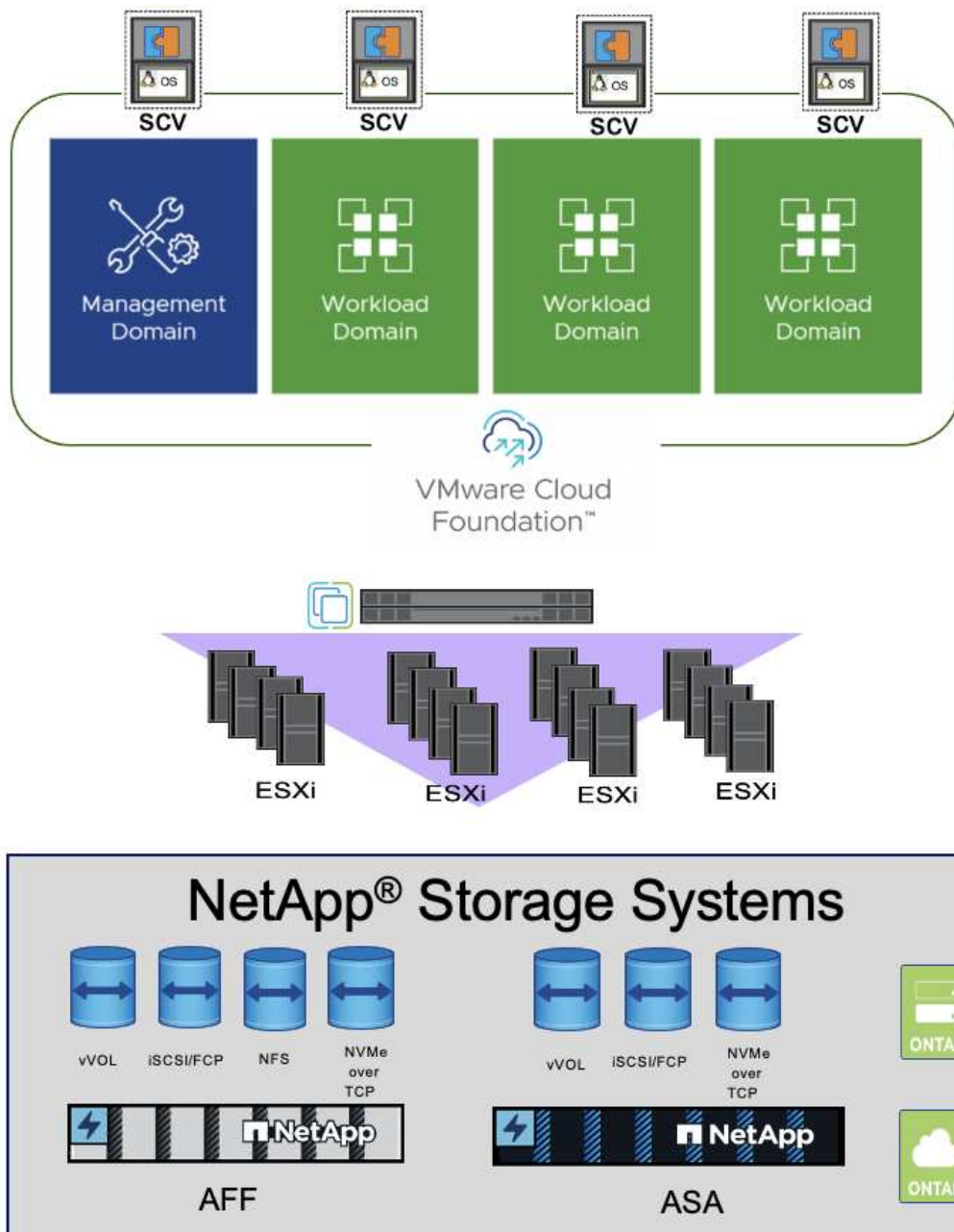
Publikum

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 Datensicherungsstrategie, die das Erstellen von drei Datenkopien, deren Speicherung auf zwei verschiedenen Medientypen und die Aufbewahrung einer Kopie an einem externen Standort beinhaltet. NetApp Backup and Recovery ist ein cloudbasiertes Tool für das Datenmanagement, das eine einheitliche Steuerungsebene für eine breite Palette von Backup- und Wiederherstellungsvorgängen in lokalen und Cloud-Umgebungen bietet. Weitere Einzelheiten finden Sie unter "[NetApp Backup and Recovery](#)". Die

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](#)".



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

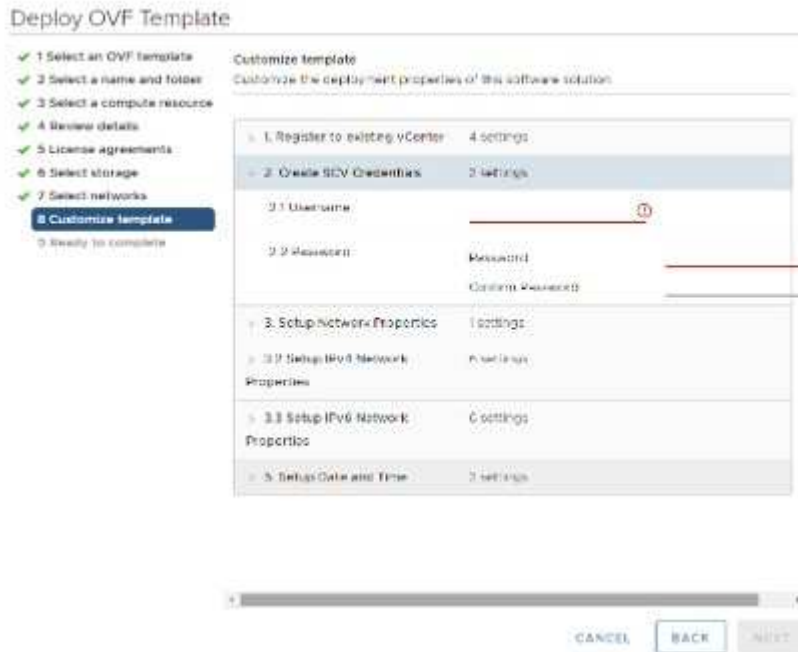
vcf-mgmt-sc

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

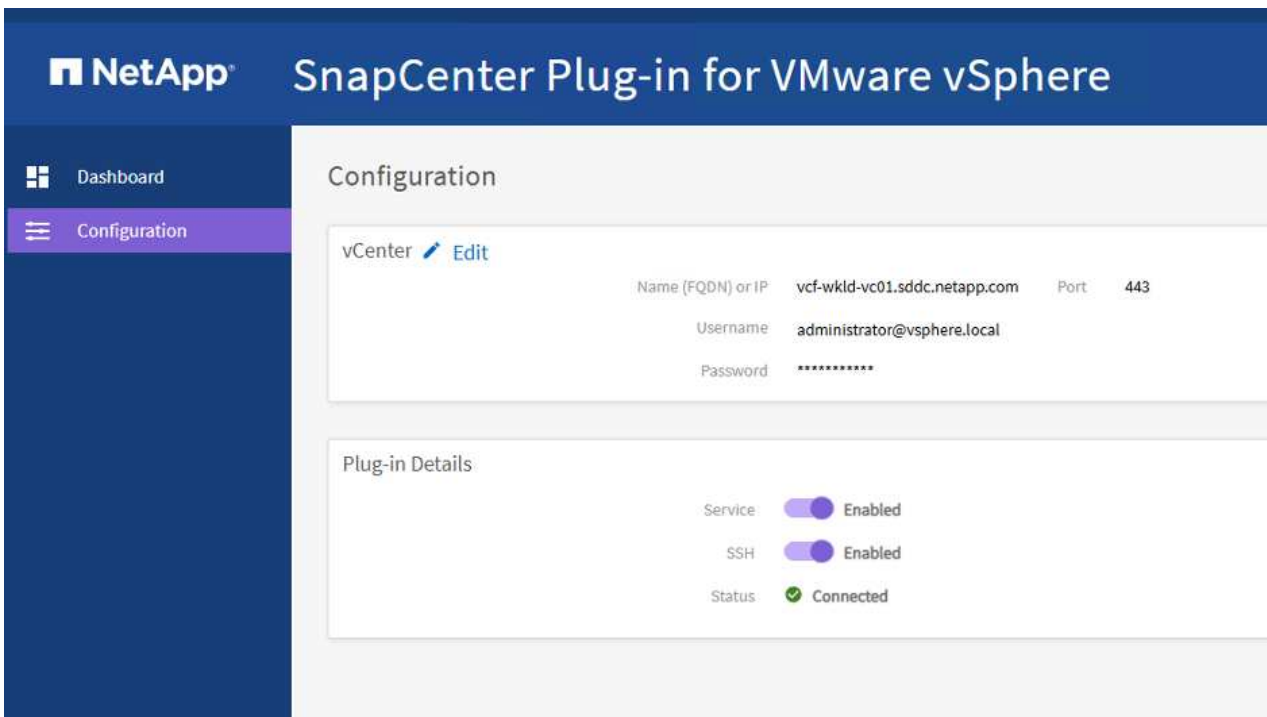
Enter your choice: 10

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.

Getting Started with SnapCenter Plug-in for VMware vSphere



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“.

New Backup Policy

Name

wkld01

Description

description

Frequency

Daily

Locking Period

☒ Enable Snapshot Locking

1

Days

Retention

Days to keep

7

Replication

☐ Update SnapMirror after backup

☐ Update SnapVault after backup

Snapshot label

Advanced

CANCEL

ADD

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	<table><thead><tr><th>Name</th><th>Frequency</th><th>Snapshot Locking Period</th></tr></thead><tbody><tr><td>wkld01</td><td>Daily</td><td>1 Day</td></tr></tbody></table>	Name	Frequency	Snapshot Locking Period	wkld01	Daily	1 Day		
Name	Frequency	Snapshot Locking Period							
wkld01	Daily	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“.

Restore


✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

Virtual machine to be restored	win2022
Backup name	wkld02_recent
Restart virtual machine	No
Restore Location	Alternate Location
Destination vCenter Server	172.21.166.202
ESXi host to be used to mount the backup	vcf-wkld-esx07.sddc.netapp.com
VM Network	vcf-m01wk-vc02-vcf-wkld02-vds-01-pg-mgmt
Destination datastore	wkld02
VM name after restore	win2022.1

 Change IP address of the newly created VM after restore operation to avoid IP conflict.

BACK

NEXT

FINISH

CANCEL

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“.

Mount Datastore



ESXi host name

vcf-wkld-esx05.sddc.netapp.com

Backup

Search for Backups



(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
wkld02_recent	2/9/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-09-202...	2/9/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-08-2025_20.0...	2/8/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-08-202...	2/8/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-07-2025_20.0...	2/7/2025 8:00:01 PM	No	wkld02	Yes
RG-Datastore_02-07-202...	2/7/2025 6:56:01 PM	No	wkld02	Yes
wkld02_02-06-2025_20.0...	2/6/2025 8:00:01 PM	No	wkld02	Yes

Backup location

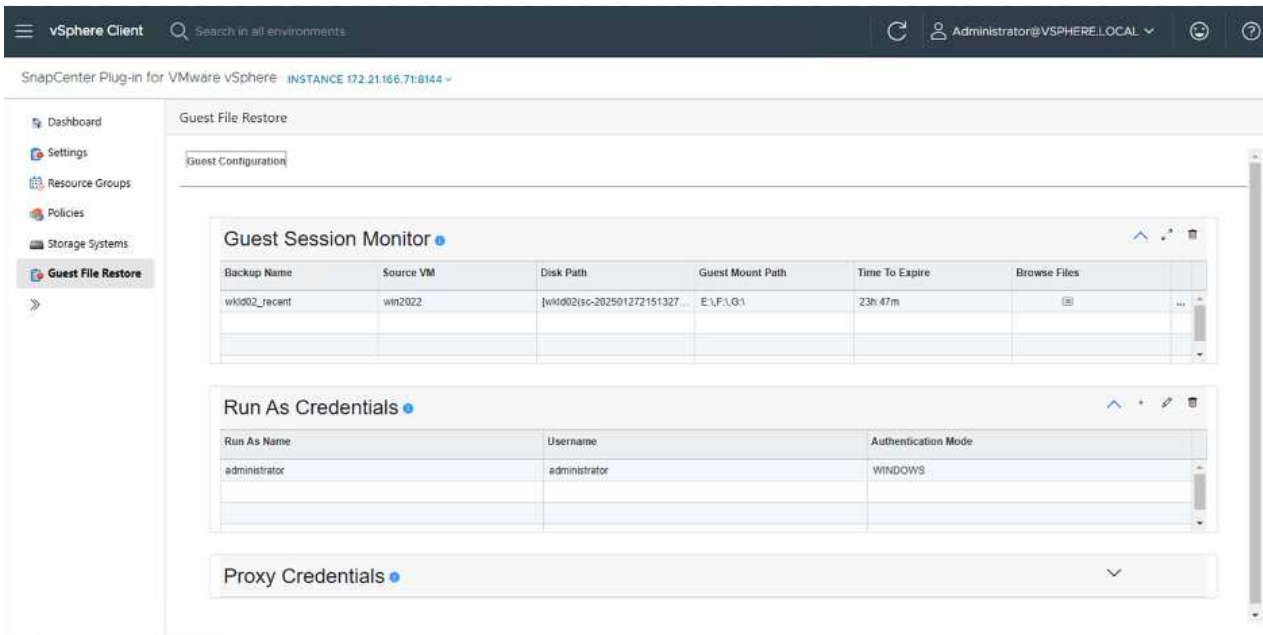
Backup type	Location
Primary	172.21.118.118:vcf_md_wkld02:wkld02_recent

CANCEL

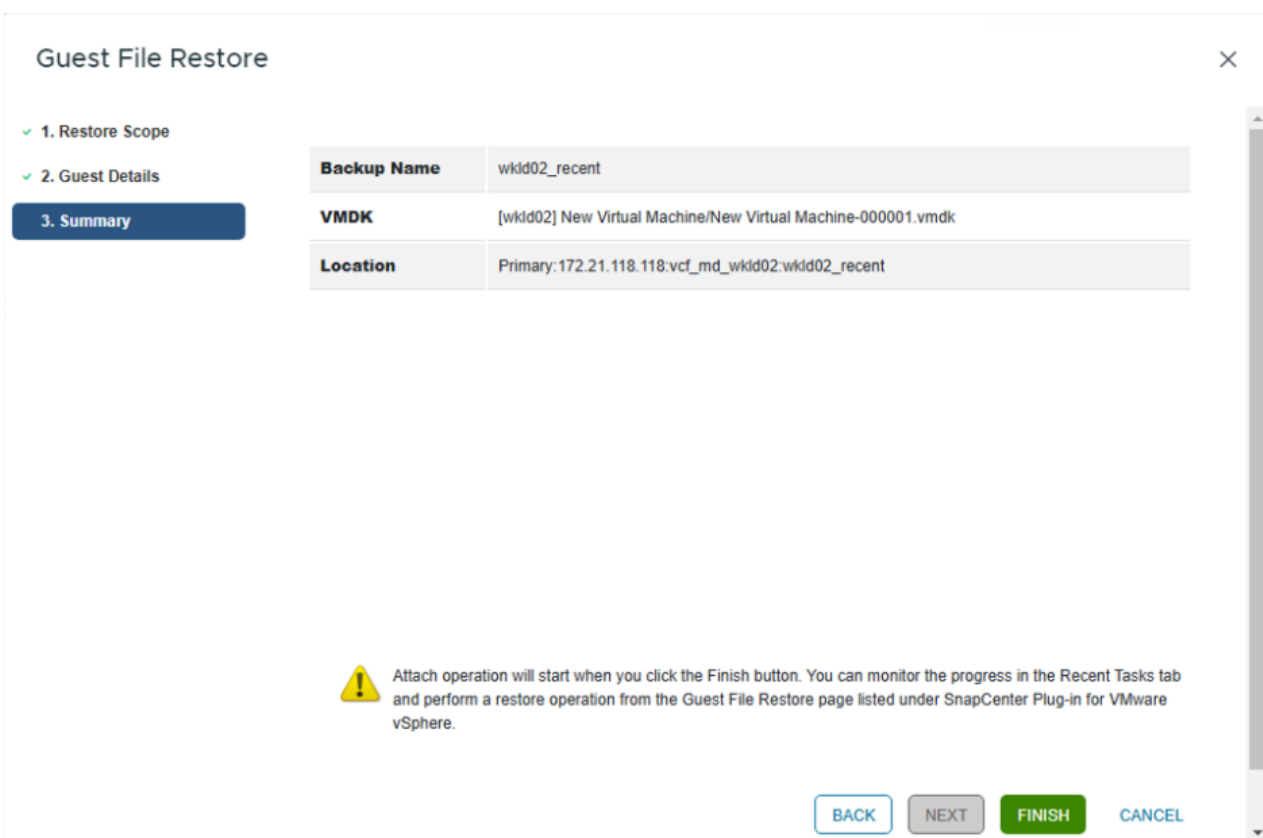
MOUNT

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.

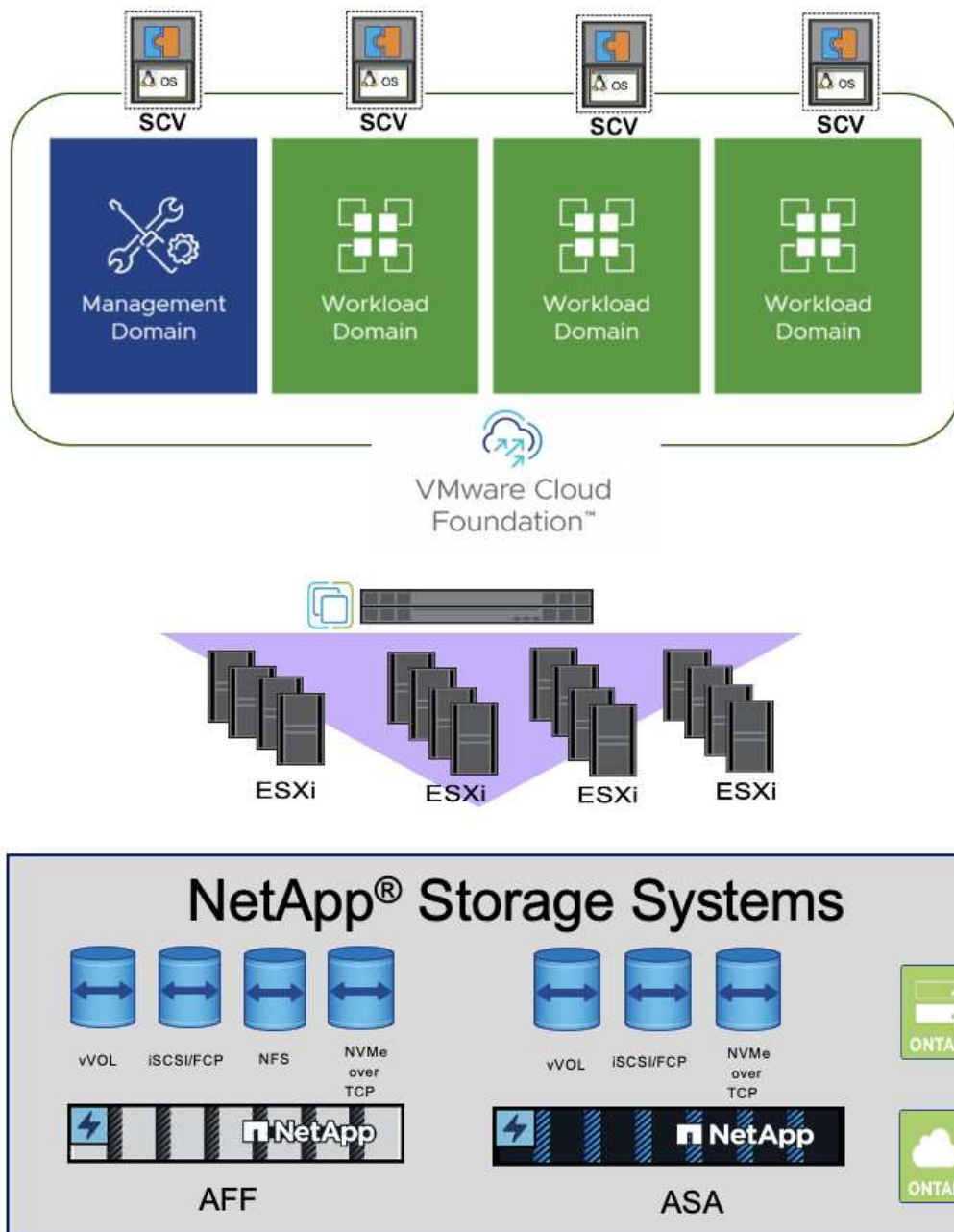
Architekturübersicht

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 Datensicherungsstrategie, die das Erstellen von drei Datenkopien, deren Speicherung auf zwei verschiedenen Medientypen und die Aufbewahrung einer Kopie an einem externen Standort beinhaltet. NetApp Backup and Recovery ist ein cloudbasiertes Tool für das Datenmanagement, das eine einheitliche Steuerungsebene für eine breite Palette von Backup- und Wiederherstellungsvorgängen in lokalen und Cloud-Umgebungen bietet. Weitere Einzelheiten finden Sie unter "[NetApp Backup and Recovery](#)". Die

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“.

Restore


✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

Virtual machine to be restored	Win2022NVMe
Backup name	VCF-NVMe_02-12-2025_19.13.55.0912
Restart virtual machine	No
Restore Location	Original Location
ESXi host to be used to mount the backup	vcf-wkdd-esx04.sddc.netapp.com

 This virtual machine will be powered down during the process.

BACK

NEXT

FINISH

CANCEL

- 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“.

Mount Datastore



ESXi host name

vcf-wkld-esx03.sddc.netapp.com

Backup

Search for Backups



(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-19-2025_...	2/19/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-18-2025_...	2/18/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-17-2025_...	2/17/2025 6:57:01 PM	Yes	wkld01	No
VCF-NVMe_02-16-2025_...	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_...	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_...	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_...	2/13/2025 6:57:01 PM	No	wkld01	No

Backup location

Backup type	Location
Primary	VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-19-2025_18.57.02.0052

CANCEL

MOUNT

- 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.

Attach Virtual Disk(s)



[Click here to attach to alternate VM](#)

Backup

Search for Backups



(This list shows primary backups. You can modify the filter to display primary and secondary backups.)

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF-NVMe_02-17-2025_18....	2/17/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-16-2025_18....	2/16/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-15-2025_18....	2/15/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-14-2025_18....	2/14/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-13-2025_18....	2/13/2025 6:57:01 PM	No	wkld01	No
VCF-NVMe_02-12-2025_19....	2/12/2025 7:13:55 PM	No	wkld01	No

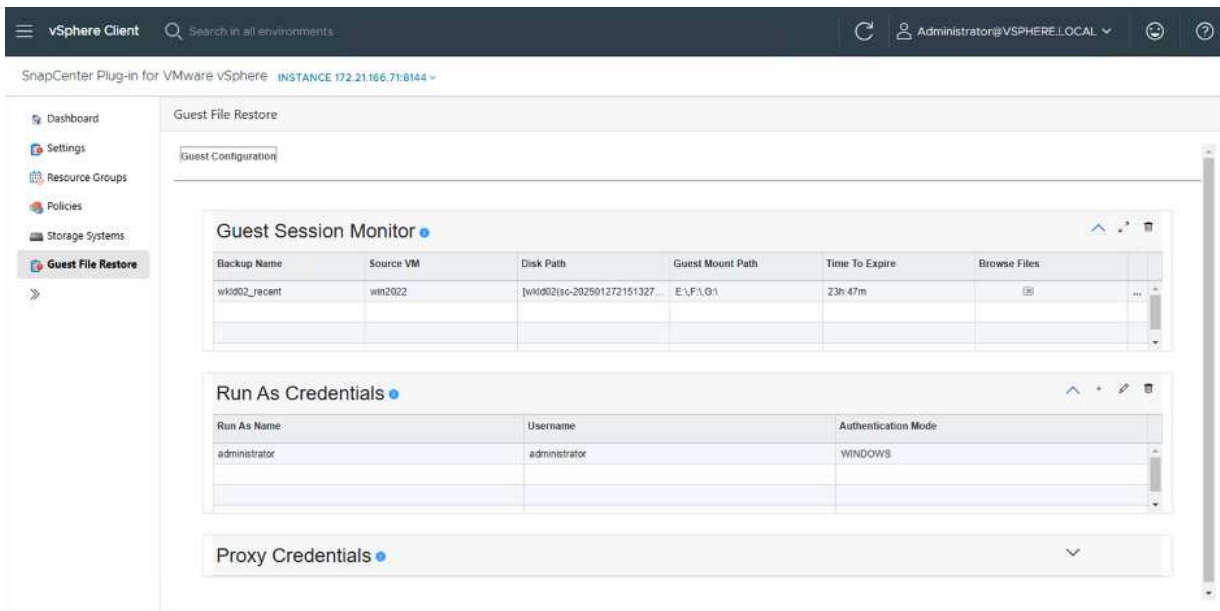
Select disks

<input type="checkbox"/> Virtual disk	Location
<input checked="" type="checkbox"/> [VCF_NVMe_DS] Win2022NVMe/Win2022NVMe.vmdk	Primary:VCF_NVMe:VCF_WKLD_DS:VCF-NVMe_02-17-2025_18.57.02.0697

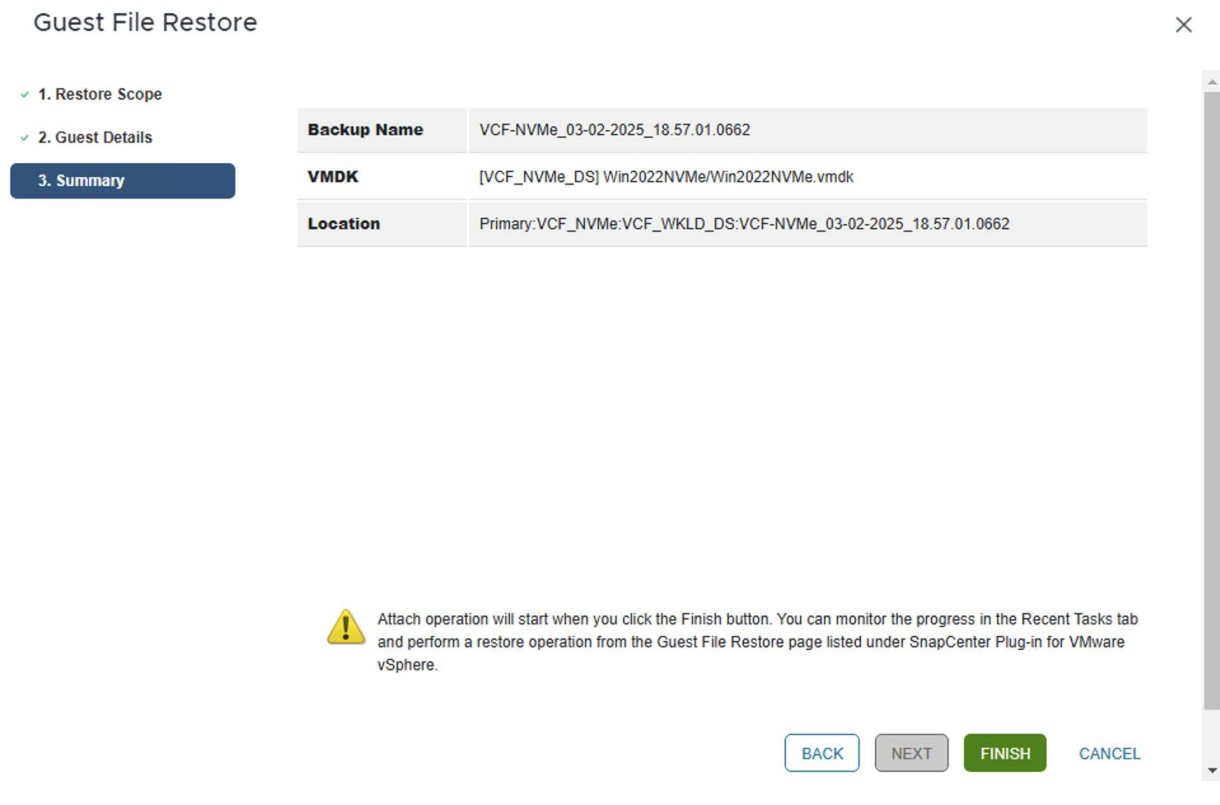
CANCEL

ATTACH

- 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.

