



VMware Cloud Foundation

NetApp Solutions

NetApp
May 14, 2024

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions/vmware/vmware_vcf_asa_supp_mgmt_iscsi.html on May 14, 2024. Always check docs.netapp.com for the latest.

Inhalt

- VMware Cloud Foundation 1
 - VMware Cloud Foundation mit NetApp All-Flash-SAN-Arrays 1
 - VMware Cloud Foundation mit NetApp AFF-Arrays 116

VMware Cloud Foundation

VMware Cloud Foundation mit NetApp All-Flash-SAN-Arrays

Autor: Josh Powell

VMware Cloud Foundation mit NetApp All-Flash-SAN-Arrays

VMware Cloud Foundation (VCF) ist eine integrierte softwaredefinierte Datacenter-Plattform (SDDC), die einen vollständigen Stack von softwaredefinierter Infrastruktur für die Ausführung von Enterprise-Applikationen in einer Hybrid-Cloud-Umgebung bereitstellt. Sie kombiniert Computing-, Storage-, Netzwerk- und Managementfunktionen in einer einheitlichen Plattform und ermöglicht so ein konsistentes Betriebserlebnis in Private und Public Clouds.

Dieses Dokument enthält Informationen zu Storage-Optionen, die für VMware Cloud Foundation mit dem NetApp All-Flash-SAN-Array zur Verfügung stehen. Unterstützte Storage-Optionen werden mit spezifischen Anweisungen zur Implementierung von iSCSI-Datstores als ergänzenden Storage für Management-Domänen sowie für vVol (iSCSI)- und NVMe/TCP-Datstores als ergänzende Datstores für Workload-Domänen abgedeckt. Ebenfalls behandelt wird die Datensicherung von VMs und Datstores mit SnapCenter für VMware vSphere.

Anwendungsfälle

Anwendungsfälle in dieser Dokumentation:

- Storage-Optionen für Kunden, die einheitliche Umgebungen sowohl in privaten als auch in öffentlichen Clouds benötigen.
- Automatisierte Lösung zur Bereitstellung einer virtuellen Infrastruktur für Workload-Domänen.
- Skalierbare Storage-Lösung, die auf neue Anforderungen zugeschnitten ist, auch wenn sie nicht direkt auf die Anforderungen von Computing-Ressourcen ausgerichtet ist
- Mit ONTAP Tools für VMware vSphere stellen Sie zusätzlichen Storage für Management- und VI-Workload-Domänen bereit.
- Sichern Sie VMs und Datstores mit dem SnapCenter Plug-in für VMware vSphere.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

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

Technologischer Überblick

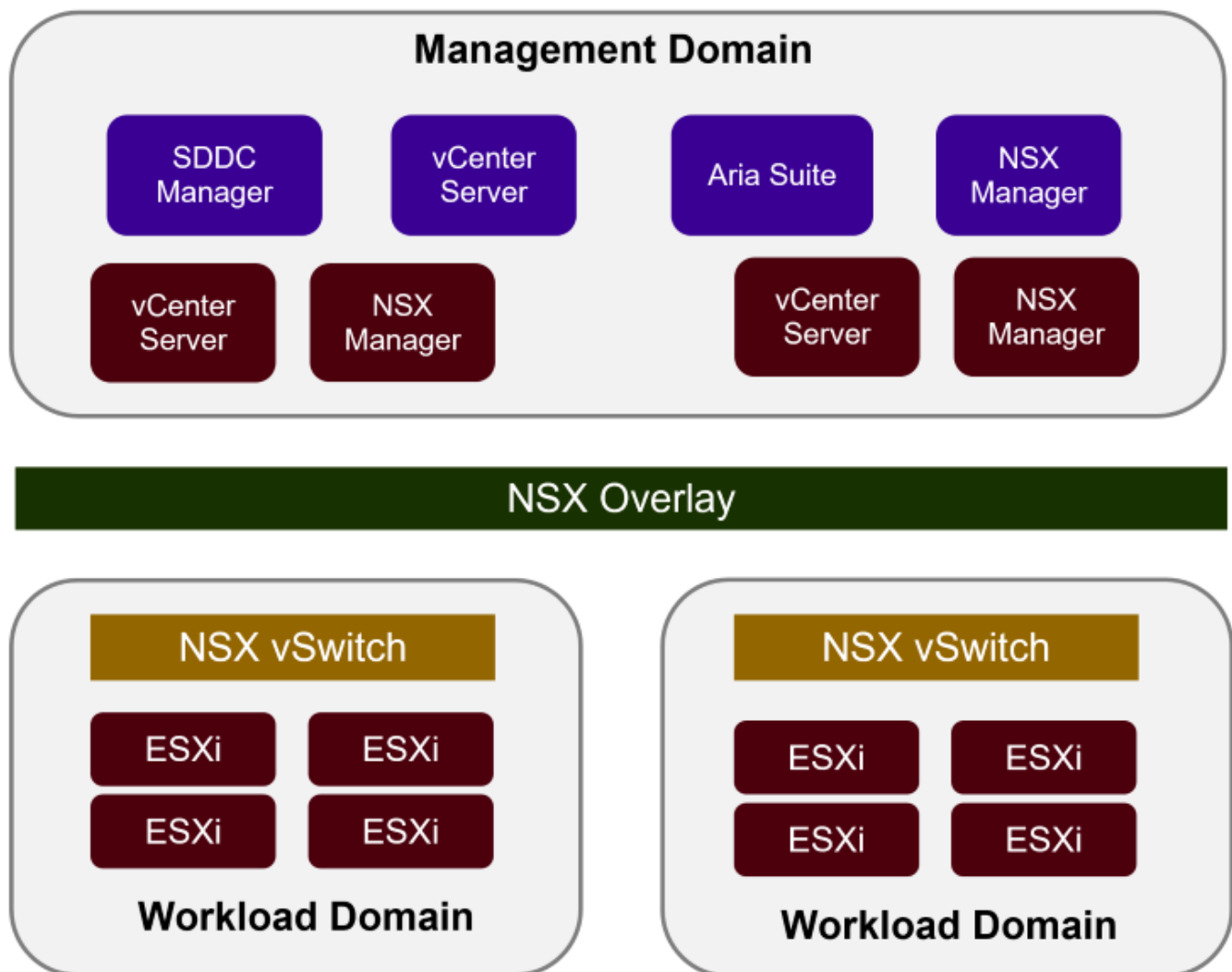
Die VCF mit NetApp ASA-Lösung besteht aus den folgenden Hauptkomponenten:

VMware Cloud Foundation

VMware Cloud Foundation erweitert die vSphere Hypervisor-Angebote von VMware durch die Kombination wichtiger Komponenten wie SDDC Manager, vSphere, vSAN, NSX und VMware Aria Suite zur Erstellung eines softwaredefinierten Datacenters.

Die VCF Lösung unterstützt sowohl native Kubernetes-Workloads als auch Workloads, die auf Virtual Machines basieren. Zentrale Services wie VMware vSphere, VMware vSAN, VMware NSX-T Data Center und VMware Aria Cloud Management sind Bestandteile des VCF-Pakets. Zusammen bilden diese Services eine softwaredefinierte Infrastruktur, die ein effizientes Management von Computing, Storage, Netzwerken, Sicherheit und Cloud-Management ermöglicht.

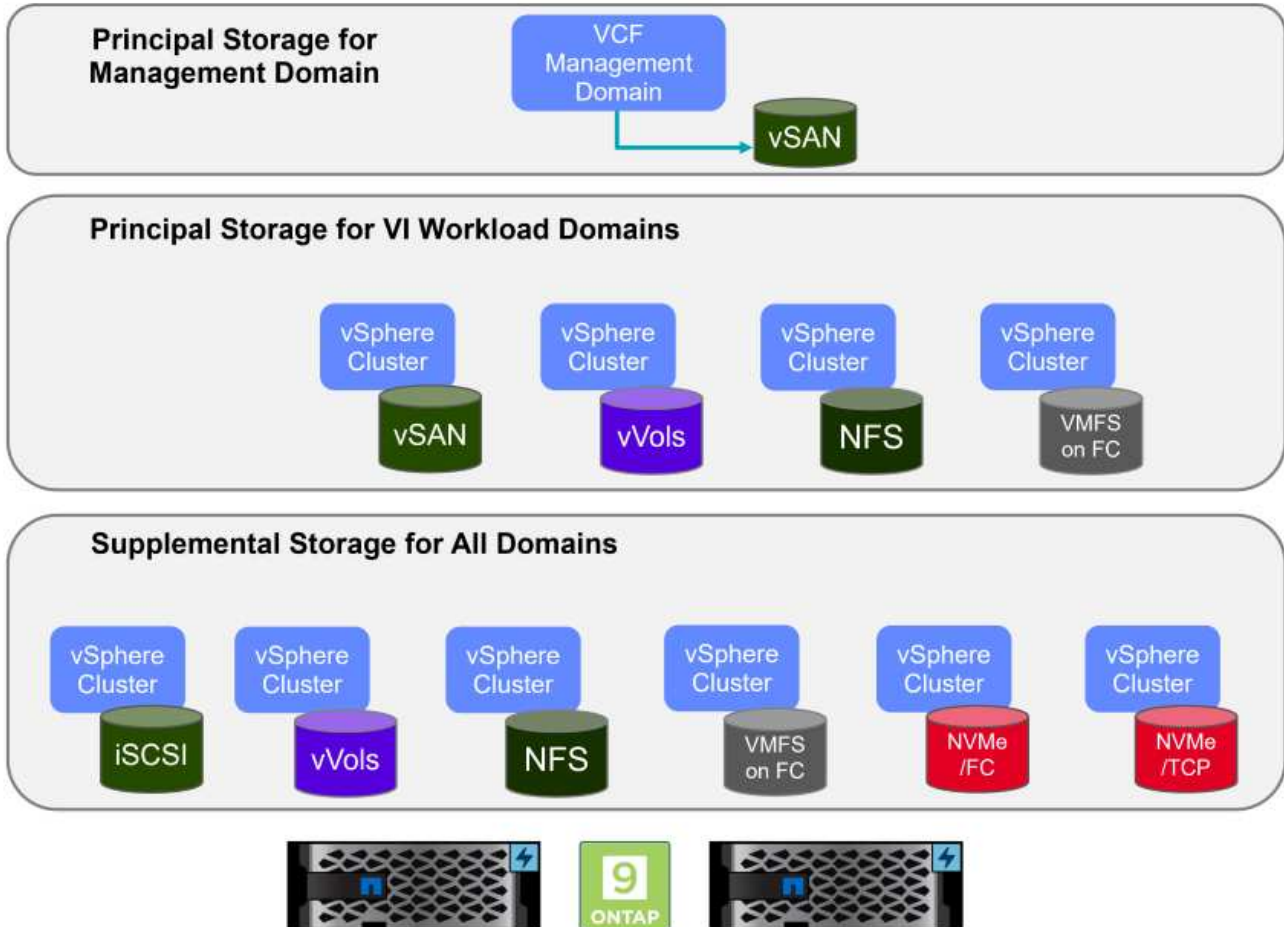
VCF besteht aus einer einzelnen Management-Domäne und bis zu 24 VI-Workload-Domänen, die jeweils eine Einheit für applikationsfähige Infrastrukturen darstellen. Eine Workload-Domäne besteht aus einem oder mehreren vSphere Clustern, die von einer einzelnen vCenter Instanz gemanagt werden.



Weitere Informationen zur Architektur und Planung von VCF finden Sie unter ["Architekturmodelle und Workload-Domänen-Typen in VMware Cloud Foundation"](#).

VCF Storage-Optionen

VMware unterteilt Speicheroptionen für VCF in **Principal** und **Supplemental** Speicher. Die VCF-Management-Domäne muss vSAN als Haupt-Storage verwenden. Es gibt jedoch zahlreiche zusätzliche Storage-Optionen für die Managementdomäne sowie Haupt- und ergänzende Storage-Optionen für VI-Workload-Domänen.



Hauptspeicher für Workload-Domänen

Hauptspeicher bezieht sich auf jeden Storage-Typ, der während des Setups im SDDC Manager direkt mit einer VI-Workload-Domäne verbunden werden kann. Der Hauptspeicher wird mit dem SDDC Manager als Teil der Cluster-Erstellungs-Orchestrierung bereitgestellt und ist der erste für eine Workload-Domäne konfigurierte Datastore. Sie umfasst vSAN, vVols (VMFS), NFS und VMFS auf Fibre Channel.

Ergänzender Speicher für Management- und Workload-Domänen

Zusätzlicher Storage ist der Storage-Typ, der dem Management oder den Workload-Domänen jederzeit nach der Erstellung des Clusters hinzugefügt werden kann. Zusätzlicher Storage umfasst die größte Auswahl an unterstützten Storage-Optionen, die alle von NetApp ASA Arrays unterstützt werden. Für die meisten Storage-Protokolltypen kann zusätzlicher Storage mit den ONTAP Tools für VMware vSphere implementiert werden.

Zusätzliche Dokumentationsressourcen für VMware Cloud Foundation:

- * ["Dokumentation zu VMware Cloud Foundation"](#)
- * ["Unterstützte Storage-Typen für VMware Cloud Foundation"](#)
- * ["Management von Storage in VMware Cloud Foundation"](#)

NetApp All-Flash-SAN-Arrays

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

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

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



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



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

Unterstützte Storage-Protokolle

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

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

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

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

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

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

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

Aktiv/aktiv-Technologie

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

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

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

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

Storage-Garantien

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

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

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

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

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

NetApp ONTAP Tools für VMware vSphere

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

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

ONTAP Tools umfassen zudem einen **VMware vSphere APIs for Storage Awareness (VASA) Provider** für ONTAP Storage-Systeme, der die Bereitstellung von VMware Virtual Volumes (VVols) Datastores, die Erstellung und Verwendung von Storage-Funktionsprofilen, Compliance-Überprüfung und Performance-Monitoring ermöglicht.

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

SnapCenter Plug-in für VMware vSphere

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

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

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

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

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

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

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

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

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

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

Lösungsüberblick

Die in dieser Dokumentation vorgestellten Szenarien zeigen, wie ONTAP-Storage-Systeme als zusätzlicher Storage für Management- und Workload-Domänen eingesetzt werden. Darüber hinaus wird das SnapCenter Plug-in für VMware vSphere zur Sicherung von VMs und Datastores verwendet.

Szenarien in dieser Dokumentation:

- **Verwenden Sie ONTAP-Tools, um iSCSI-Datastores in einer VCF-Management-Domain bereitzustellen.** Klicken Sie Auf "[Hier](#)" Für Bereitstellungsschritte.
- **Verwenden von ONTAP-Tools zur Bereitstellung von VVols (iSCSI) Datastores in einer VI Workload-Domäne.** Klicken Sie Auf "[Hier](#)" Für Bereitstellungsschritte.
- **Konfiguration von NVMe over TCP Datastores für die Verwendung in einer VI Workload Domain.** Klicken Sie Auf "[Hier](#)" Für Bereitstellungsschritte.
- **Bereitstellen und Verwenden des SnapCenter Plug-ins für VMware vSphere zum Schutz und zur Wiederherstellung von VMs in einer VI-Workload-Domäne.** Klicken Sie Auf "[Hier](#)" Für Bereitstellungsschritte.

Verwenden Sie ONTAP-Tools, um zusätzlichen Speicher für VCF-Verwaltungsdomänen zu konfigurieren

Autor: Josh Powell

Verwenden Sie ONTAP-Tools, um zusätzlichen Speicher für VCF-Verwaltungsdomänen zu konfigurieren

Szenarioübersicht

In diesem Szenario zeigen wir, wie Sie ONTAP Tools für VMware vSphere (OTV) bereitstellen und verwenden, um einen iSCSI-Datastore für eine VCF-Verwaltungsdomäne zu konfigurieren.

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

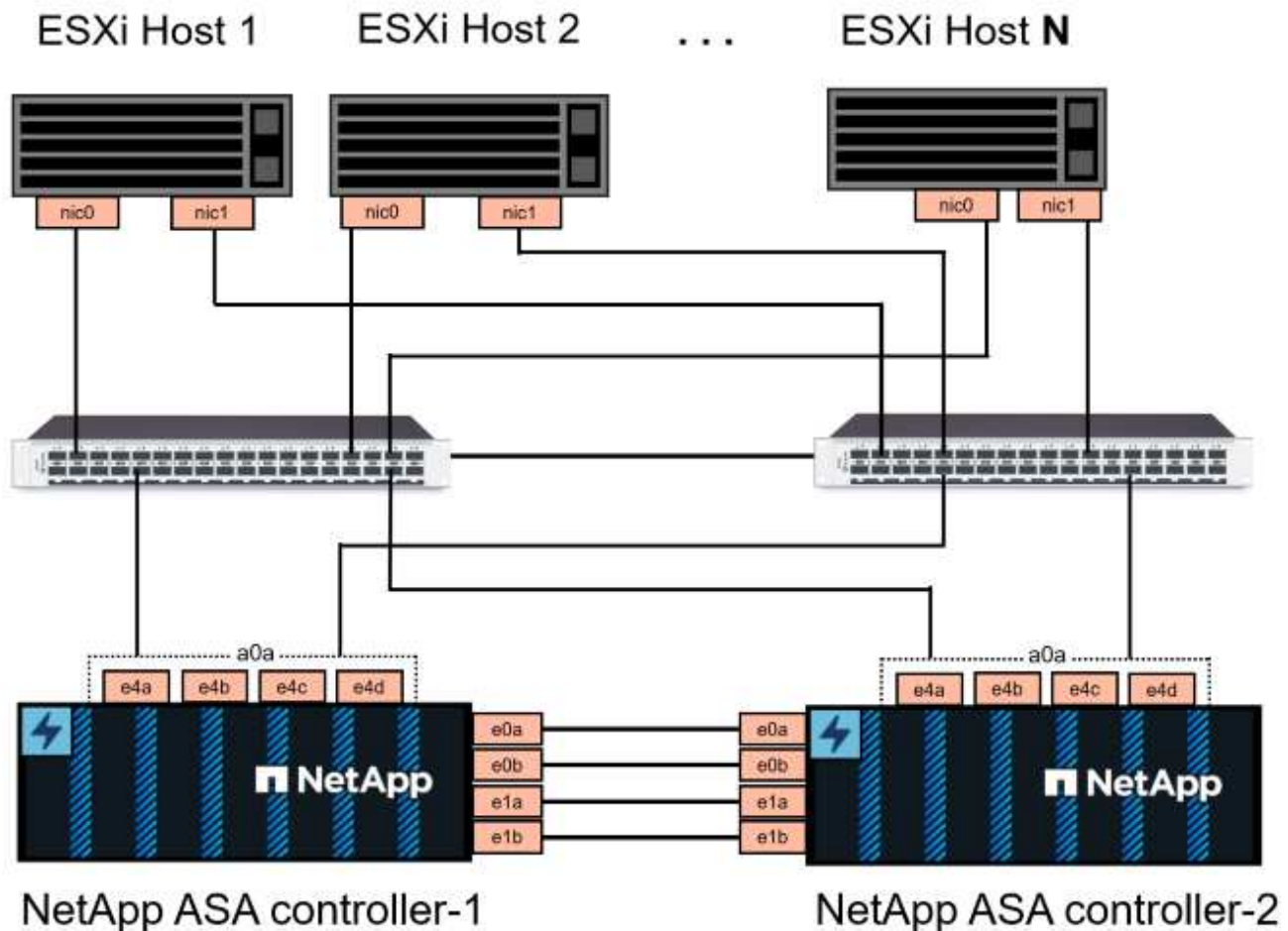
- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VCF-Verwaltungsdomäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VCF-Managementdomäne.
- Stellen Sie ONTAP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

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.

NetApp empfiehlt für iSCSI vollständig redundante Netzwerkdesigns. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration für Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Weitere Informationen finden Sie im NetApp "[Referenz zur SAN-Konfiguration](#)" Finden Sie weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten ethernet-Netzwerken.

In dieser Dokumentation wird der Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adressinformationen für die Erstellung mehrerer LIFs für iSCSI-Datenverkehr demonstriert. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter ["LIF erstellen \(Netzwerkschnittstelle\)"](#).

Weitere Informationen zur Verwendung von VMFS iSCSI-Datstores mit VMware finden Sie unter ["VSphere VMFS Datenspeicher – iSCSI-Storage-Back-End mit ONTAP"](#).



In Situationen, in denen mehrere VMkernel-Adapter auf demselben IP-Netzwerk konfiguriert sind, wird empfohlen, die iSCSI-Port-Bindung für die ESXi-Hosts zu verwenden, um sicherzustellen, dass der Lastausgleich über die Adapter hinweg erfolgt. Siehe KB-Artikel ["Überlegungen zur Verwendung der Software-iSCSI-Portbindung in ESX/ESXi \(2038869\)"](#).

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools bereitzustellen und zum Erstellen eines VMFS-Datstore in der VCF-Managementdomäne zu verwenden:

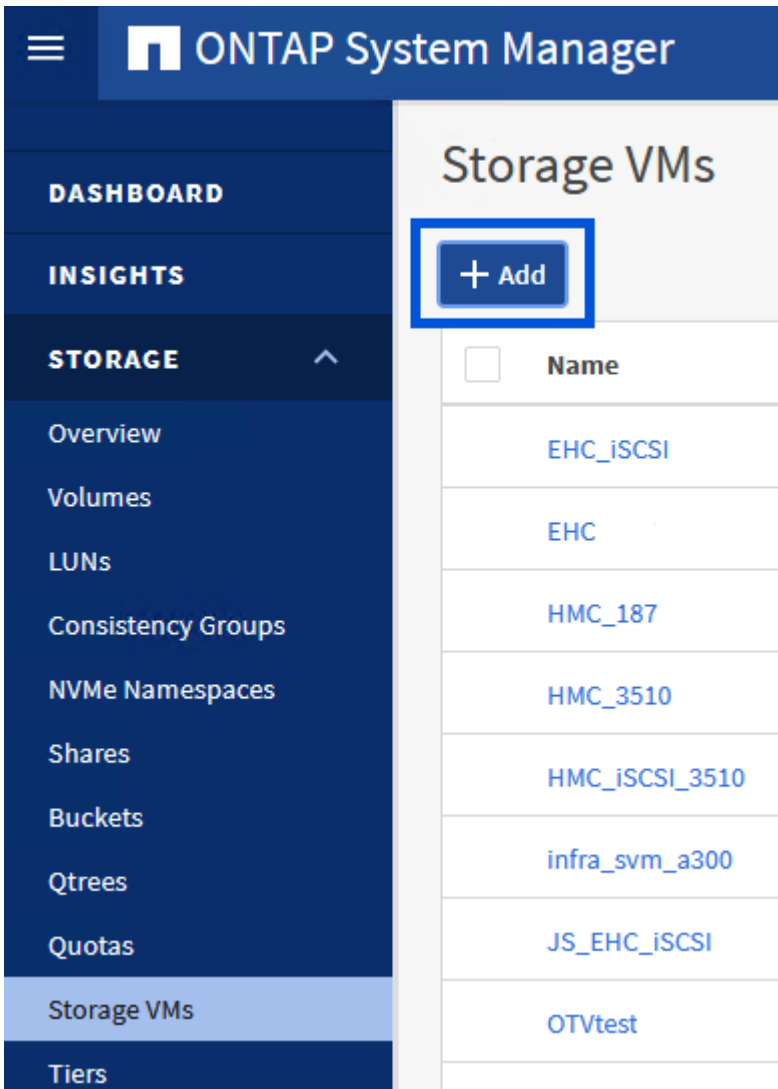
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager durchgeführt.

Storage-VM und LIFs erstellen

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

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



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

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

✓ iSCSI

FC

NVMe

☒ Enable iSCSI

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



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten Ethernet-Netzwerken.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI



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

IP ADDRESS

172.21.119.179

PORT

a0a-3375



ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374



IP ADDRESS

172.21.119.180

PORT

a0a-3375



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

Storage VM Administration

☐

Manage administrator account

Save

Cancel

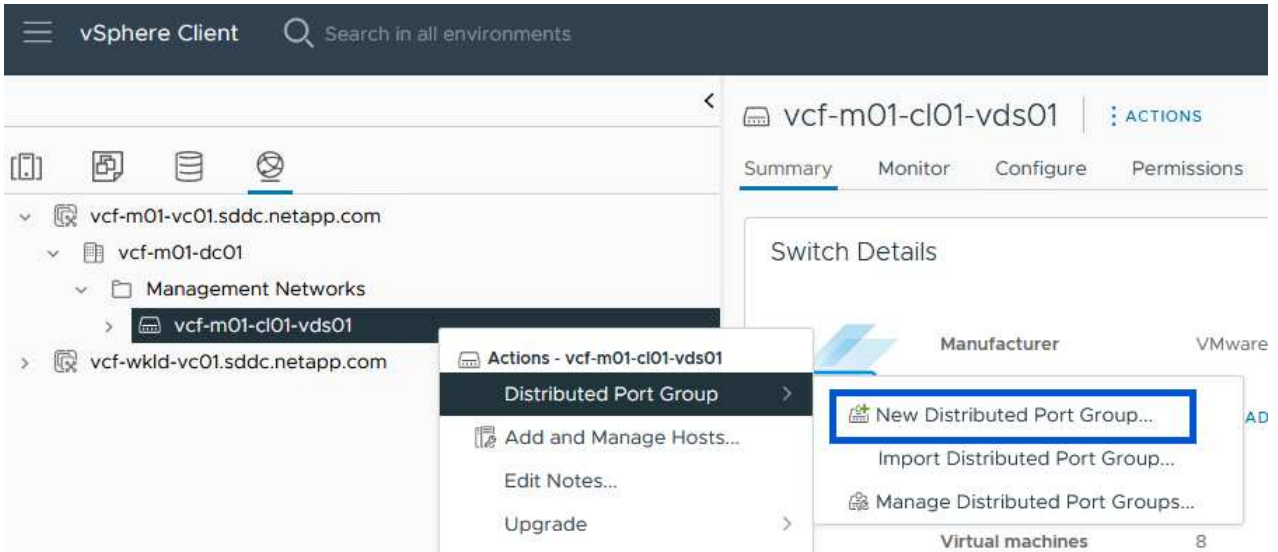
Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein

Die folgenden Schritte werden auf dem VCF-Management-Domain-Cluster unter Verwendung des vSphere-Clients durchgeführt.

Erstellen Sie verteilte Portgruppen für iSCSI-Datenverkehr

Gehen Sie wie folgt vor, um eine neue verteilte Portgruppe für jedes iSCSI-Netzwerk zu erstellen:

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



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

New Distributed Port Group

- 1 Name and location
- 2 **Configure settings**
- 3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic ⓘ

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen und sicherzustellen, dass Sie die richtige **VLAN-ID** eingegeben haben.
- Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.

vSphere Client

Search in all environments

vcf-m01-cl01-vds01-pg-iscsi-a

ACTIONS

Summary

Monitor

Configure

Permissions

Ports

Distributed Port Group Details

Port binding

Static binding

Port allocation

Elastic

VLAN ID

3374

Distributed switch

vcf-m01-cl01-vds01

Network protocol profile

--

Network resource pool

--

Hosts

4

vcf-m01-vc01.sddc.netapp.com

vcf-m01-dc01

Management Networks

vcf-m01-cl01-vds01

SDDC-DPortGroup-VM-Mgmt

vcf-m01-cl01-vds-DVUplinks-19

vcf-m01-cl01-vds01-pg-iscsi-a

vcf-m01-cl01-vds01

vcf-m01-cl01-vds01

vcf-m01-cl01-vds01

vcf-m01-cl01-vds01

vcf-wkld-vc01.sddc.netapp.com

Actions - vcf-m01-cl01-vds01-pg-iscsi-a

Edit Settings...

Export Configuration...

Restore Configuration...

7. Navigieren Sie auf der Seite **Distributed Port Group - Edit Settings** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **unused Uplinks** zu verschieben.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-a ×

General	Load balancing	Route based on originating virtual port ▼
Advanced	Network failure detection	Link status only ▼
VLAN	Notify switches	Yes ▼
Security	Failback	Yes ▼
Traffic shaping		
Teaming and failover		
Monitoring	Failover order ⓘ	
Miscellaneous		

MOVE UP MOVE DOWN

Active uplinks

uplink1

Standby uplinks

Unused uplinks

uplink2

CANCEL

OK

8. Wiederholen Sie diesen Schritt für die zweite iSCSI-Portgruppe. Allerdings bewegt sich dieses Mal **Uplink1** zu **unbenutzten Uplinks**.

Distributed Port Group - Edit Settings | vcf-m01-cl01-vds01-pg-iscsi-b

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual port ▾

Network failure detection

Link status only ▾

Notify switches

Yes ▾

Failback

Yes ▾

Failover order ⓘ

MOVE UP MOVE DOWN

Active uplinks

uplink2

Standby uplinks

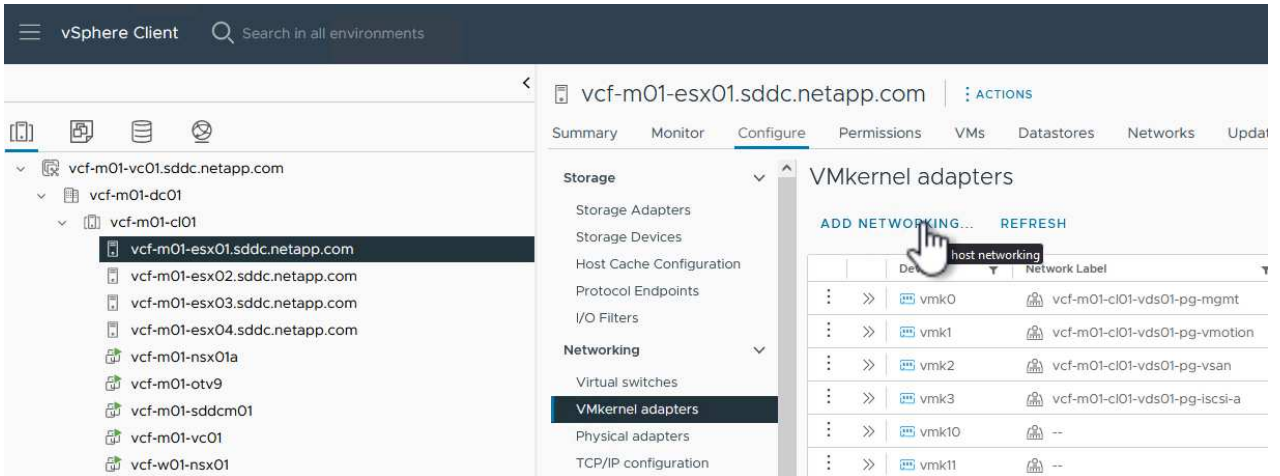
Unused uplinks

uplink1

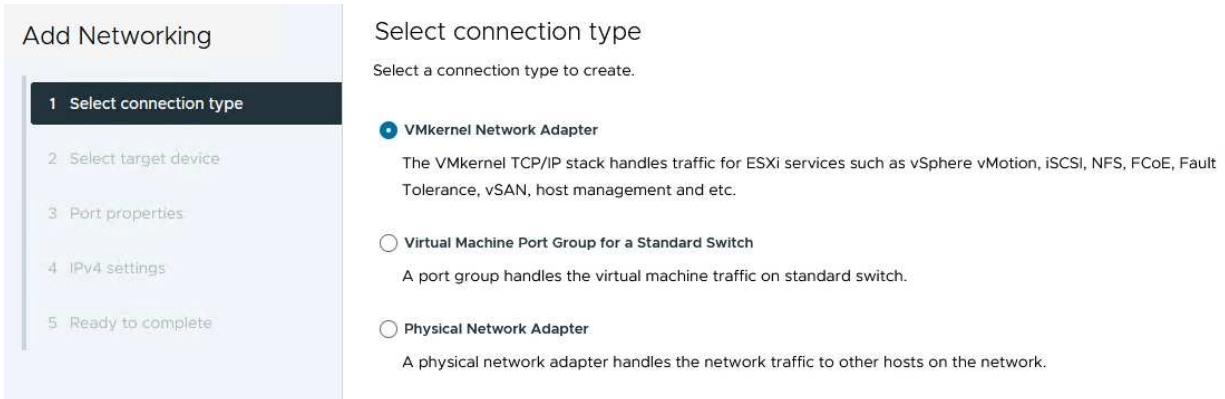
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

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



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



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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

☒ Select an existing network

☐ Select an existing standard switch

☐ New standard switch

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	SDDC-DPortGroup-VM-Mgmt	--	vcf-m01-ci01-vds01
<input checked="" type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-a	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-iscsi-b	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-mgmt	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vmotion	--	vcf-m01-ci01-vds01
<input type="radio"/>	vcf-m01-ci01-vds01-pg-vsan	--	vcf-m01-ci01-vds01

Manage Columns

6 items

CANCEL

BACK

NEXT

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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Port properties

Specify VMkernel port settings.

Network label

vcf-m01-ci01-vds01-pg-iscsi-a (vcf-m01-ci01-vds01)

MTU

Get MTU from switch

9000

TCP/IP stack

Default

Available services

Enabled services

☒ vMotion

☐ Provisioning

☐ Fault Tolerance logging

☐ Management

☐ vSphere Replication

☐ vSphere Replication NFC

☐ vSAN

☐ vSAN Witness

☐ vSphere Backup NFC

☐ NVMe over TCP

☐ NVMe over RDMA

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically
☒ Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway ☐ Override default gateway for this adapter

DNS server addresses

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- Ready to complete**

Ready to complete

Review your selections before finishing the wizard

Select target device

Distributed port group	vcf-m01-cl01-vds01-pg-iscsi-a
Distributed switch	vcf-m01-cl01-vds01

Port properties

New port group	vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)
MTU	9000
vMotion	Disabled
Provisioning	Disabled
Fault Tolerance logging	Disabled
Management	Disabled
vSphere Replication	Disabled
vSphere Replication NFC	Disabled
vSAN	Disabled
vSAN Witness	Disabled
vSphere Backup NFC	Disabled
NVMe over TCP	Disabled
NVMe over RDMA	Disabled

IPv4 settings

IPv4 address	172.21.118.114 (static)
Subnet mask	255.255.255.0

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

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

Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools

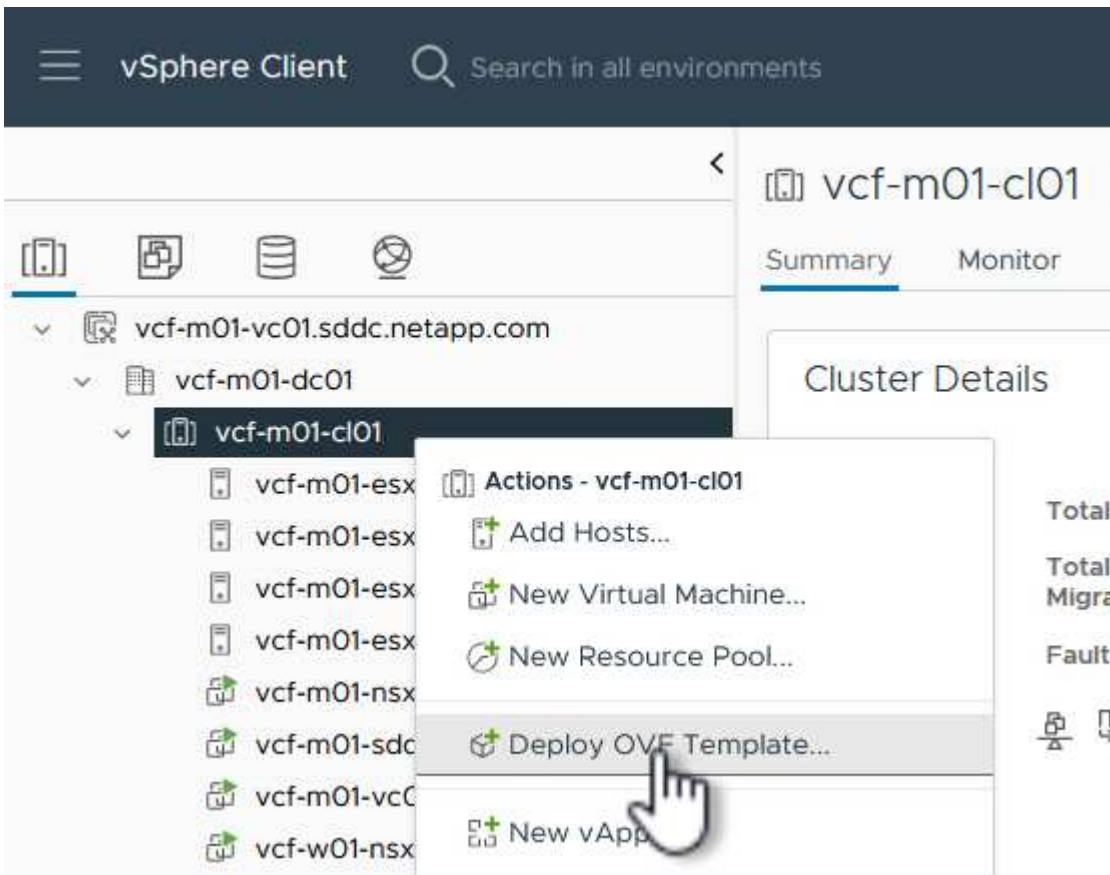
Die folgenden Schritte werden auf dem VCF-Management-Domänencluster unter Verwendung des vSphere-Clients durchgeführt und umfassen die Bereitstellung von OTV, die Erstellung eines VMFS-iSCSI-Datastore und die Migration von Management-VMs auf den neuen Datastore.

Implementieren Sie ONTAP-Tools für VMware vSphere

ONTAP Tools für VMware vSphere (OTV) werden als VM-Appliance implementiert und verfügen über eine integrierte vCenter-Benutzeroberfläche zum Management von ONTAP Storage.

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

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



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

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

[http | https://remoteserver-address/filetoinstall.ovf|.ova](http://remoteserver-address/filetoinstall.ovf|.ova)

☒ Local file

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

- Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
- Wählen Sie für den Speicherort der Konfigurations- und Festplattendateien den vSAN Datastore des VCF Management Domain Clusters aus.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

VM Storage Policy

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	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

Manage Columns

Items per page 10 ▾ 5 items

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

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

Select networks

Select a destination network for each source network.

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

Manage Columns

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

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

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

- Passwort für administrativen Zugriff auf OTV.
- NTP-Server-IP-Adresse.
- Passwort für das OTV-Wartungskonto.
- OTV Derby DB-Kennwort.
- Aktivieren Sie nicht das Kontrollkästchen, um VMware Cloud Foundation (VCF)* zu aktivieren. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
- FQDN oder IP-Adresse der vCenter-Appliance und Anmeldeinformationen für vCenter angeben.
- Geben Sie die erforderlichen Felder für Netzwerkeigenschaften an.

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

Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

System Configuration	4 settings
Application User Password (*)	Password to assign to the administrator account. For security reasons, it is recommended to use a password that is of eight to thirty characters and contains a minimum of one upper, one lower, one digit, and one special character. Password <input type="password"/> 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. <input type="text" value="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

Configure vCenter or Enable VCF	5 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="172.21.166.140"/>
Port (*)	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
Username (*)	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
Password (*)	Specify the password of an existing vCenter to register to. Password <input type="password"/> 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-m01-otvs9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is

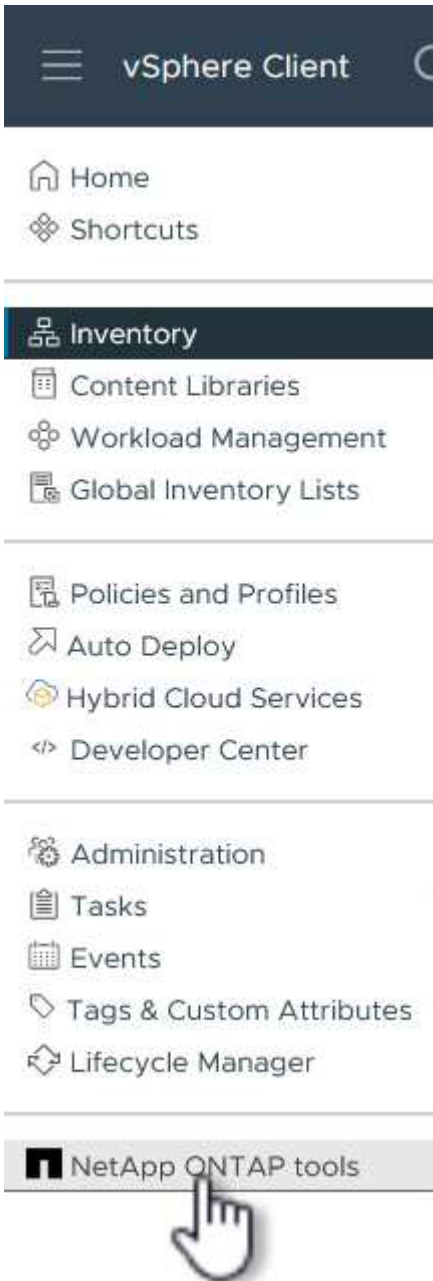
CANCEL BACK NEXT

9. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der OTV-Appliance zu beginnen.

Konfigurieren Sie einen VMFS-iSCSI-Datastore in der Management-Domain mit OTV

Führen Sie die folgenden Schritte aus, um einen VMFS-iSCSI-Datastore als zusätzlichen Speicher in der Management-Domäne zu konfigurieren:

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



2. Klicken Sie in **ONTAP-Tools** auf der Seite erste Schritte (oder von **Speichersystemen**) auf **Hinzufügen**, um ein neues Speichersystem hinzuzufügen.

vSphere Client
Search in all environments


NetApp ONTAP tools
INSTANCE 172.21.166.139:8443

Overview
Storage Systems
Storage capability profile
Storage Mapping
Settings
Reports
Datastore Report
Virtual Machine Report
vVols Datastore Report
vVols Virtual Machine Report
Log Integrity Report

ONTAP tools for VMware vSphere

Getting Started
Traditional Dashboard
vVols Dashboard


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



Add Storage System

Add storage systems to ONTAP tools for VMware vSphere.

ADD




Provision Datastore


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**.

Add Storage System

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

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

CANCEL


SAVE & ADD MORE

ADD



4. Klicken Sie auf **Yes**, um das Clusterzertifikat zu autorisieren und das Speichersystem hinzuzufügen.

Add Storage System

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

vCenter server

vcf-m01-vc01.sddc.netapp.com

Authorize Cluster Certificate

Host 172.16.9.25 has identified itself with a self-signed certificate.

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

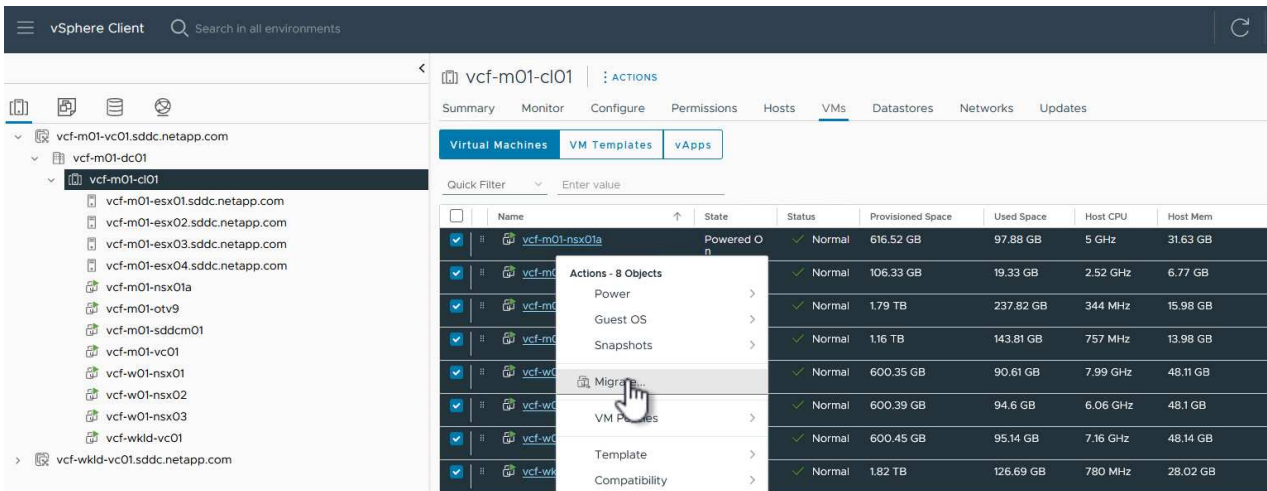
ADD

Migration von Management-VM's auf iSCSI-Datenspeicher

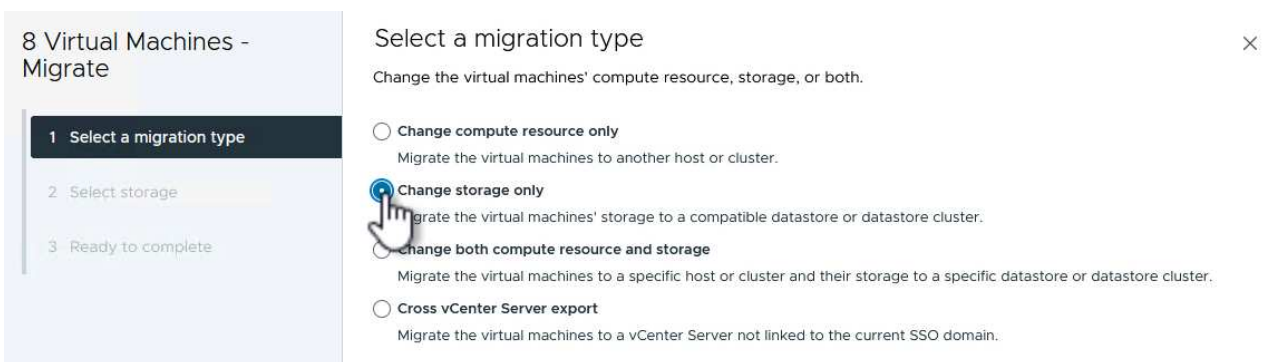
In Fällen, in denen es bevorzugt wird, ONTAP Storage zum Schutz der VCF Management-VM zu verwenden, kann vMotion zur Migration der VMs zum neu erstellten iSCSI-Datenspeicher verwendet werden.

Führen Sie die folgenden Schritte aus, um die VCF-Management-VMs auf den iSCSI-Datenspeicher zu migrieren.

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



3. Wählen Sie im Assistenten **Virtual Machines - Migrate** als Migrationstyp **nur Speicher ändern** aus und klicken Sie auf **Weiter**, um fortzufahren.



4. Wählen Sie auf der Seite **Select Storage** den iSCSI-Datenspeicher aus und wählen Sie **Next**, um fortzufahren.

8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

Select storage

Select the destination storage for the virtual machine migration.

BATCH CONFIGURE

CONFIGURE PER DISK

Select virtual disk format

Same format as source

VM Storage Policy

Datastore Default

☐ Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	mgmt_01_iscsi	--	3 TB	1.46 GB	3 TB	
<input type="radio"/>	vcf-m01-cl01-ds-vsan01	--	999.97 GB	7.28 TB	52.38 GB	

Compatibility

















✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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

Task Name	Target	Status	Details
Relocate virtual machine	 vcf-w01-nsx03	<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 zum Konfigurieren von ONTAP-Speichersystemen finden Sie im ["ONTAP 9-Dokumentation"](#) Zentrieren.

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

Video-Demo für diese Lösung

[iSCSI-Datenspeicher als ergänzender Speicher für VCF-Management-Domänen](#)

Konfigurieren Sie zusätzlichen Storage (VVols) für VCF-Workload-Domänen mit den ONTAP-Tools

Autor: Josh Powell

Konfigurieren Sie zusätzlichen Storage (VVols) für VCF-Workload-Domänen mit den ONTAP-Tools

Szenarioübersicht

In diesem Szenario zeigen wir, wie Sie ONTAP Tools für VMware vSphere (OTV) implementieren und verwenden, um einen **VVols-Datastore** für eine VCF-Workload-Domäne zu konfigurieren.

iSCSI wird als Storage-Protokoll für den VVols Datastore verwendet.