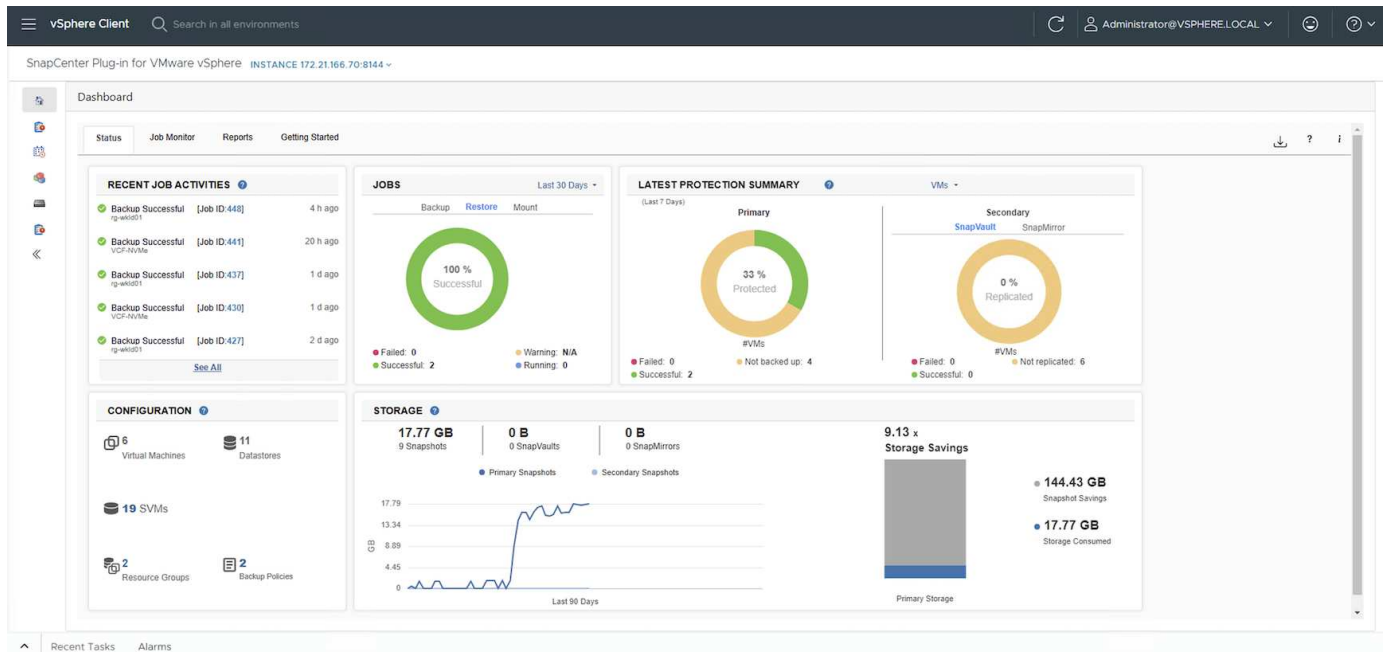


- b. Klicken Sie im vSphere-Client mit der rechten Maustaste auf die VM und wählen Sie „SnapCenter Plug-in for VMware vSphere > Guest File Restore“. Geben Sie auf der Seite „Wiederherstellungsbereich“ den Sicherungsnamen, die virtuelle VMDK-Festplatte und den Speicherort – primär oder sekundär – an. 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-Workloadumgebungen erreichen. Dieser Ansatz gewährleistet schnelle und zuverlässige Sicherungs- und Wiederherstellungsvorgänge, minimiert Ausfallzeiten und schützt kritische Daten.

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-Workloadumgebungen.

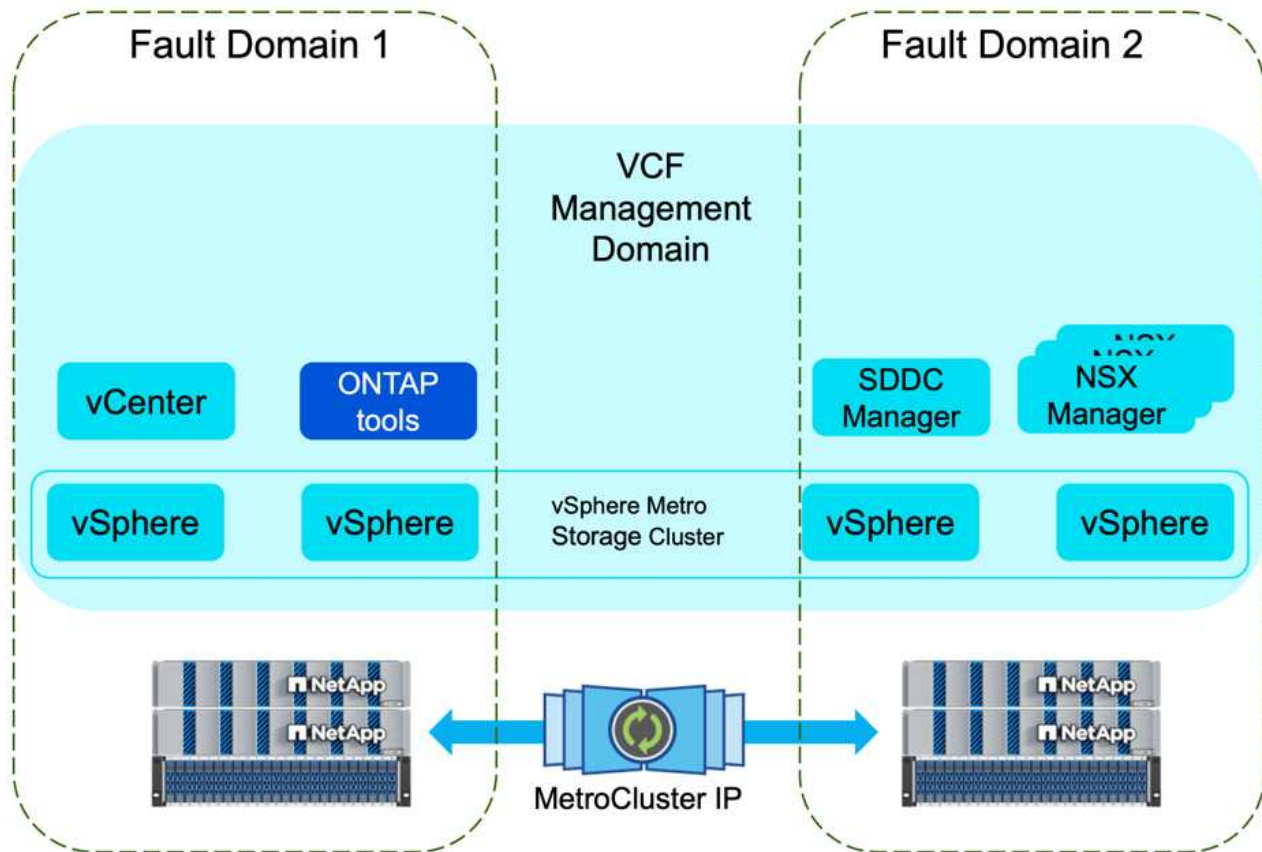
Diese Kombination gewährleistet kontinuierliche Datenverfügbarkeit, nahtloses Failover und Notfallwiederherstellung an geografisch verteilten Standorten und verbessert so die Ausfallsicherheit und Betriebskontinuität für kritische Workloads. SnapMirror Active Sync ermöglicht die Weiterführung des Betriebs 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-Workloadumgebungen mit SnapMirror Active Sync"](#)
- ["Stretch Cluster für VI-Workloadumgebungen 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.

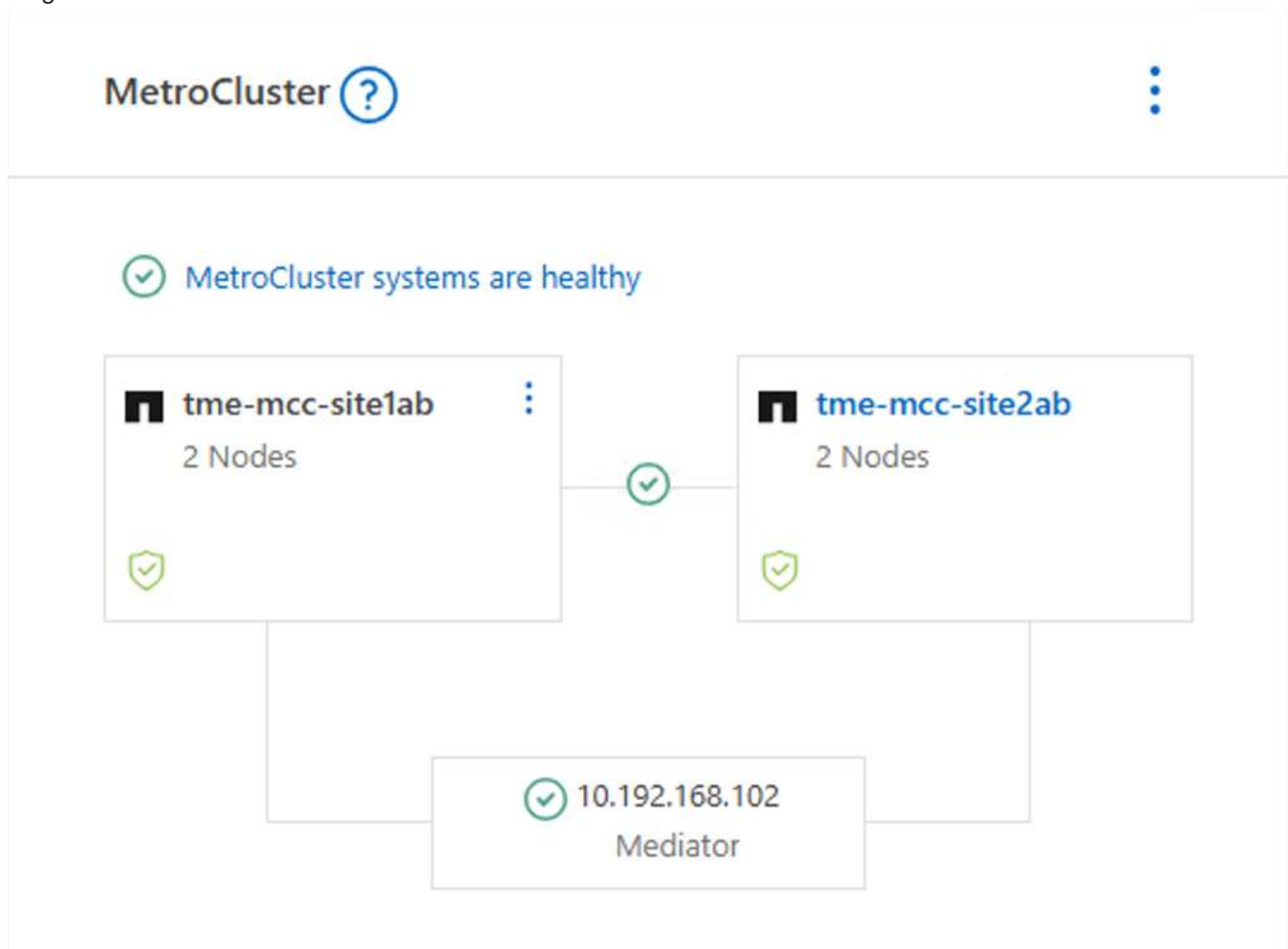
- Verwenden Sie das VCF-Importtool, um den vSphere-Cluster zu validieren.
- Konfigurieren Sie eine JSON-Datei zum Erstellen eines NSX während der VCF-Konvertierung.
- Verwenden Sie das VCF-Importtool, um die vSphere 8-Umgebung in eine VCF-Verwaltungsdomäne zu konvertieren.

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	↑
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	↑
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.

NetApp ONTAP System Manager | tme-mcc-site1ab

Search actions, objects, and pages

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	ⓘ
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	ⓘ

NetApp ONTAP System Manager | tme-mcc-site2ab

Search actions, objects, and pages

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	ⓘ
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	ⓘ

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.

Add volume

Name

NFS01

☐ Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity

1024

GiB

Performance service level

Extreme

Not sure?

[Get help selecting type](#)

Optimization options

☒ Distribute volume data across the cluster (FlexGroup) ?
☐ Advanced capacity balancing
ONTAP distributes file data to maintain balance as files grow.

Access permissions

☒ Export via NFS

GRANT ACCESS TO HOST

default

Create a new export policy, or select an existing export policy.

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	Vmknfc	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	Vmknfc	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.

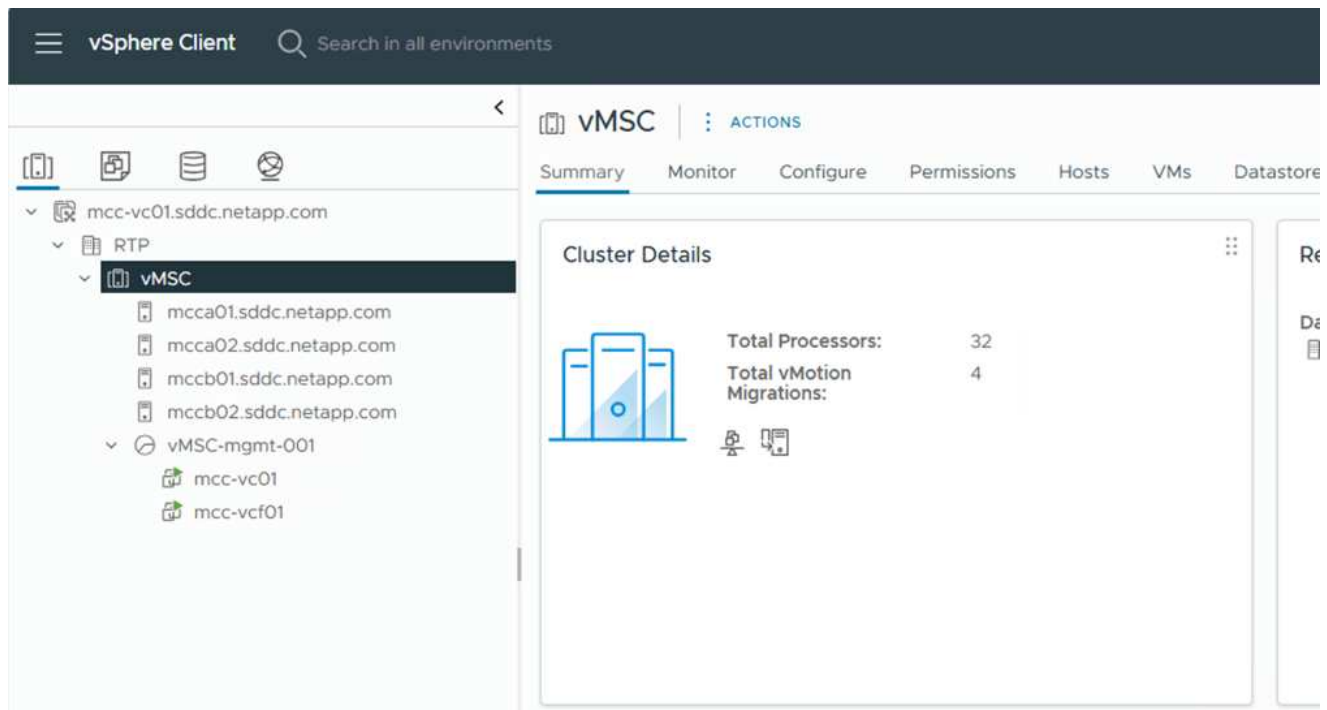
1. Folgen Sie den Schritten unter ["Führen Sie vor der Konvertierung eine Vorprüfung des Ziel-vCenters durch"](#) um die Validierung auszuführen.
2. Die folgende Ausgabe zeigt, dass die vCenter-Appliance die Vorprüfung bestanden hat.

```
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 23:02:10,499] [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-Workloadomäne 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:

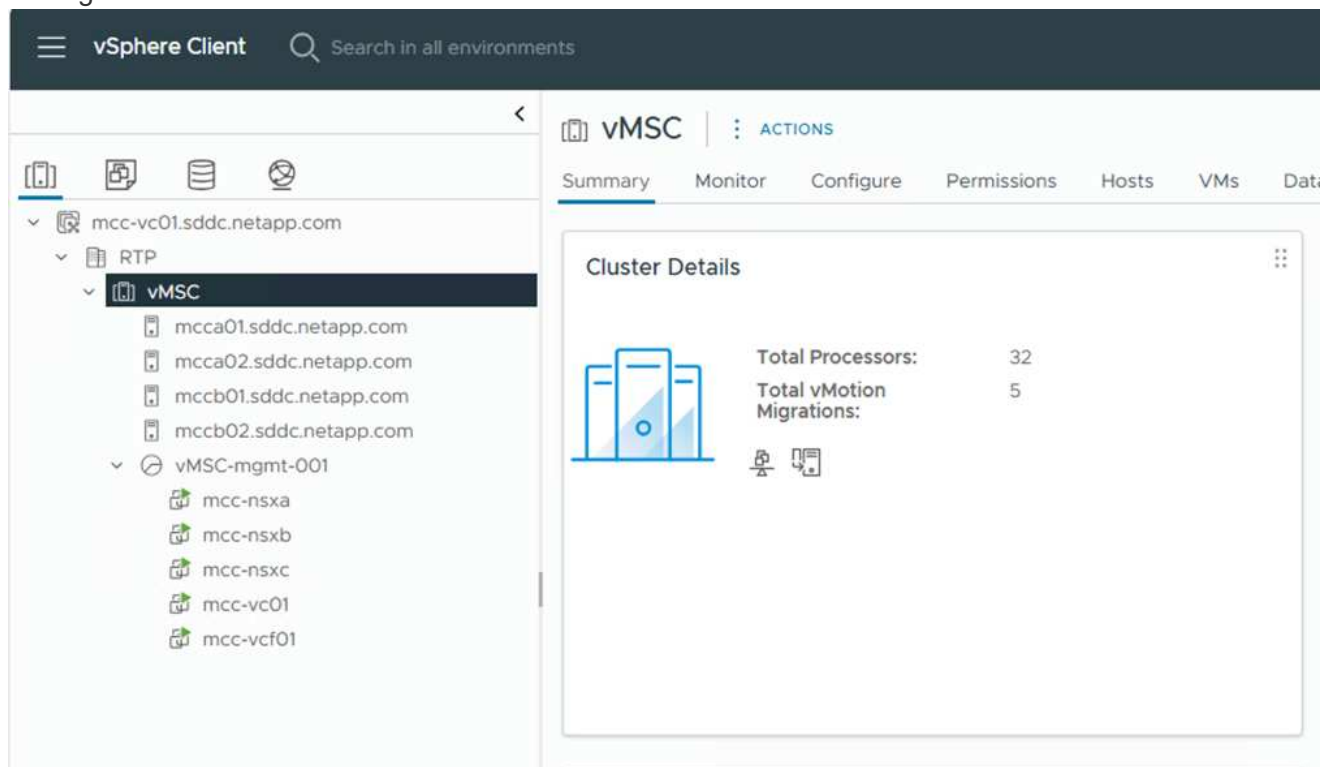
```
python3 vcf_brownfield.py convert --vcenter '<vcenter-fqdn>' --sso-user '<sso-user>' --sso-password '*****' --vcenter-root-password '*****' --local-admin-password '*****' --backup-password '*****' --domain-name '<Mgmt-domain-name>' --accept-trust --nsx-deployment-spec-path /home/vcf/nsx.json
```

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
```

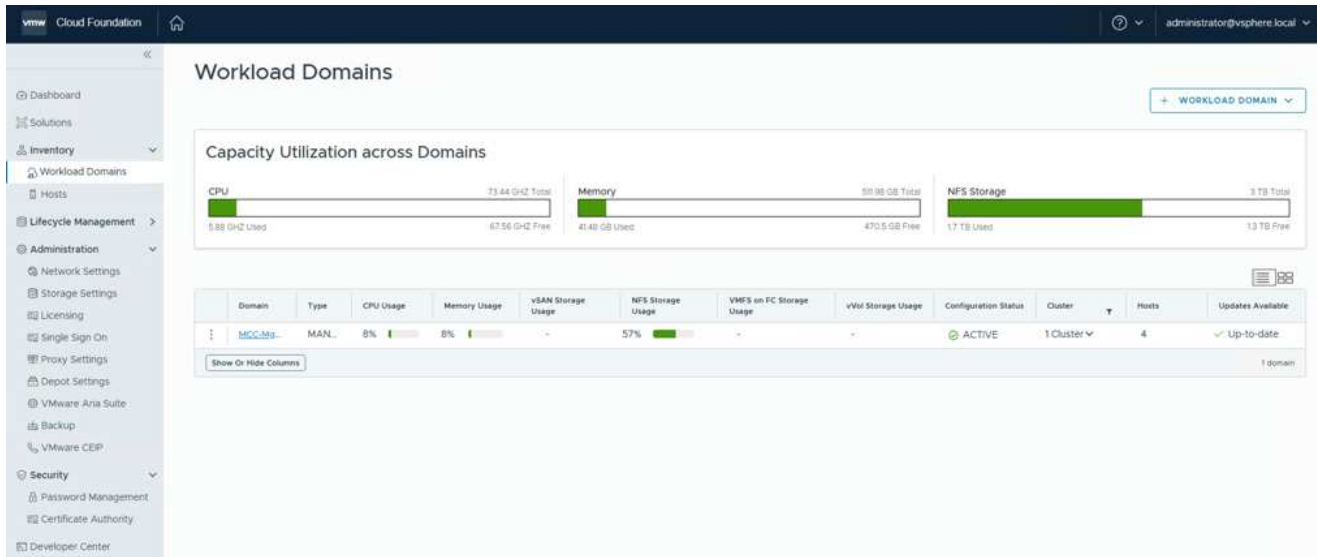
Vollständige Anweisungen finden Sie unter ["VCF-Konvertierungsverfahren"](#).

NSX-VMs werden in vCenter bereitgestellt.

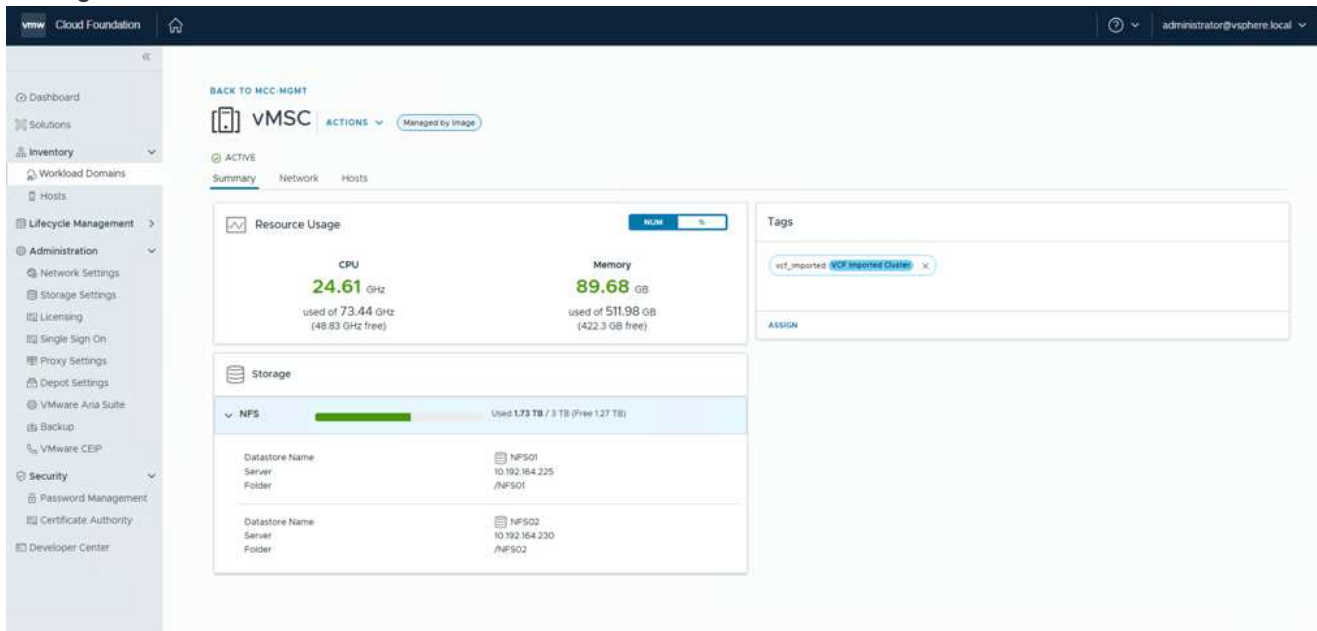


SDDC Manager zeigt die erstellte Verwaltungsdomäne mit dem angegebenen Namen und NFS als

Datenspeicher an.



Bei der Überprüfung des Clusters werden die Informationen zum NFS-Datenspeicher bereitgestellt.



Lizenzierung zu VCF hinzufügen

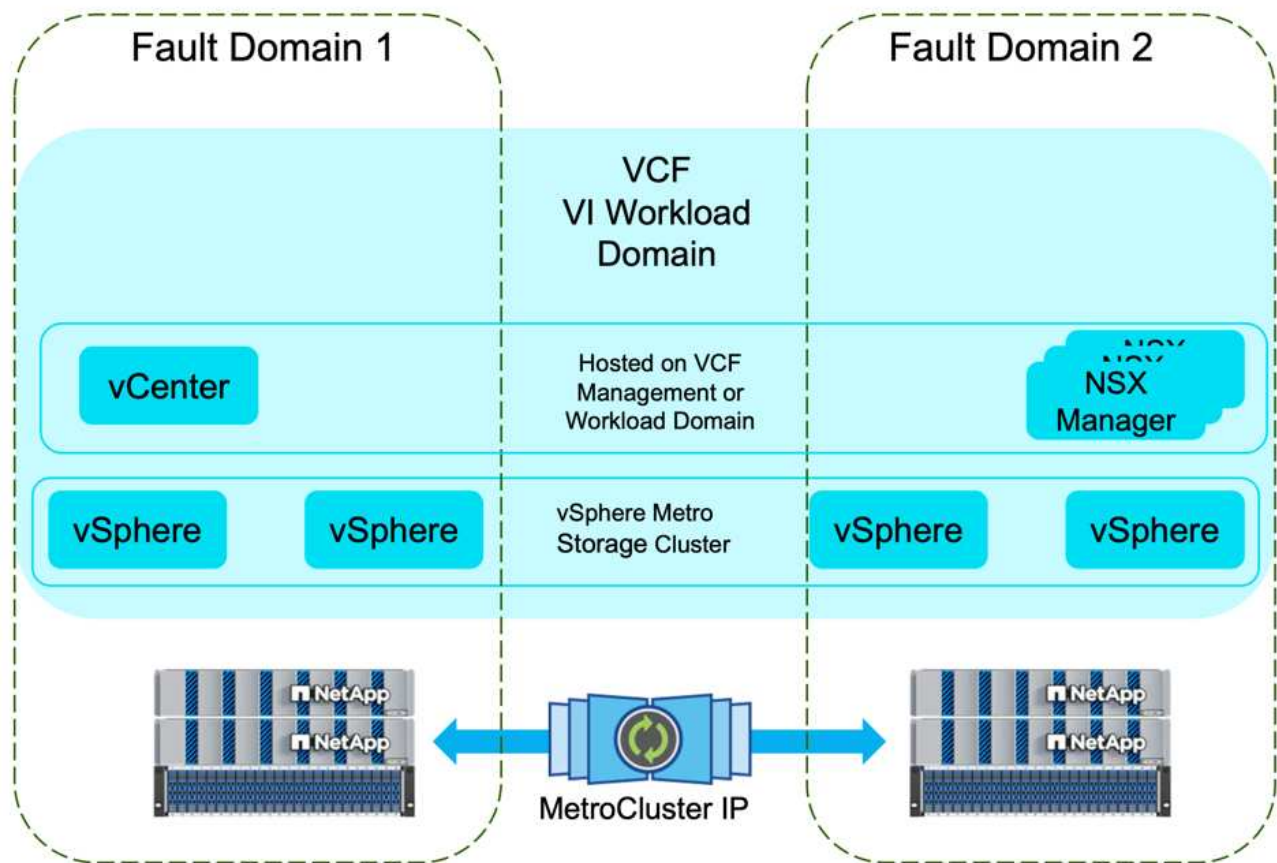
Nach Abschluss der Konvertierung muss der Umgebung eine Lizenzierung hinzugefügt werden.

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.

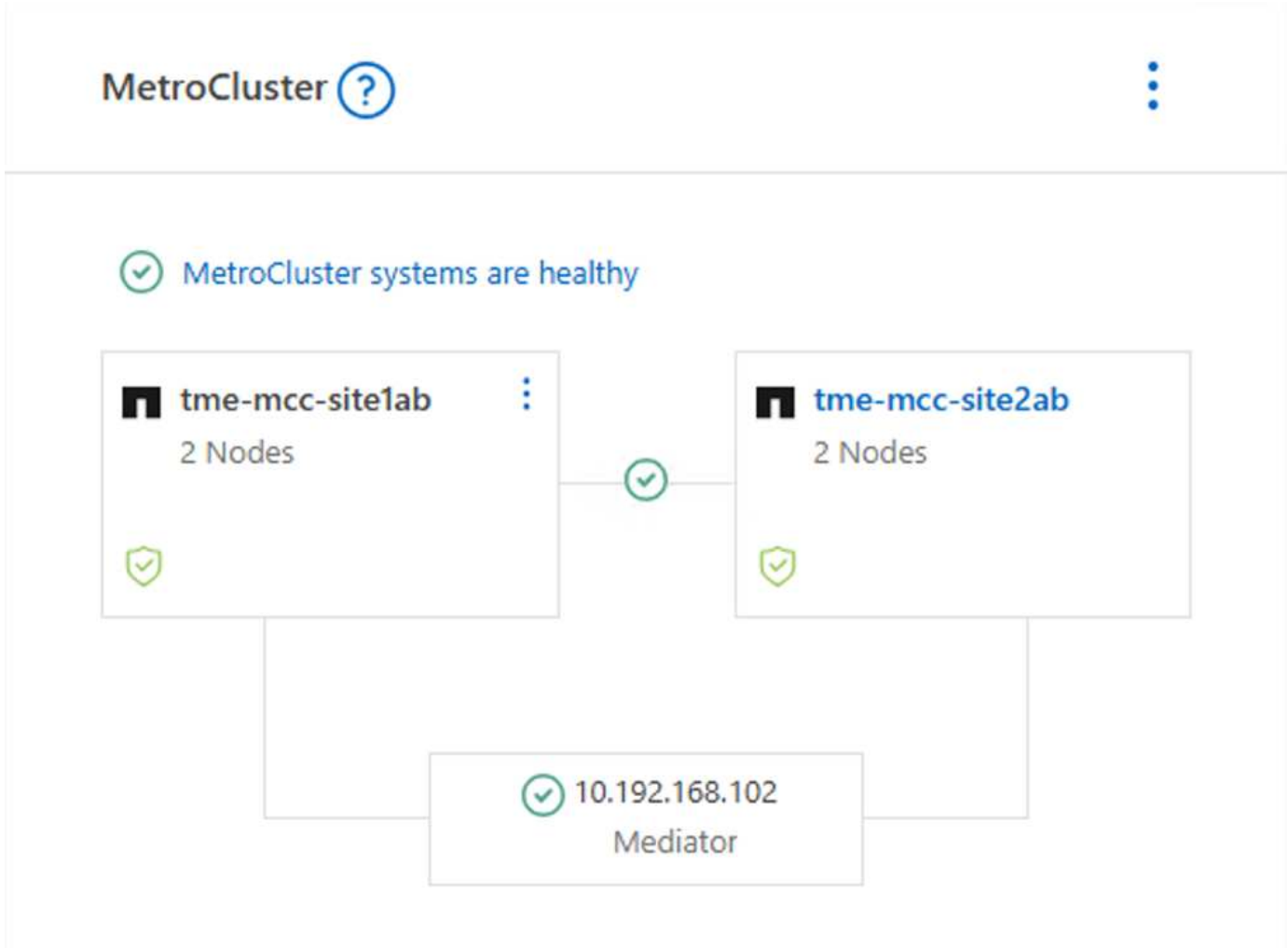
Voraussetzungen

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	↑
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	↑
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.

NetApp ONTAP System Manager | tme-mcc-site1ab

Search actions, objects, and pages

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	🛡
ch-svm-mcc02-mc	Stopped	Sync_destination		Default	n/a	🛡

NetApp ONTAP System Manager | tme-mcc-site2ab

Search actions, objects, and pages

Storage VMs

+ Add

Name	State	Subtype	Configured protocols	IPspace	Maximum capacity	Protection
ch-svm-mcc01-mc	Stopped	Sync_destination		Default	n/a	🛡
ch-svm-mcc02	Running	Sync_source	NFS, SMB/CIFS	Default	The maximum capacity is disabled	🛡

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.

Add volume

Name

WLD01_DS01

☐ Add as a cache for a remote volume (FlexCache)
Simplifies file distribution, reduces WAN latency, and lowers WAN bandwidth costs.

Storage and optimization

Capacity

500

GIB

Performance service level

Extreme

Not sure?

[Get help selecting type](#)

Optimization options

☐ Distribute volume data across the cluster (FlexGroup) ?

Access permissions

☒ Export via NFS

GRANT ACCESS TO HOST

default

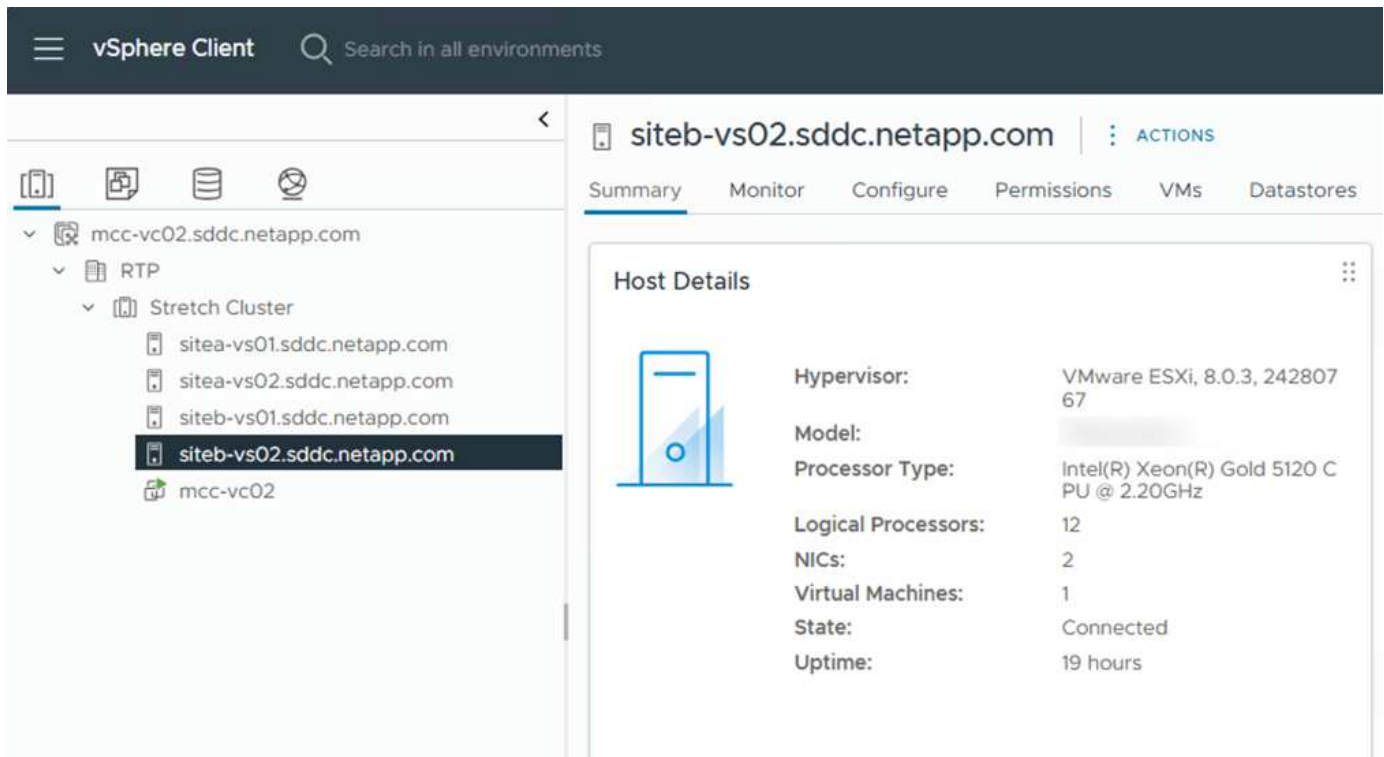
Create a new export policy, or select an existing export policy.

Rule index	Clients	Access protocols	Read-only rule	Rea
9	0.0.0.0/0	NFSv3, NFSv4, SMB/CIFS, NFS	Any	Any