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

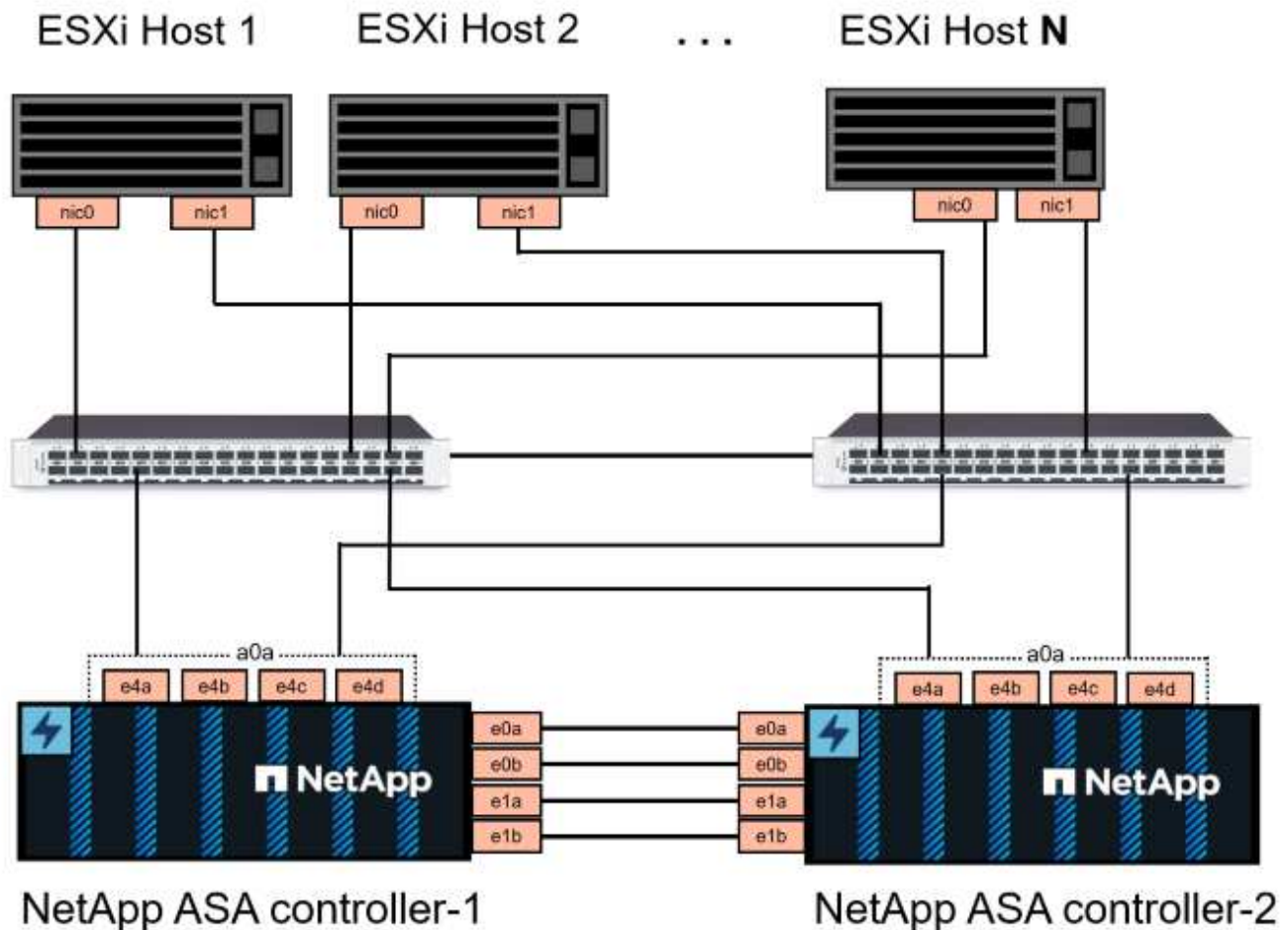
- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workload-Domäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workload-Domäne.
- Implementieren Sie ONTAP Tools in der VI-Workload-Domäne.
- Erstellen Sie einen neuen VVols-Datastore auf der VI-Workload-Domäne.

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.

NetApp empfiehlt für iSCSI vollständig redundante Netzwerkdesigns. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration für Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Weitere Informationen finden Sie im NetApp ["Referenz zur SAN-Konfiguration"](#) Finden Sie weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten ethernet-Netzwerken.

In dieser Dokumentation wird der Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adressinformationen für die Erstellung mehrerer LIFs für iSCSI-Datenverkehr demonstriert. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter "[LIF erstellen \(Netzwerkschnittstelle\)](#)".



In Situationen, in denen mehrere VMkernel-Adapter auf demselben IP-Netzwerk konfiguriert sind, wird empfohlen, die iSCSI-Port-Bindung für die ESXi-Hosts zu verwenden, um sicherzustellen, dass der Lastausgleich über die Adapter hinweg erfolgt. Siehe KB-Artikel "[Überlegungen zur Verwendung der Software-iSCSI-Portbindung in ESX/ESXi \(2038869\)](#)".

Weitere Informationen zur Verwendung von VMFS iSCSI-Datstores mit VMware finden Sie unter "[VSphere VMFS Datenspeicher – iSCSI-Storage-Back-End mit ONTAP](#)".

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um ONTAP Tools zu implementieren und damit einen VVols Datastore auf der VCF-Managementdomäne zu erstellen:

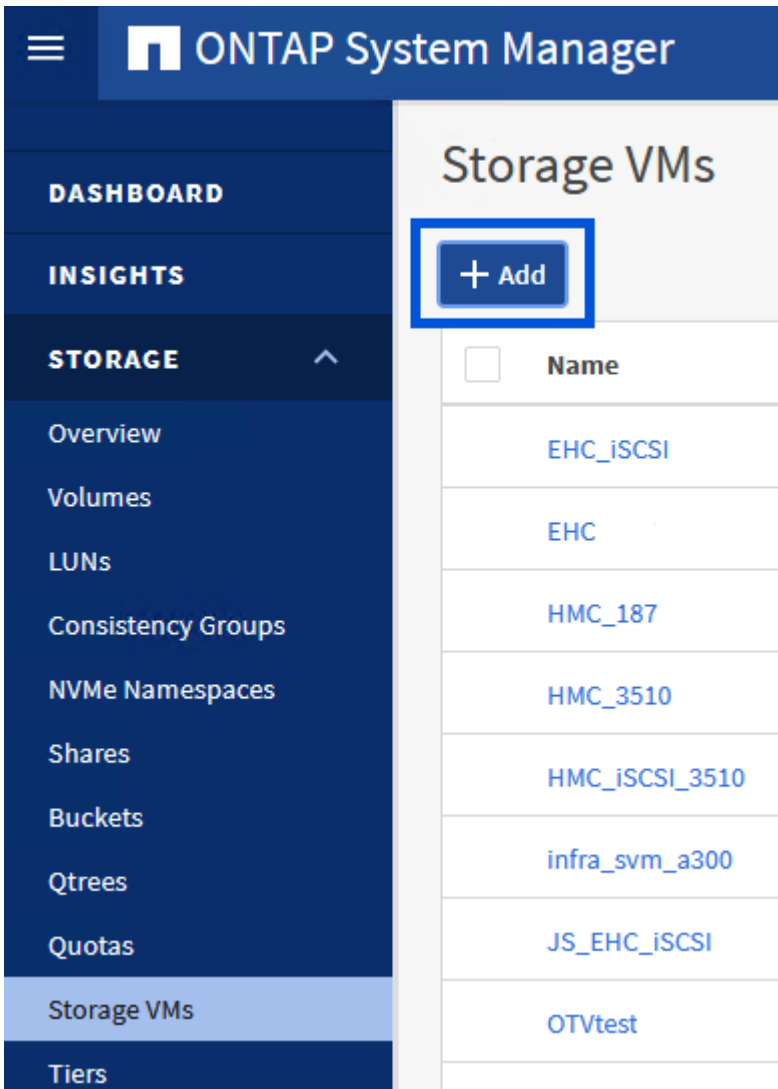
Erstellung der SVM und LIFs auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

Storage-VM und LIFs erstellen

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

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



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

Add Storage VM



STORAGE VM NAME

SVM_ISCSI

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

✓ iSCSI

FC

NVMe

☒ Enable iSCSI

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



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in iSCSI-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten Ethernet-Netzwerken.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.179

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI



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

IP ADDRESS

172.21.119.179

PORT

a0a-3375



ntaphci-a300-02

IP ADDRESS

172.21.118.180

PORT

a0a-3374



IP ADDRESS

172.21.119.180

PORT

a0a-3375



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

Storage VM Administration

☐

Manage administrator account

Save

Cancel

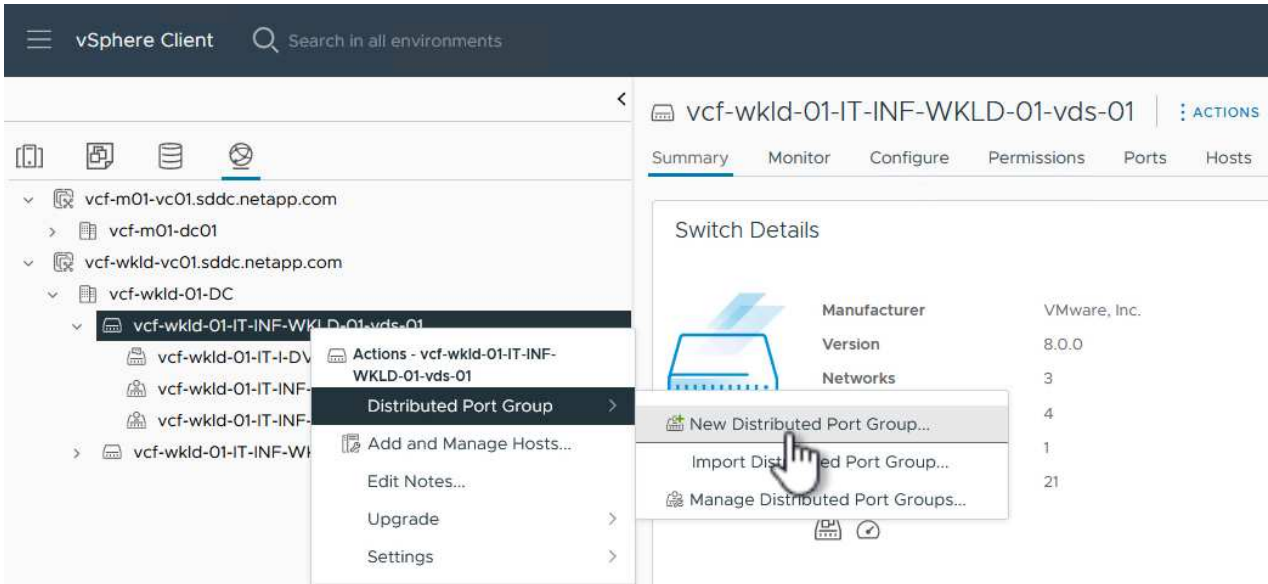
Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein

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

Erstellen Sie verteilte Portgruppen für iSCSI-Datenverkehr

Gehen Sie wie folgt vor, um eine neue verteilte Portgruppe für jedes iSCSI-Netzwerk zu erstellen:

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



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

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding

Static binding

Port allocation

Elastic

Number of ports

8

Network resource pool

(default)

VLAN

VLAN type

VLAN

VLAN ID

3374

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete iSCSI-Netzwerk zu erstellen und sicherzustellen, dass Sie die richtige **VLAN-ID** eingegeben haben.
- Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.

vSphere Client Search in all environments

vcf-wkld-01-iscsi-a ACTIONS

Summary Monitor Configure Permissions Ports Hc

Distributed Port Group Details

Port binding Static binding

Port allocation Elastic

VLAN ID 3374

Distributed switch [vcf-wkld-01-IT-INF-WKLD-01-vds-01](#)

Network protocol profile --

vcf-m01-vc01.sddc.netapp.com

vcf-m01-dc01

vcf-wkld-vc01.sddc.netapp.com

vcf-wkld-01-DC

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

vcf-wkld-01-iscsi-a

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

vcf-wkld-01-i

Actions - vcf-wkld-01-iscsi-a

Edit Settings...

Edit Configuration...

7. Navigieren Sie auf der Seite **Distributed Port Group - Edit Settings** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **unused Uplinks** zu verschieben.

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

General

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

uplink1

Standby uplinks

Unused uplinks

uplink2

Route based on originating virtual por

Link status only

Yes

Yes

CANCEL

OK

8. Wiederholen Sie diesen Schritt für die zweite iSCSI-Portgruppe. Allerdings bewegt sich dieses Mal **Uplink1** zu **unbenutzten Uplinks**.

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

General

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 por

Link status only

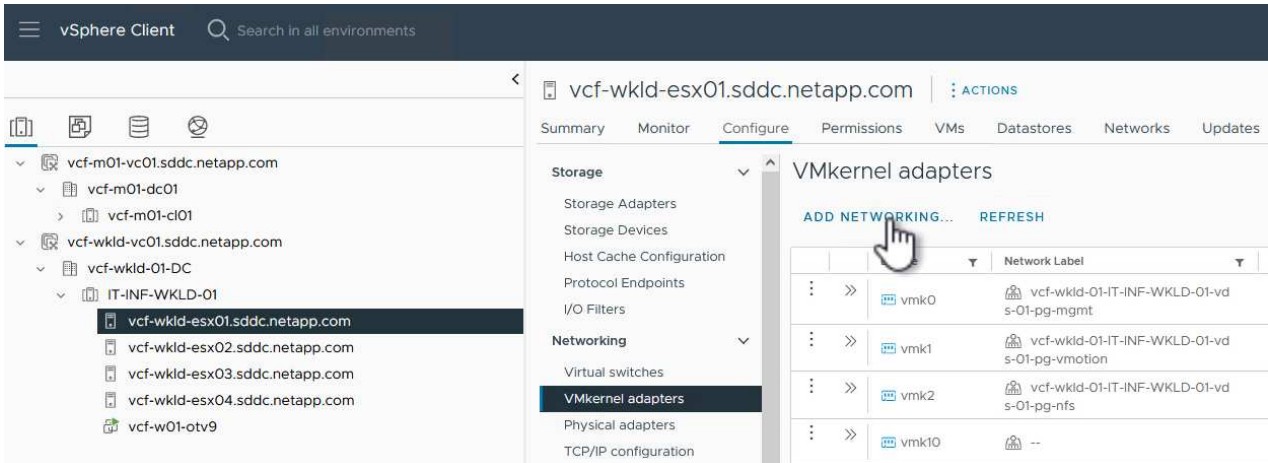
Yes

Yes

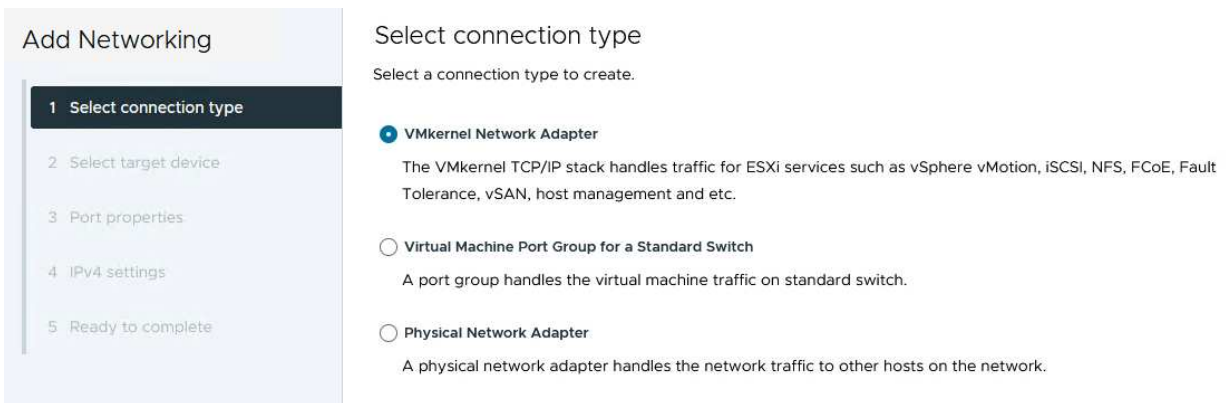
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

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



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



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

Add Networking

- Select connection type
- Select target device**
- Port properties
- IPv4 settings
- Ready to complete

Select target device

Select a target device for the new connection.

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

Quick Filter

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

5 items

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

Add Networking

- Select connection type
- Select target device
- Port properties**
- IPv4 settings
- Ready to complete

Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

Available services

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

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically
☒ Use static IPv4 settings

IPv4 address

Subnet mask

Default gateway ☐ Override default gateway for this adapter

DNS server addresses

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- Ready to complete**

Ready to complete

Review your selections before finishing the wizard

Select target device

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

Port properties

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

IPv4 settings

- IPv4 address: 172.21.118.127 (static)
- Subnet mask: 255.255.255.0

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

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

Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools

Die folgenden Schritte werden auf dem VCF-Management-Domänencluster mithilfe des vSphere-Clients durchgeführt. Dazu gehören die Bereitstellung von OTV, die Erstellung eines VVols-iSCSI-Datastore und die Migration von Management-VMs auf den neuen Datastore.

Für VI-Workload-Domänen wird OTV im VCF Management Cluster installiert, aber bei dem vCenter registriert, das der VI-Workload-Domäne zugeordnet ist.

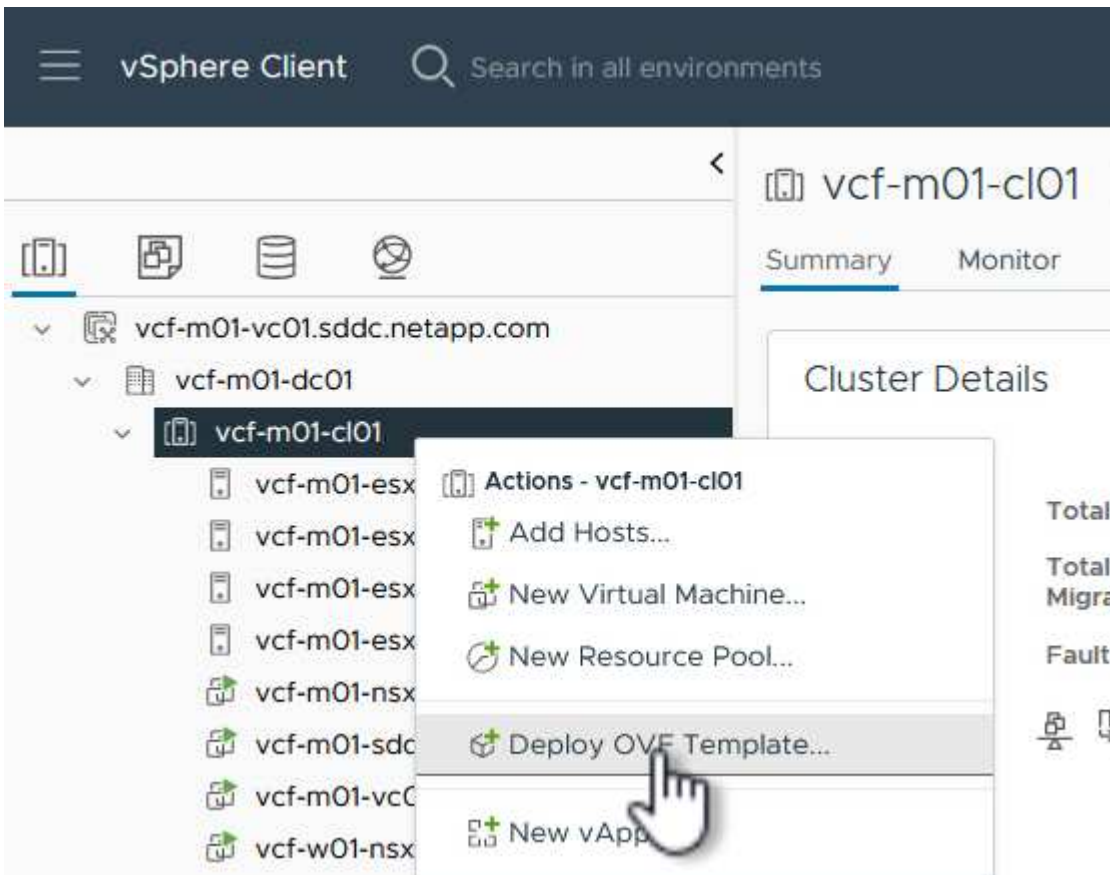
Weitere Informationen zum Implementieren und Verwenden von ONTAP Tools in einer Umgebung mit mehreren vCenter finden Sie unter ["Voraussetzungen für die Registrierung von ONTAP-Tools in einer Umgebung mit mehreren vCenter-Servern"](#).

Implementieren Sie ONTAP-Tools für VMware vSphere

ONTAP Tools für VMware vSphere (OTV) werden als VM-Appliance implementiert und verfügen über eine integrierte vCenter-Benutzeroberfläche zum Management von ONTAP Storage.

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

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



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

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

[http | https://remoteserver-address/filetoinstall.ovf|.ova](http://remoteserver-address/filetoinstall.ovf|.ova)

☒ Local file

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

- Wählen Sie für die Schritte 2 bis 5 des Assistenten einen Namen und Ordner für die VM aus, wählen Sie die Rechenressource aus, überprüfen Sie die Details und akzeptieren Sie die Lizenzvereinbarung.
- Wählen Sie für den Speicherort der Konfigurations- und Festplattendateien den vSAN Datastore des VCF Management Domain Clusters aus.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

VM Storage Policy

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	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

Manage Columns Items per page 10 5 items

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

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

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

1 item

IP Allocation Settings

IP allocation: Static - Manual

IP protocol: IPv4

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

- Passwort für administrativen Zugriff auf OTV.
- NTP-Server-IP-Adresse.
- Passwort für das OTV-Wartungskonto.
- OTV Derby DB-Kennwort.
- Aktivieren Sie nicht das Kontrollkästchen, um VMware Cloud Foundation (VCF)* zu aktivieren. Der VCF-Modus ist für die Bereitstellung von zusätzlichem Speicher nicht erforderlich.
- FQDN oder IP-Adresse der vCenter-Appliance für die **VI Workload Domain**
- Zugangsdaten für die vCenter-Appliance der **VI Workload Domain**
- Geben Sie die erforderlichen Felder für Netzwerkeigenschaften an.

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

Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

2 properties have invalid values

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

Deploy OVF Template

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

Customize template

Configure vCenter or Enable VCF	3 settings
Enable VMware Cloud Foundation (VCF)	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
vCenter Server Address (*)	Specify the IP address/hostname of an existing vCenter to register to. <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" value="....."/> Confirm Password <input type="password" value="....."/>

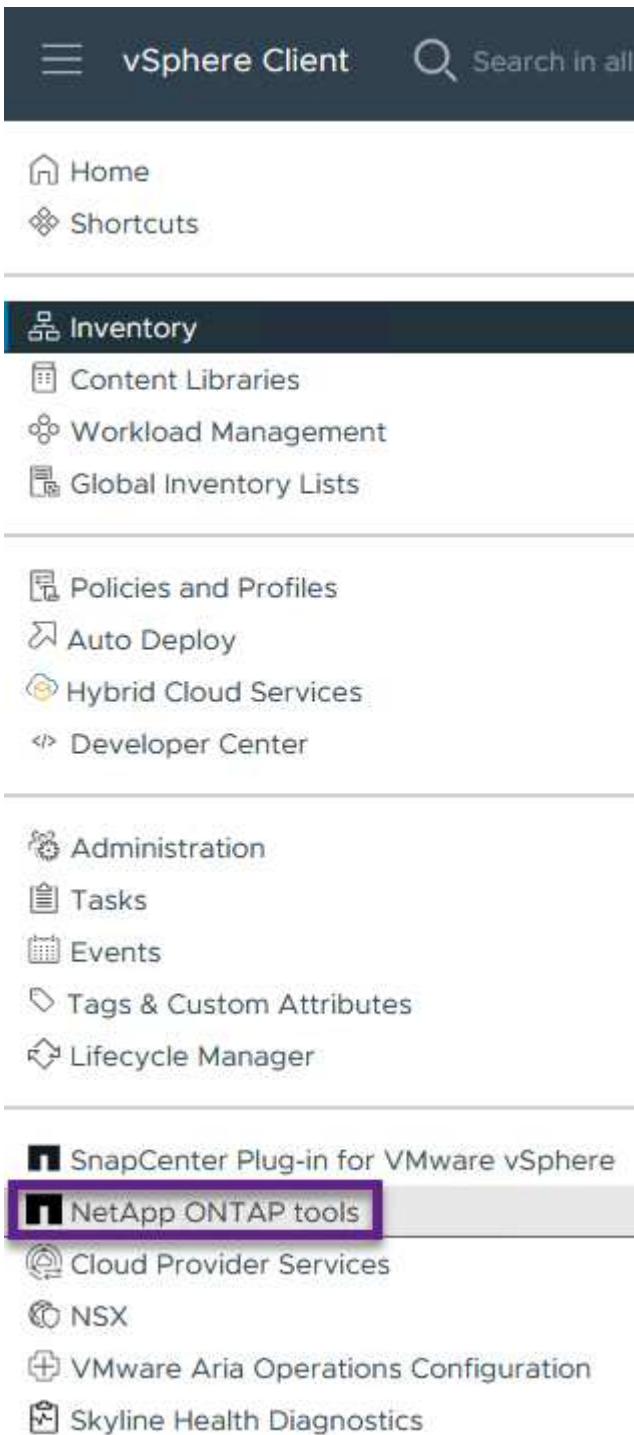
Network Properties	8 settings
Host Name	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-w01-otv9"/>
IP Address	Specify the IP address for the appliance. (Leave blank if DHCP is desired)

CANCEL BACK NEXT

9. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der OTV-Appliance zu beginnen.

Fügen Sie ONTAP Tools ein Storage-System hinzu.

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




2. Wählen Sie aus dem Dropdown-Menü **INSTANCE** in der Benutzeroberfläche des ONTAP-Tools die OTV-Instanz aus, die der zu verwaltenden Workload-Domain zugeordnet ist.

NetApp ONTAP tools **INSTANCE 172.21.166.139:8443** ▾

	Plugin Instance	Version	vCenter Server
Overview			
Storage Systems	172.21.166.139:8443	9.13.0.36905	vcf-m01-vc01.sddc.netapp.com
Storage capability profile	172.21.166.149:8443	9.13.0.36905	vcf-wkld-vc01.sddc.netapp.com
Storage Mapping			
Settings			

provide



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

NetApp ONTAP tools **INSTANCE 172.21.166.149:8443** ▾

	Storage Systems	
Overview		
Storage Systems	ADD	REDISCOVER ALL
Storage capability profile		


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



VVol erfordert ONTAP-Cluster-Anmeldeinformationen statt der SVM-Anmeldeinformationen. Weitere Informationen finden Sie unter ["Storage-Systeme hinzufügen"](#) In der Dokumentation zu ONTAP Tools.

Add Storage System

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

vCenter server vcf-m01-vc01.sddc.netapp.com 

Name or IP address: 172.16.9.25

Username: admin

Password: ●●●●●●●●

Port: 443

Advanced options 

ONTAP Cluster Certificate: ☒ Automatically fetch ☐ Manually upload

CANCEL

SAVE & ADD MORE

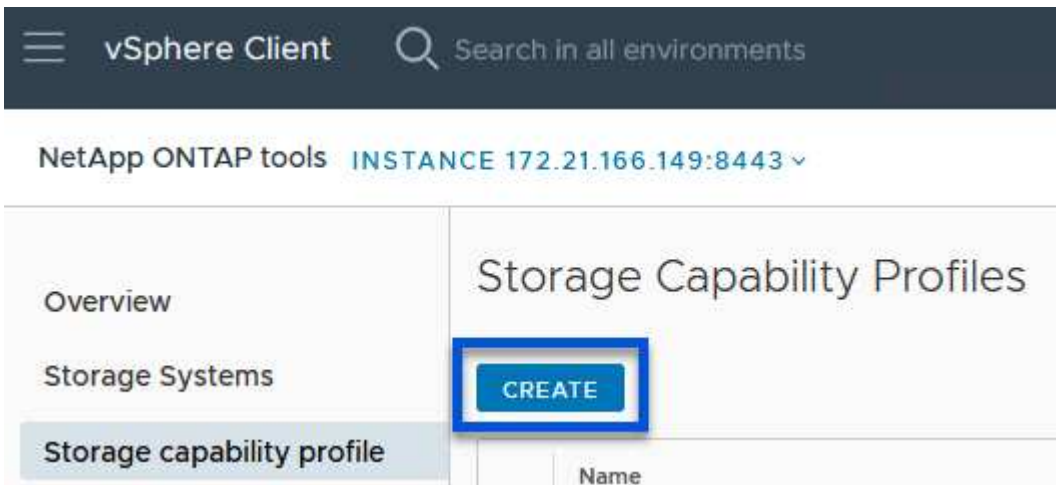
ADD

Erstellen Sie in ONTAP-Tools ein Storage-Funktionsprofil

Storage-Funktionsprofile beschreiben die Funktionen eines Storage-Arrays oder Storage-Systems. Sie umfassen Definitionen zur Servicequalität und werden zur Auswahl von Storage-Systemen verwendet, die die im Profil definierten Parameter erfüllen. Eines der zur Verfügung gestellten Profile kann verwendet oder neue erstellt werden.

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

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



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

The screenshot shows the 'Create Storage Capability Profile' wizard. On the left, there is a sidebar with a list of steps: '1 General', '2 Platform', '3 Protocol', '4 Performance', '5 Storage attributes', and '6 Summary'. The '1 General' step is selected and highlighted. The main area is titled 'General' and contains the instruction 'Specify a name and description for the storage capability profile. ?'. There are two input fields: 'Name:' with the value 'Gold_ASA_ISCSI' and 'Description:' with an empty text area. At the bottom right, there are two buttons: 'CANCEL' and 'NEXT'.

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Platform

Platform: Performance

Asymmetric:



CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Protocol

Protocol:

Any

Any

FCP

iSCSI

NVMe/FC

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Performance

☐ None ⓘ

☒ QoS policy group ⓘ

Min IOPS:

Max IOPS:

6000

☐ Unlimited

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

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

Create Storage Capability Profile

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

Summary

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

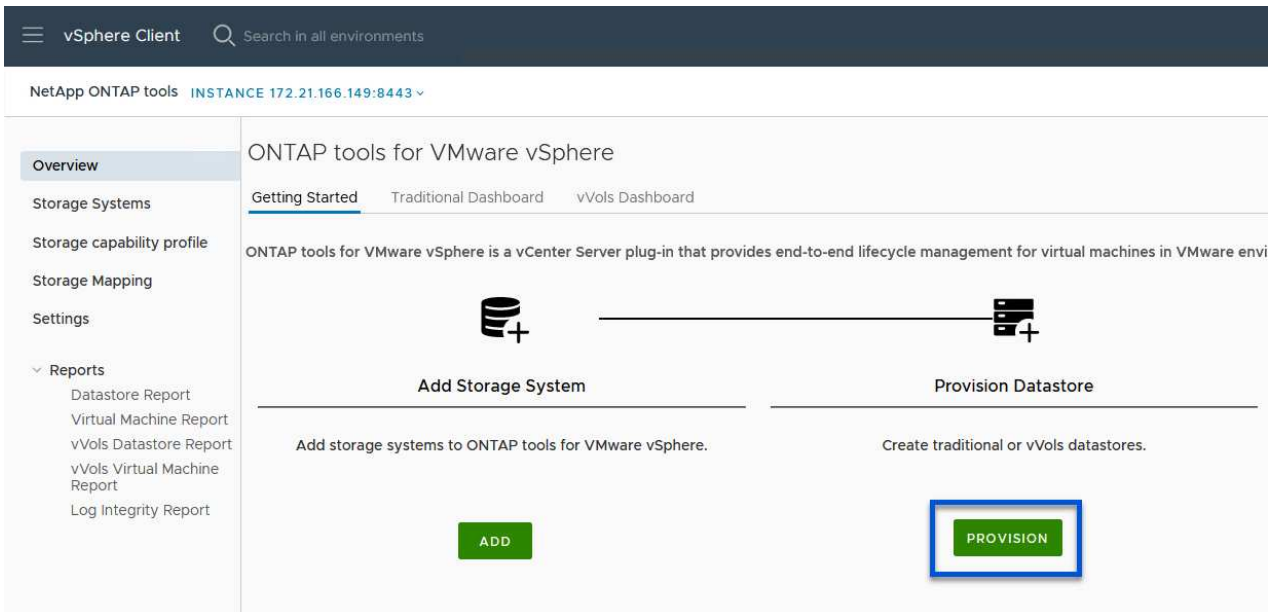
CANCEL BACK FINISH



Erstellen Sie einen VVols-Datastore in ONTAP Tools

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

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



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

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage system

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

Storage capability profiles:

AFF_Encrypted_Min50_ASA_A
FAS_Default
FAS_Max20
Custom profiles
ASA_Gold_iSCSI

Storage system:

ntaphci-a300e9u25 (172.16.9.25)

Storage VM:

VCF_iSCSI

CANCEL

BACK

NEXT

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

New Datastore

1 General

2 Storage system

3 Storage attributes

4 Summary

Storage attributes

Specify the storage details for provisioning the datastore.

Volumes: ☒ Create new volumes ☐ Select volumes

Create new volumes

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

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

ADD

CANCEL

BACK

NEXT

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

New Datastore

- General
- Storage system
- Storage attributes
- Summary**

Summary

Datastore type: vVols
 Protocol: iSCSI
 Storage capability profile: ASA_Gold_iSCSI

Storage system details

Storage system: ntaphci-a300e9u25
 SVM: VCF_iSCSI

Storage attributes

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

Click 'Finish' to provision this datastore.

CANCEL
BACK
FINISH

Weitere Informationen

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

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

Konfigurieren Sie zusätzlichen NVMe/TCP-Storage für VCF-Workload-Domänen

Autor: Josh Powell

Konfigurieren Sie zusätzlichen NVMe/TCP-Storage für VCF-Workload-Domänen

Szenarioübersicht

In diesem Szenario zeigen wir, wie zusätzlicher NVMe/TCP Storage für eine VCF-Workload-Domäne konfiguriert wird.

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für NVMe/TCP-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workload-Domäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workload-Domäne.
- Fügen Sie NVMe/TCP-Adapter auf ESXi-Hosts hinzu.
- Implementieren von NVMe/TCP-Datastore

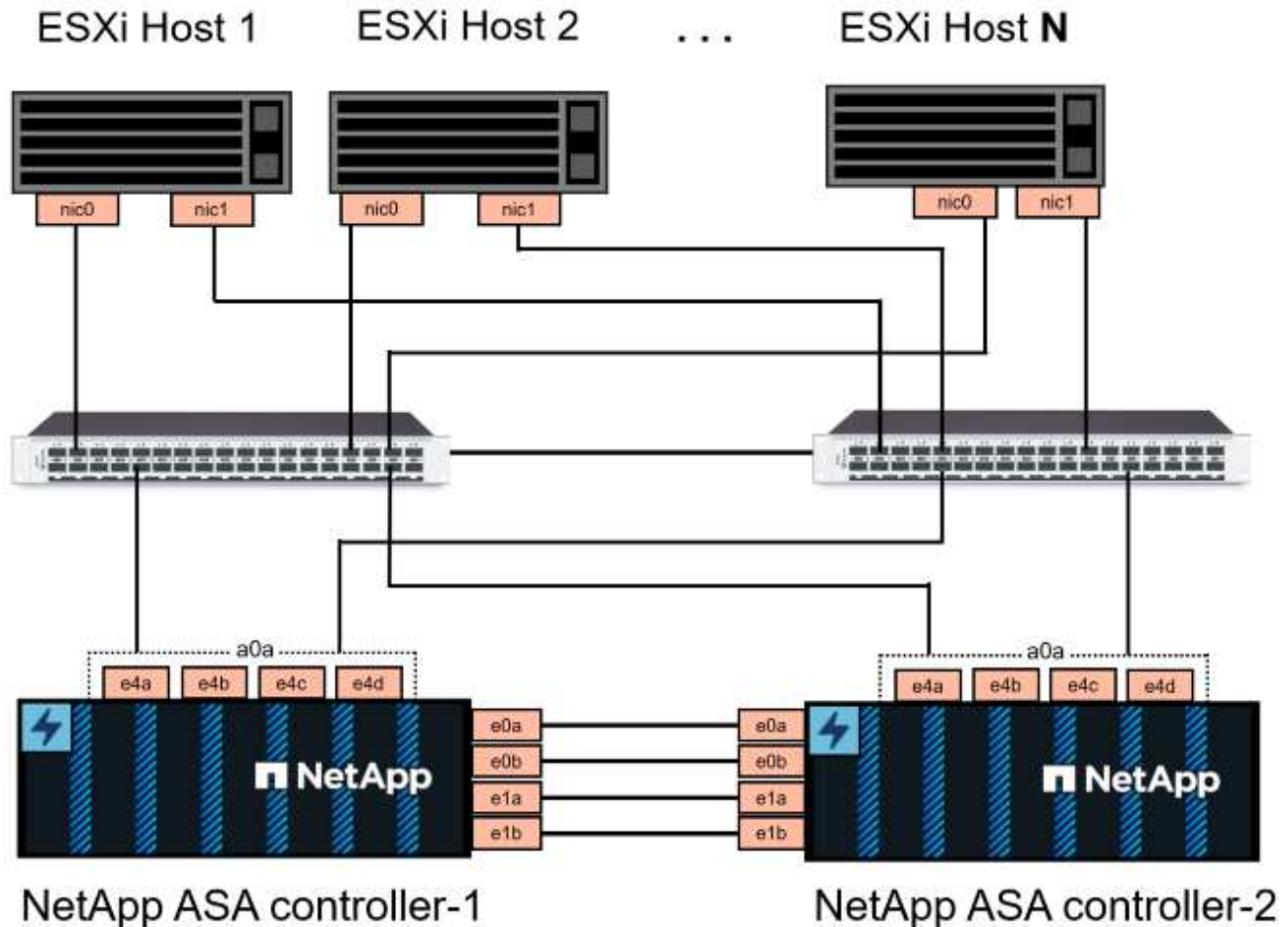
Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA Storage-System mit physischen Datenports an ethernet-Switches, die dediziert für Storage-Datenverkehr sind.

- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.

NetApp empfiehlt vollständig redundante Netzwerkdesigns für NVMe/TCP. Das folgende Diagramm zeigt ein Beispiel einer redundanten Konfiguration für Fehlertoleranz für Storage-Systeme, Switches, Netzwerkadapter und Host-Systeme. Weitere Informationen finden Sie im NetApp ["Referenz zur SAN-Konfiguration"](#) Finden Sie weitere Informationen.



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in NVMe/TCP-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten ethernet-Netzwerken.

Diese Dokumentation zeigt den Prozess der Erstellung einer neuen SVM und der Angabe der IP-Adressinformationen für die Erstellung mehrerer LIFs für NVMe/TCP-Datenverkehr. Informationen zum Hinzufügen neuer LIFs zu einer vorhandenen SVM finden Sie unter ["LIF erstellen \(Netzwerkschnittstelle\)"](#).

Weitere Informationen zu Überlegungen zum NVMe-Design für ONTAP Storage-Systeme finden Sie unter ["Konfiguration, Support und Einschränkungen von NVMe"](#).

Implementierungsschritte

Führen Sie die folgenden Schritte aus, um einen VMFS Datastore auf einer VCF-Workload-Domäne mithilfe von NVMe/TCP zu erstellen.

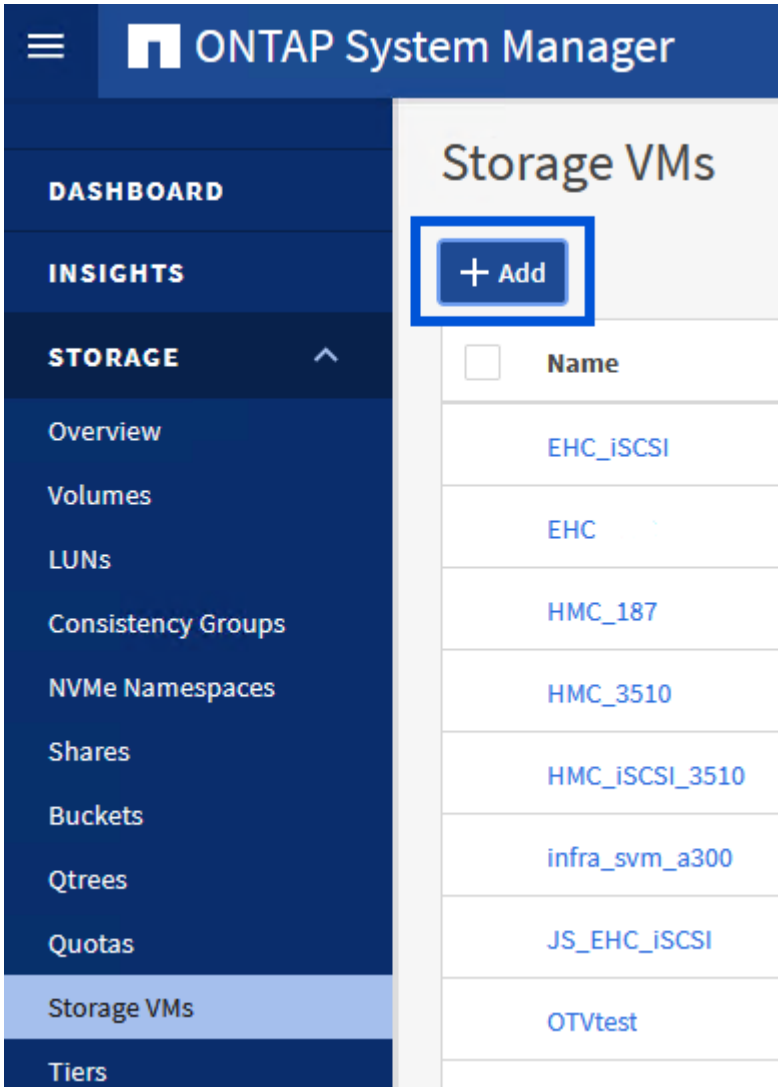
Erstellung von SVMs, LIFs und NVMe Namespace auf dem ONTAP Storage-System

Der folgende Schritt wird im ONTAP System Manager ausgeführt.

Storage-VM und LIFs erstellen

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

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



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

Add Storage VM



STORAGE VM NAME

VCF_NVMe

IPSPACE

Default



Access Protocol

SMB/CIFS, NFS, S3

iSCSI

FC

✓ NVMe

☐ Enable NVMe/FC

☒ Enable NVMe/TCP

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



Für Multipathing und Failover über mehrere Pfade empfiehlt NetApp für alle SVMs in NVMe/TCP-Konfigurationen die Verwendung von mindestens zwei LIFs pro Storage-Node in separaten Ethernet-Netzwerken.

NETWORK INTERFACE

ntaphci-a300-01

IP ADDRESS

172.21.118.189

SUBNET MASK

24

GATEWAY

[Add optional gateway](#)

BROADCAST DOMAIN AND PORT

NFS_iSCSI

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

IP ADDRESS

172.21.119.189

PORT

a0a-3375

ntaphci-a300-02

IP ADDRESS

172.21.118.190

PORT

a0a-3374

IP ADDRESS

172.21.119.190

PORT

a0a-3375

Storage VM Administration

☐ Manage administrator account

Save

Cancel

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

Storage VM Administration

☐ Manage administrator account

Save

Cancel

Erstellen des NVMe-Namespace

NVMe-Namespace entsprechen LUNs für iSCSI oder FC. Der NVMe-Namespace muss erstellt werden, bevor ein VMFS-Datastore aus dem vSphere Client heraus implementiert werden kann. Zum Erstellen des NVMe Namespace muss zunächst der NVMe Qualified Name (NQN) von jedem ESXi Host im Cluster abgerufen werden. ONTAP verwendet die NQN, um die Zugriffssteuerung für den Namespace bereitzustellen.

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

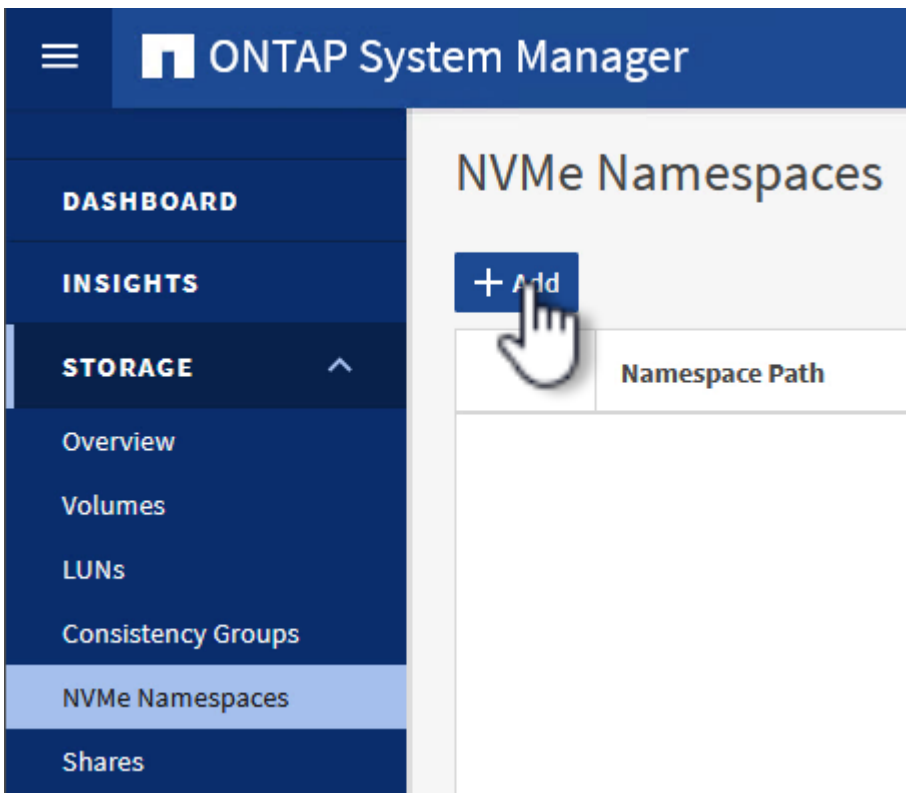
1. Öffnen Sie eine SSH-Sitzung mit einem ESXi-Host im Cluster, um dessen NQN zu erhalten. Verwenden Sie den folgenden Befehl aus der CLI:

```
esxcli nvme info get
```

Es sollte eine Ausgabe ähnlich der folgenden angezeigt werden:

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

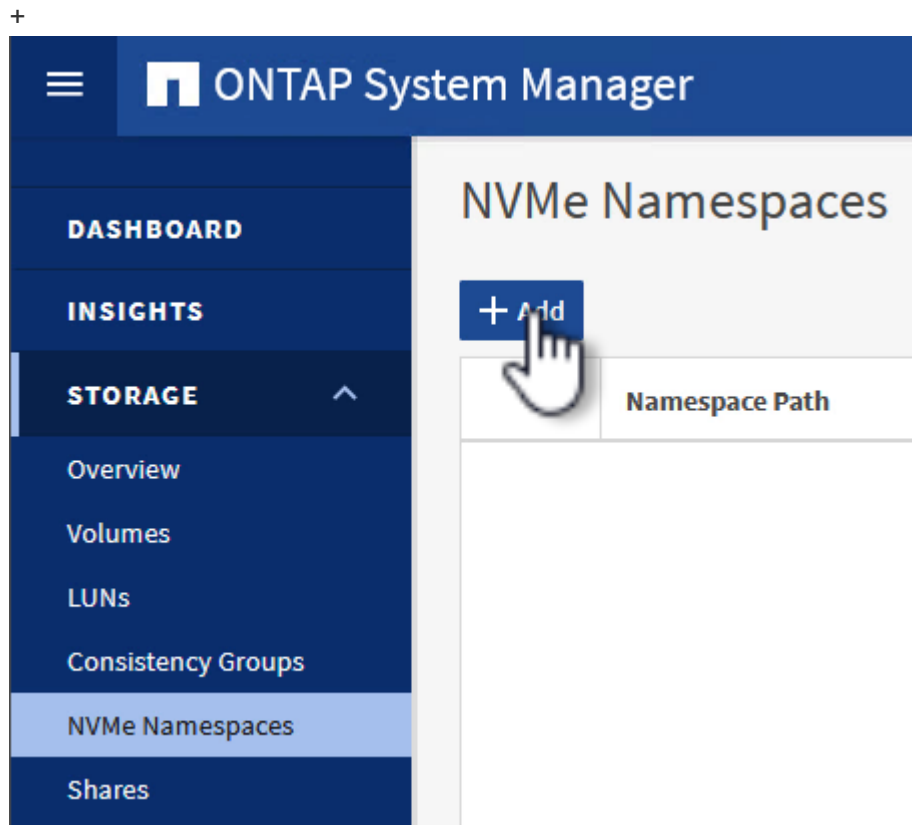
2. Notieren Sie die NQN für jeden ESXi-Host im Cluster
3. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **NVMe Namespaces** und klicken Sie auf **+ Hinzufügen**, um zu starten.



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

Namespaces, die Größe des Namespace und das Host-Betriebssystem ein, das auf den Namespace zugreift. Erstellen Sie im Abschnitt **Host NQN** eine kommagetrennte Liste der NQN's, die zuvor von den ESXi-Hosts erfasst wurden, die auf die Namespaces zugreifen werden.