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
```

```
vcf@ms-vcf01: ~$ cd vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset/
vcf@ms-vcf01: ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset$ python3 vcf_brownfield.py check
[2025-03-23 17:48:44.979] [INFO] vcf_brownfield: brownfield import main version: 5.2.1.2-24494579
[2025-03-23 17:48:44.980] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
usage: vcf_brownfield.py check [-h] --vcenter VCENTER_ADDRESS --sso-user SSO_USERNAME [--sso-password SSO_PASSWORD] [--local-admin-password LOCAL_ADMIN_PASSWORD] [--skip-nsx-deployment-checks] [--accept-trust]
vcf_brownfield.py check: error: the following arguments are required: --vcenter, --sso-user
vcf@ms-vcf01: ~/vcf-brownfield-import-5.2.1.2-24494579/vcf-brownfield-toolset$ python3 vcf_brownfield.py check --vcenter mcc-vc02.sddc.netapp.com --sso-user administrator@vsphere.local --sso-password '*****' --local-admin-passwor
d '*****' --accept-trust
[2025-03-23 17:41:46.491] [INFO] vcf_brownfield: brownfield import main version: 5.2.1.2-24494579
[2025-03-23 17:41:46.491] [INFO] vcf_brownfield: Please make sure you are always using the latest version of the scripts
[2025-03-23 17:41:46.500] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:46.601] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:46.941] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:46.942] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47.015] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47.016] [INFO] sddc_manager_helper: Retrieving SDDC Manager controller info
[2025-03-23 17:41:47.016] [INFO] sddc_manager_helper: Using cached SDDC Manager token header
[2025-03-23 17:41:47.511] [INFO] request_helper: Response status from SDDC Manager controller info retrieval: 200
[2025-03-23 17:41:47.510] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47.594] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47.595] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:47.661] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:47.900] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:47.900] [INFO] sddc_manager_helper: Using cached SDDC Manager token header
[2025-03-23 17:41:48.114] [INFO] request_helper: Response status from retrieving domain: 200
[2025-03-23 17:41:48.115] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:48.115] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:48.180] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:48.212] [INFO] request_helper: Response status from retrieving trusted certificates: 200
[2025-03-23 17:41:48.418] [INFO] trust_vcenter: Retrieved server mcc-vc02.sddc.netapp.com thumbprint (SHA256): 94:F3:C7:05:DF:FF:E6:C9:68:06:50:92:3C:B7:7D:15:85:68:38:A1:FD:27:2B:56:6D:85:FA:D5:02:AE:3C:46
[2025-03-23 17:41:48.419] [WARNING] trust_vcenter: Auto accept trust is turned ON.
[2025-03-23 17:41:48.419] [INFO] vcenter_rest_api_helper: Generating session to vcenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:48.552] [INFO] request_helper: Response status from vcenter session authentication: 201
[2025-03-23 17:41:48.553] [INFO] vcenter_rest_api_helper: Retrieving trusted root CA chain IDs of vcenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:50.065] [INFO] request_helper: Response status from vcenter trusted root CA chain IDs retrieval: 200
[2025-03-23 17:41:50.086] [INFO] vcenter_rest_api_helper: Retrieving trusted root CA chain with id: 9c0a09d6d6c81d51adce988e7f7f85c4a9b7f of vcenter: mcc-vc02.sddc.netapp.com
[2025-03-23 17:41:50.073] [INFO] request_helper: Response status from vcenter trusted root CA chain retrieval: 200
[2025-03-23 17:41:50.074] [INFO] sddc_manager_helper: Retrieving SDDC Manager trusted certificates
[2025-03-23 17:41:50.074] [INFO] sddc_manager_helper: Generating SDDC Manager public API token
[2025-03-23 17:41:50.949] [INFO] request_helper: Response status from SDDC Manager token generation: 200
[2025-03-23 17:41:50.970] [INFO] request_helper: Response status from retrieving trusted certificates: 200
[2025-03-23 17:41:50.985] [INFO] sddc_manager_certificate_util: Adding new trusted certificate for alias: 9c0a09d6d6c81d51adce988e7f7f85c4a9b7f with thumbprint: DA:6F:94:90:09:83:66:66:E7:CD:60:49:EC:98:2E:03:EA:AB:57:ED:0B:EC:03:5C:3
A:85:40:4C:60:40:F4:EF
[2025-03-23 17:41:50.985] [INFO] sddc_manager_certificate_util: Adding new trusted certificate for alias: mcc-vc02.sddc.netapp.com with thumbprint: 94:F3:C7:05:DF:FF:E6:C9:68:06:50:92:3C:B7:7D:15:85:68:38:A1:FD:27:2B:56:6D:85:FA:D5:02:AE:3C:46
[2025-03-23 17:41:50.985] [INFO] sddc_manager_helper: Importing trusted certificates to SDDC Manager trust store
[2025-03-23 17:41:52.074] [INFO] request_helper: Response status from certificates import: 200
[2025-03-23 17:41:53.101] [INFO] request_helper: Response status from certificates refresh: 200
```

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.

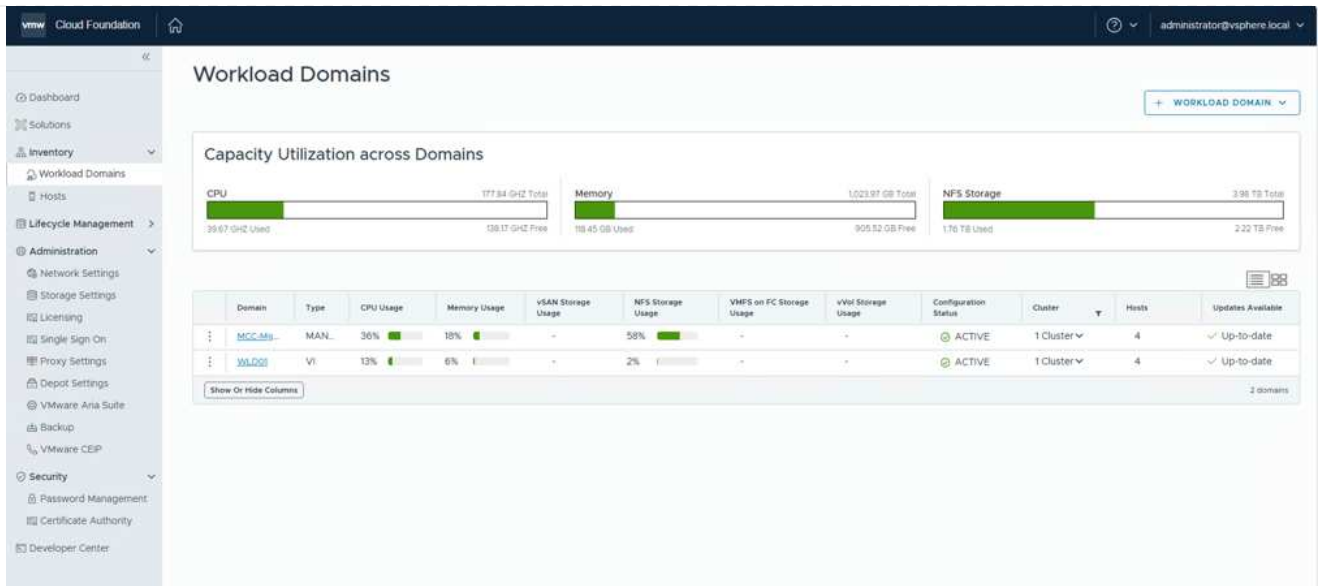
Vollständige Anweisungen finden Sie unter ["VCF-Konvertierungsverfahren"](#).

NSX-VMs werden in vCenter bereitgestellt.

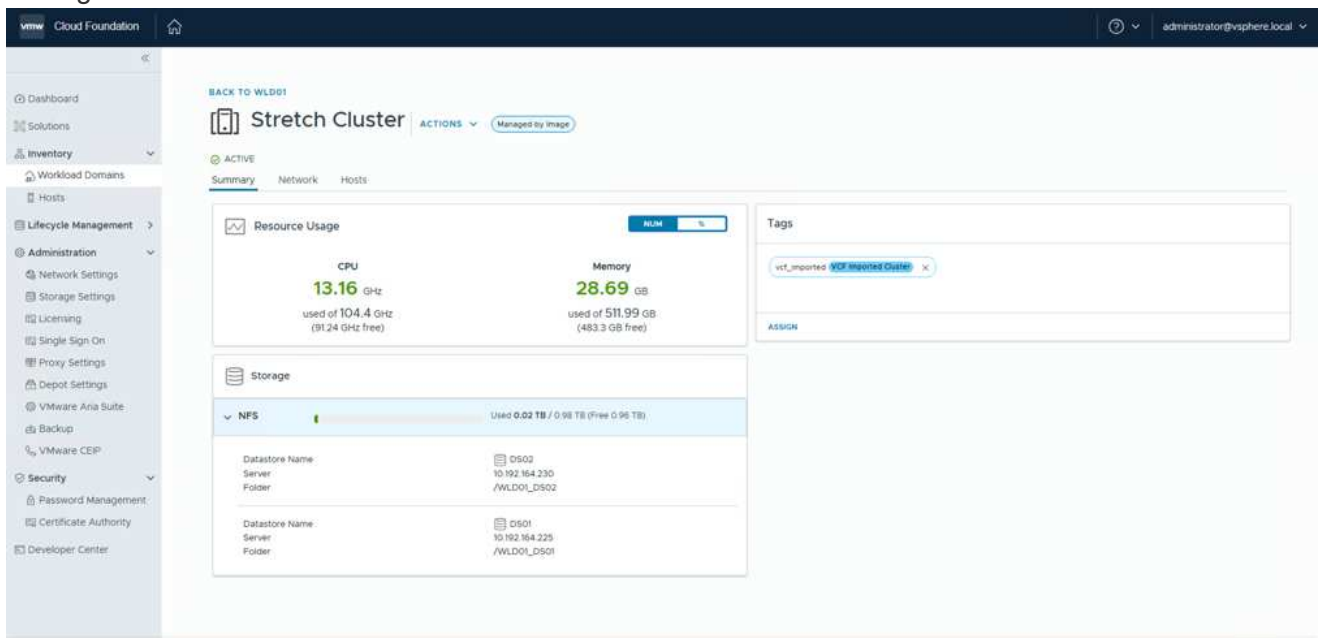
The screenshot shows the vSphere Client interface. On the left, the inventory tree displays the hierarchy: **mcc-vc02.sddc.netapp.com** > **RTP** > **Stretch Cluster**. Under the Stretch Cluster, several hosts are listed, with **siteb-vs02.sddc.netapp.com** selected and highlighted. Below the hosts, other resources like **mcc-vc02**, **mcc-wld01-nsxa**, **mcc-wld01-nsxb**, and **mcc-wld01-nsxc** are visible. On the right, the **Host Details** panel for the selected host is shown. It includes a summary of the host's configuration:

Property	Value
Hypervisor:	VMware ESXi, 8.0.3, 24280767
Model:	
Processor Type:	Intel(R) Xeon(R) Gold 5120 C PU @ 2.20GHz
Logical Processors:	12
NICs:	2
Virtual Machines:	2
State:	Connected
Uptime:	20 hours

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.



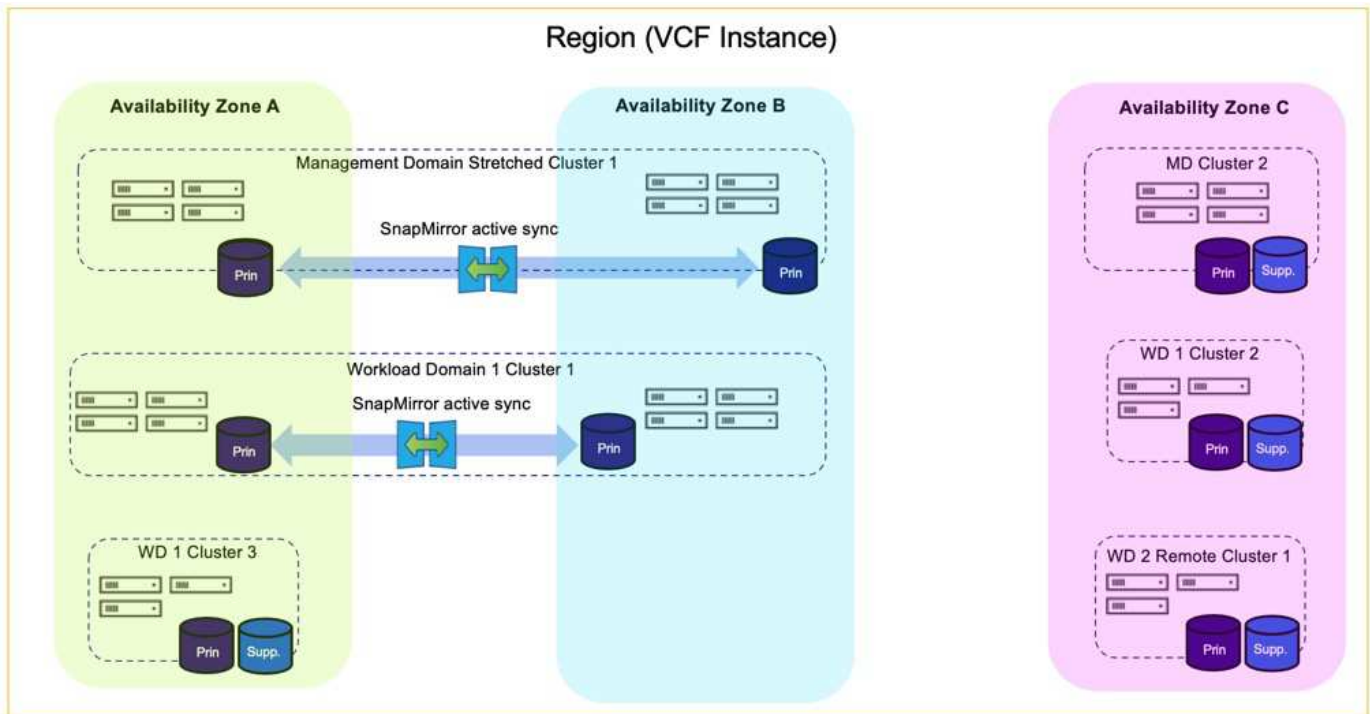
Lizenzierung zu VCF hinzufügen

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.

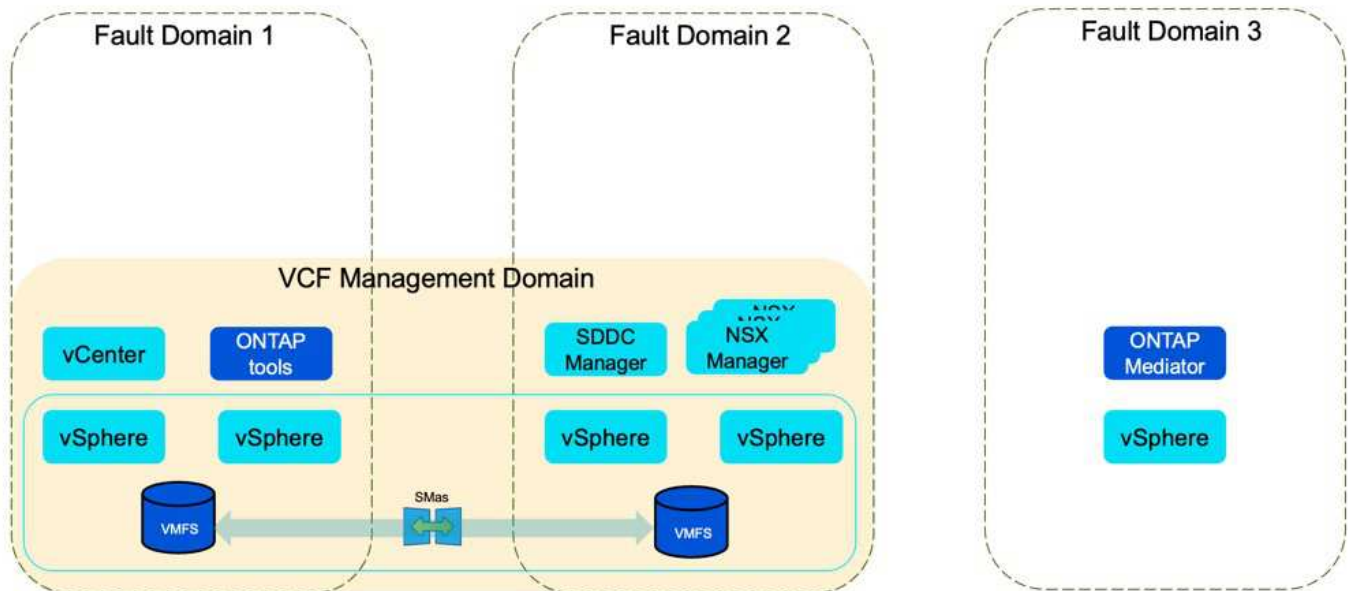


Szenarioübersicht

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 .

VMFS with FC



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.

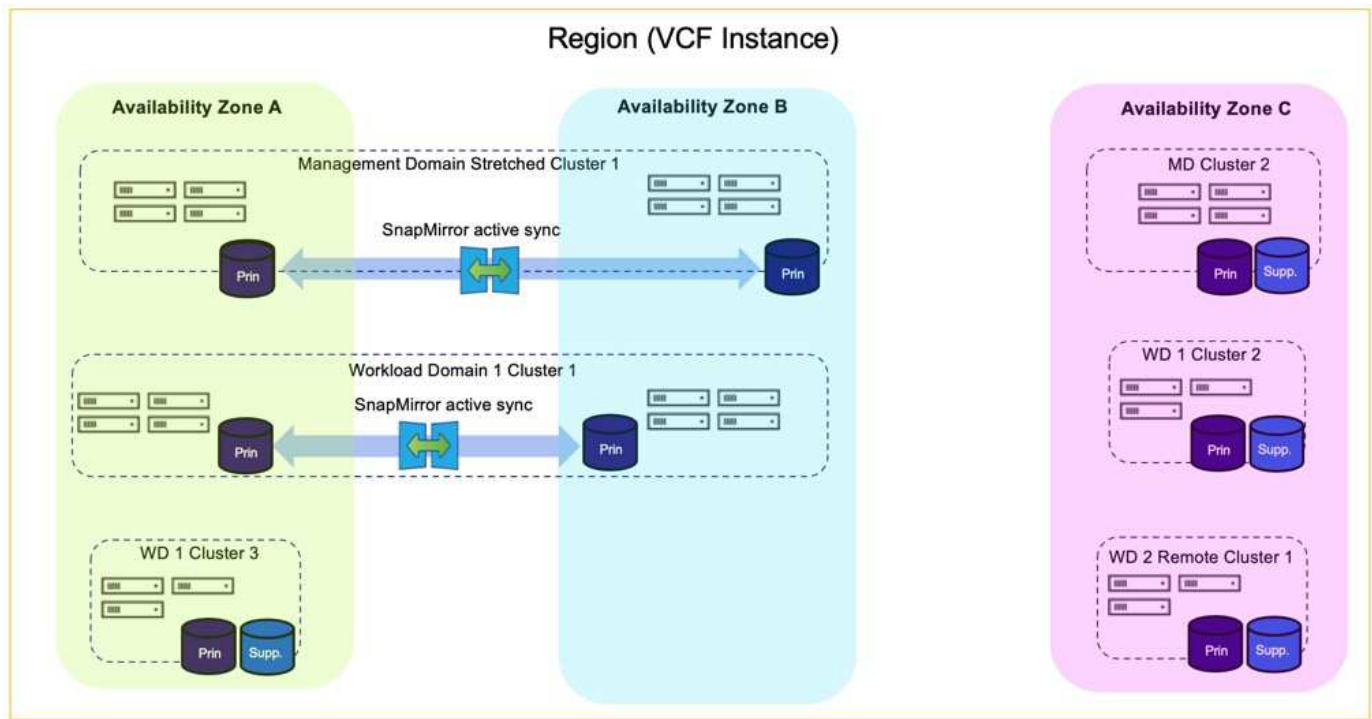
Informationen zur Konfiguration von VCF finden Sie unter ["Dokumentation zu VMware Cloud Foundation 5.2"](#) .

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.



Bei einigen VMs, die mit externen Management-Tools wie VCF Automation, vSphere Supervisor (oder anderen Kubernetes-Varianten) bereitgestellt werden, kommt es üblicherweise auf die Speicherrichtlinie der VM an. Bei einer Migration zwischen Datenspeichern innerhalb derselben VM-Speicherrichtlinie sollte dies geringere Auswirkungen auf die Anwendungen haben. Klären Sie mit den Anwendungsbesitzern ab, wie die VMs ordnungsgemäß in den neuen Datenspeicher migriert werden können. vSphere 8 führte ein ["vSphere vMotion-Benachrichtigungen für latenzempfindliche Anwendungen"](#) um Anträge für vMotion vorzubereiten.

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.

Summary

Monitor

Configure

Permissions

VMs

Databases

Networks

Updates

Storage

Storage Adapters

Storage Devices

Host Cache Configuration

Protocol Endpoints

I/O Filters

Networking

Virtual switches

VMkernel adapters

Physical adapters

RDMA adapters

TCP/IP configuration

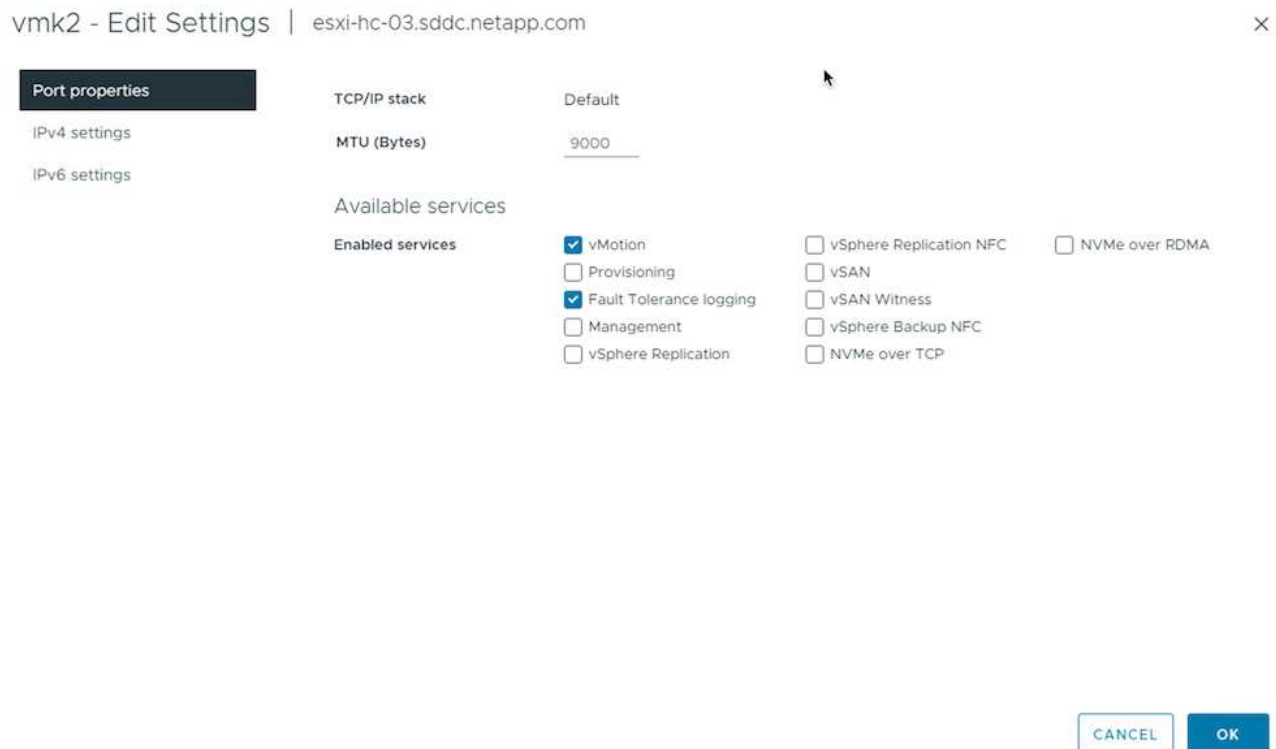
Virtual Machines

VMkernel adapters

ADD NETWORKING... REFRESH

	Device	Network Label	Switch	IP Address	TCP/IP Stack	Enabled Services
⋮	vmk0	Mgmt 181	DSwitch	10.61.181.213	Default	Management
⋮	vmk1	vSAN 3376	DSwitch	172.21.120.103	Default	vSAN
⋮	vmk2	vMotion 3373	DSwitch	172.21.117.113	Default	vMotion +2
⋮	vmk3	iSCSI A - 1172	DSwitch	10.63.172.91	Default	--
⋮	vmk4	iSCSI B - 1172	DSwitch	10.63.172.92	Default	--
⋮	vmk5	Data A - 3374	DSwitch	172.21.118.123	Default	--
⋮	vmk6	VLAN 3418	DSwitch	172.21.162.103	Default	Provisioning

Wenn Sie die VMKernel-Schnittstelle bearbeiten, besteht hier die Möglichkeit, die erforderlichen Dienste zu aktivieren.



vmk2 - Edit Settings | esxi-hc-03.sddc.netapp.com

Port properties

IPv4 settings

IPv6 settings

TCP/IP stack: Default

MTU (Bytes): 9000

Available services

Enabled services

- ☒ vMotion
- ☐ Provisioning
- ☒ Fault Tolerance logging
- ☐ Management
- ☐ vSphere Replication
- ☐ vSphere Replication NFC
- ☐ vSAN
- ☐ vSAN Witness
- ☐ vSphere Backup NFC
- ☐ NVMe over TCP
- ☐ NVMe over RDMA

CANCEL OK



Stellen Sie sicher, dass mindestens zwei aktive Hochgeschwindigkeits-Uplink-Netzwerkarten 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.

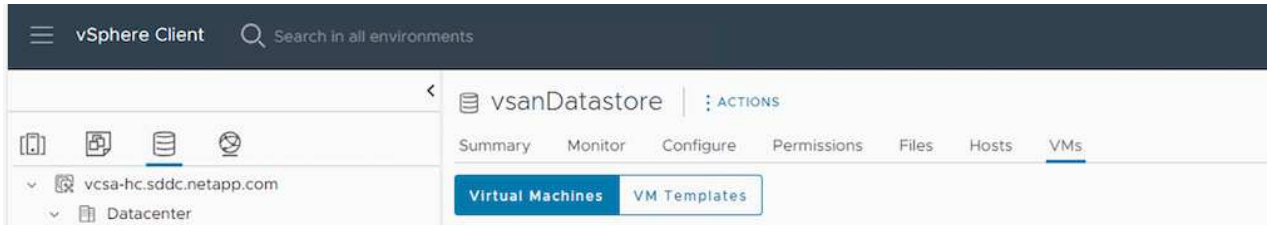


Verstehen "[VM-Bedingungen und Einschränkungen von vSphere vMotion](#)" bevor Sie mit VM-Migrationsoptionen fortfahren.

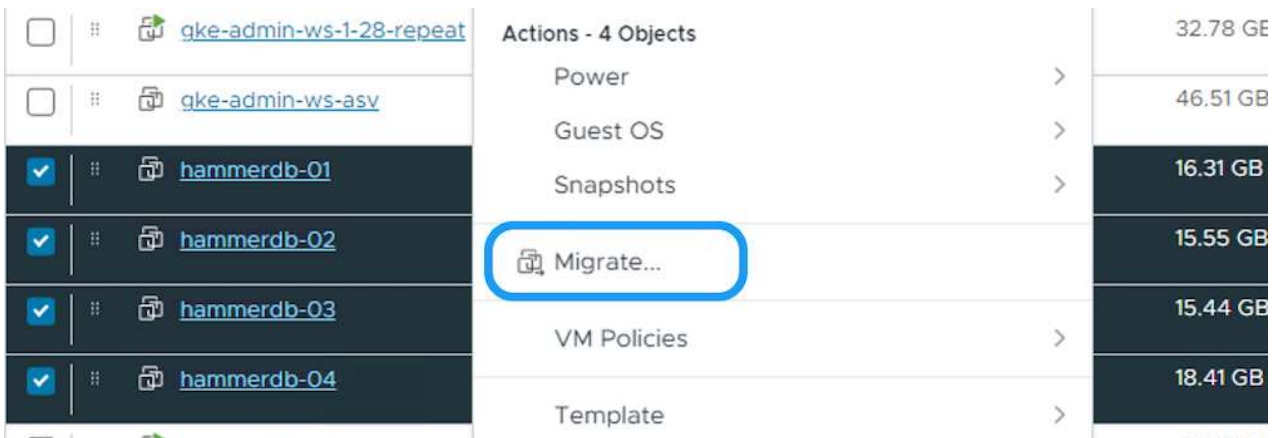
Migration von VMs aus einem bestimmten vSphere-Datenspeicher

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 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

☐ Change compute resource only

Migrate the virtual machines to another host or cluster.

☒ Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

☐ Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

☐ Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Thin Provision

VM Storage Policy

NetApp Storage

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/>	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	
<input type="radio"/>	destination	Incompatible	250 GB	31.8 MB	249.97 GB	
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	
<input type="radio"/>	E13A400_JSCSI	Incompatible	2 TB	858.66 GB	1.85 TB	

Manage Columns

Items per page 5 1 - 5 of 14 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Überprüfen Sie den Eintrag und klicken Sie auf „Fertig stellen“.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete



Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

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

```

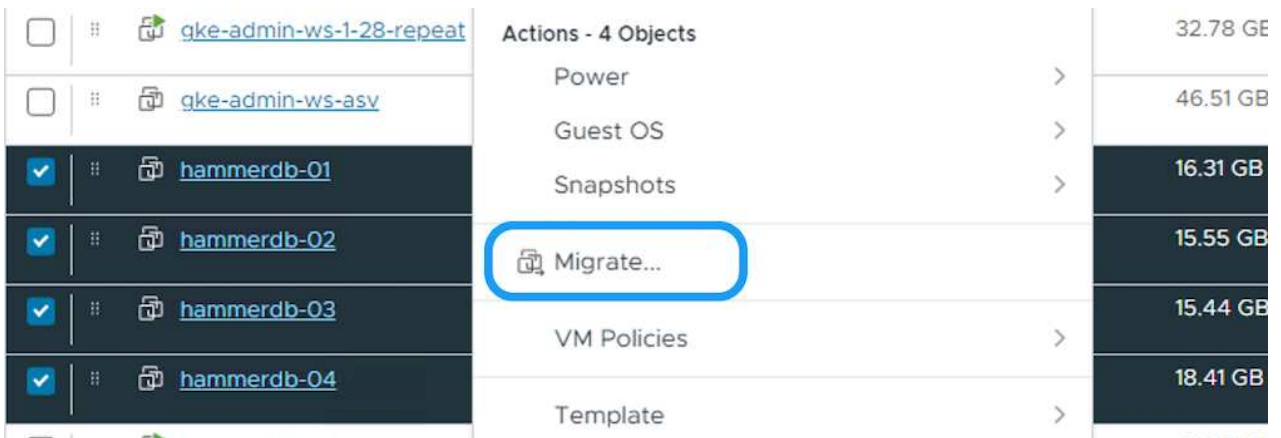
Migration von VMs im selben vSphere-Cluster

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 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

☐ Change compute resource only

Migrate the virtual machines to another host or cluster.

☒ Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

☐ Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

☐ Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Thin Provision

VM Storage Policy

NetApp Storage

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	34.38 GB	1.95 TB	
<input type="radio"/>	DemoDS	Incompatible	800 GB	7.23 GB	792.77 GB	
<input type="radio"/>	destination	Incompatible	250 GB	31.8 MB	249.97 GB	
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	201.13 GB	880.86 GB	
<input type="radio"/>	E13A400_JSCSI	Incompatible	2 TB	858.66 GB	1.85 TB	

Manage Columns

Items per page 5 1 - 5 of 14 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Überprüfen Sie den Eintrag und klicken Sie auf „Fertig stellen“.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Ready to complete



Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL

BACK

FINISH

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.

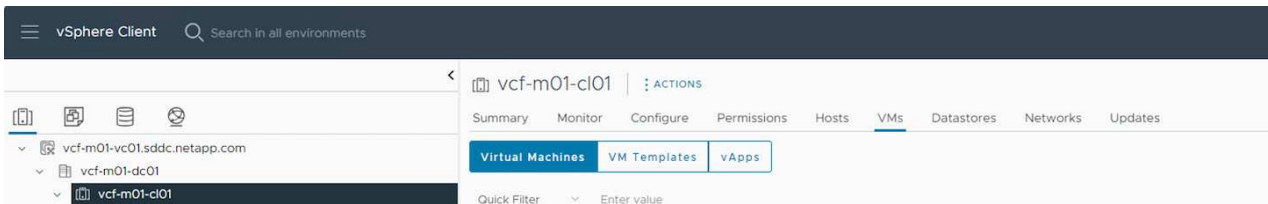
Migration von VMs über mehrere vSphere-Cluster



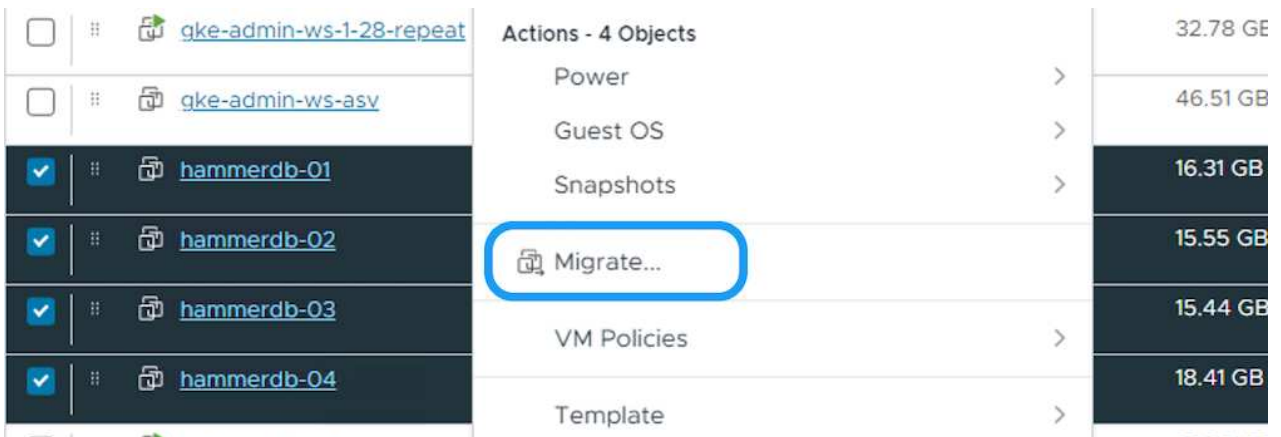
Verweisen "[CPU-Kompatibilität und vSphere Enhanced vMotion-Kompatibilität](#)" wenn Quell- und Zielhosts zu unterschiedlichen CPU-Familien oder Modellen gehören.

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 Virtual Machines - Migrate

- 1 Select a migration type**
- Select a compute resource
- Select storage
- Select networks
- Select vMotion priority
- Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

- ☐ **Change compute resource only**
Migrate the virtual machines to another host or cluster.
- ☐ **Change storage only**
Migrate the virtual machines' storage to a compatible datastore or datastore cluster.
- ☒ **Change both compute resource and storage**
Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.
- ☐ **Cross vCenter Server export**
Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL
NEXT

4. Navigieren Sie und wählen Sie den richtigen Cluster für die Migration aus.

4 Virtual Machines - Migrate

- Select a migration type
- 2 Select a compute resource**
- Select storage
- Select networks
- Select vMotion priority
- Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- vcf-m01-vc01.sddc.netapp.com
 - vcf-m01-dc01
- vcf-wkld-vc01.sddc.netapp.com
 - IT-INF-WKLD-01**

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

5. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage**
- Select folder
- Select networks
- Select vMotion priority
- Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision

VM Storage Policy NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	

Manage Columns Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

6. Wählen Sie den VM-Ordner aus, in dem die Ziel-VMs platziert werden sollen.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage
- Select folder**
- Select networks
- Select vMotion priority
- Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - Discovered virtual machine**
 - vCLS

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

7. Wählen Sie die Zielpartgruppe aus.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage
- Select folder
- Select networks**
- Select vMotion priority
- Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Überprüfen Sie den Eintrag und klicken Sie auf „Fertig stellen“.

4 Virtual Machines - Migrate

- Select a migration type
- Select storage
- Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

```

#Authenticate to vCenter
Connect-VIServer -server vc.sa.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

```

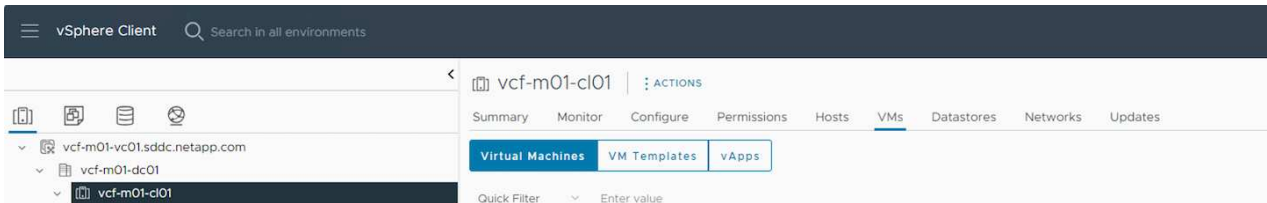
Migration von VMs über vCenter-Server in derselben SSO-Domäne

Befolgen Sie die nachstehenden Schritte, um VMs auf einen neuen vCenter-Server zu migrieren, der auf derselben vSphere-Client-Benutzeroberfläche aufgeführt ist.

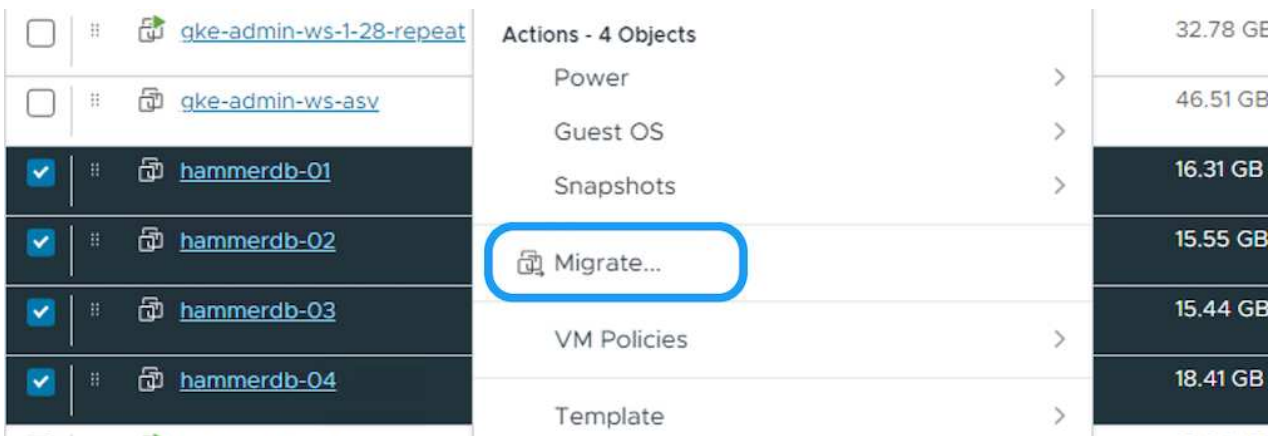


Weitere Anforderungen wie Quell- und Ziel-vCenter-Versionen usw. finden Sie unter ["vSphere-Dokumentation zu den Anforderungen für vMotion zwischen vCenter-Serverinstanzen"](#)

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 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

☐ Change compute resource only

Migrate the virtual machines to another host or cluster.

☐ Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

☒ Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

☐ Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

CANCEL

NEXT

4. Wählen Sie den Zielcluster im Ziel-vCenter-Server aus.

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a compute resource

3 Select storage

4 Select networks

5 Select vMotion priority

6 Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

- ▼ vcf-m01-vc01.sddc.netapp.com
 - > vcf-m01-dc01
- ▼ vcf-wkld-vc01.sddc.netapp.com
 - ▼ vcf-wkld-01-DC
 - > IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

5. Wählen Sie die gewünschte VM-Speicherrichtlinie und den kompatiblen Datenspeicher aus. Klicken Sie auf Weiter.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage**
- Select folder
- Select networks
- Select vMotion priority
- Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE **CONFIGURE PER DISK**

Select virtual disk format Thin Provision

VM Storage Policy NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.91 GB	5 TB	
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	18 MB	2.93 TB	
<input type="radio"/>	VCF_WKLD_03_ISCSI	Incompatible	3 TB	858.61 GB	2.85 TB	
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	
<input type="radio"/>	vcf-wkld-esx03-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	

[Manage Columns](#) Items per page: 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

6. Wählen Sie den VM-Ordner aus, in dem die Ziel-VMs platziert werden sollen.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage
- Select folder**
- Select networks
- Select vMotion priority
- Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

Select location for the virtual machine migration.

- vcf-wkld-01-DC
 - Discovered virtual machine**
 - vCLS

✓ Compatibility checks succeeded.

CANCEL
BACK
NEXT

7. Wählen Sie die Zielpartgruppe aus.

4 Virtual Machines - Migrate

- Select a migration type
- Select a compute resource
- Select storage
- Select folder
- Select networks**
- Select vMotion priority
- Ready to complete

Select networks

Select destination networks for the virtual machine migration.
Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

Source Network	Used By	Destination Network
>> SDDC-DPortGroup-VM-Mgmt	4 VMs / 4 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-0

1 item

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL BACK NEXT

8. Überprüfen Sie die Migrationsoptionen und klicken Sie auf „Fertig stellen“.

4 Virtual Machines - Migrate

- Select a migration type
- Select storage
- Ready to complete**

Ready to complete

Verify that the information is correct and click Finish to start the migration.

Migration Type	Change storage. Leave VM on the original compute resource
Virtual Machine	Migrating 4 VMs
Storage	ASA_VVOLS_1
VM storage policy	NetApp Storage
Disk Format	Thin Provision

CANCEL BACK FINISH

Hier ist das Beispielskript zum Migrieren von VMs mit PowerCLI.

```

#Authenticate to Source vCenter
$sourcevc = Connect-VIServer -server vc01.sddc.netapp.local -force
$targetvc = Connect-VIServer -server vc02.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

```

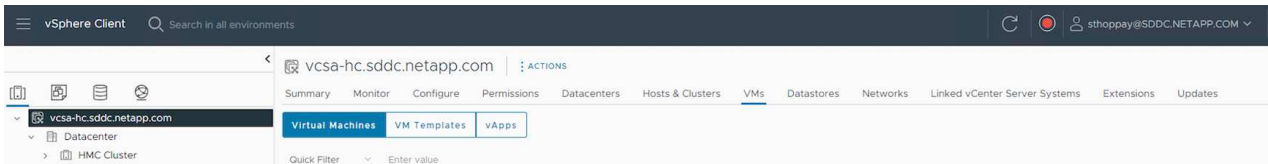
Migration von VMs über vCenter-Server in verschiedenen SSO-Domänen



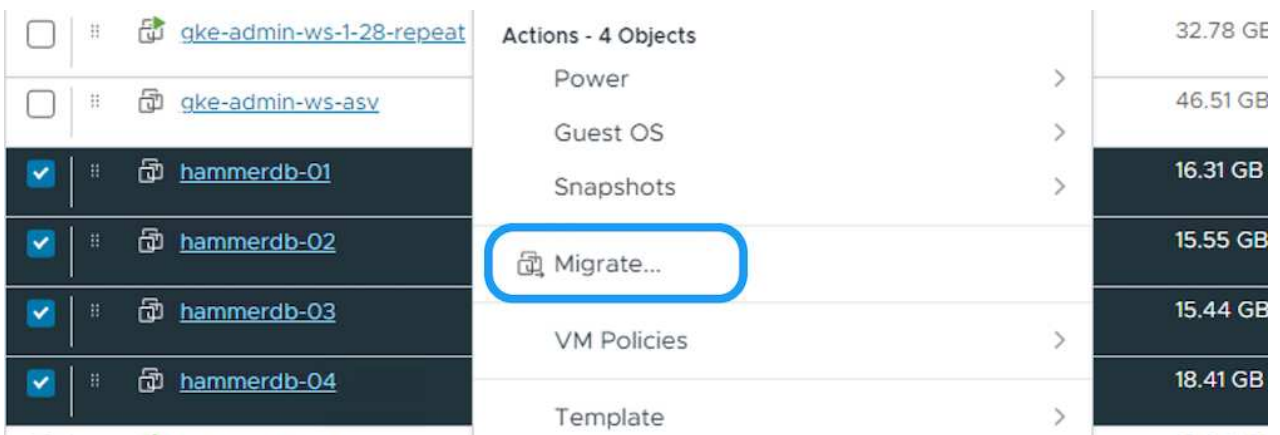
Dieses Szenario geht davon aus, dass die Kommunikation zwischen den vCenter-Servern besteht. Andernfalls prüfen Sie das unten aufgeführte Szenario für mehrere Rechenzentrumsstandorte. Voraussetzungen finden Sie unter ["vSphere-Dokumentation zu Advanced Cross vCenter vMotion"](#)

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

4 Virtual Machines - Migrate

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select networks

6 Select vMotion priority

7 Ready to complete

Select a migration type

Change the virtual machines' compute resource, storage, or both.

☐ Change compute resource only

Migrate the virtual machines to another host or cluster.

☐ Change storage only

Migrate the virtual machines' storage to a compatible datastore or datastore cluster.

☐ Change both compute resource and storage

Migrate the virtual machines to a specific host or cluster and their storage to a specific datastore or datastore cluster.

☒ Cross vCenter Server export

Migrate the virtual machines to a vCenter Server not linked to the current SSO domain.

☐ Keep VMs on the source vCenter Server (performs a VM clone operation).

CANCEL

NEXT



VM kann auch vom Ziel-vCenter-Server importiert werden. Überprüfen Sie für dieses Verfahren ["Importieren oder Klonen einer virtuellen Maschine mit Advanced Cross vCenter vMotion"](#)

4. Geben Sie die vCenter-Anmeldeinformationen ein und klicken Sie auf „Anmelden“.

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select networks

6 Ready to complete

Select a target vCenter Server

Export Virtual Machines to the selected target vCenter Server.

SAVED VCENTER SERVERS

NEW VCENTER SERVER

vCenter Server address

vcf-wkld-vc01.sddc.netapp.com

vCenter Server FQDN or IP address

Username

administrator@vcf.local

example@domain.local

Password

Password

Save vCenter Server address ⓘ



LOGIN

CANCEL

BACK


NEXT

5. Bestätigen und akzeptieren Sie den Fingerabdruck des SSL-Zertifikats des vCenter-Servers

Security Alert

Unable to verify the authenticity of the external vCenter Server.

The SHA1 thumbprint of the vCenter Server certificate is:
17:42:0C:EB:82:1E:A9:86:F1:E0:70:93:AD:EB:8C:0F:27:41:F1:30

 Connect anyway?

Click Yes if you trust the vCenter Server.
Click No to cancel connecting to the vCenter Server.

6. Erweitern Sie das Ziel-vCenter und wählen Sie den Ziel-Compute-Cluster aus.

Migrate | SQLSRV-05

- Select a migration type
- Select a target vCenter Server
- Select a compute resource**
- Select storage
- Select networks
- Ready to complete

Select a compute resource

Select a cluster, host, vApp or resource pool to run the virtual machines.

VM ORIGIN ⓘ

vcf-wkld-vc01.sddc.netapp.com

vcf-wkld-01-DC

IT-INF-WKLD-01

Compatibility

✓ Compatibility checks succeeded.

7. Wählen Sie den Zieldatenspeicher basierend auf der VM-Speicherrichtlinie aus.

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select folder

6 Select networks

7 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

VM ORIGIN ⓘ

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Thin Provision

VM Storage Policy

NFS

	Name	Storage Compatibility	Capacity	Provisioned	Free	T
<input checked="" type="radio"/>	VCF_WKLD_01	Compatible	5 TB	5.93 GB	5 TB	N
<input type="radio"/>	VCF_WKLD_02_VVOLS	Incompatible	2.93 TB	24 MB	2.93 TB	v
<input type="radio"/>	VCF_WKLD_03_JSCSI	Incompatible	3 TB	1.35 TB	2.59 TB	v
<input type="radio"/>	vcf-wkld-esx01-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	v
<input type="radio"/>	vcf-wkld-esx02-esx-install-datastore	Incompatible	25.75 GB	3.68 GB	22.07 GB	v

Manage Columns

Items per page 10 7 items

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Wählen Sie den Ziel-VM-Ordner aus.

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select folder

6 Select networks

7 Ready to complete

Select folder

Select the destination virtual machine folder for the virtual machine migration.

VM ORIGIN ⓘ

Select location for the virtual machine migration.

vcf-wkld-01-DC

Discovered virtual machine

Oracle

SQL Server

vCLS

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

9. Wählen Sie die VM-Portgruppe für jede Netzwerkschnittstellenkartenzuordnung aus.

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select folder

6 Select networks

7 Ready to complete

Select networks

Select destination networks for the virtual machine migration.

VM ORIGIN ⓘ

Migrate VM networking by selecting a new destination network for all VM network adapters attached to the same source network.

	Source Network	Used By	Destination Network
»	Mgmt 181	1 VMs / 1 Network adapters	vcf-wkld-01-IT-INF-WKLD-01-vds-01-p
»	Data A - 3374	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-a
»	Data B - 3375	1 VMs / 1 Network adapters	vcf-wkld-01-iscsi-b

3 items

ADVANCED >>

Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

10. Überprüfen Sie die Angaben und klicken Sie auf „Fertig stellen“, um vMotion auf den vCenter-Servern zu starten.

Migrate | SQLSRV-05

1 Select a migration type

2 Select a target vCenter Server

3 Select a compute resource

4 Select storage

5 Select folder

6 Select networks

7 Ready to complete

Ready to complete

Verify that the information is correct and click Finish to start the migration.

VM ORIGIN ⓘ

Migration Type	Change compute resource and storage
Virtual Machine	SQLSRV-05
vCenter	vcf-wkld-vc01.sddc.netapp.com
Folder	SQL Server
Cluster	IT-INF-WKLD-01
Networks	Virtual network adapters from 3 networks will be reassigned to new destination networks
Storage	VCF_WKLD_01
VM storage policy	NFS
Disk Format	Thin Provision

CANCEL

BACK

FINISH

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.
- Continuous 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.
- ["NetApp Notfallwiederherstellung"](#) nutzt speicherarraybasierte 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"](#)
- ["NetApp Disaster Recovery"](#) nutzt speicherarraybasierte Replikation und automatisiert bestimmte Aufgaben, um die VMs am Zielstandort wiederherzustellen.
- Mit unterstützten Continuous 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.

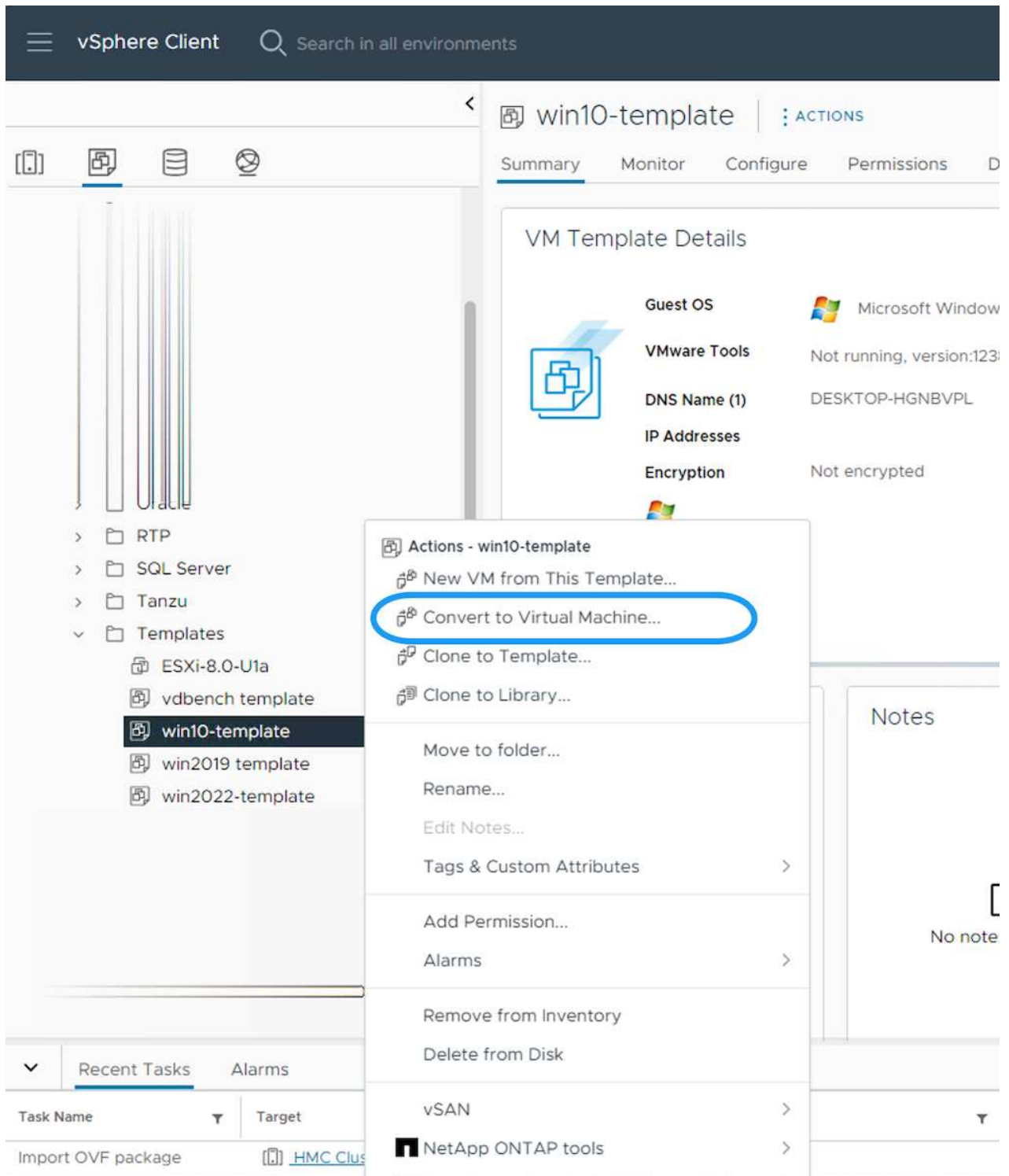
- Im vCenter-Inventar gespeicherte VM-Vorlagen können in VMs konvertiert werden und die VM-

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



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

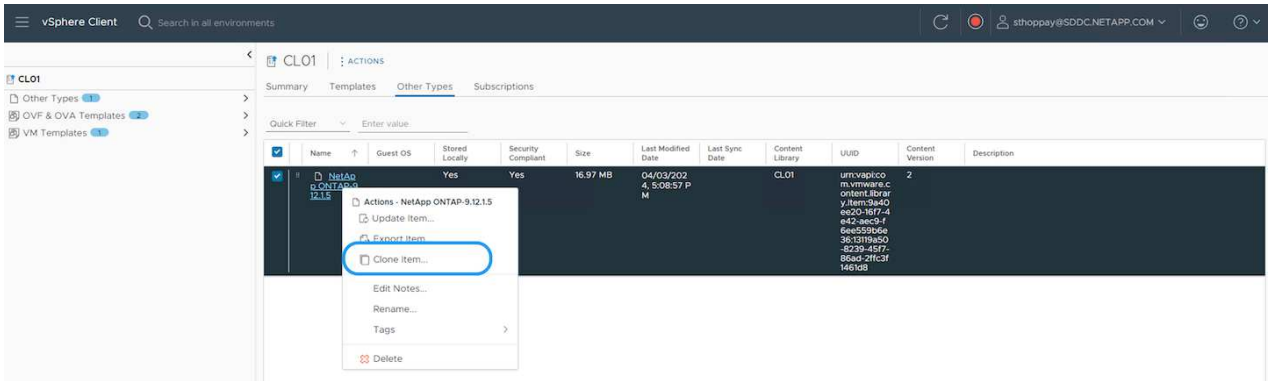


VMware Aria Operations Configuration



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.

Clone Library Item

NetApp ONTAP-9.12.1.5

×

Name

NetApp ONTAP-9.12.1.5

Notes

Select a content library where to clone the library item.

	Name	Notes	Creation Date
<input type="radio"/>	CL01		9/26/2023, 5:02:03 PM
<input checked="" type="radio"/>	CL02		4/1/2024, 12:37:51 PM

CANCEL

OK

5. Überprüfen Sie, ob das Element in der Zielinhaltsbibliothek verfügbar ist.

	Name	Guest OS	Stored Locally	Security Compliant	Size	Last Modified Date	Last Sync Date	Content Library	UUID	Content Version	Description
<input type="checkbox"/>	vmware-workstation-ovf		Yes	Yes	16.97 MB	04/03/2024, 5:39:01 PM		CL02	urn:vmware:content-library-item:a7cf728a-702a-473a-a0fa-8e330562f03b:1b19a50-0-6239-45f7-86aa-2ffc3f1460b8	2	

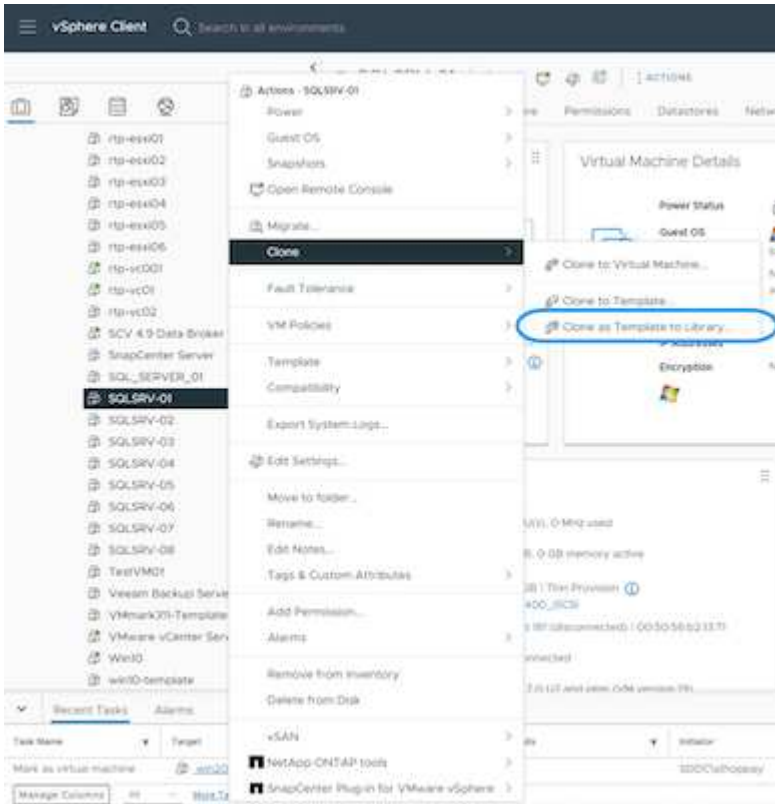
Hier ist das PowerCLI-Beispielskript zum Kopieren der Inhaltsbibliothekselemente von der Inhaltsbibliothek CL01 nach CL02.

```
#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-ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL01' -Server
$sourcevc) | Where-Object { $_.ItemType -ne 'vm-template' } | Copy-
ContentLibraryItem -ContentLibrary (Get-ContentLibrary 'CL02' -Server
$targetvc)
```

Hinzufügen von VM als Vorlagen 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.

SQLSRV-01 - Clone Virtual Machine To Template

1 Basic information

2 Location

3 Select a compute resource

4 Select storage

5 Ready to complete

Basic information

Template type

VM Template

Name

SQLSRV-01

Notes

Select a folder for the template

vcasa-hc.sddc.netapp.com

Datacenter

CANCEL

NEXT



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-Workload-Domäne.



Um die Netzwerkkommunikation mit vorhandenen VMs auf anderen Clustern im Quell-vCenter zu ermöglichen, erweitern Sie entweder das NSX-Segment, indem Sie die 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"](#)

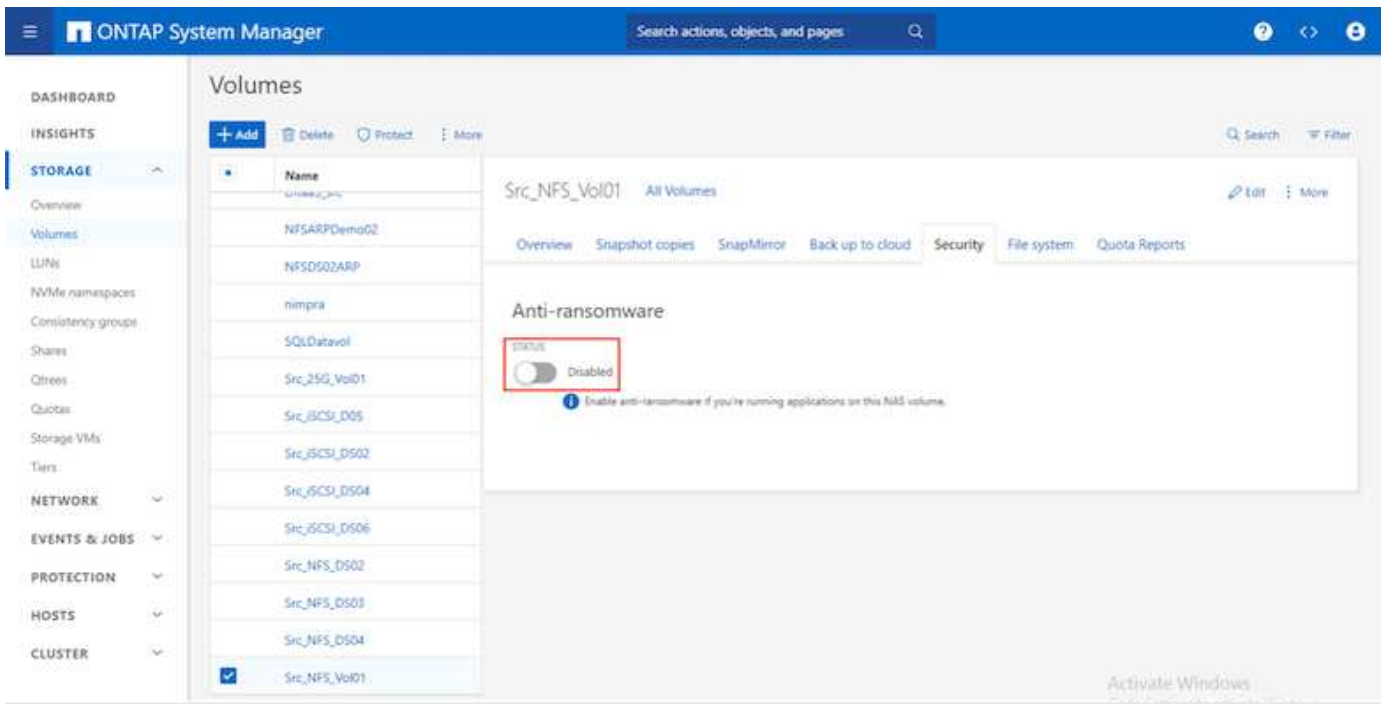
Weitere Ressourcen

- ["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"](#)
- ["NetApp 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 Härtingsrichtlinien. 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-Volumen, 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.