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



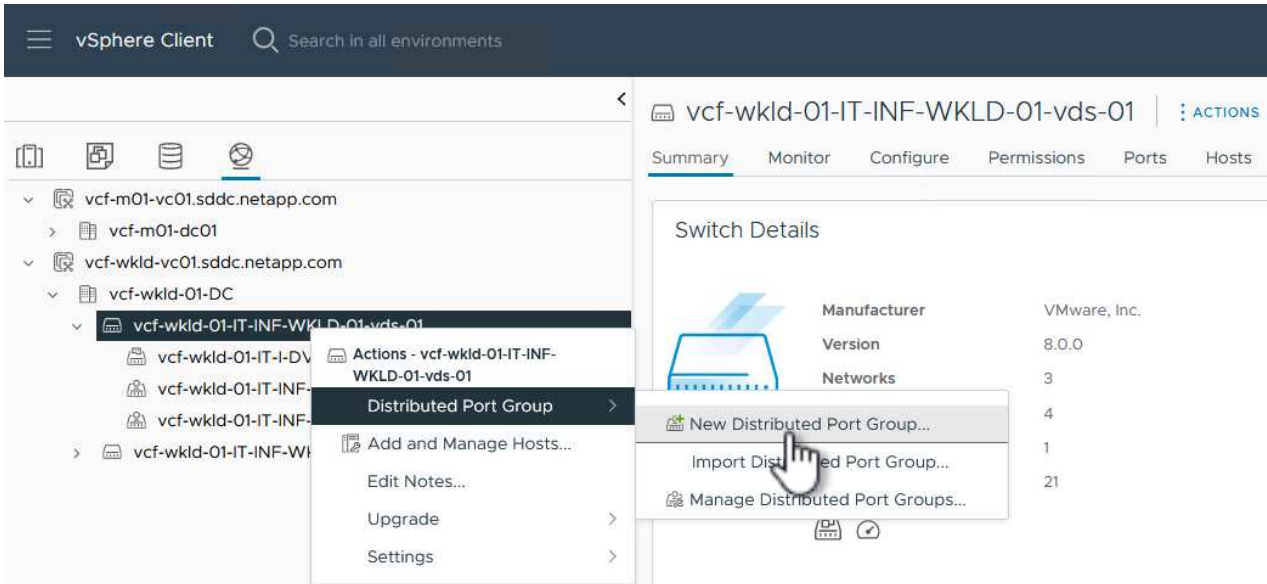
Richten Sie Netzwerk- und NVMe-Softwareadapter auf ESXi-Hosts ein

Folgende Schritte werden für den VI-Workload-Domänen-Cluster mithilfe des vSphere Clients durchgeführt. In diesem Fall wird vCenter Single Sign-On verwendet, sodass der vSphere-Client sowohl für die Management- als auch für die Workload-Domäne gemeinsam ist.

Verteilte Portgruppen für NVMe/TCP-Datenverkehr erstellen

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

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



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

New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

Configure settings

Set general properties of the new port group.

Port binding Static binding

Port allocation Elastic ⓘ

Number of ports 8

Network resource pool (default)

VLAN

VLAN type VLAN

VLAN ID 3374

Advanced

☐ Customize default policies configuration

CANCEL

BACK

NEXT

- Überprüfen Sie auf der Seite **Ready to Complete** die Änderungen und klicken Sie auf **Finish**, um die neue verteilte Portgruppe zu erstellen.
- Wiederholen Sie diesen Vorgang, um eine verteilte Portgruppe für das zweite verwendete NVMe/TCP-Netzwerk zu erstellen und sicherzustellen, dass Sie die korrekte **VLAN-ID** eingegeben haben.
- Nachdem beide Portgruppen erstellt wurden, navigieren Sie zur ersten Portgruppe und wählen Sie die Aktion **Einstellungen bearbeiten...** aus.

vSphere Client

Search in all environments

vcf-wkld-01-nvme-a

ACTIONS

Summary

Monitor

Configure

Permissions

vcf-m01-vc01.sddc.netapp.com

vcf-wkld-vc01.sddc.netapp.com

vcf-wkld-01-DC

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

vcf-wkld-01-iscsi-a

vcf-wkld-01-iscsi-b

vcf-wkld-01-IT-I-DVUplinks-10

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

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

vcf-wkld-01-nvme-a

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

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

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

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

Actions - vcf-wkld-01-nvme-a

Edit Settings...

Export Configuration...

Restore Configuration...

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

7. Navigieren Sie auf der Seite **Distributed Port Group - Edit Settings** im linken Menü zu **Teaming und Failover** und klicken Sie auf **Uplink2**, um es nach unten zu **unused Uplinks** zu verschieben.

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

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

uplink1

Standby uplinks

Unused uplinks

uplink2

Route based on originating virtual port

Link status only

Yes

Yes

8. Wiederholen Sie diesen Schritt für die zweite NVMe/TCP-Portgruppe. Allerdings bewegt sich dieses

68

Mal **Uplink1** zu **unbenutzten Uplinks**.

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

General

Advanced

VLAN

Security

Traffic shaping

Teaming and failover

Monitoring

Miscellaneous

Load balancing

Route based on originating virtual por 

Network failure detection

Link status only 

Notify switches

Yes 

Failback

Yes 

Failover order 

MOVE UP **MOVE DOWN**

Active uplinks

 uplink2

Standby uplinks

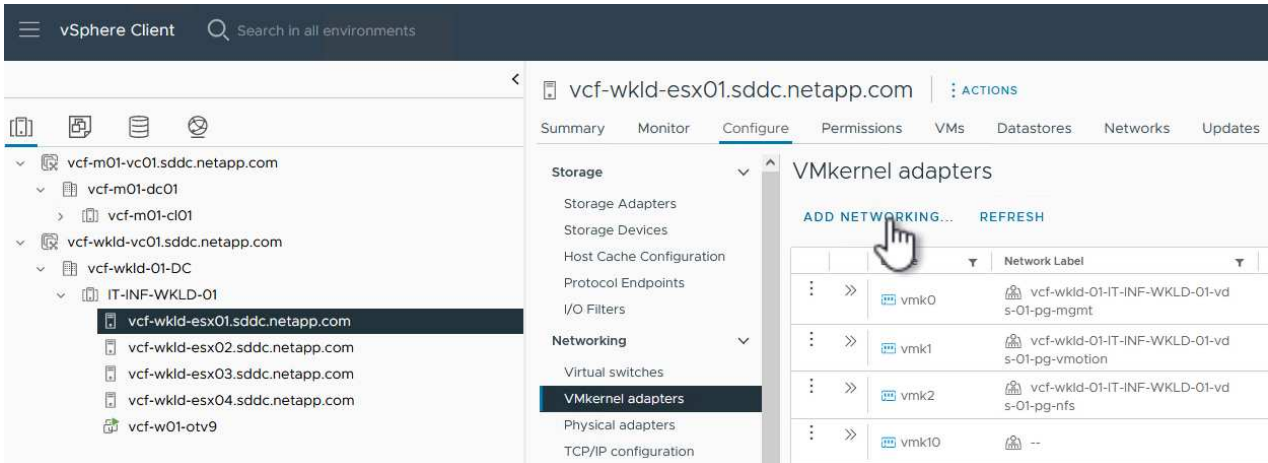
Unused uplinks

 uplink1

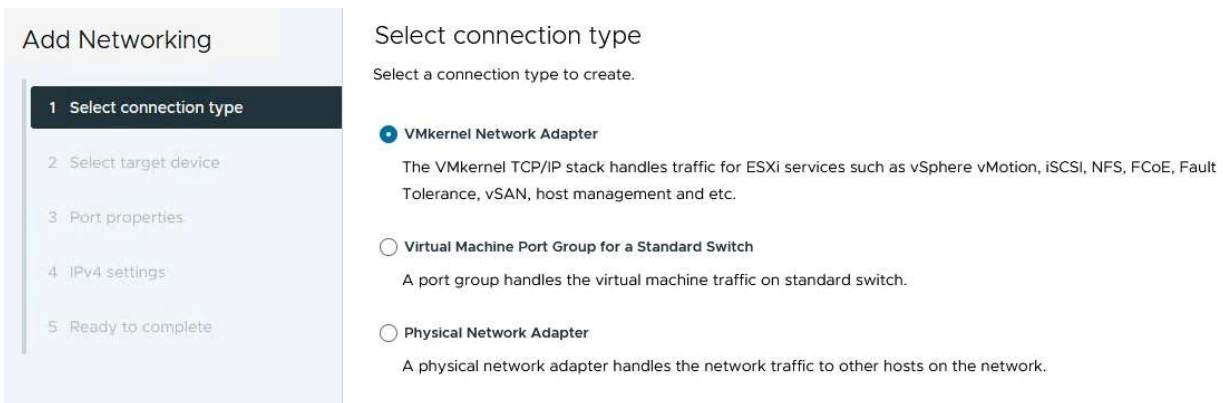
Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

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



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



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

Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

Select target device

Select a target device for the new connection.

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

Quick Filter

Enter value

	Name	NSX Port Group ID	Distributed Switch
<input type="radio"/>	vcf-wkld-01-iscsi-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-iscsi-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-mgmt	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-nfs	--	vcf-wkld-01-IT-INF-WKLD-01-vds-02
<input type="radio"/>	vcf-wkld-01-IT-INF-WKLD-01-vds-01-pg-vmotion	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input checked="" type="radio"/>	vcf-wkld-01-nvme-a	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
<input type="radio"/>	vcf-wkld-01-nvme-b	--	vcf-wkld-01-IT-INF-WKLD-01-vds-01
Manage Columns 7 items			

CANCEL

BACK

NEXT

4. Klicken Sie auf der Seite **Port Properties** auf das Feld für **NVMe over TCP** und klicken Sie auf **Next**, um fortzufahren.

Add Networking

- Select connection type
- Select target device
- Port properties**
- IPv4 settings
- Ready to complete

Port properties

Specify VMkernel port settings.

Network label:

MTU:

TCP/IP stack:

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 BACK NEXT

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings**
- Ready to complete

IPv4 settings

Specify VMkernel IPv4 settings.

☐ Obtain IPv4 settings automatically

☒ Use static IPv4 settings

IPv4 address:

Subnet mask:

Default gateway: ☐ Override default gateway for this adapter

DNS server addresses:

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

Add Networking

- Select connection type
- Select target device
- Port properties
- IPv4 settings
- Ready to complete

Ready to complete

Review your selections before finishing the wizard

▼ Select target device

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

▼ Port properties

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

▼ IPv4 settings

IPv4 address 172.21.118.191 (static)
Subnet mask 255.255.255.0

CANCEL

BACK

FINISH

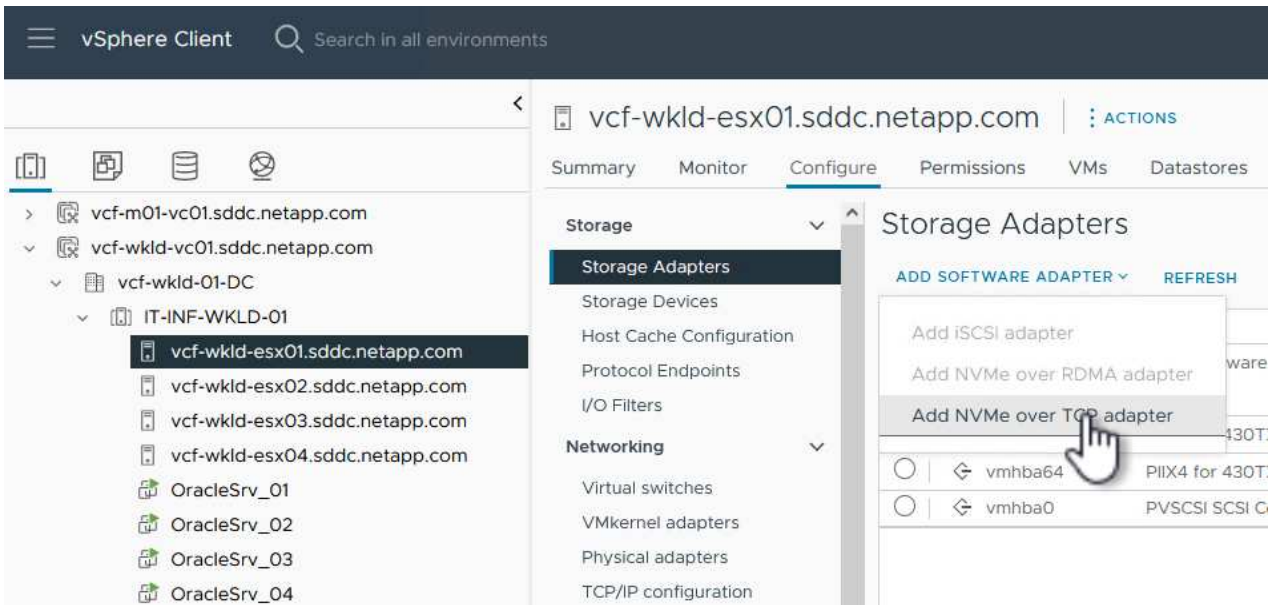
7. Wiederholen Sie diesen Vorgang, um einen VMkernel Adapter für das zweite iSCSI-Netzwerk zu erstellen.

Fügen Sie einen NVMe-over-TCP-Adapter hinzu

Für jedes etablierte NVMe/TCP-Netzwerk, das für Storage-Datenverkehr reserviert ist, muss auf jedem ESXi Host im Workload-Domänencluster ein NVMe-over-TCP-Softwareadapter installiert sein.

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

1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Klicken Sie auf der Registerkarte **Configure** im Menü auf **Speicheradapter** und wählen Sie dann aus dem Dropdown-Menü **Add Software Adapter Add NVMe over TCP Adapter**.



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

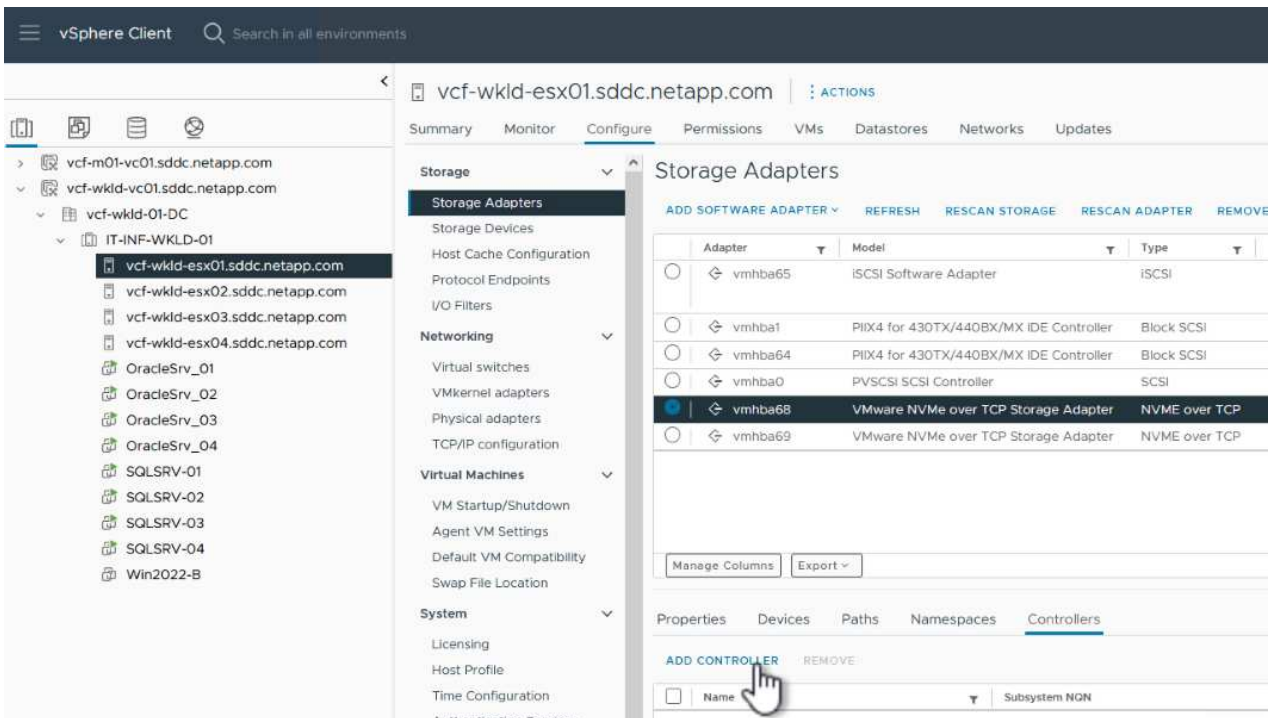
Add Software NVMe over TCP adapter | vcf-wkld-esx01.sddc.netapp.com

Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter



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



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

Add controller | vmhba68



Automatically

Manually

Host NQN

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

COPY

IP

1

172.21.118.189

Enter IPv4 / IPv6 address

☐ Central discovery controller

Port Number

Range more from 0

Digest parameter

☐ Header digest

☐ Data digest

DISCOVER CONTROLLERS

2

Select which controller to connect

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

Manage Columns

4 items

3

4

OK

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

Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

	Adapter ▾	Model ▾	Type ▾	Status ▾	Identifier ▾	Targets ▾	Devices ▾	Paths ▾
<input type="radio"/>	vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.net app.com:794177624:65)	4	2	8
<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

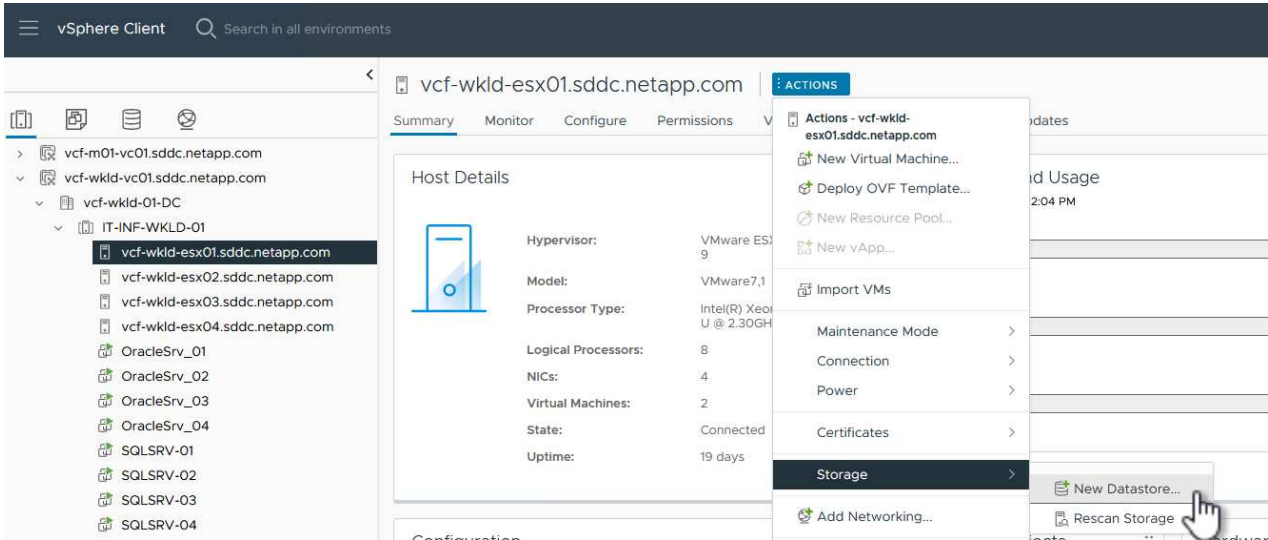
<input type="checkbox"/>	Name ▾	LUN ▾	Type ▾	Capacity ▾	Datastore ▾	Operational State ▾	Hardware Acceleration ▾	Drive Type ▾	Transport
<input type="checkbox"/>	NVMe TCP Disk (uuid.929a6a9045764784 9146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTTRAN: RT

7. Wiederholen Sie dieses Verfahren, um einen NVMe over TCP-Adapter für das zweite Netzwerk zu erstellen, das für NVMe/TCP-Datenverkehr eingerichtet wurde.

NVMe over TCP Datastore implementieren

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

1. Navigieren Sie im vSphere-Client zu einem der ESXi-Hosts im Workload-Domänencluster. Wählen Sie im Menü **actions Storage > New Datastore...**



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

New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

Name and device selection



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

Name 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

4. Wählen Sie auf der Seite **VMFS Version** die Version von VMFS für den Datastore aus.
5. Nehmen Sie auf der Seite **Partition Configuration** die gewünschten Änderungen am Standard-Partitionsschema vor. Klicken Sie auf **Weiter**, um fortzufahren.

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 **Ready to Complete** die Zusammenfassung und klicken Sie auf **Finish**, um den Datastore zu erstellen.
- Navigieren Sie zum neuen Datastore im Bestand und klicken Sie auf die Registerkarte **Hosts**. Bei korrekter Konfiguration sollten alle ESXi-Hosts im Cluster aufgeführt sein und Zugriff auf den neuen Datastore haben.

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
	vcf-wkld-esx01.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-01	15%	13%	✓ Connected (Secondary)	19 days
	vcf-wkld-esx02.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-01	9%	15%	✓ Running (Primary)	19 days
	vcf-wkld-esx03.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-01	9%	21%	✓ Connected (Secondary)	19 days
	vcf-wkld-esx04.sddc.netapp.co	Connected	✓ Normal	IT-INF-WKLD-01	11%	4%	✓ Connected (Secondary)	19 days

Weitere Informationen

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

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

Schützen Sie VMs in VCF-Workload-Domänen mit dem SnapCenter Plug-in für VMware vSphere

Autor: Josh Powell

Schützen Sie VMs in VCF-Workload-Domänen mit dem SnapCenter Plug-in für VMware vSphere

Szenarioübersicht

In diesem Szenario wird gezeigt, wie das SnapCenter Plug-in für VMware vSphere (SCV) implementiert und verwendet wird, um VMs und Datastores in einer VCF Workload-Domäne zu sichern und wiederherzustellen. SCV verwendet die ONTAP Snapshot-Technologie, um schnelle und effiziente Backup-Kopien der ONTAP-Speicher-Volumes zu erstellen, die vSphere-Datastores hosten. SnapMirror und SnapVault Technologie werden verwendet, um sekundäre Backups auf einem separaten Storage-System und mit Aufbewahrungsrichtlinien zu erstellen, die das Original-Volume imitieren oder zur langfristigen Aufbewahrung vom Original-Volume unabhängig sein können.

ISCSI wird als Speicherprotokoll für den VMFS-Datastore in dieser Lösung verwendet.

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Stellen Sie das SnapCenter Plug-in für VMware vSphere (SCV) in der VI-Workload-Domäne bereit.
- Fügen Sie dem SCV Speichersysteme hinzu.
- Erstellen Sie Backup-Richtlinien in SCV.
- Ressourcengruppen in SCV erstellen.
- Verwenden Sie SCV, um Datastores oder bestimmte VMs zu sichern.
- Verwenden Sie SCV, um VMs an einem anderen Speicherort im Cluster wiederherzustellen.
- Verwenden Sie SCV, um Dateien in einem Windows-Dateisystem wiederherzustellen.

Voraussetzungen

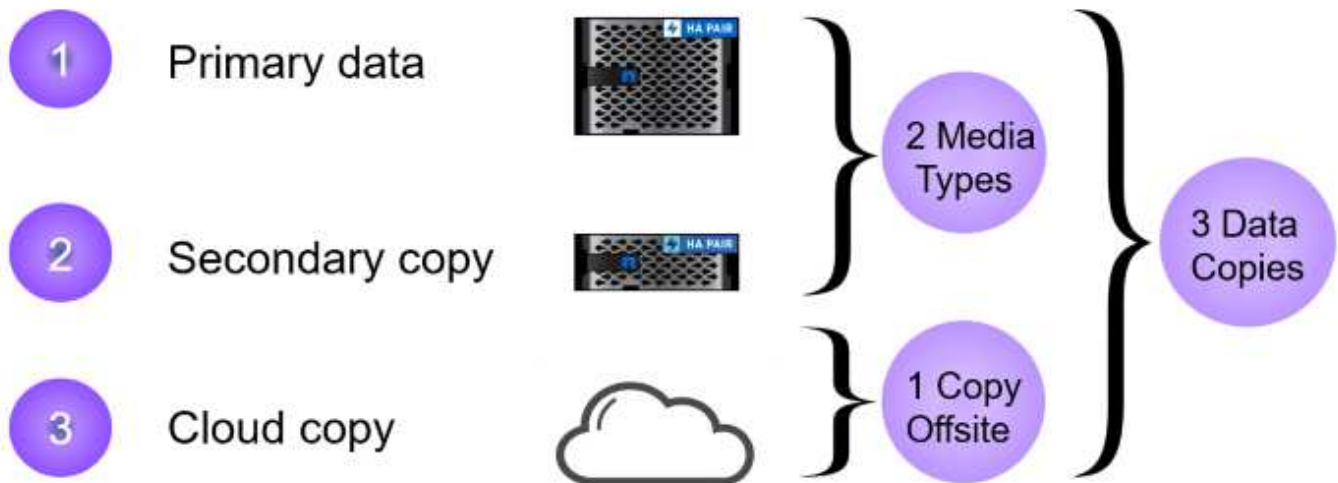
Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- Ein ONTAP ASA-Speichersystem mit iSCSI-VMFS-Datenspeichern, die dem Workload-Domänencluster zugewiesen sind.
- Ein sekundäres ONTAP Storage-System, das für empfangene sekundäre Backups mit SnapMirror konfiguriert ist.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und der vSphere-Client ist verfügbar.
- Eine VI-Workload-Domäne wurde bereits bereitgestellt.
- Virtuelle Maschinen sind auf dem Cluster vorhanden SCV ist zum Schutz vorgesehen.