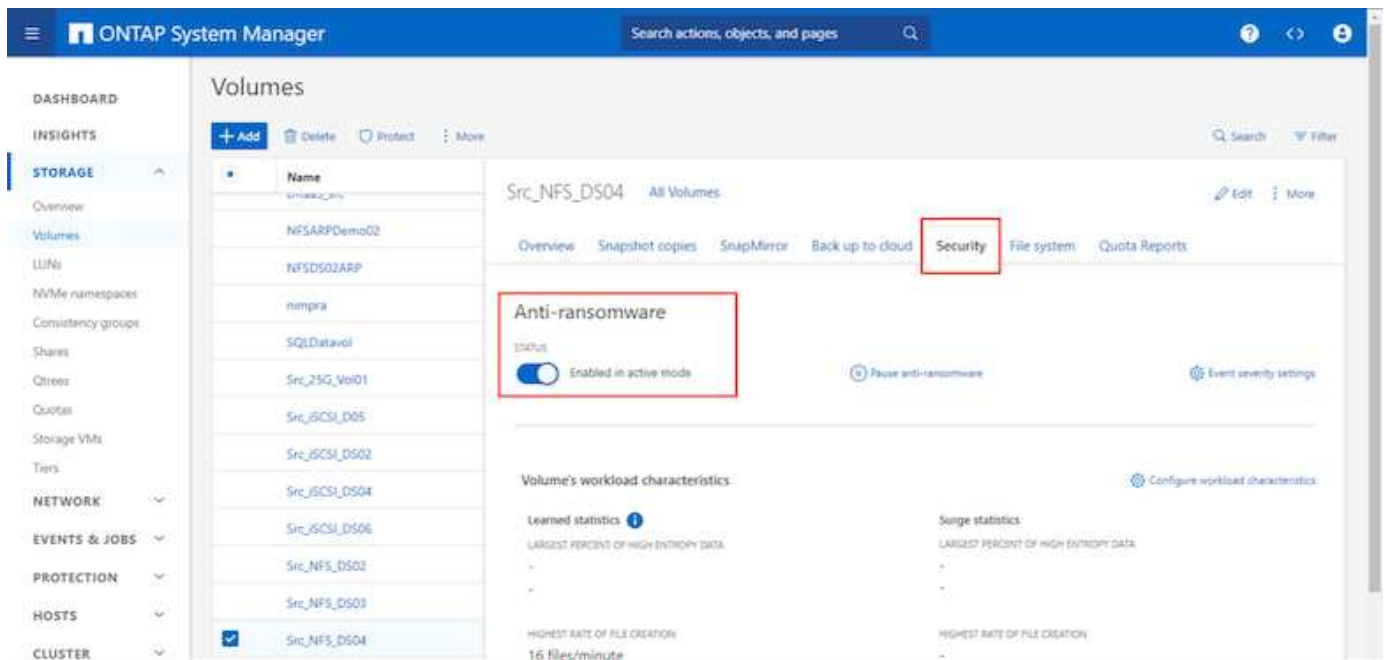


Mit dem neuen NetApp ARP/AI, das sich derzeit in der Tech Preview befindet, ist kein Lernmodus erforderlich. Stattdessen kann es mit seiner KI-gestützten Ransomware-Erkennungsfunktion direkt in den aktiven Modus wechseln.



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.

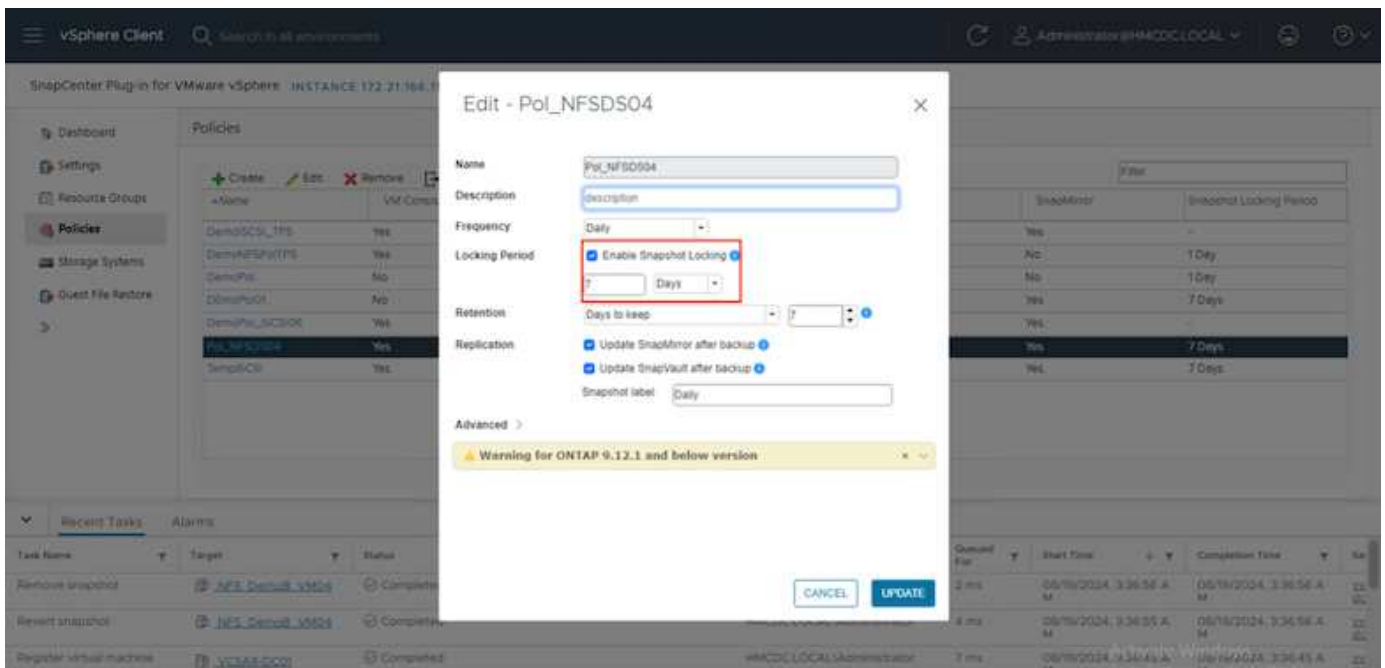
Sobald es sich im aktiven Modus befindet, beginnt es mit der Suche nach abnormaler Volumenaktivität, bei der es sich möglicherweise um Ransomware handeln könnte. Wenn eine ungewöhnliche Aktivität erkannt wird, wird sofort automatisch eine Snapshot-Kopie erstellt, die einen Wiederherstellungspunkt bereitstellt, der möglichst nahe an der Dateinfektion 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.



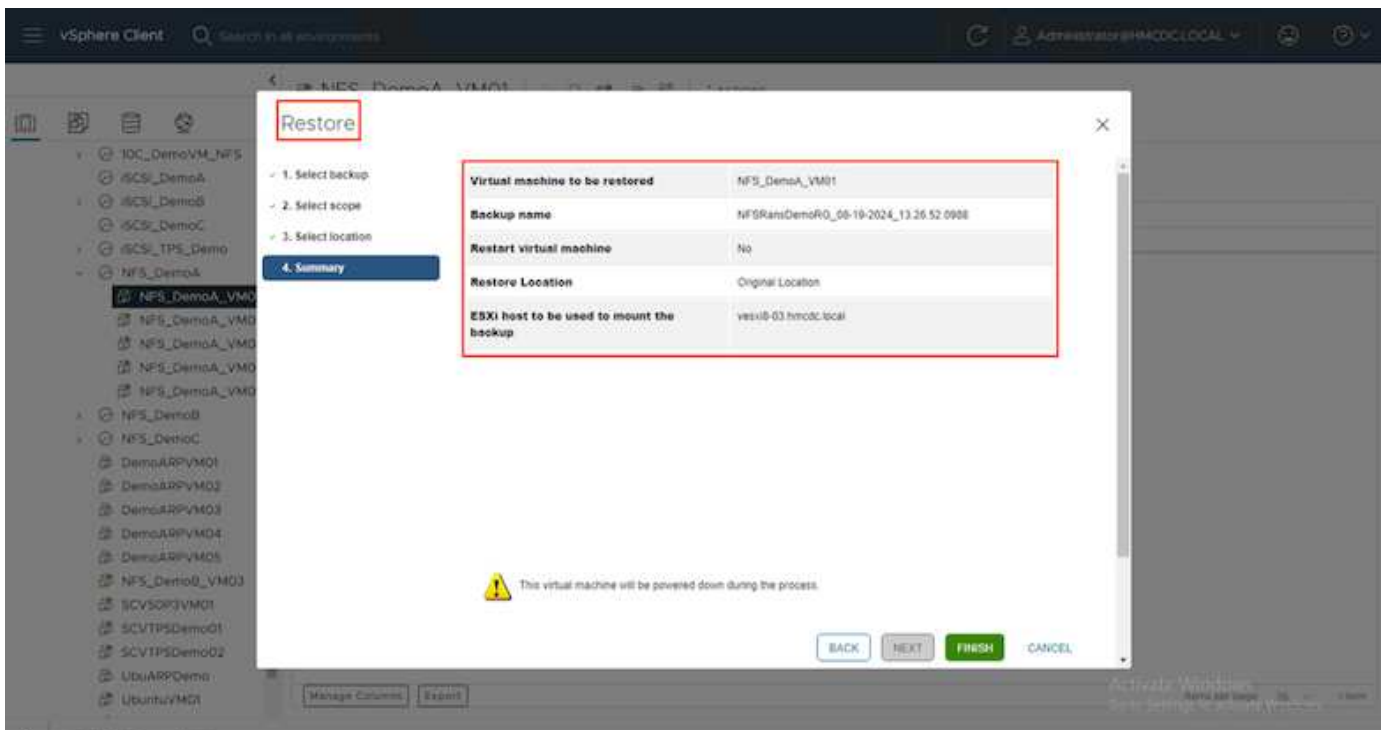
Wenn ein Ransomware-Angriff auf die virtuelle Maschine (VM) abzielt und Dateien innerhalb der VM ändert, ohne Änderungen außerhalb der VM vorzunehmen, erkennt Advanced Ransomware Protection (ARP) die Bedrohung dennoch, wenn die Standardentropie der VM niedrig ist, beispielsweise bei Dateitypen wie .txt-, .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 orchestriert und mit SIEM-Tools integriert werden muss, kann ein Offtap-Dienst wie NetApp Ransomware Resilience verwendet werden. Es handelt sich um einen Dienst, der Daten vor Ransomware

schützen soll. 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 NetApp Ransomware Resilience geschützt.



Die unten beschriebenen Schritte beziehen sich auf BlueXP. Der Arbeitsablauf ist bei der NetApp Console ähnlich.

NetApp BlueXP									
Ransomware protection									
Dashboard Protection Alerts Recovery Reports									
Free trial (55 days left) - view details									
Workloads (10)									
Workload	Type	Connector	Importance	Protection st...	Detection sta...	Detection pol...	Snapshot an...	Backup destine...	
Src_nfs_ds02	VM datastore	GISABXPConn	Critical	Protected	Learning mode	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Draas_arc_test_3130	VM file share	GISABXPConn	Standard	At risk	None	None	None	n/a	Protect
Nfsdc02zrp_804	VM file share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection
Draas_src_7027	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_vol01_7948	VM file share	GISABXPConn	Standard	At risk	None	None	None	netapp-backup-add...	Protect
Src_nfs_ds03	VM datastore	GISABXPConn	Standard	At risk	None	None	SnapCenter for VMw...	netapp-backup-add...	Protect
Src_nfs_ds04	VM datastore	GISABXPConn	Standard	Protected	Active	rps-policy-primary	SnapCenter for VMw...	netapp-backup-add...	Edit protection
Src_nfs_ds04	File share	GISABXPConn	Critical	Protected	Active	rps-policy-primary	BlueXP backup and ...	netapp-backup-ba3...	Edit protection
Testvol_1787	File share	GISABXPConn	Standard	Protected	Learning mode	rps-policy-primary	None	netapp-backup-ba3...	Edit protection
Nfsarpdemo02_1419	File share	GISABXPConn	Standard	Protected	Active	rps-policy-primary	None	netapp-backup-add...	Edit protection

NetApp BlueXP

BlueXP Search

Standard Importance

Protected Protection health Edit protection

0 Alerts

Not marked for recovery Recovery

Protection

These policies managed by SnapCenter for VMware will not be modified by applying a detection policy to this workload.

Pol_NFS0504 Snapshot policy

1 Year Daily LTR Backup policy

VM datastore

Location um:scv:scvml:Resou...

vCenter server vc:sa8-01.hmdc.local

Connector GISABXPConn

Storage

Cluster id add38d26-348c-11ef-B...

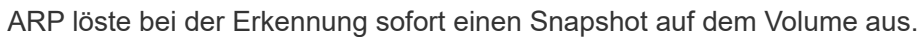
Working Env name NTAP915_Src

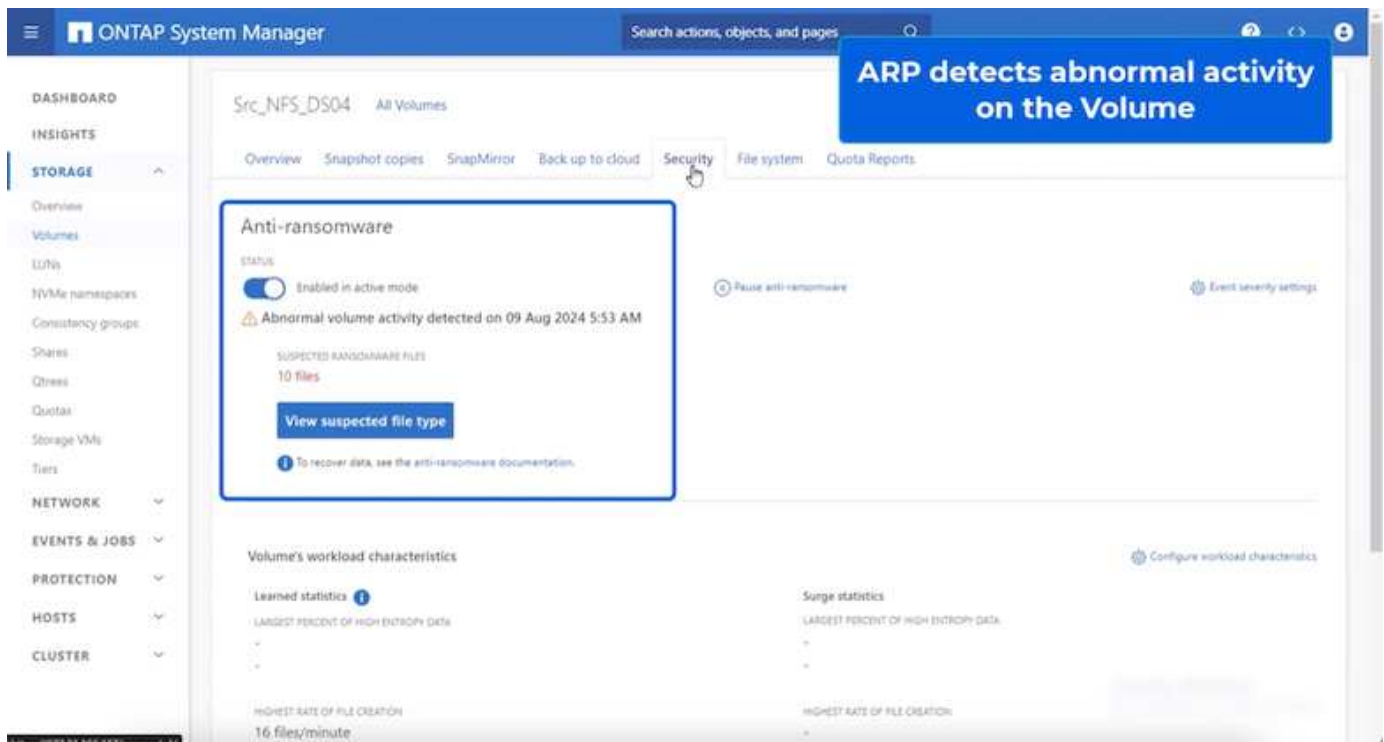
Storage VM name svm_NFS

Volume name Src_NFS_DS04

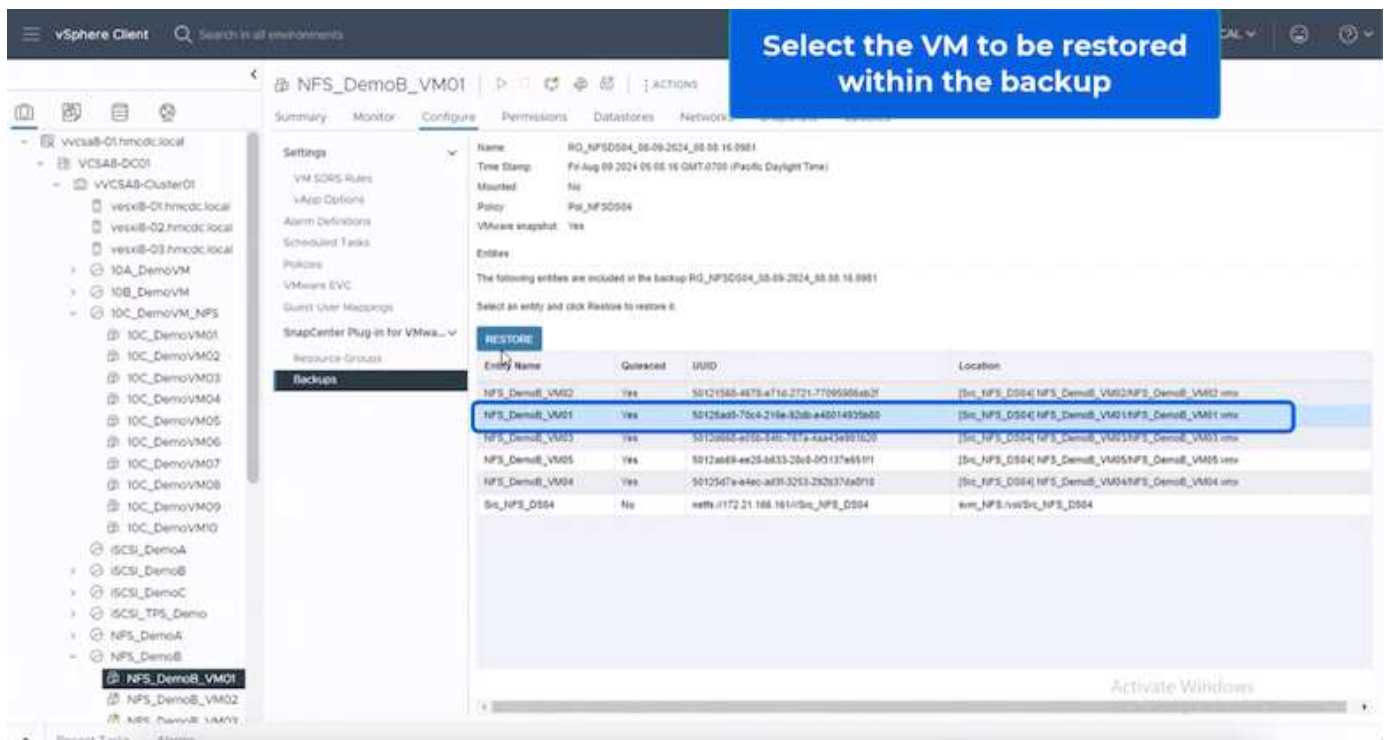
Used size 29 GiB

Es ist an der Zeit, dies anhand eines Beispiels zu verdeutlichen. In dieser exemplarischen Vorgehensweise ist der Datenspeicher „Src_NFS_DS04“ betroffen.





Sobald die forensische Analyse abgeschlossen ist, können die Wiederherstellungen schnell und nahtlos mit SnapCenter oder NetApp Ransomware Resilience durchgeführt werden. Mit SnapCenter navigieren Sie zu den betroffenen virtuellen Maschinen und wählen den entsprechenden Snapshot zur Wiederherstellung aus.

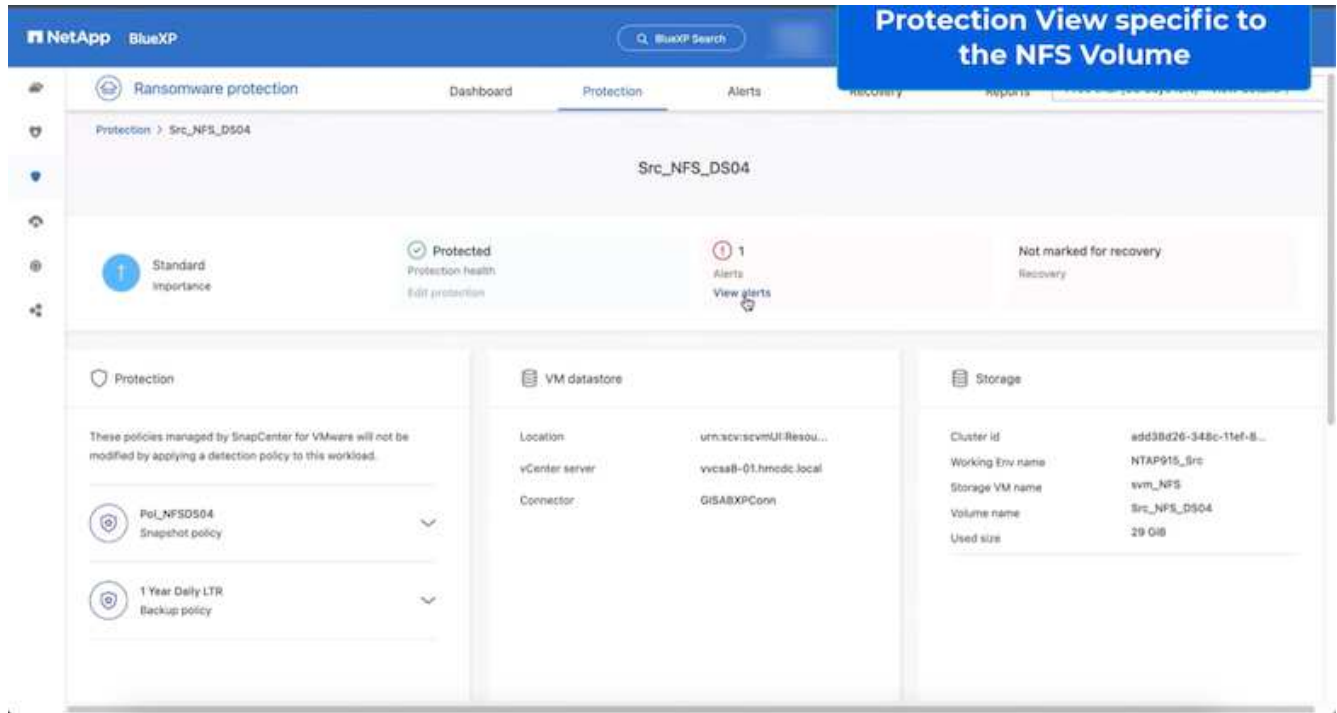


In diesem Abschnitt wird erläutert, wie NetApp Ransomware Resilience die Wiederherstellung nach einem Ransomware-Vorfall orchestriert, bei dem die VM-Dateien verschlüsselt wurden.

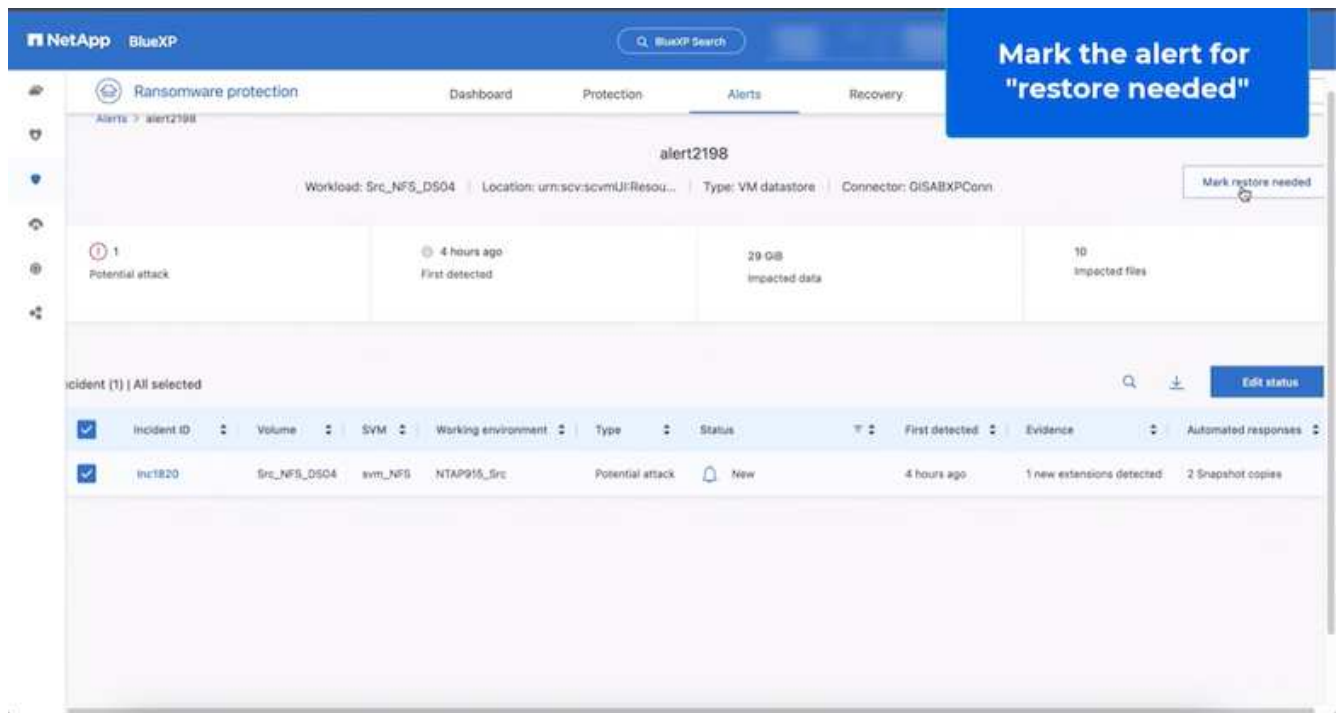


Wenn die VM von SnapCenter verwaltet wird, stellt NetApp Ransomware Resilience die VM mithilfe des VM-konsistenten Prozesses in ihren vorherigen Zustand zurück.

1. Wenn Sie auf NetApp Ransomware Resilience zugreifen, wird eine Warnung im NetApp Ransomware Resilience Dashboard angezeigt.
2. Klicken Sie auf die Warnung, um die Vorfälle auf diesem bestimmten Datenträger für die generierte Warnung zu überprüfen

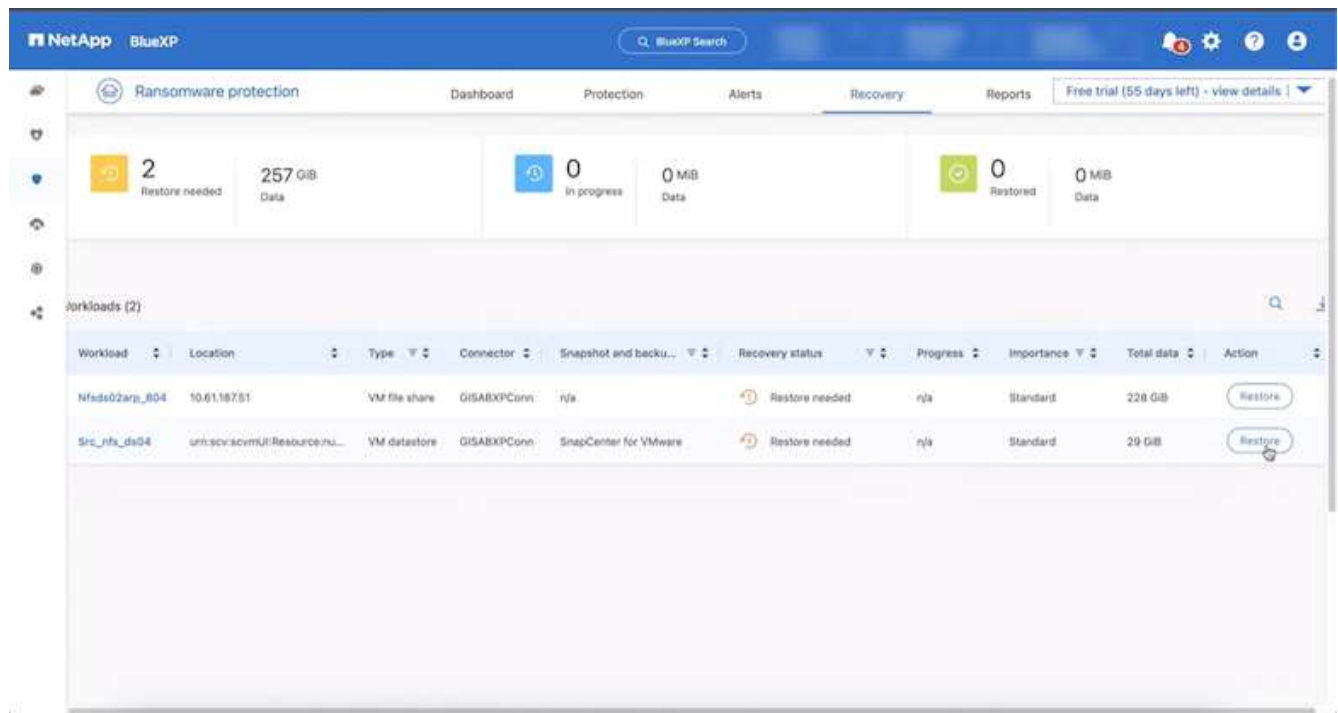


3. Markieren Sie den Ransomware-Vorfall als bereit zur Wiederherstellung (nachdem die Vorfälle neutralisiert wurden), indem Sie „Als Wiederherstellung erforderlich markieren“ auswählen.

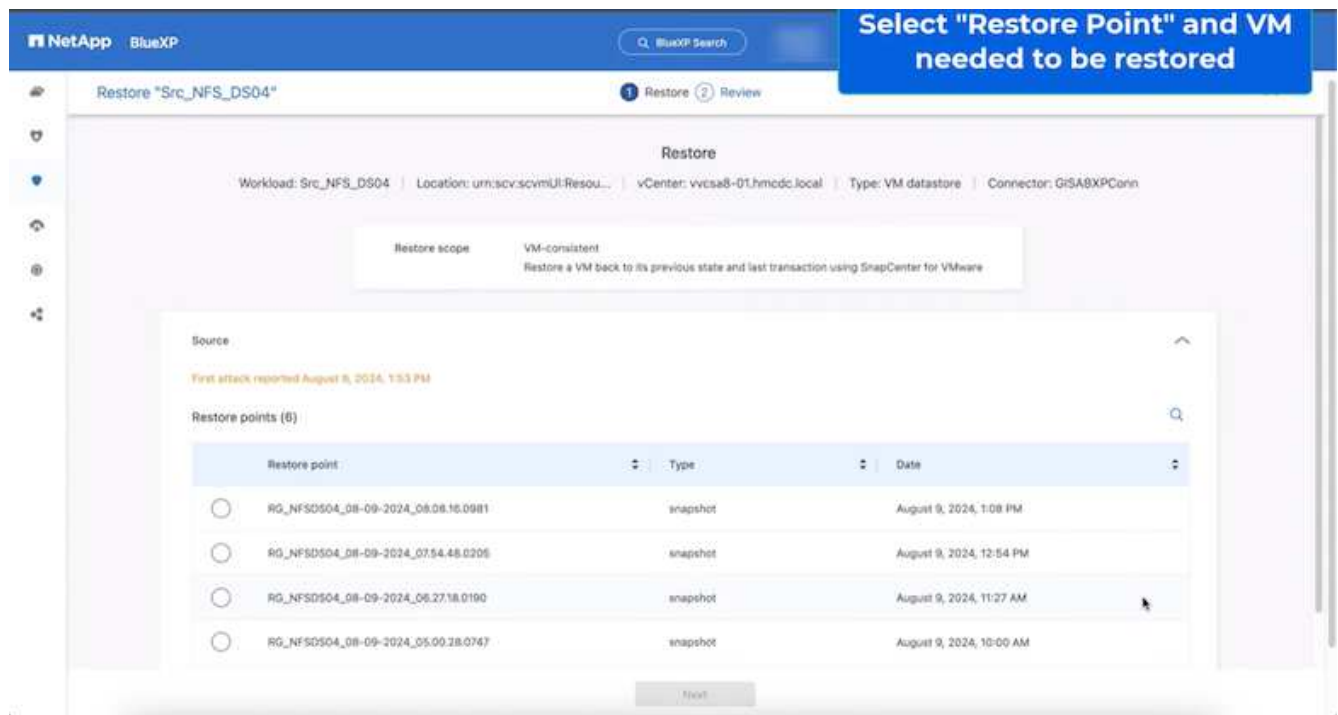


Die Warnung kann verworfen werden, wenn sich der Vorfall als falsch positiv herausstellt.

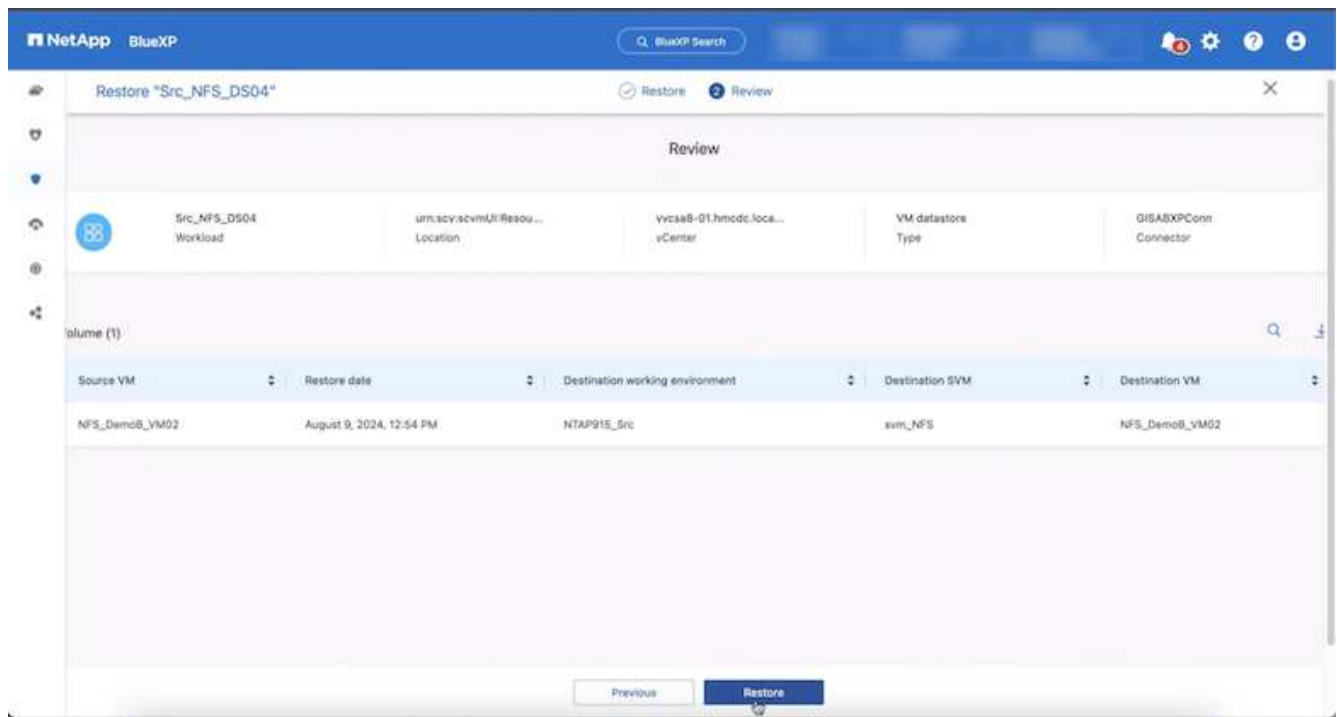
4. Gehen Sie zur Registerkarte „Wiederherstellung“, überprüfen Sie die Arbeitslastinformationen auf der Seite „Wiederherstellung“, wählen Sie das Datenspeichervolume aus, das sich im Status „Wiederherstellung erforderlich“ befindet, und wählen Sie „Wiederherstellen“ aus.



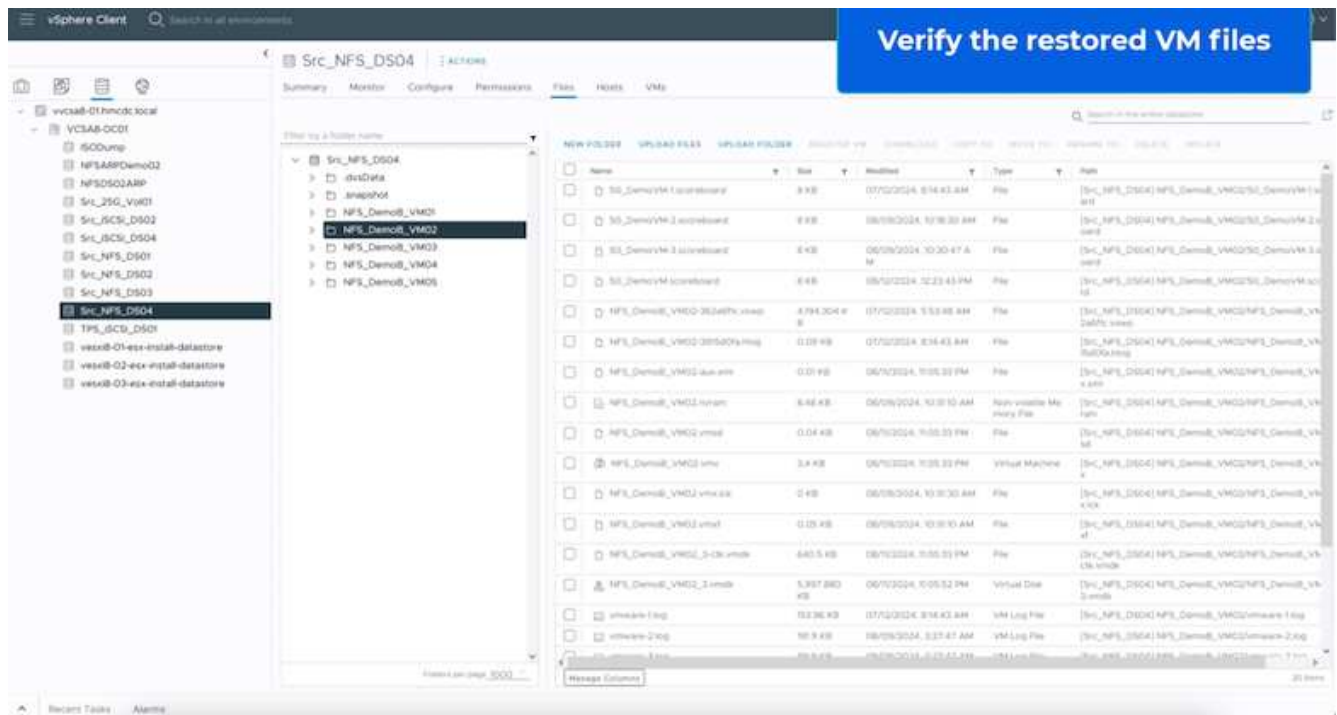
5. In diesem Fall ist der Wiederherstellungsumfang „Nach VM“ (für SnapCenter für VMs ist der Wiederherstellungsumfang „Nach VM“).



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.

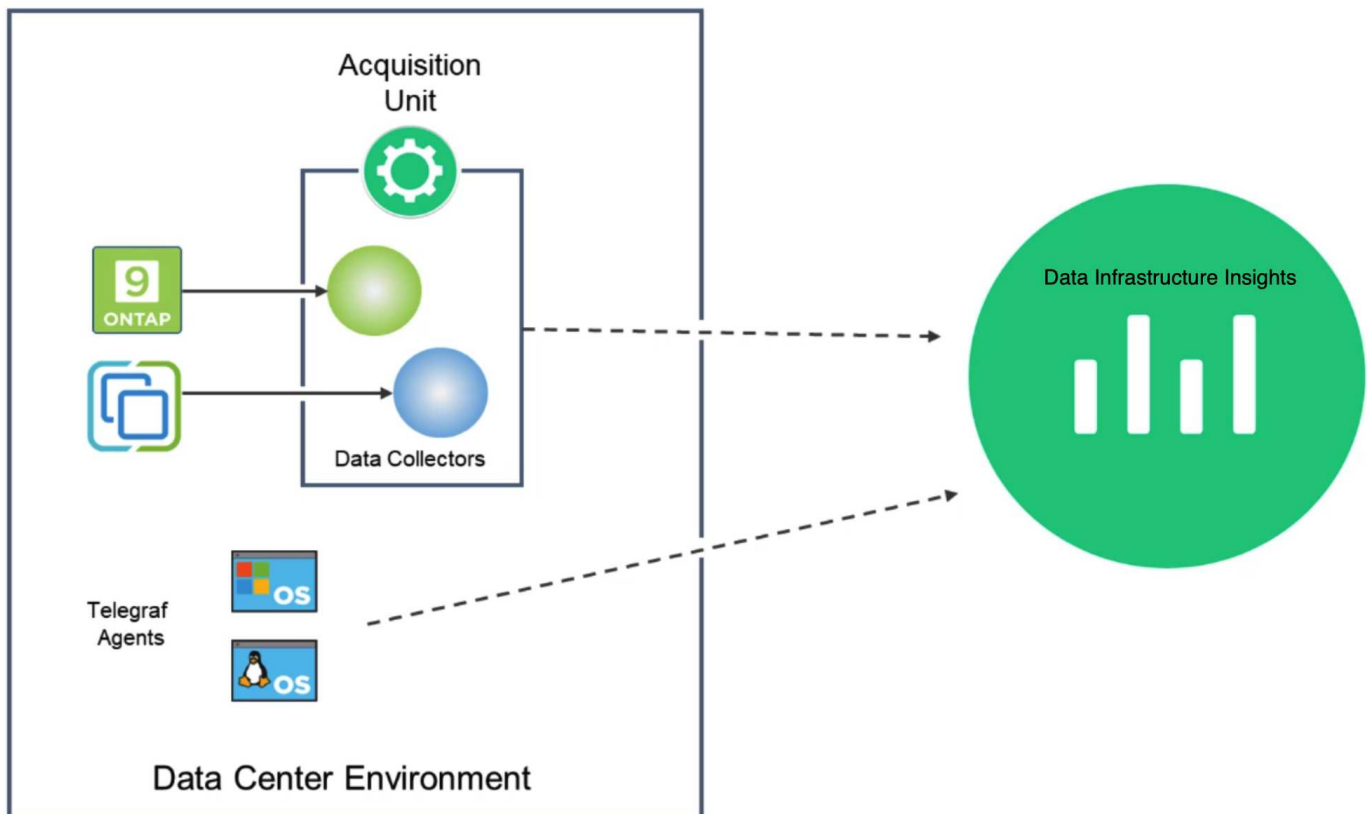
Überwachen Sie den lokalen Speicher mit Data Infrastructure Insights

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 Anmerksungsregeln, 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 Console Konsolenkonto.
4. Auf einer lokalen VM installierte NetApp Data Infrastructure Insights Acquisition Unit-Software mit Netzwerkkonnektivität zu Assets zur Datenerfassung.

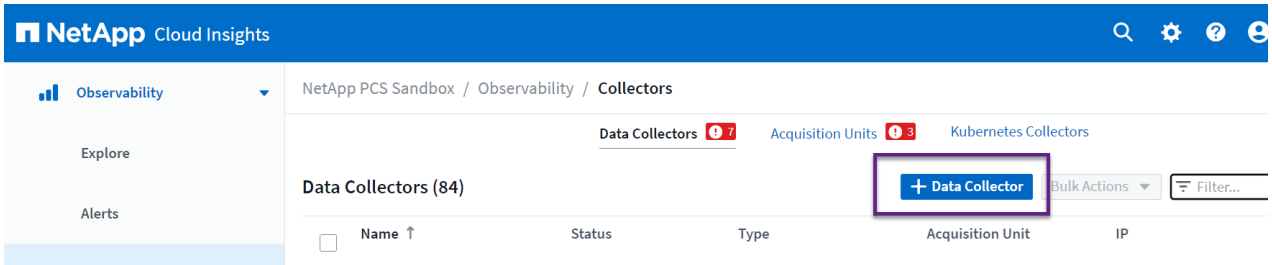
Lösungsbereitstellung

Konfigurieren von Datensammlern

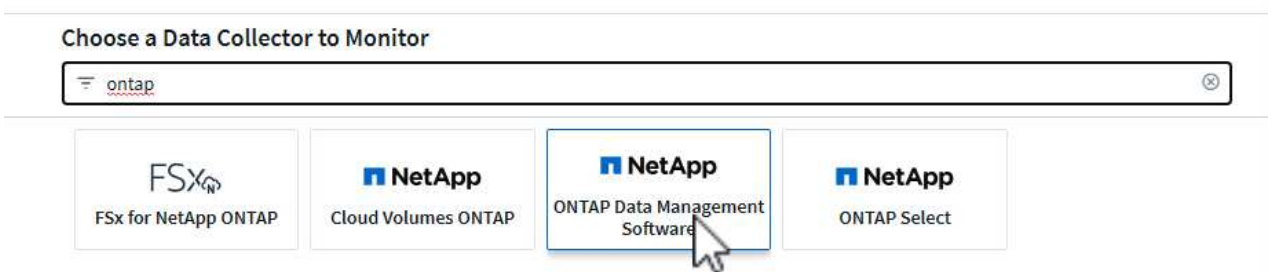
Führen Sie die folgenden Schritte aus, um Datenkollektoren für VMware vSphere- und ONTAP-Speichersysteme zu konfigurieren:

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.



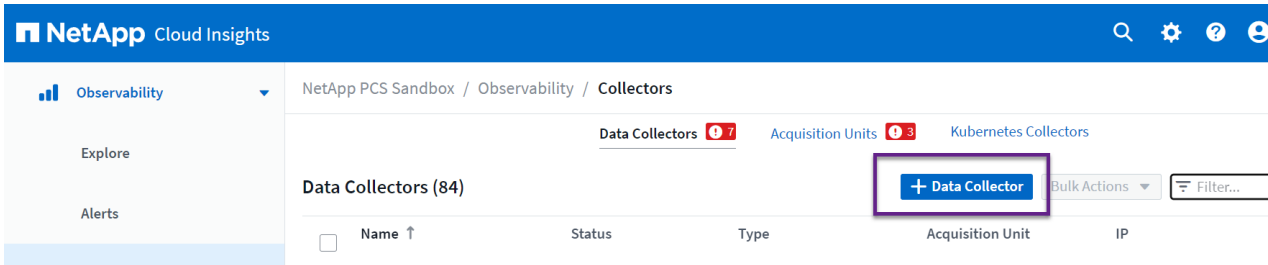
2. Suchen Sie hier nach * ONTAP* und klicken Sie auf * ONTAP Data Management Software*.



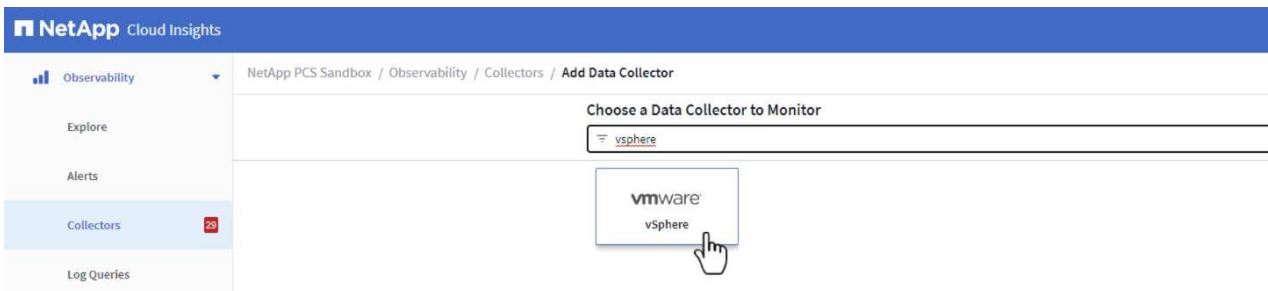
3. Geben Sie auf der Seite **Collector konfigurieren** einen Namen für den Collector ein, geben Sie die richtige **Erfassungseinheit** an und geben Sie die Anmeldeinformationen für das ONTAP -Speichersystem ein. Klicken Sie auf **Speichern und fortfahren** und dann unten auf der Seite auf **Setup abschließen**,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

Select a Data Collector

Configure Data Collector



Configure Collector

Add credentials and required settings

[Need Help?](#)

Name ?

VCSA7

Acquisition Unit

bxp-au01

Virtual Center IP Address

10.61.181.210

User Name

administrator@vsphere.local

Password

Complete Setup

Test Connection

☐ Advanced Configuration

Collecting:

☒ Inventory

☒ VM Performance

Inventory Poll Interval (min)

20

Communication Port

443

Filter VMs by

ESX_HOST

Choose 'Exclude' or 'Include' to Specify a List

Exclude

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)

Performance Poll Interval (sec)

300

☐ Collect basic performance metrics only

Complete Setup

Test Connection

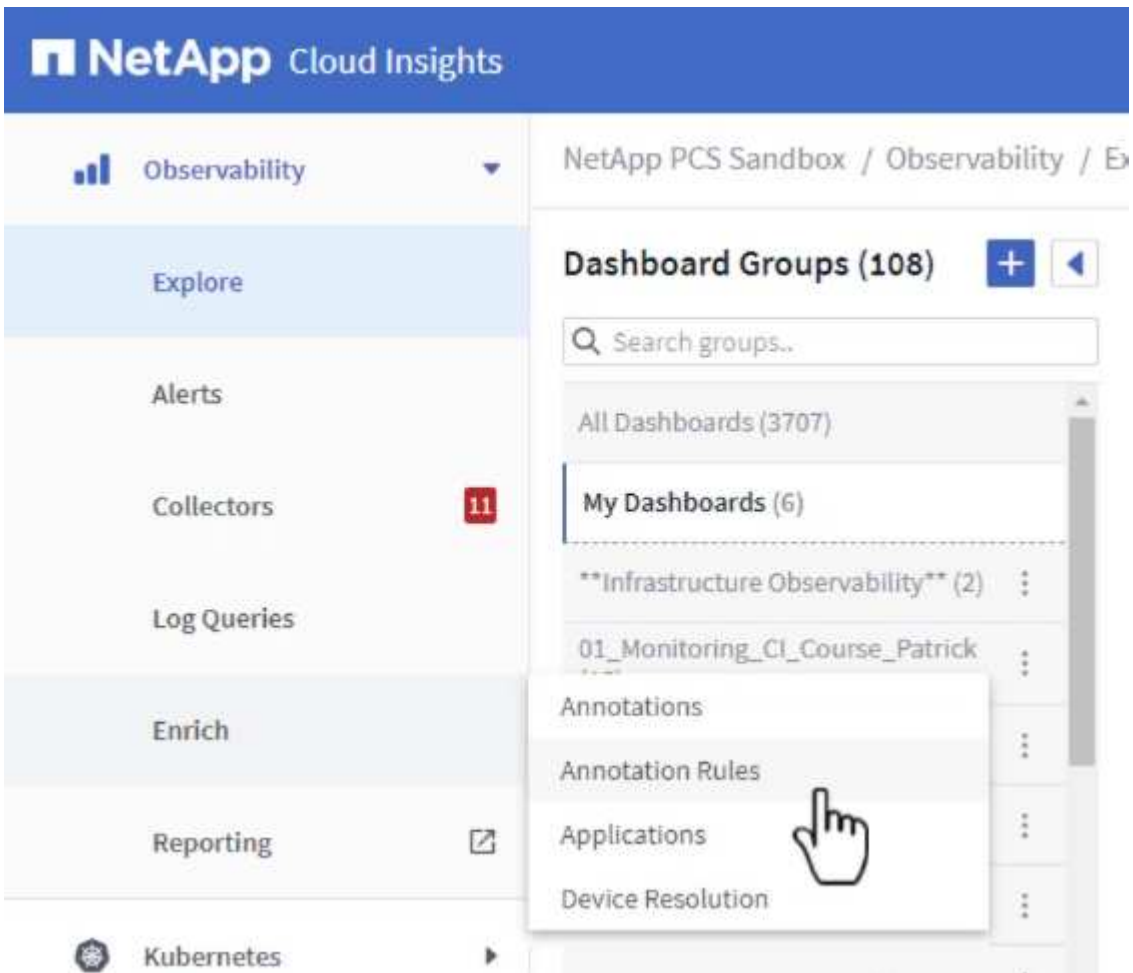
Hinzufügen von Anmerkungen zu Assets

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.