Informationen zum Konfigurieren von iSCSI-VMFS-Datastores als zusätzlichen Speicher finden Sie unter ["ISCSI als zusätzlicher Speicher für Management Domains"](#) Genutzt werden. Die Verwendung von OTV zur Implementierung von Datastores ist in Management- und Workload-Domänen identisch.



Zusätzlich zur Replizierung von Backups, die mit SCV auf sekundärem Storage erstellt werden, können externe Datenkopien auf Objekt-Storage auf einem der drei (3) führenden Cloud-Provider erstellt werden, der NetApp BlueXP Backup und Recovery für VMs nutzt. Weitere Informationen finden Sie in der Lösung ["3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs"](#).



Implementierungsschritte

Gehen Sie wie folgt vor, um das SnapCenter-Plug-in zu implementieren und zum Erstellen von Backups sowie zum Wiederherstellen von VMs und Datastores zu verwenden:

Stellen Sie SCV bereit und verwenden Sie diese, um Daten in einer VI-Workload-Domäne zu sichern

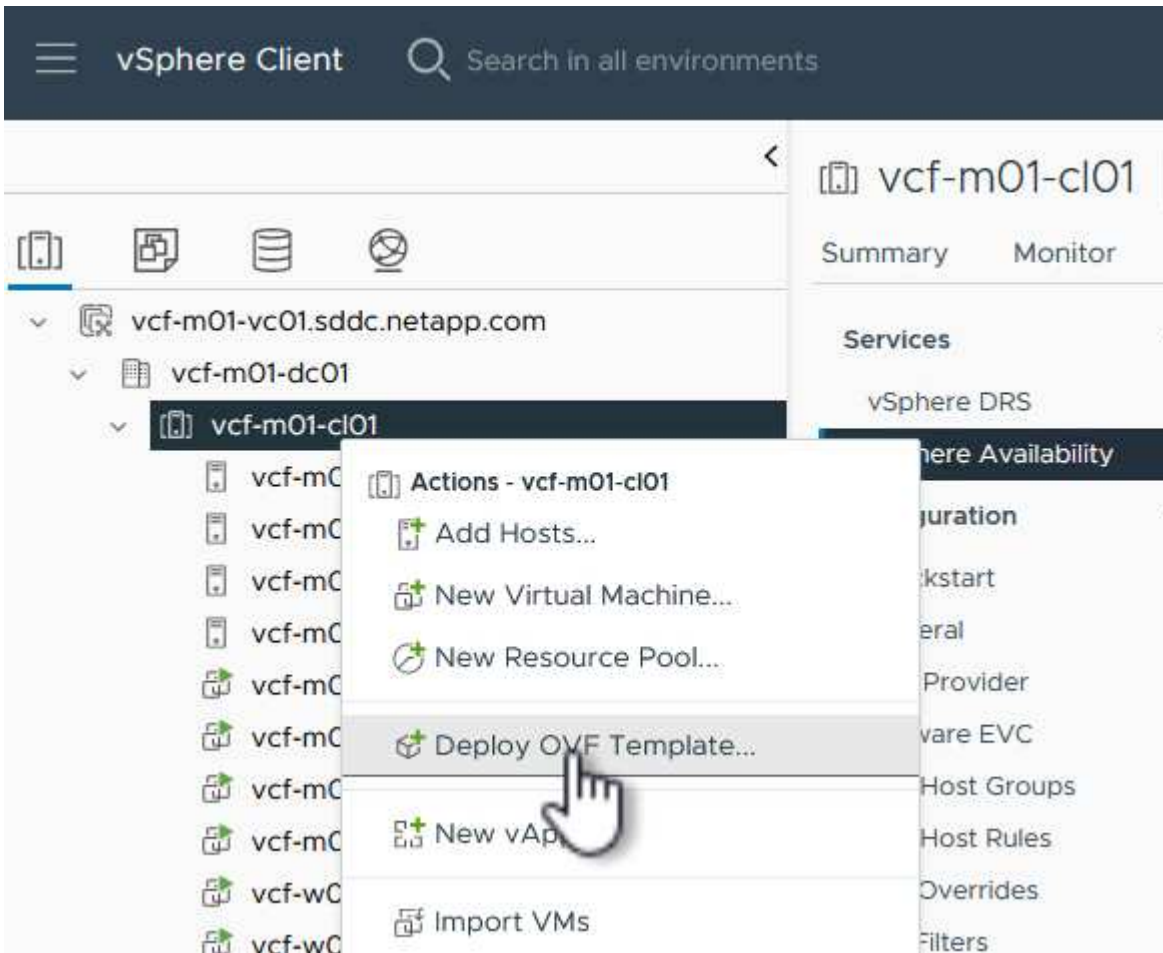
Führen Sie die folgenden Schritte durch, um SCV bereitzustellen, zu konfigurieren und zum Schutz von Daten in einer VI-Workload-Domäne zu verwenden:

Implementieren Sie das SnapCenter Plug-in für VMware vSphere

Das SnapCenter-Plug-in wird in der VCF-Managementdomäne gehostet, aber für die VI-Workload-Domäne in vCenter registriert. Eine SCV-Instanz ist für jede vCenter-Instanz erforderlich. Beachten Sie, dass eine Workload-Domäne mehrere Cluster umfassen kann, die von einer einzelnen vCenter-Instanz gemanagt werden.

Führen Sie die folgenden Schritte vom vCenter-Client aus, um SCV für die VI-Workload-Domäne bereitzustellen:

1. Laden Sie die OVA-Datei für die SCV-Bereitstellung im Downloadbereich der NetApp Support-Website herunter "[HIER](#)".
2. Wählen Sie in der Management Domain vCenter Client **Deploy OVF Template...** aus.



3. Klicken Sie im Assistenten **Deploy OVF Template** auf das Optionsfeld **Lokale Datei** und wählen Sie dann aus, um die zuvor heruntergeladene OVF-Vorlage hochzuladen. Klicken Sie auf **Weiter**, um fortzufahren.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

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

☐ URL

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

☒ Local file

UPLOAD FILES

scv-5.0P2-240310_1514.ova

- Geben Sie auf der Seite **Select Name and folder** einen Namen für die SCV Data Broker VM und einen Ordner auf der Management Domain an. Klicken Sie auf **Weiter**, um fortzufahren.
- Wählen Sie auf der Seite **Select a Compute Resource** den Management Domain Cluster oder einen bestimmten ESXi Host innerhalb des Clusters aus, auf dem die VM installiert werden soll.
- Lesen 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 **Select Storage** den Datenspeicher aus, auf den die VM installiert werden soll, und wählen Sie das **virtuelle Laufwerksformat** und **VM-Speicherrichtlinie** aus. In dieser Lösung wird die VM auf einem iSCSI-VMFS-Datenspeicher auf einem ONTAP-Speichersystem installiert, wie zuvor in einem separaten Abschnitt dieser Dokumentation bereitgestellt. Klicken Sie auf **Weiter**, um fortzufahren.

Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

Select storage

Select the storage for the configuration and disk files

☐ Encrypt this virtual machine ⓘ

Select virtual disk format

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

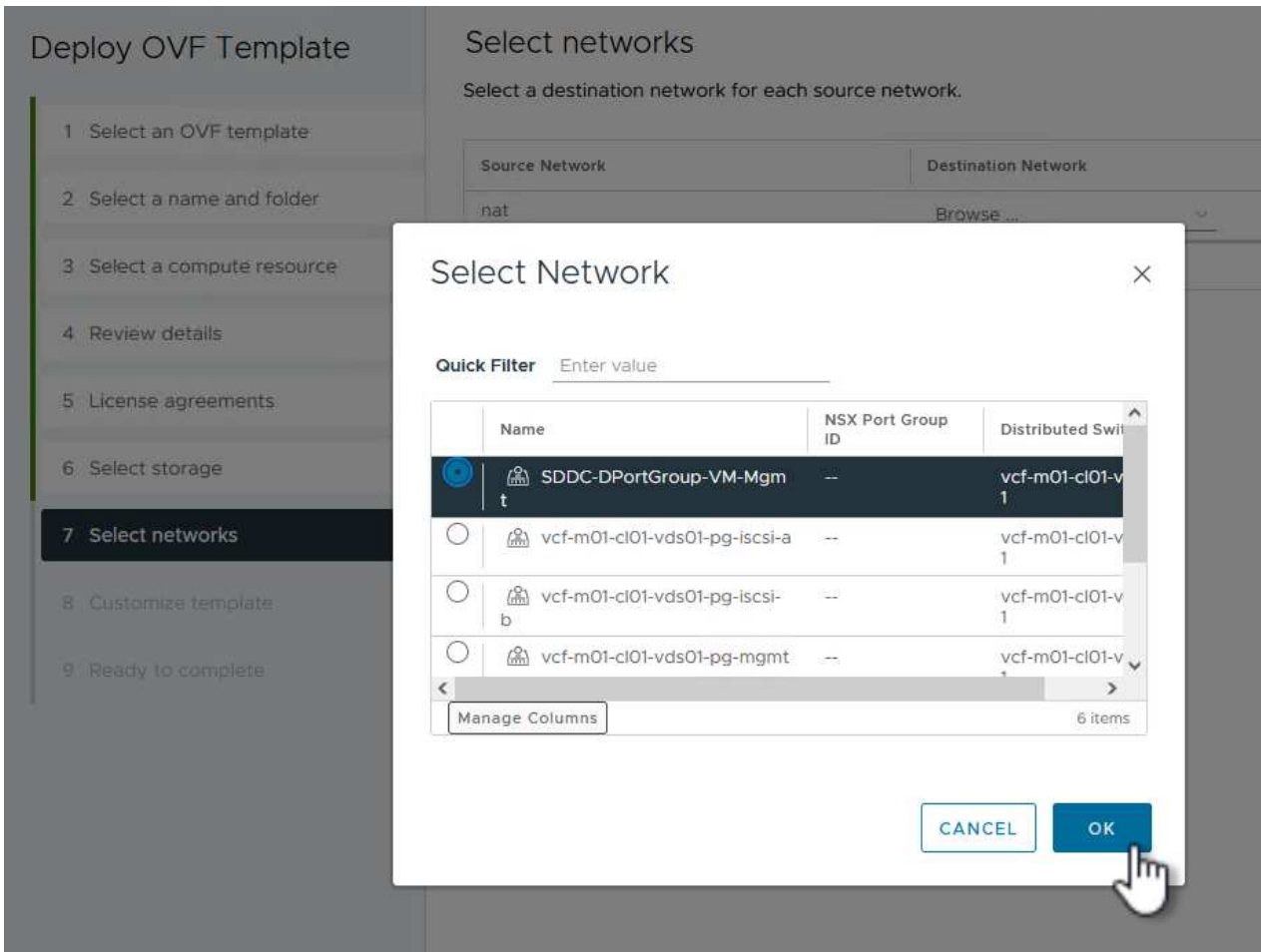
✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

8. Wählen Sie auf der Seite **Select Network** das Managementnetzwerk aus, das mit der Workload Domain vCenter Appliance und den primären und sekundären ONTAP Speichersystemen kommunizieren kann.



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

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

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

Deploy OVF Template

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

Customize template

Customize the deployment properties of this software solution.

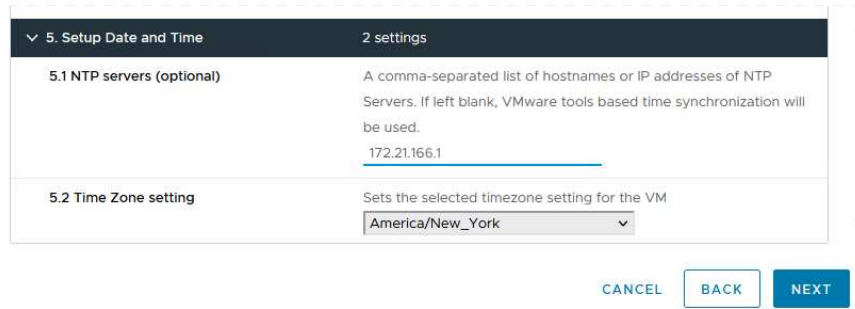
1. Register to existing vCenter		4 settings
1.1 vCenter Name(FQDN) or IP Address	cf-wkld-vc01.sddc.netapp.com	
1.2 vCenter username	administrator@vcf.local	
1.3 vCenter password	Password
	Confirm Password
1.4 vCenter port	443	
2. Create SCV Credentials		2 settings
2.1 Username	admin	
2.2 Password	Password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

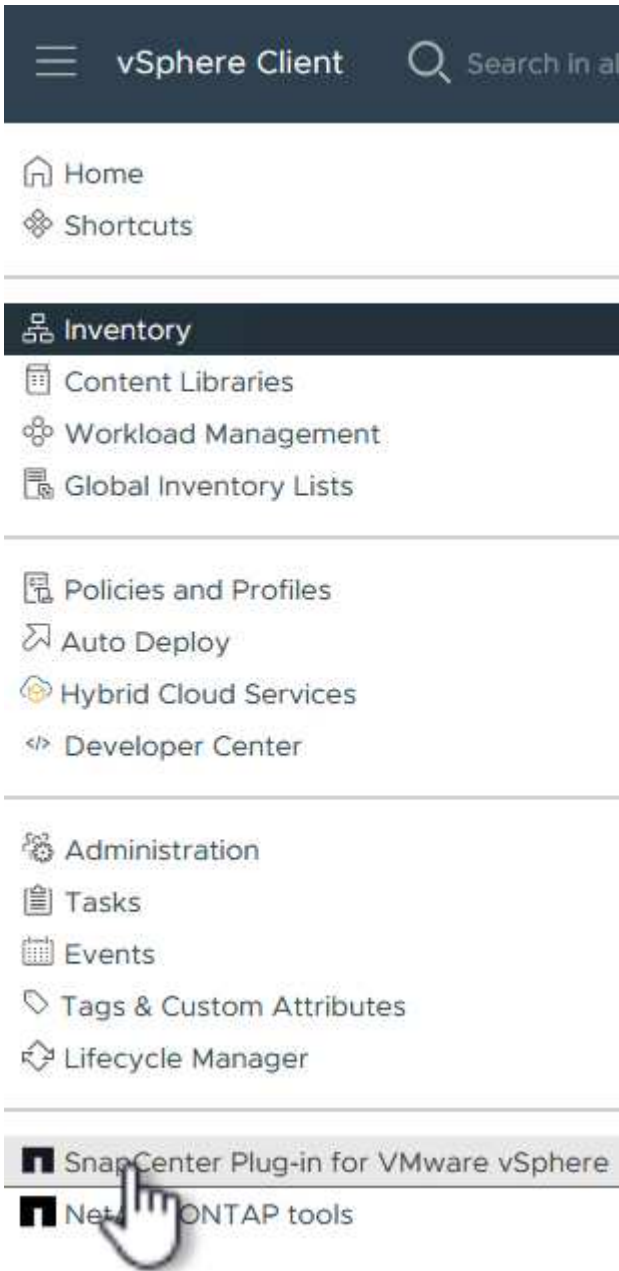
CANCEL BACK NEXT

10. Überprüfen Sie abschließend auf der Seite **bereit zur Fertigstellung** alle Einstellungen und klicken Sie auf Fertig stellen, um die Bereitstellung zu starten.

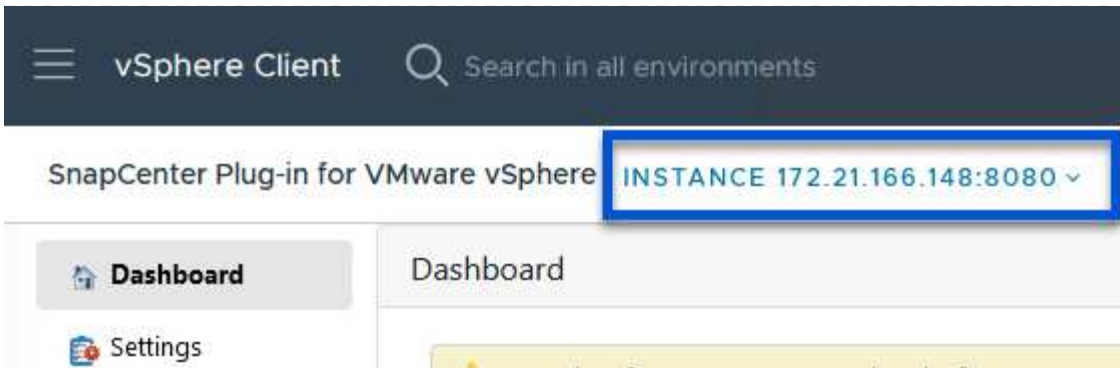
Fügen Sie dem SCV Speichersysteme hinzu

Führen Sie nach der Installation des SnapCenter-Plug-ins die folgenden Schritte aus, um dem SCV Speichersysteme hinzuzufügen:

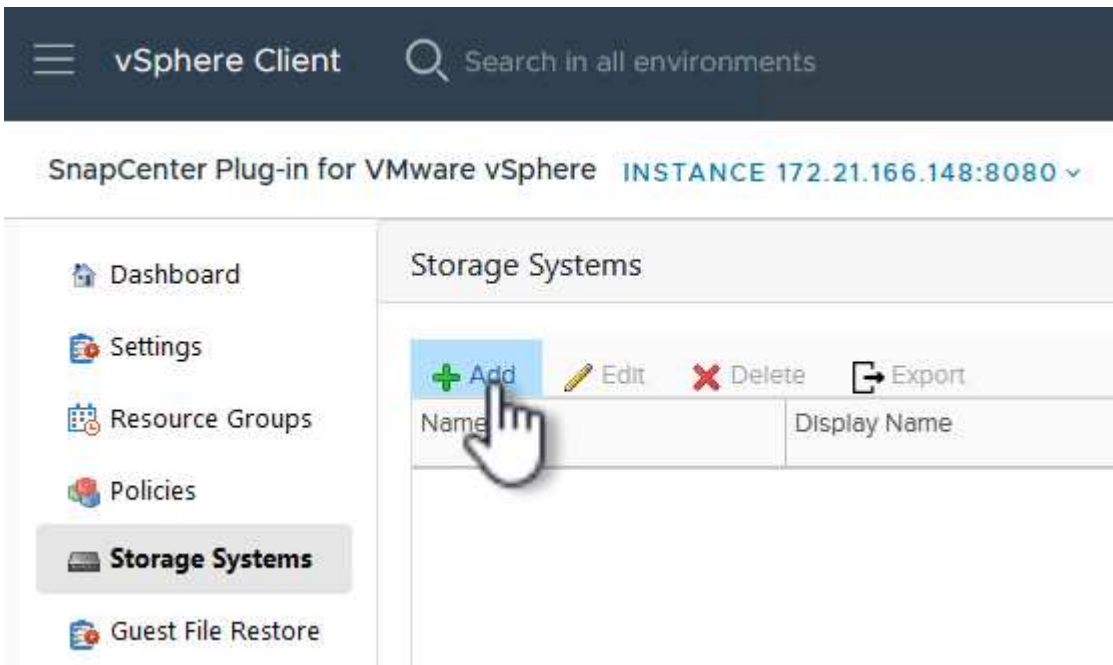
1. Auf SCV kann über das Hauptmenü im vSphere Client zugegriffen werden.



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



3. Navigieren Sie im linken Menü zu **Storage Systems** und klicken Sie auf **Add**, um zu beginnen.



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

Add Storage System



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

Event Management System(EMS) & AutoSupport Setting

☐ Log Snapcenter server events to syslog

☐ Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



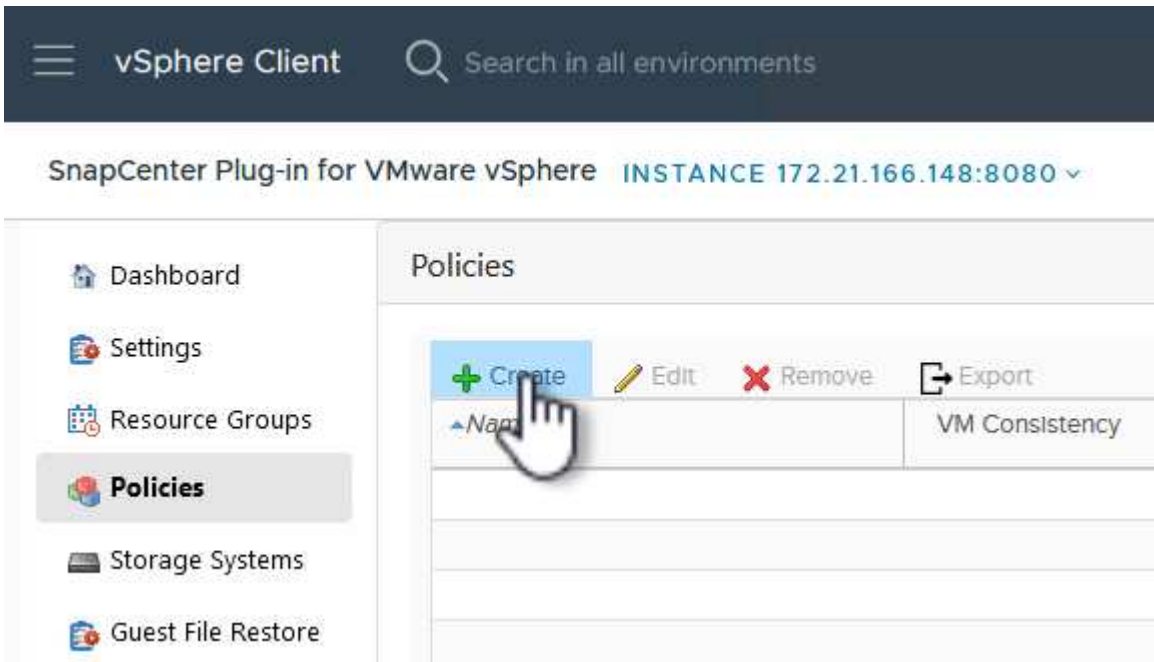
5. Wiederholen Sie diesen Vorgang für alle zusätzlichen zu verwaltenden Speichersysteme, einschließlich aller Systeme, die als sekundäre Backup-Ziele verwendet werden sollen.

Konfigurieren Sie Backup-Richtlinien in SCV

Weitere Informationen zum Erstellen von SCV-Backup-Richtlinien finden Sie unter "[Erstellen von Backup-Richtlinien für VMs und Datastores](#)".

Führen Sie die folgenden Schritte durch, um eine neue Backup-Richtlinie zu erstellen:

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



2. Geben Sie im Formular **New Backup Policy** einen **Namen** und eine **Beschreibung** für die Policy, die **Häufigkeit**, bei der die Backups durchgeführt werden, und die **Aufbewahrungsfrist** an, die angibt, wie lange das Backup aufbewahrt wird.

Sperrfrist aktiviert die ONTAP SnapLock-Funktion, um manipulationssichere Schnappschüsse zu erstellen und ermöglicht die Konfiguration der Sperrfrist.

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



SnapMirror und SnapVault Replizierung ähneln darin, dass sie beide zur asynchronen Replizierung von Storage Volumes auf ein sekundäres Storage-System ONTAP SnapMirror Technologie einsetzen. Dies steigert den Schutz und die Sicherheit. Bei SnapMirror Beziehungen regelt der in der SCV-Backup-Richtlinie angegebene Aufbewahrungszeitplan die Aufbewahrung sowohl für das primäre als auch für das sekundäre Volume. Bei SnapVault Beziehungen kann auf dem sekundären Storage-System für längere Zeiträume oder unterschiedliche Zeitpläne für die Aufbewahrung ein separater Aufbewahrungsplan erstellt werden. In diesem Fall wird das Snapshot-Label in der SCV-Backup-Policy und in der Policy im Zusammenhang mit dem sekundären Volume angegeben, um zu ermitteln, auf welche Volumes der unabhängige Aufbewahrungsplan angewendet werden soll.

Wählen Sie zusätzliche erweiterte Optionen und klicken Sie auf **Hinzufügen**, um die Richtlinie zu

erstellen.

New Backup Policy



Name

Daily_Snapmirror

Description

description

Frequency

Daily

Locking Period

☐ Enable Snapshot Locking

Retention

Days to keep

15

Replication

☒ Update SnapMirror after backup

☐ Update SnapVault after backup

Snapshot label

Advanced

☐ VM consistency

☐ Include datastores with independent disks

Scripts

Enter script path

CANCEL

ADD



Erstellen Sie Ressourcengruppen in SCV

Weitere Informationen zum Erstellen von SCV-Ressourcengruppen finden Sie unter ["Erstellen von Ressourcengruppen"](#).

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

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



2. Geben Sie auf der Seite **General info & notification** einen Namen für die Ressourcengruppe, Benachrichtigungseinstellungen und alle zusätzlichen Optionen für die Benennung der Snapshots ein.
3. Wählen Sie auf der Seite **Resource** die Datastores und VMs aus, die in der Ressourcengruppe geschützt werden sollen. Klicken Sie auf **Weiter**, um fortzufahren.