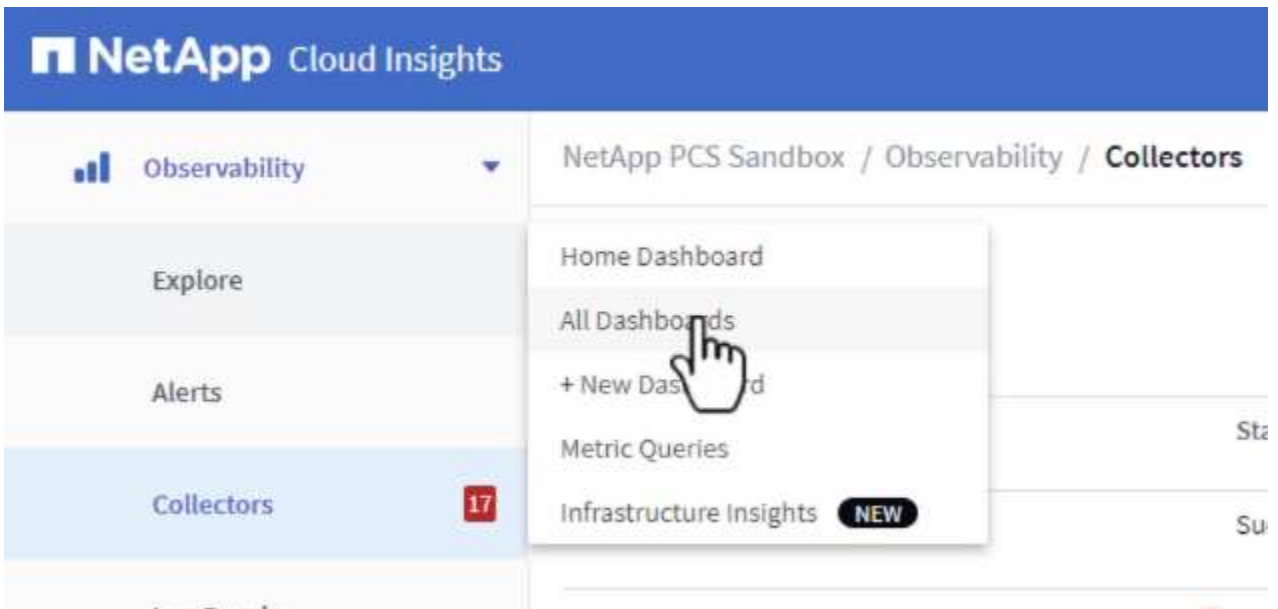
Erkunden und Korrelieren von Assets

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**.

☐ ONTAP FAS/AFF - Cluster Capacity

☐ ONTAP FAS/AFF - Efficiency

☒ ONTAP FAS/AFF - FlexVol Performance

☐ ONTAP FAS/AFF - Node Operational/Optimal Points

☐ ONTAP FAS/AFF - PrePost Capacity Efficiencies

☐ Storage Admin - Which nodes are in high demand?

☐ Storage Admin - Which pools are in high demand?

☐ StorageGRID - Capacity Summary

☐ StorageGRID - ILM Performance Monitoring

☐ StorageGRID - MetaData Usage

☐ StorageGRID - S3 Performance Monitoring

☐ VMware Admin - ESX Hosts Overview

☐ VMware Admin - Overview

☐ VMware Admin - VM Performance

☐ VMware Admin - Where are opportunities to right size?

☐ VMware Admin - Where can I potentially reclaim waste?

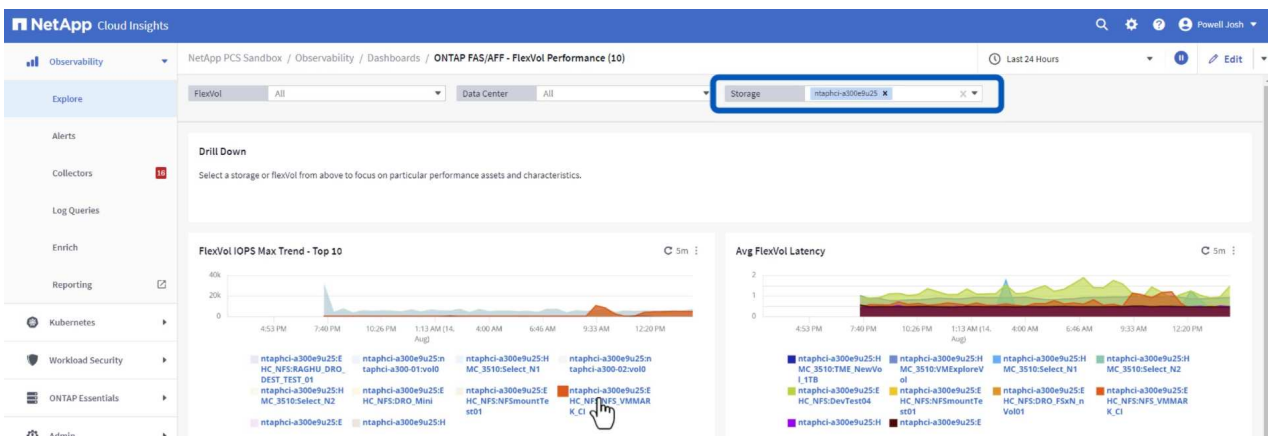
☐ VMware Admin - Where do I have VM Latency?

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

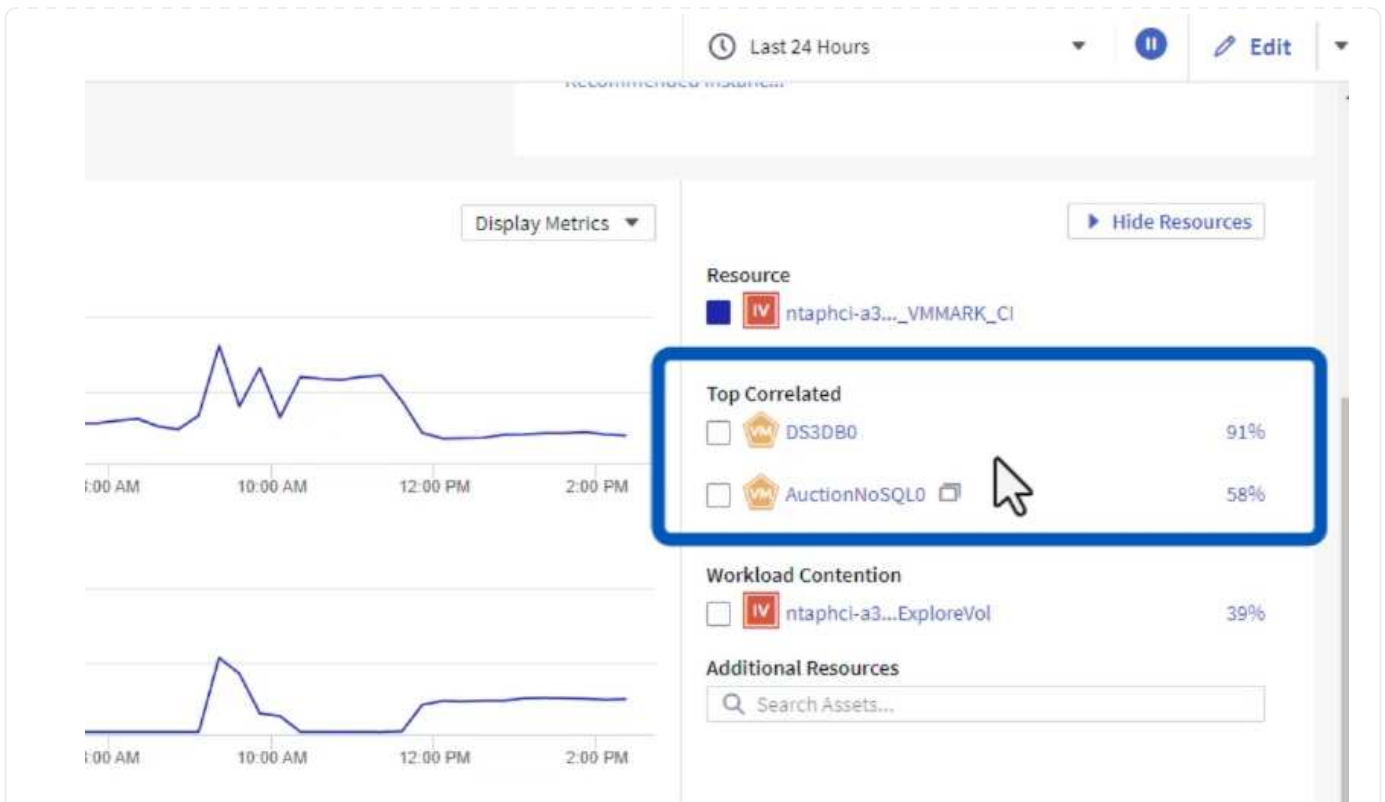
Add Dashboards

Go Back

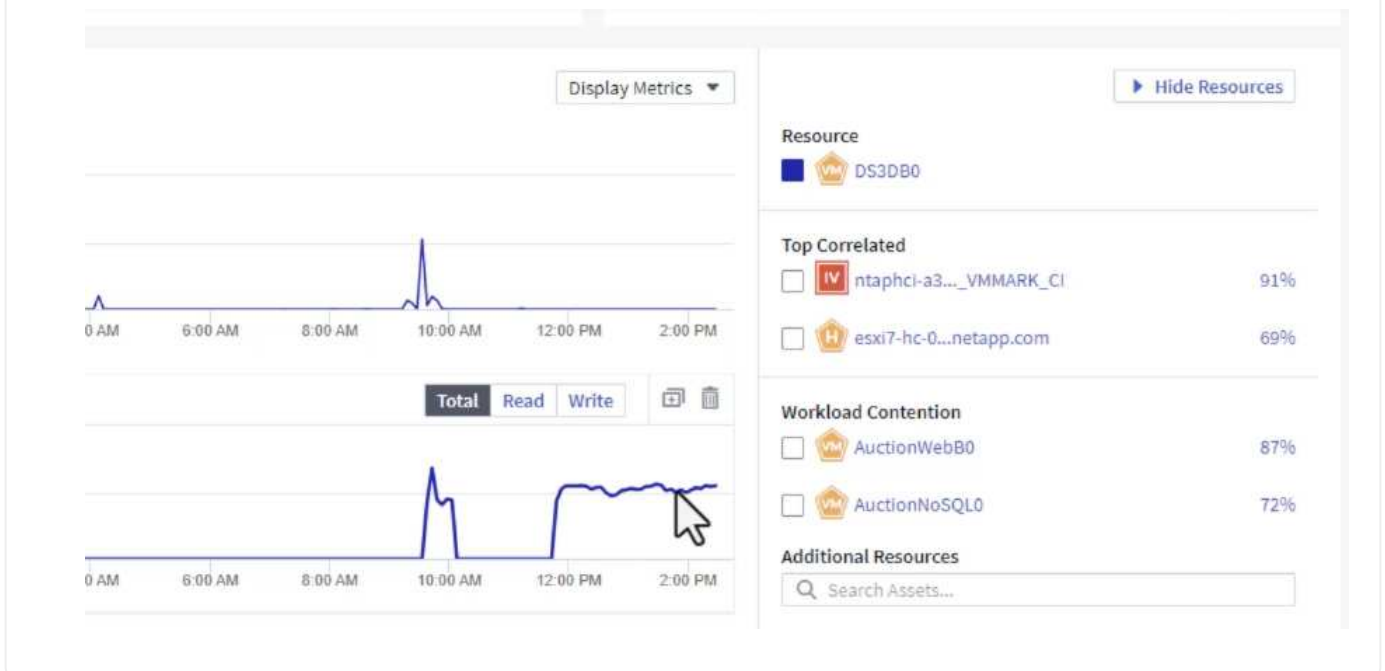
4. Öffnen Sie nach dem Import das Dashboard. Von hier aus können Sie verschiedene Widgets mit detaillierten Leistungsdaten sehen. Fügen Sie einen Filter hinzu, um ein einzelnes Speichersystem anzuzeigen, und wählen Sie ein Speichervolumen aus, um dessen Details zu untersuchen.



5. In dieser Ansicht können Sie verschiedene Kennzahlen zu diesem Speichervolumen 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.

NetApp PCS Sandbox / Observability / Explore / Dashboards

Dashboard Groups (108)

Search groups..

All Dashboards (3709)

My Dashboards (6)

Infrastructure Observability (2)

01_Monitoring_CI_Course_Patrick (15)

02_Monitoring_CI_Course_Vish (5)

1_Str Dashboards (8)

My Dashboards (6)

+ From Gallery

+ Dashboard

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

2. Filtern Sie als Nächstes nach der im vorherigen Schritt erstellten Anmerkung **Data Center**, um eine Teilmenge der Assets anzuzeigen.

/ VMware Admin - Where do I have VM Latency? (9) Last 3 Hours

VirtualMachine All Data Center Solutions Engineering X diskLatency.total ≥ All

! 5m Avg Latency (all hypervisors) C 5m VM Count With Latency Concern C 5m Avg Latency (all VMs)

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.

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

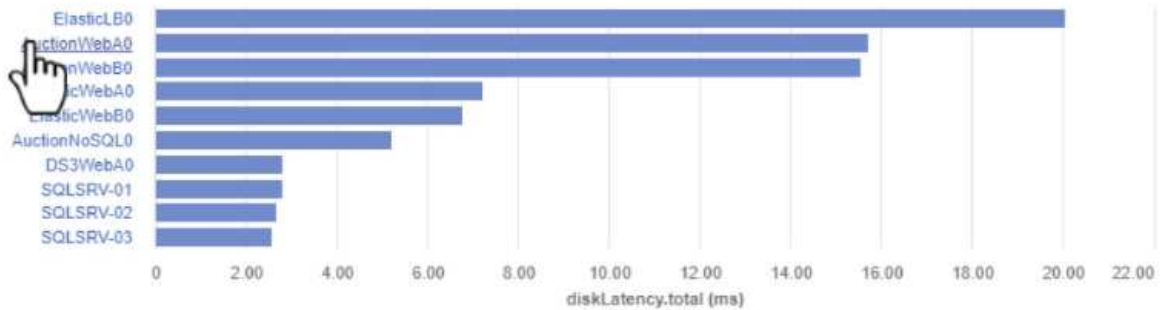
5m

1.55 ms

diskLatency.total

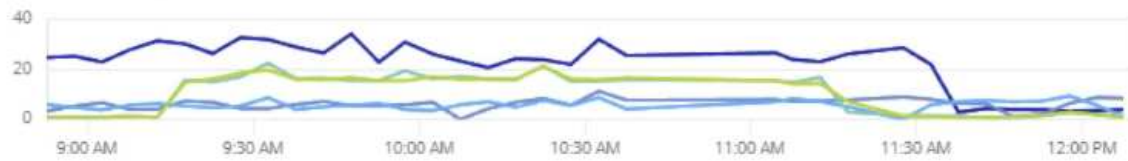
Avg VM Latency - Top 10

5m

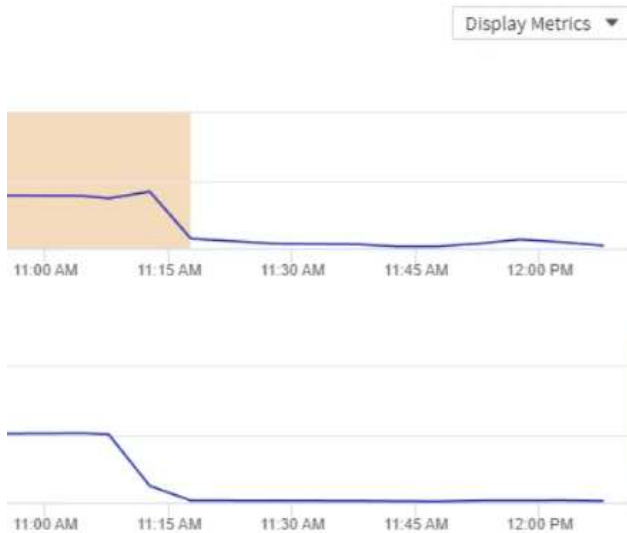


Top 5 Avg VM Latency Trend

30s



4. Die VMs, die möglicherweise zu Workload-Konflikten führen, sind aufgelistet und verfügbar. Untersuchen Sie die Leistungsmetriken dieser VMs, um mögliche Probleme zu untersuchen.



Resource

VM AuctionWebA0

Top Correlated

☐ esxi7-hc-0...netapp.com 91%

☐ ntaphci-a3..._VMMARK_CI 84%

Workload Contention

☐ AuctionNoSQL0 92%

☐ AuctionWebB0 57%

Additional Resources

Search Assets...

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.

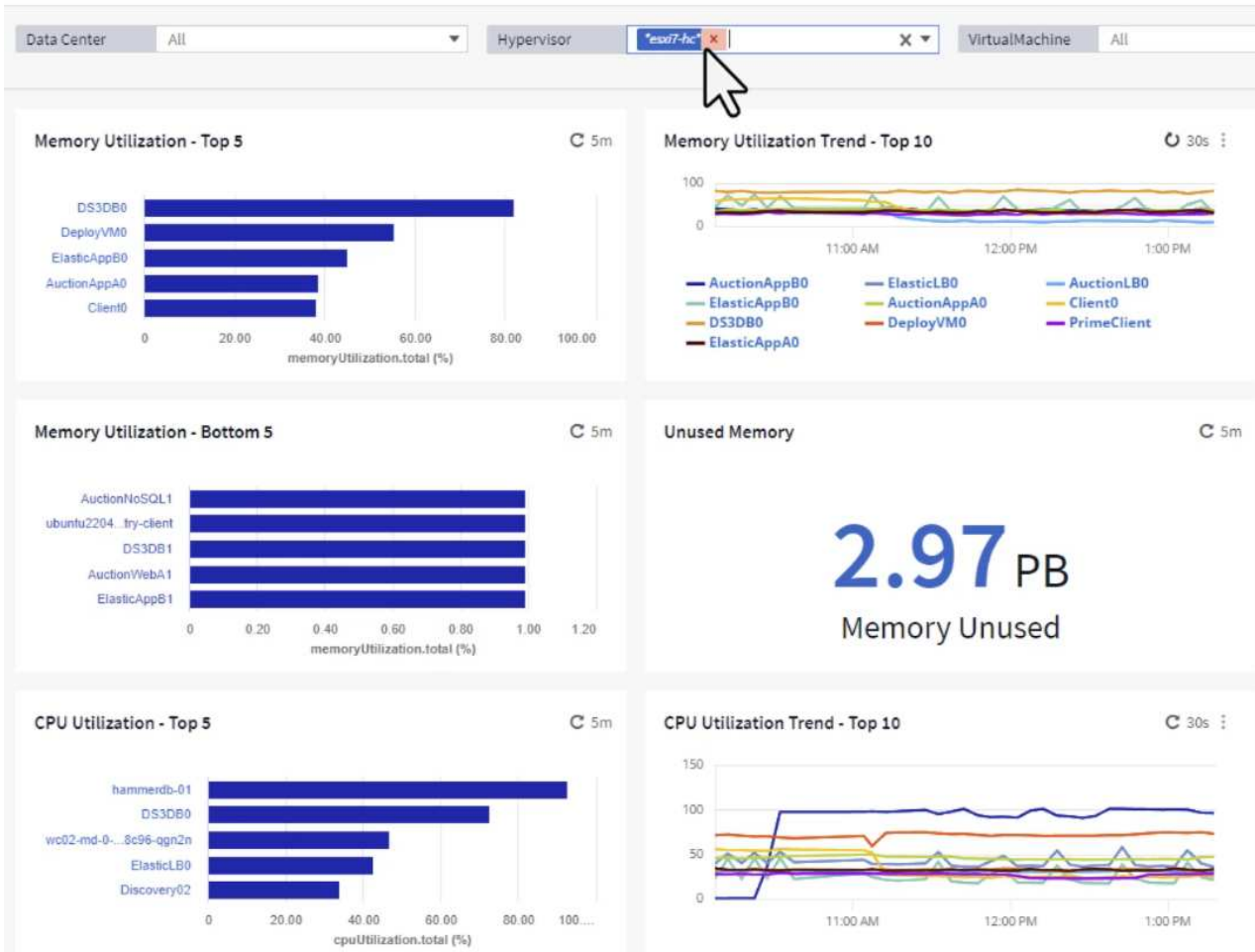
Identifizieren Sie Möglichkeiten zur richtigen VM-Größe

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.

My Dashboards (6)

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

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.



- Tabellen ermöglichen das Sortieren und bieten basierend auf den ausgewählten Datenspalten mehr Details.

Memory Usage

5m

121 items found

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

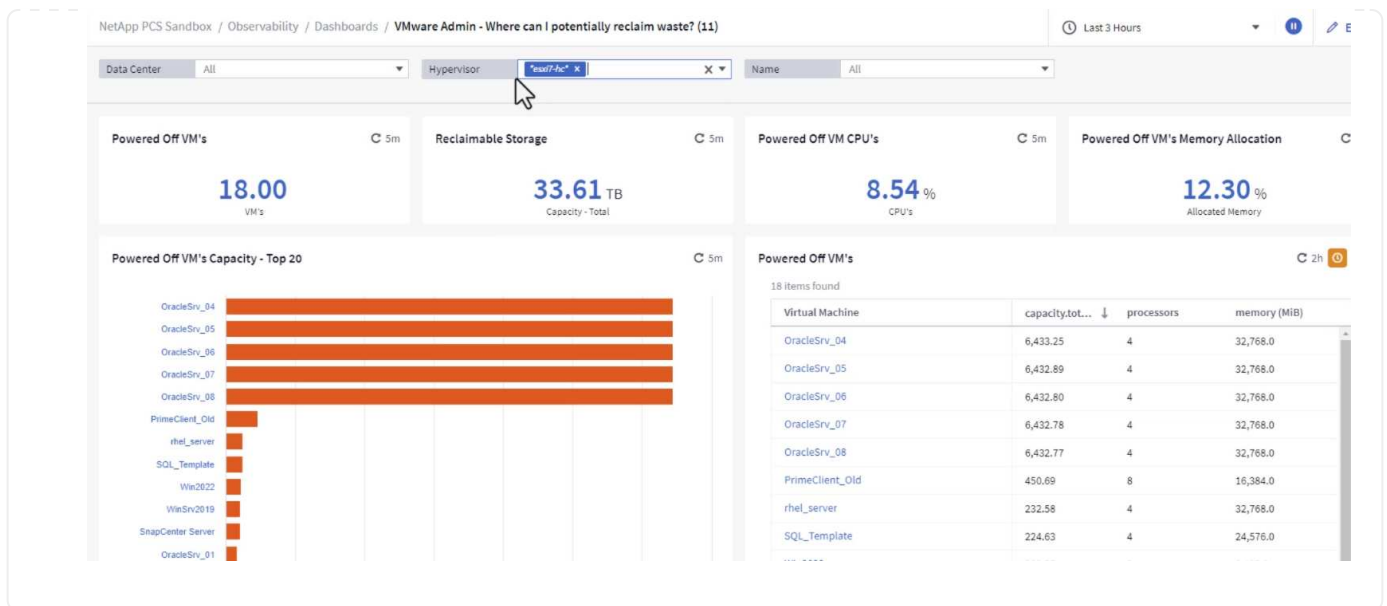
CPU Utilization

5m

121 items found

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

4. Ein weiteres Dashboard mit dem Namen **VMware Admin – Wo kann ich möglicherweise Abfall zurückgewinnen?** zeigt ausgeschaltete VMs sortiert nach ihrer Kapazitätsnutzung.

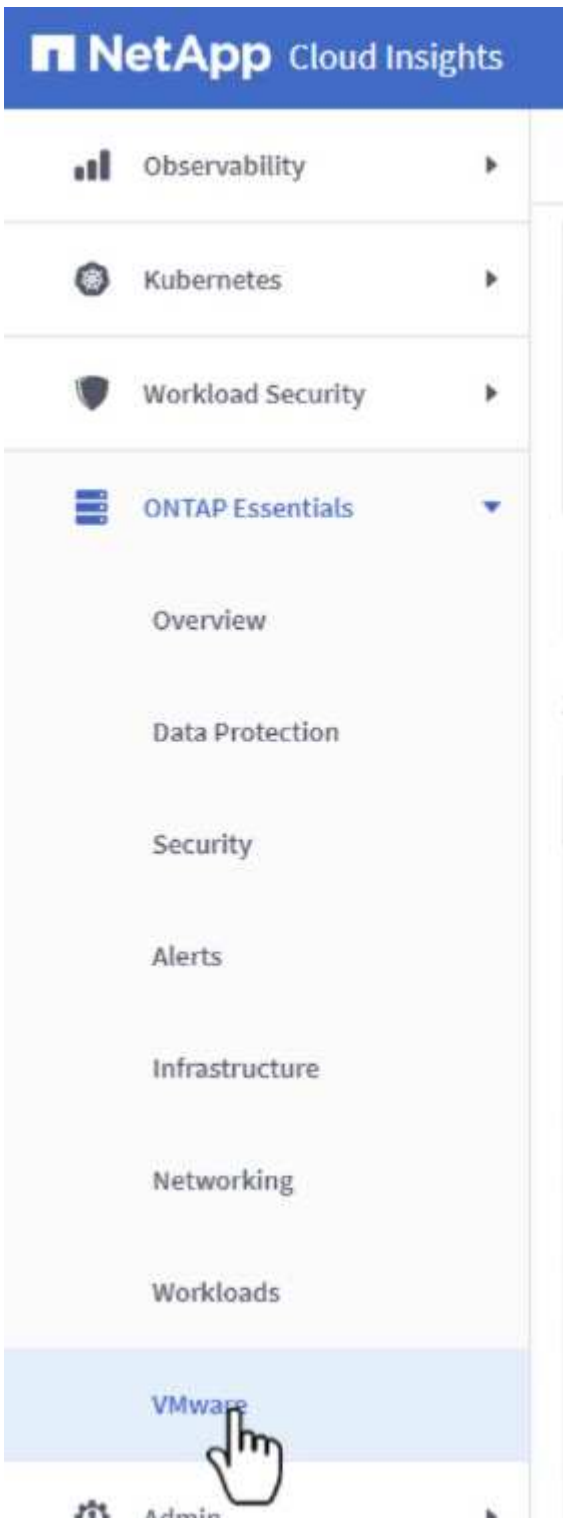


Verwenden Sie Abfragen, um Metriken zu isolieren und zu sortieren

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.

VirtualMachine | All Virtual Machines

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

Filter by Metric: +

Group By: Virtual Machine

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

281 Items found

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

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.

- ["NetApp Console -Startseite"](#)
- ["NetApp Data Infrastructure Insights -Landingpage"](#)
- ["Dokumentation zu NetApp Data Infrastructure Insights"](#)

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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