Auch wenn nur bestimmte VMs ausgewählt sind, wird der gesamte Datastore immer gesichert. Das liegt daran, dass ONTAP Snapshots des Volumes erstellt, das den Datastore hostet. Beachten Sie jedoch, dass die Auswahl von nur bestimmten VMs für Backups die Möglichkeit zur Wiederherstellung auf nur diese VMs beschränkt.

Create Resource Group

✓ 1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF_WKLD_03_iSCSI

Enter available entity name

Available entities

OracleSrv_01
OracleSrv_02
OracleSrv_03
OracleSrv_04

Selected entities

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

BACK

NEXT

FINISH

CANCEL

4. Wählen Sie auf der Seite **Spanning Disks** die Option für den Umgang mit VMs mit VMDK's, die mehrere Datastores umfassen. Klicken Sie auf **Weiter**, um fortzufahren.

Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

☐ Always exclude all spanning datastores

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

☒ Always include all spanning datastores

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

☐ Manually select the spanning datastores to be included ⓘ

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

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

BACK

NEXT

FINISH

CANCEL

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

Create Resource Group

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

[+ Create](#)

[illegible]

BACK NEXT FINISH CANCEL

6. Stellen Sie auf der Seite **Zeitpläne** fest, wann die Sicherung ausgeführt wird, indem Sie die Wiederholung und 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 stellen**, um die Ressourcengruppe zu erstellen.

Create Resource Group

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

Name	SQL_Servers						
Description							
Send email	Never						
Latest Snapshot name	None ⓘ						
Custom snapshot format	None ⓘ						
Entities	SQLSRV-01, SQLSRV-02, SQLSRV-03, SQLSRV-04						
Spanning	False						
Policies	<table><thead><tr><th>Name</th><th>Frequency</th><th>Snapshot Locking Period</th></tr></thead><tbody><tr><td>Daily_Snapmir...</td><td>Daily</td><td>-</td></tr></tbody></table>	Name	Frequency	Snapshot Locking Period	Daily_Snapmir...	Daily	-
Name	Frequency	Snapshot Locking Period					
Daily_Snapmir...	Daily	-					

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

8. Klicken Sie bei der erstellten Ressourcengruppe auf die Schaltfläche **Jetzt ausführen**, um das erste Backup auszuführen.

☰ vSphere Client

🔍 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

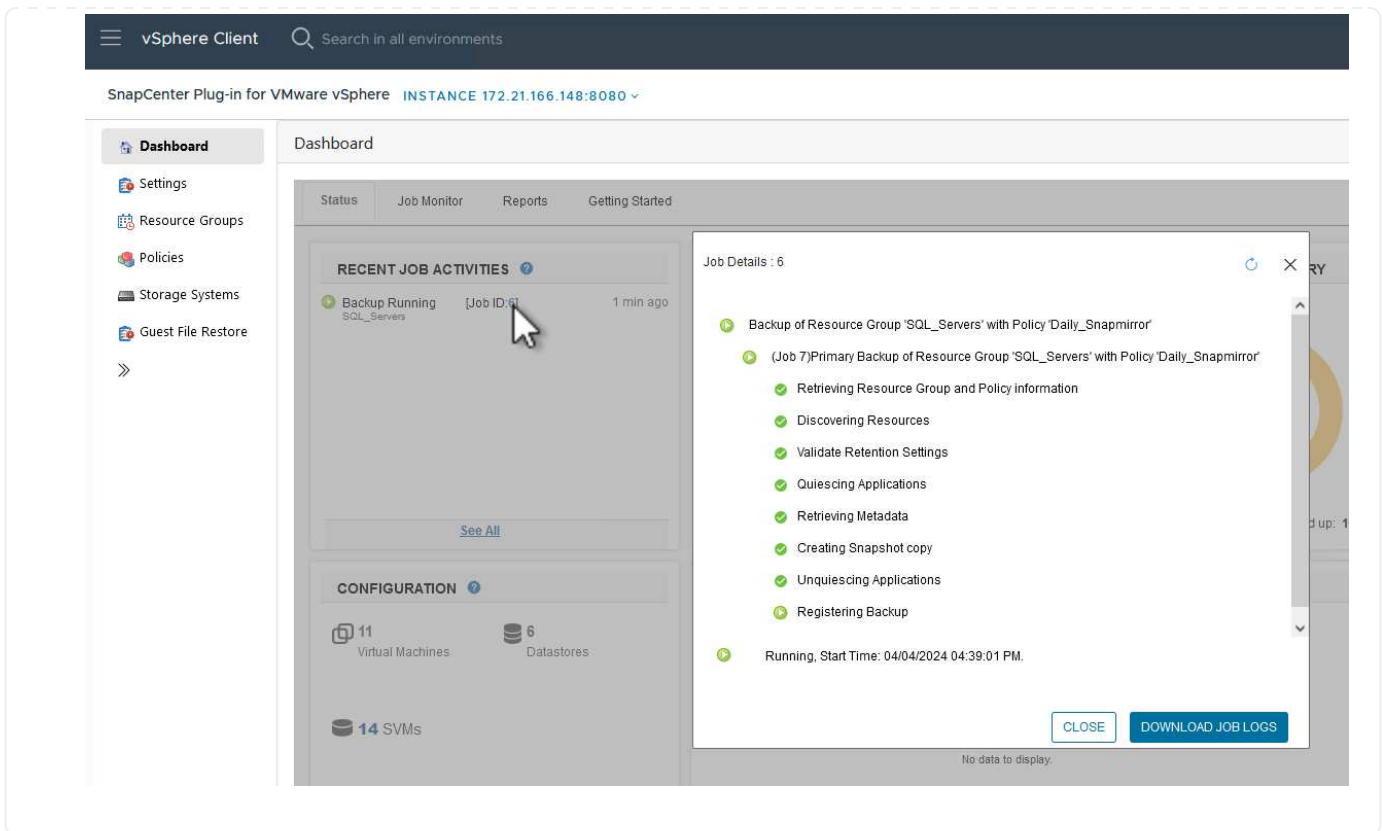
⏸ Suspend

▶ Resume

📄 Export

Name	Description	Policy
SQL_Servers		Daily_

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



Stellen Sie VMs, VMDKs und Dateien mit SCV wieder her

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

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

VVol VMs können auf dem ursprünglichen Host wiederhergestellt werden.

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

VMDKs in vVol VMs können im ursprünglichen Datenspeicher wiederhergestellt werden.

Einzelne Dateien und Ordner in einer Gastdatei-Wiederherstellungssitzung können wiederhergestellt werden, wodurch eine Sicherungskopie einer virtuellen Festplatte angehängt und die ausgewählten Dateien oder Ordner wiederhergestellt werden.

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

Stellen Sie VMs mit dem SnapCenter Plug-in wieder her

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

1. Navigieren Sie zu der VM, die im vSphere-Client wiederhergestellt werden soll, klicken Sie mit der rechten Maustaste, und navigieren Sie zu **SnapCenter-Plug-in für VMware vSphere**. Wählen Sie im Untermenü * Restore* aus.

OracleSrv_04

Summary Monitor Configure Permissions

Guest OS Virtual Mac

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

TE CONSOLE

CONSOLE

4 CPU(s), 22 MHz used

32 GB, 0 GB memory active

100 GB | Thin Provision

VCF_WKLD_03_ISCSI

(of 2) vcf-wkld-01-IT-INF-WKLD-01-vc (connected) | 00:50:56:83:02:f

Disconnected

ESXi 7.0 U2 and later (VM vers

Recent Tasks

Task Name

Create Resource Group

Add to Resource Group

Attach Virtual Disk(s)

Detach Virtual Disk(s)

Restore

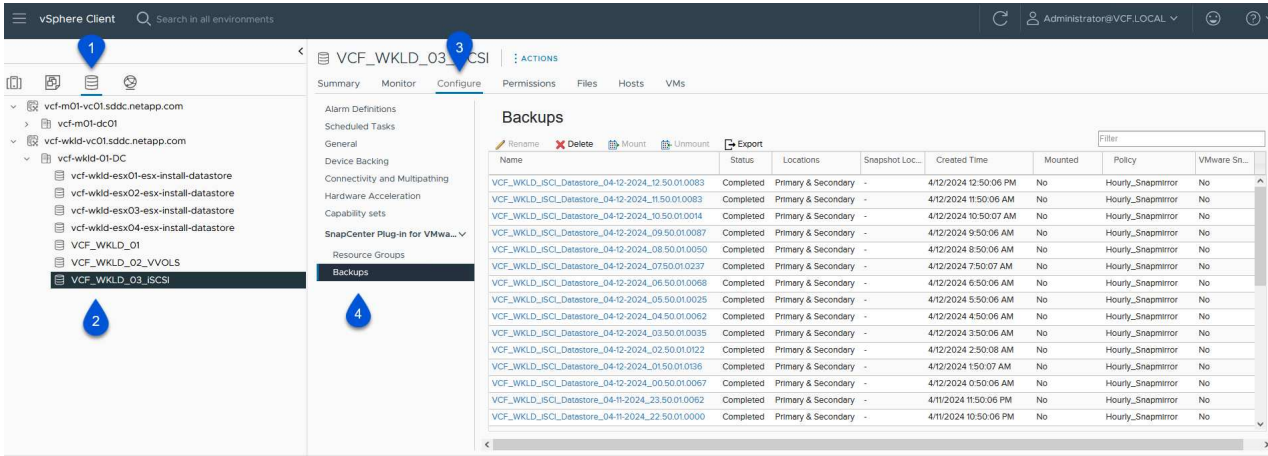
File Restore

Manage Columns

Run



Alternativ können Sie zum Datastore im Bestand navigieren und dann unter der Registerkarte **Configure** zu **SnapCenter Plug-in für VMware vSphere > Backups** wechseln. Wählen Sie aus dem ausgewählten Backup die VMs aus, die wiederhergestellt werden sollen.



2. Wählen Sie im **Restore**-Assistenten das zu verwendende Backup aus. Klicken Sie auf **Weiter**, um fortzufahren.

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:

- **Umfang wiederherstellen** - Wählen Sie, um die gesamte virtuelle Maschine wiederherzustellen.
- **Neustart VM** - Wählen Sie, ob die VM nach der Wiederherstellung gestartet werden soll.
- **Speicherort wiederherstellen** - Wählen Sie die Wiederherstellung an der ursprünglichen Position oder an einem anderen Ort. Wählen Sie bei der Auswahl eines alternativen Speicherorts die Optionen aus den einzelnen Feldern aus:

- **Ziel vCenter Server** - Lokales vCenter oder alternatives vCenter im verknüpften Modus
- **Ziel-ESXi-Host**
- **Netzwerk**
- **VM-Name nach Wiederherstellung**
- **Datastore auswählen:**

Restore

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

Restore scope: Entire virtual machine

Restart VM: ☐

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

Destination vCenter Server: 172.21.166.143

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

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

VM name after restore: OracleSrv_04_restored

Select Datastore: VCF_WKLD_03_ISCSI

BACK NEXT FINISH CANCEL

VCF_WKLD_03_ISCSI

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

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

Restore

✓ 1. Select backup

✓ 2. Select scope

3. Select location

4. Summary

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

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

Restore

✓ 1. Select backup

✓ 2. Select scope

✓ 3. Select location

4. Summary

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



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

BACK

NEXT

FINISH

CANCEL

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

Dashboard

Settings

Resource Groups

Policies

Storage Systems

Guest File Restore

>>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago
VCF_WKLD_ISCI_Datastore_04-04-20...
- 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 Alarms

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

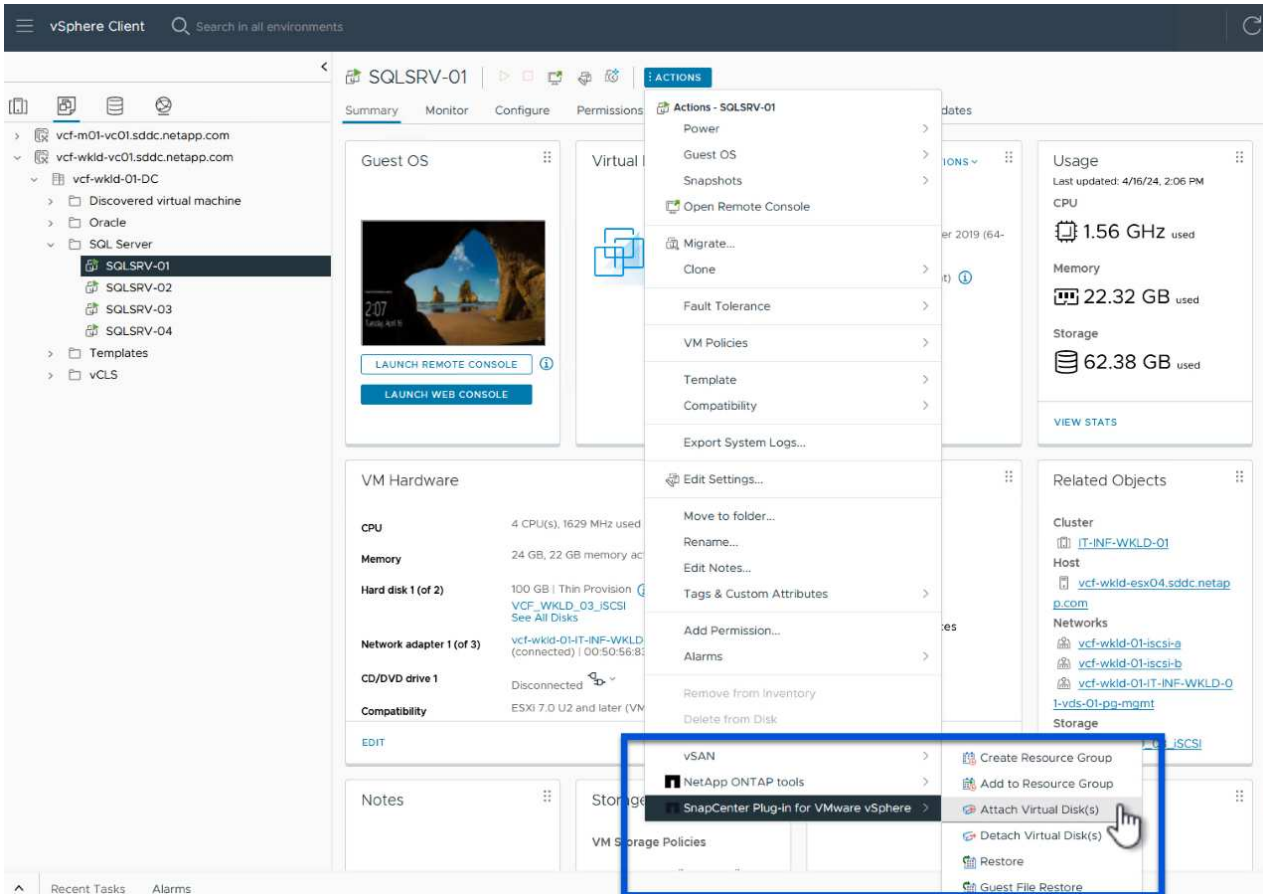
[More Tasks](#)

Stellen Sie VMDKs mit dem SnapCenter Plug-in wieder her

Mit den ONTAP-Tools können VMDK-Dateien am ursprünglichen Speicherort vollständig wiederhergestellt werden, oder es kann eine VMDK als neue Festplatte an ein Host-System angeschlossen werden. In diesem Szenario wird eine VMDK an einen Windows Host angeschlossen, um auf das Dateisystem zuzugreifen.

Gehen Sie wie folgt vor, um eine VMDK aus einem Backup anzubinden:

1. Navigieren Sie im vSphere-Client zu einer VM und wählen Sie im Menü **actions SnapCenter Plug-in für VMware vSphere > Virtuelle Festplatte(n) anhängen** aus.



2. Wählen Sie im **Attach Virtual Disk(s)** Wizard die zu verwendende Backup-Instanz und die anzuhängende VMDK aus.

Attach Virtual Disk(s)



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

Backup

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



Filteroptionen können verwendet werden, um Backups zu suchen und Backups von primären und sekundären Speichersystemen anzuzeigen.

Attach Virtual Disk(s)



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

Backup

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

☐ Virtual disk

☐ [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01.vmdk

☒ [VCF_WKLD_03_ISCSI] SQLSRV-01/SQLSRV-01_1.vmdk

Time range

From

12

Hour

00

Minute

00

Second

AM

To

12

Hour

00

Minute

00

Second

AM

VMware snapshot

Mounted

Location

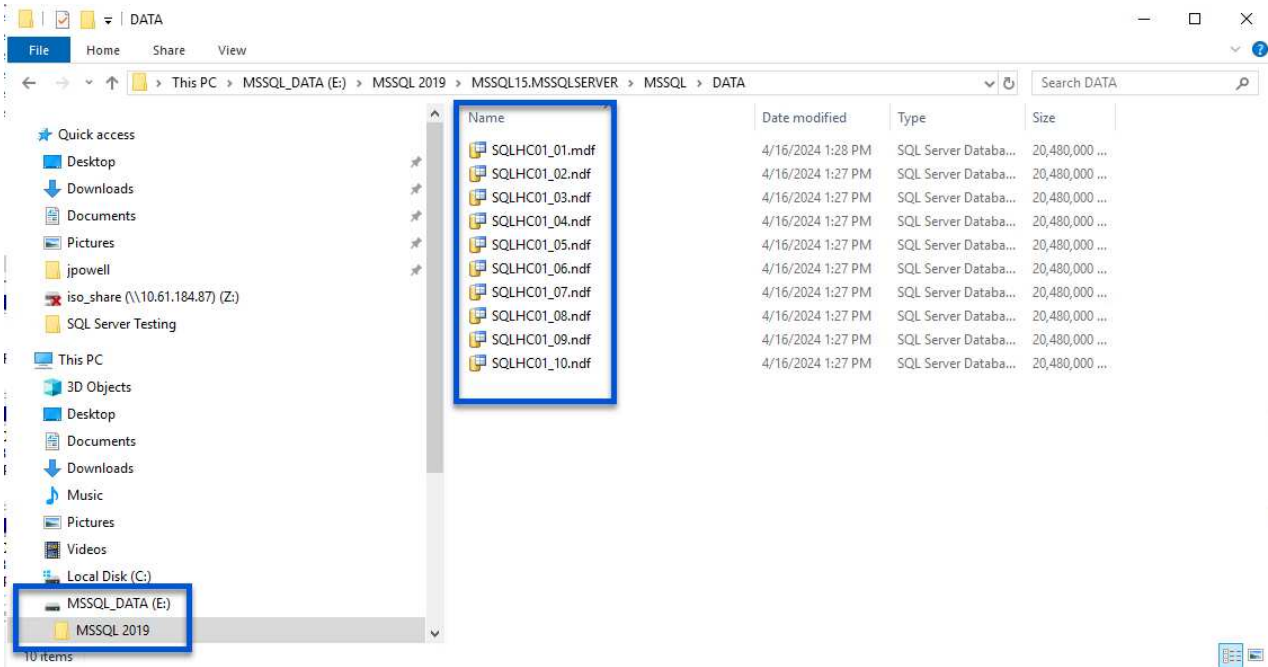
CLEAR

OK

CANCEL

ATTACH

3. Nachdem Sie alle Optionen ausgewählt haben, klicken Sie auf die Schaltfläche **Anhängen**, um den Wiederherstellungsvorgang zu starten und die VMDK an den Host anzuhängen.
4. Nach Abschluss des Anschlussvorgangs kann über das Betriebssystem des Hostsystems auf die Festplatte zugegriffen werden. In diesem Fall hat SCV die Festplatte mit ihrem NTFS-Dateisystem an das Laufwerk E: Unseres Windows SQL Servers angeschlossen und die SQL-Datenbankdateien auf dem Dateisystem sind über den Datei-Explorer zugänglich.



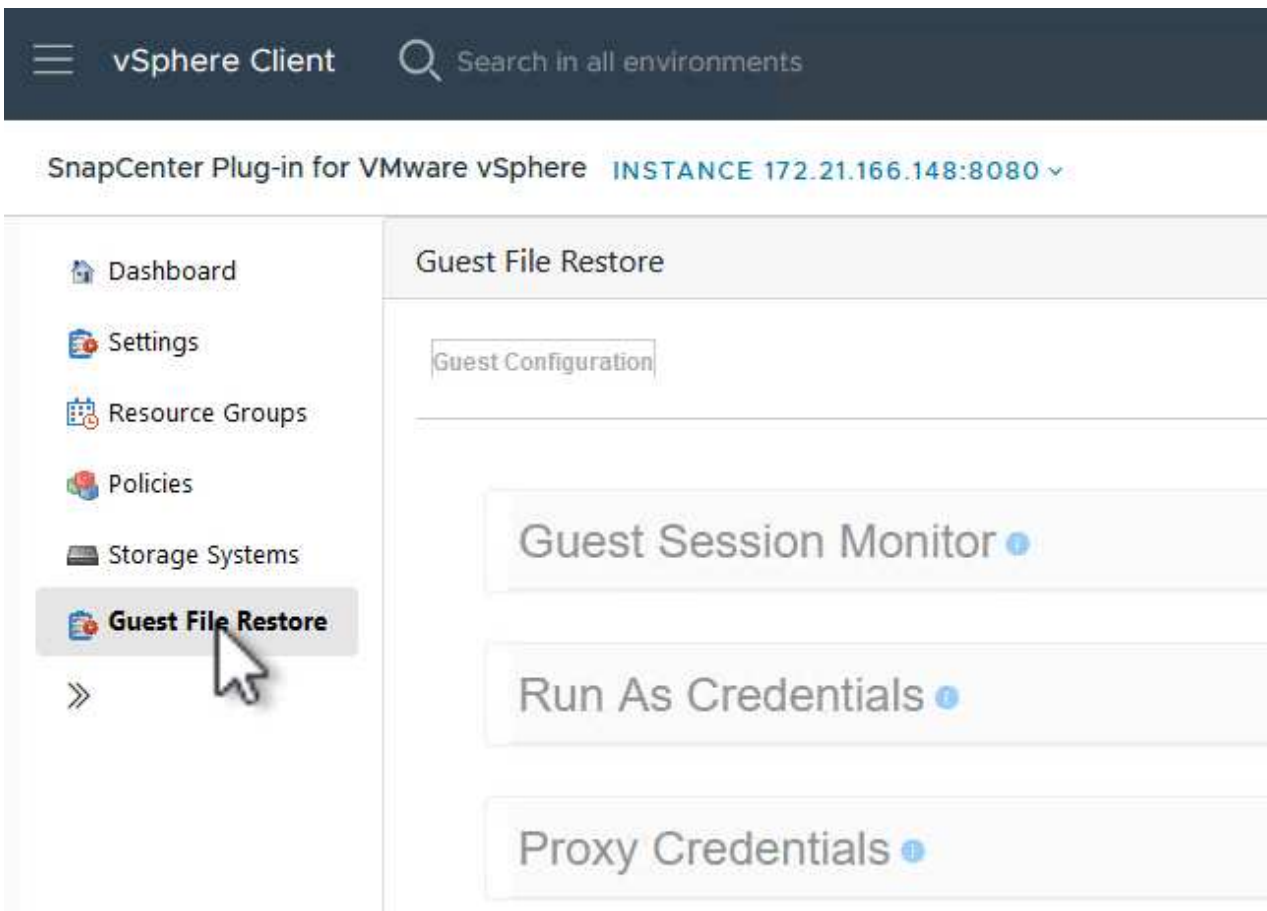
Wiederherstellung des Gastdateisystems mit dem SnapCenter Plug-in

ONTAP Tools bietet Gast-Dateisystem-Wiederherstellung von einer VMDK auf Windows Server Betriebssystemen. Diese wird zentral über die SnapCenter-Plug-in-Schnittstelle vorgeformt.

Ausführliche Informationen finden Sie unter "[Wiederherstellung von Gastdateien und Ordnern](#)" An der SCV-Dokumentationsstelle.

Führen Sie die folgenden Schritte durch, um eine Wiederherstellung des Gastdateisystems für ein Windows-System durchzuführen:


1. Der erste Schritt besteht darin, Run As Credentials zu erstellen, um Zugriff auf das Windows-Hostsystem zu ermöglichen. Navigieren Sie im vSphere Client zur CSV-Plug-in-Oberfläche und klicken Sie im Hauptmenü auf **Guest File Restore**.




2. Klicken Sie unter **Run As Credentials** auf das **+**-Symbol, um das Fenster **Run As Credentials** zu öffnen.
3. Geben Sie einen Namen für den Datensatz mit den Anmeldeinformationen, einen Administratorbenutzernamen und ein Kennwort für das Windows-System ein, und klicken Sie dann auf die Schaltfläche **Select VM**, um eine optionale Proxy-VM auszuwählen, die für die Wiederherstellung verwendet werden soll.

Run As Credentials



Run As Name 

Username 

Password 

Authentication Mode

VM Name

Select VM



CANCEL

SAVE

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

Proxy VM ✕

VM Name

SQLSRV-01

☒ Search by ESXi Host

ESXi Host

vcf-wkld-esx04.sddc.netapp.com

Virtual Machine

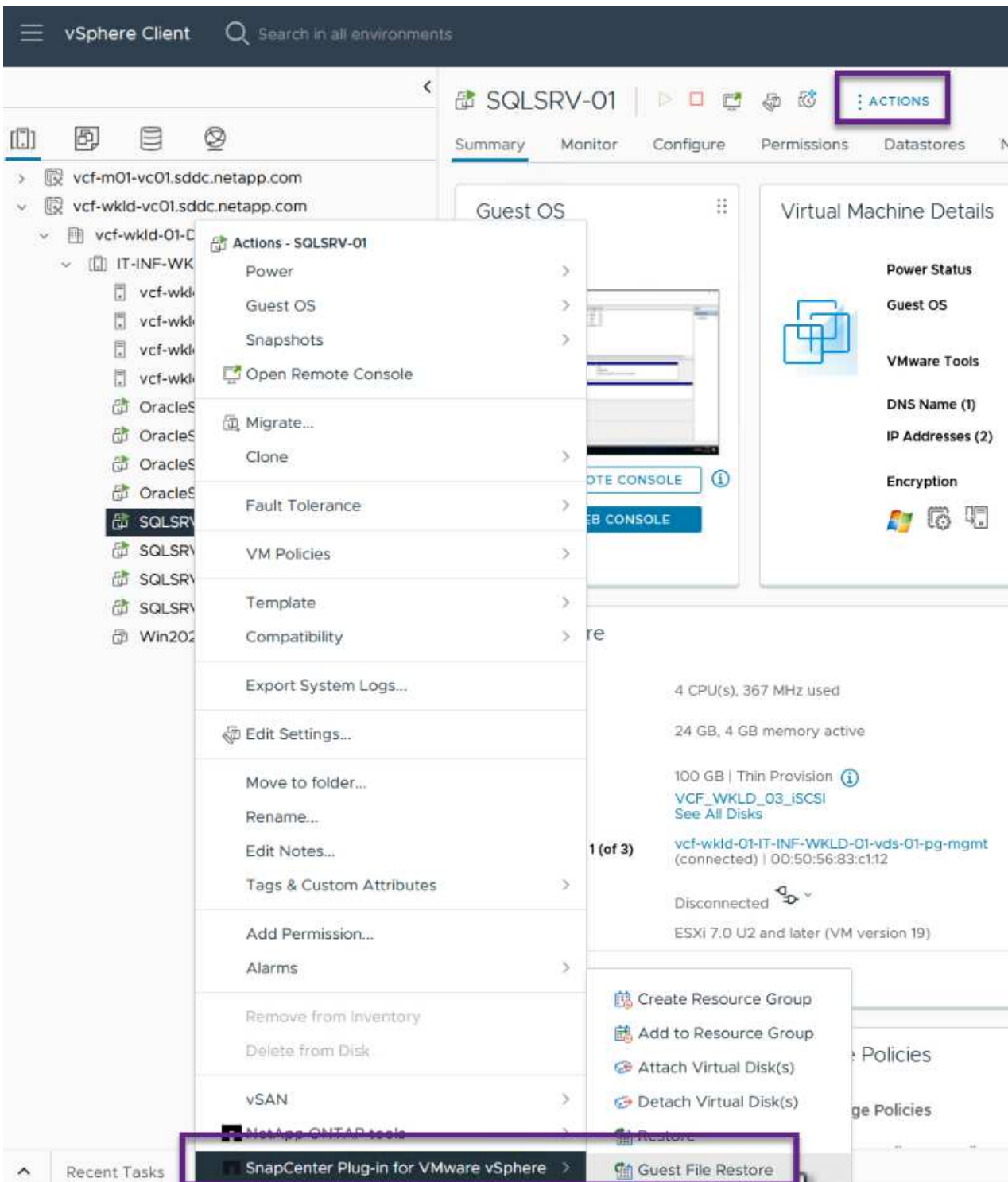
SQLSRV-01

☐ Search by Virtual Machine name

CANCEL

SAVE

5. Klicken Sie im Fenster **Run As Credentials** erneut auf **Save**, um das Speichern des Datensatzes abzuschließen.
6. Navigieren Sie anschließend zu einer VM im Bestand. Wählen Sie im Menü **actions** oder durch Rechtsklick auf die VM **SnapCenter Plug-in für VMware vSphere > Gastdateiwiederherstellung** aus.



- Wählen Sie auf der Seite **Restore Scope** des **Guest File Restore**-Assistenten das wiederherzustellende Backup, die jeweilige VMDK und den Speicherort (primär oder sekundär) aus, um die VMDK wiederherzustellen. Klicken Sie auf **Weiter**, um fortzufahren.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

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

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

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

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

8. Wählen Sie auf der Seite **Guest Details** die Option **Guest VM** oder **Use Gues File Restore Proxy VM** für die Wiederherstellung aus. Füllen Sie auf Wunsch auch hier die Einstellungen für die E-Mail-Benachrichtigung aus. Klicken Sie auf **Weiter**, um fortzufahren.

Guest File Restore



1. Restore Scope

2. Guest Details

3. Summary

Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

Use Guest File Restore proxy VM

Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

- Überprüfen Sie abschließend die Seite **Zusammenfassung** und klicken Sie auf **Fertig stellen**, um die Sitzung zur Systemwiederherstellung der Gastdatei zu starten.
- Navigieren Sie wieder in der SnapCenter-Plug-in-Oberfläche zu **Gastdateiwiederherstellung** und zeigen Sie die laufende Sitzung unter **Gastsitzungsmonitor** an. Klicken Sie auf das Symbol unter **Dateien durchsuchen**, um fortzufahren.

The screenshot shows the vSphere Client interface with the SnapCenter Plug-in for VMware vSphere. The left sidebar contains navigation links: Dashboard, Settings, Resource Groups, Policies, Storage Systems, and Guest File Restore. The main content area displays the 'Guest File Restore' configuration page, which includes a 'Guest Configuration' section and a 'Guest Session Monitor' table. The table has columns for Backup Name, Source VM, Disk Path, Guest Mount Path, Time To Expire, and Browse Files. A hand icon is shown clicking on the 'Browse Files' column header. Below the table, there are sections for 'Run As Credentials' and 'Proxy Credentials'.

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	

- Wählen Sie im **Guest File Browse**-Assistenten den Ordner oder die Dateien, die wiederhergestellt werden sollen, und den Dateisystemspeicherort, in dem sie wiederhergestellt werden sollen. Klicken Sie abschließend auf **Wiederherstellen**, um den Vorgang **Wiederherstellen** zu starten.

Guest File Browse



Select File(s)/Folder(s) to Restore



E:\MSSQL 2019



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 Wiederherstellungsauftrag kann über den Aufgabenbereich von vSphere Client überwacht werden.

Weitere Informationen

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

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

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

VMware Cloud Foundation mit NetApp AFF-Arrays

Autor: Josh Powell, Ravi BCB

VMware Cloud Foundation mit NetApp AFF-Arrays

VMware Cloud Foundation (VCF) ist eine integrierte softwaredefinierte Datacenter-Plattform (SDDC), die einen vollständigen Stack von softwaredefinierter Infrastruktur für die Ausführung von Enterprise-Applikationen in einer Hybrid-Cloud-Umgebung bereitstellt. Sie kombiniert Computing-, Storage-, Netzwerk- und Managementfunktionen in einer einheitlichen Plattform und ermöglicht so ein konsistentes Betriebserlebnis in

Private und Public Clouds.

Dieses Dokument enthält Informationen zu Storage-Optionen, die für VMware Cloud Foundation mithilfe des NetApp All-Flash AFF Storage-Systems zur Verfügung stehen. Unterstützte Storage-Optionen werden durch spezifische Anweisungen zum Erstellen von Workload-Domänen mit NFS- und vVol-Datastores als Haupt-Storage sowie eine Reihe zusätzlicher Storage-Optionen abgedeckt.

Anwendungsfälle

Anwendungsfälle in dieser Dokumentation:

- Storage-Optionen für Kunden, die einheitliche Umgebungen sowohl in privaten als auch in öffentlichen Clouds benötigen.
- Automatisierte Lösung zur Bereitstellung einer virtuellen Infrastruktur für Workload-Domänen.
- Skalierbare Storage-Lösung, die auf neue Anforderungen zugeschnitten ist, auch wenn sie nicht direkt auf die Anforderungen von Computing-Ressourcen ausgerichtet ist
- Stellen Sie VCF VI Workload Domains unter Verwendung von ONTAP als Hauptspeicher bereit.
- Stellen Sie mit ONTAP Tools für VMware vSphere zusätzlichen Speicher für VI-Workload-Domänen bereit.

Zielgruppe

Diese Lösung ist für folgende Personen gedacht:

- Lösungsarchitekten, die flexiblere Storage-Optionen für VMware Umgebungen benötigen und ihre TCO maximieren möchten.
- Lösungsarchitekten, die auf der Suche nach VCF Storage-Optionen sind, die Datensicherungs- und Disaster Recovery-Optionen bei den großen Cloud-Providern bieten.
- Storage-Administratoren, die mehr über die Konfiguration von VCF mit Haupt- und zusätzlichem Storage erfahren möchten.

Technologischer Überblick

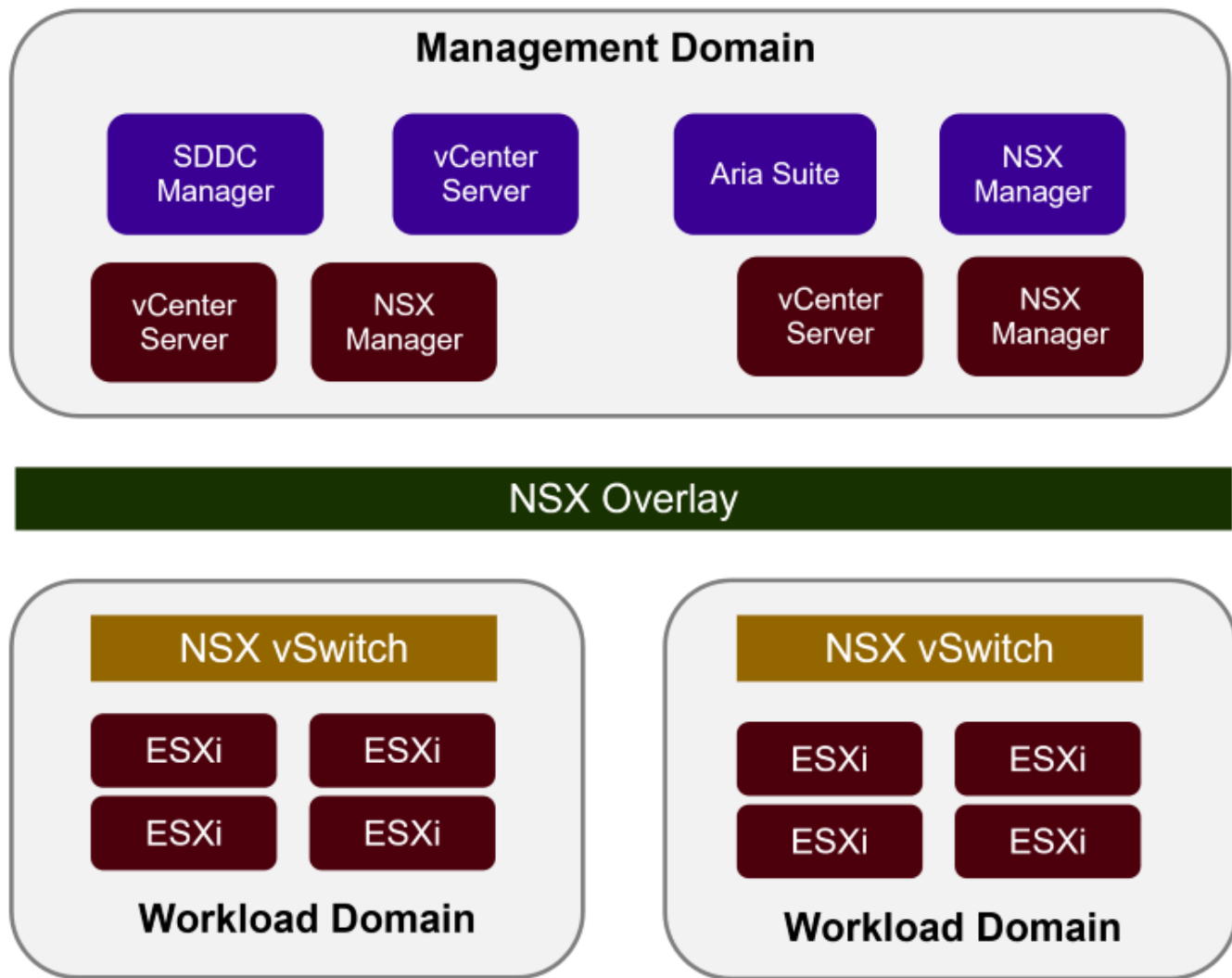
Die VCF mit NetApp AFF-Lösung besteht aus den folgenden Hauptkomponenten:

VMware Cloud Foundation

VMware Cloud Foundation erweitert die vSphere Hypervisor-Angebote von VMware durch die Kombination wichtiger Komponenten wie SDDC Manager, vSphere, vSAN, NSX und VMware Aria Suite, um ein virtualisiertes Datacenter zu erstellen.

Die VCF Lösung unterstützt sowohl native Kubernetes-Workloads als auch Workloads, die auf Virtual Machines basieren. Wichtige Services wie VMware vSphere, VMware vSAN, VMware NSX-T Data Center und VMware vRealize Cloud Management sind integrale Bestandteile des VCF Pakets. Zusammen bilden diese Services eine softwaredefinierte Infrastruktur, die ein effizientes Management von Computing, Storage, Netzwerken, Sicherheit und Cloud-Management ermöglicht.

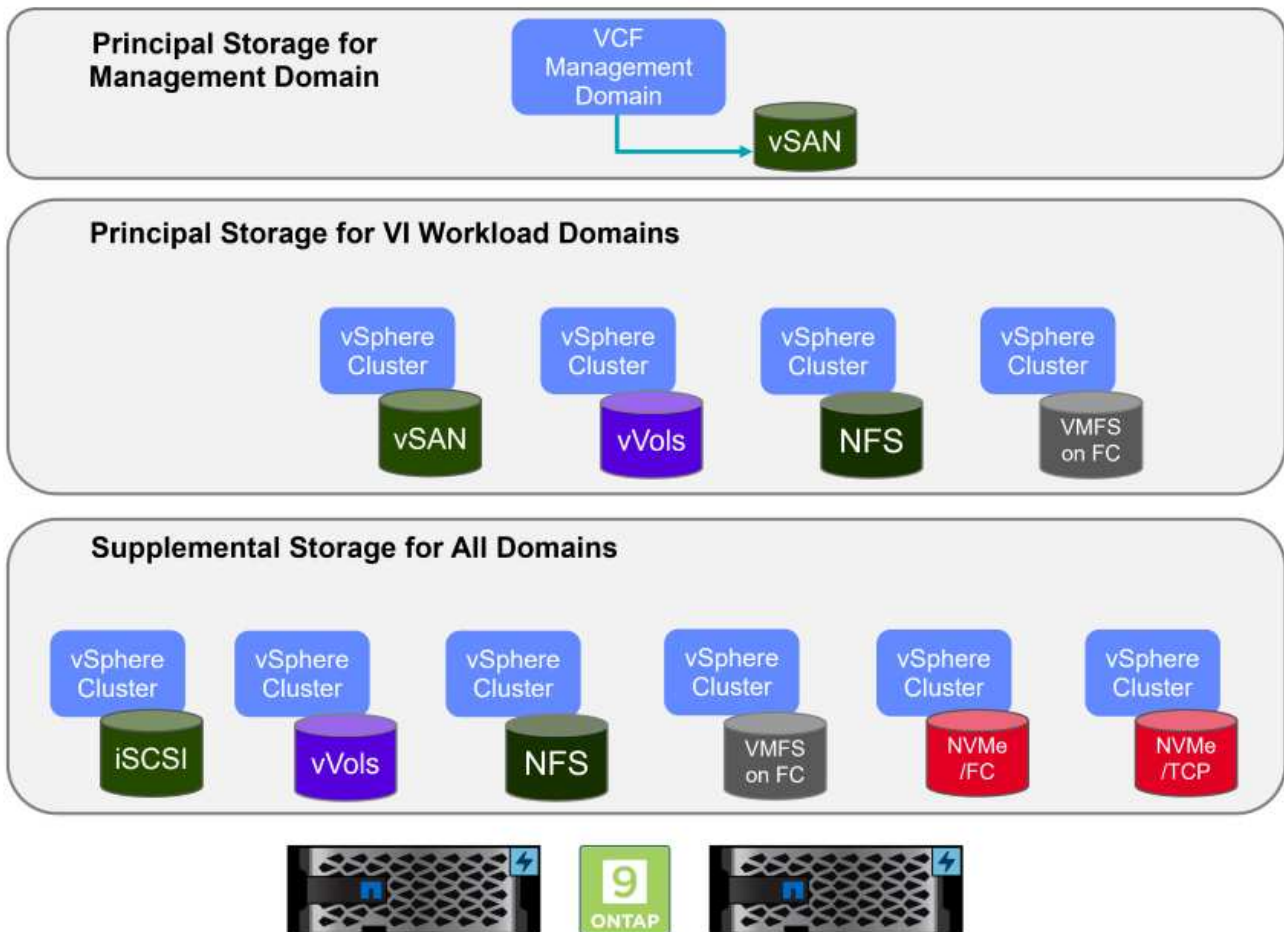
VCF besteht aus einer einzelnen Management-Domäne und bis zu 24 VI-Workload-Domänen, die jeweils eine Einheit für applikationsfähige Infrastrukturen darstellen. Eine Workload-Domäne besteht aus einem oder mehreren vSphere Clustern, die von einer einzelnen vCenter Instanz gemanagt werden.



Weitere Informationen zur Architektur und Planung von VCF finden Sie unter "[Architekturmodelle und Workload-Domänen-Typen in VMware Cloud Foundation](#)".

VCF Storage-Optionen

VMware unterteilt Speicheroptionen für VCF in **Principal** und **Supplemental** Speicher. Die VCF Management Domain muss vSAN als Hauptspeicher verwenden. Es gibt jedoch zahlreiche zusätzliche Speicheroptionen für die Verwaltungsdomäne und sowohl Haupt- als auch ergänzende Speicheroptionen für VI-Workload-Domänen.



Hauptspeicher für Workload-Domänen

Principal Storage bezieht sich auf jeden Speichertyp, der während des Setups innerhalb des SDDC Manager direkt mit einer VI Workload Domain verbunden werden kann. Principal Storage ist der erste für eine Workload Domain konfigurierte Datastore und umfasst vSAN, vVols (VMFS), NFS und VMFS auf Fibre Channel.

Ergänzender Speicher für Management- und Workload-Domänen

Zusätzlicher Storage ist der Storage-Typ, der dem Management oder den Workload-Domänen jederzeit nach der Erstellung des Clusters hinzugefügt werden kann. Zusätzlicher Storage umfasst die größte Auswahl an unterstützten Storage-Optionen, die alle von NetApp AFF Arrays unterstützt werden.

Zusätzliche Dokumentationsressourcen für VMware Cloud Foundation:

- * ["Dokumentation zu VMware Cloud Foundation"](#)
- * ["Unterstützte Storage-Typen für VMware Cloud Foundation"](#)
- * ["Management von Storage in VMware Cloud Foundation"](#)

Rein Flash-basierte Storage-Arrays von NetApp

NetApp AFF (All Flash FAS) Arrays sind hochperformante Storage-Lösungen, die die Geschwindigkeit und Effizienz der Flash-Technologie nutzen. AFF Arrays integrieren integrierte Datenmanagement-Funktionen wie Snapshot-basierte Backups, Replizierung, Thin Provisioning und Datensicherungsfunktionen.

NetApp AFF Arrays verwenden das ONTAP Storage-Betriebssystem und bieten umfassende Unterstützung der Storage-Protokolle für alle mit VCF kompatiblen Storage-Optionen innerhalb einer Unified Architecture.

NetApp AFF Storage-Arrays sind in den leistungsstärksten A-Series und QLC Flash-basierten C-Series verfügbar. Beide Serien verwenden NVMe-Flash-Laufwerke.

Weitere Informationen zu NetApp AFF Storage-Arrays der A-Serie finden Sie im ["NetApp AFF A-Series" Landing Page](#) an.

Weitere Informationen zu NetApp Speicherarrays der C-Serie finden Sie im ["NetApp AFF C-Serie" Landing Page](#) an.

NetApp ONTAP Tools für VMware vSphere

Mit den ONTAP Tools für VMware vSphere (OTV) können Administratoren NetApp Storage direkt aus dem vSphere Client heraus managen. Mit den ONTAP Tools können Sie Datastores implementieren und managen und vVol Datastores bereitstellen.

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

ONTAP Tools umfassen zudem einen **VMware vSphere APIs for Storage Awareness (VASA) Provider** für ONTAP Storage-Systeme, der die Bereitstellung von VMware Virtual Volumes (VVols) Datastores, die Erstellung und Verwendung von Storage-Funktionsprofilen, Compliance-Überprüfung und Performance-Monitoring ermöglicht.

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

Lösungsüberblick

In den Szenarien, die in dieser Dokumentation vorgestellt werden, zeigen wir, wie ONTAP-Speichersysteme als Hauptspeicher für VCF VI-Workload-Domänen-Bereitstellungen verwendet werden. Darüber hinaus installieren und verwenden wir ONTAP Tools für VMware vSphere, um zusätzliche Datastores für VI-Workload-Domänen zu konfigurieren.

Szenarien in dieser Dokumentation:

- **Konfigurieren und verwenden Sie einen NFS-Datastore als Hauptspeicher während der VI-Workload-Domain-Bereitstellung.** Klicken Sie auf ["Hier"](#) Für Bereitstellungsschritte.
- **Installieren und demonstrieren Sie die Verwendung von ONTAP-Tools, um NFS-Datastores als zusätzlichen Speicher in VI-Workload-Domänen zu konfigurieren und zu mounten.** Klicken Sie auf ["Hier"](#) Für Bereitstellungsschritte.

NFS als Hauptspeicher für VI-Workload-Domänen

Autor: Josh Powell, Ravi BCB

NFS als Hauptspeicher für VI-Workload-Domänen

Szenarioübersicht

In diesem Szenario zeigen wir, wie ein NFS-Datastore als Hauptspeicher für die Bereitstellung einer VI-Workload-Domain in VCF konfiguriert wird. Sofern zutreffend, beziehen wir uns auf die externe Dokumentation für die Schritte, die im SDDC Manager von VCF durchgeführt werden müssen, und behandeln die Schritte, die spezifisch für den Bereich der Speicherkonfiguration sind.

Dieses Szenario umfasst die folgenden grundlegenden Schritte:

- Überprüfen Sie das Netzwerk für die ONTAP Storage Virtual Machine (SVM) und ob eine logische Schnittstelle (LIF) für den NFS-Traffic vorhanden ist.
- Eine Exportrichtlinie erstellen, um den ESXi Hosts den Zugriff auf das NFS-Volume zu ermöglichen.
- Erstellen Sie ein NFS-Volume auf dem ONTAP Storage-System.
- Erstellen Sie einen Netzwerkpool für NFS- und vMotion-Datenverkehr im SDDC Manager.
- Provision für Hosts in VCF für die Verwendung in einer VI-Workload-Domäne.
- Stellen Sie eine VI-Workload-Domain in VCF unter Verwendung eines NFS-Datastore als Hauptspeicher bereit.
- Installation des NetApp NFS Plug-ins für VMware VAAI

Voraussetzungen

Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- NetApp AFF Storage-System mit einer Storage Virtual Machine (SVM), die für NFS-Datenverkehr konfiguriert ist
- Die logische Schnittstelle (LIF) wurde im IP-Netzwerk erstellt, das NFS-Datenverkehr überträgt und mit der SVM verknüpft ist.
- Die Bereitstellung der VCF-Management-Domäne ist abgeschlossen, und auf die SDDC Manager-Schnittstelle kann zugegriffen werden.
- 4 x ESXi-Hosts, die für die Kommunikation im VCF-Managementnetzwerk konfiguriert sind.
- IP-Adressen, die für vMotion und NFS-Storage-Verkehr im zu diesem Zweck eingerichteten VLAN oder Netzwerksegment reserviert sind.



Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk zum NFS-Server routingfähig ist oder 2) eine LIF für das Managementnetzwerk zur SVM, die das NFS-Datastore-Volumen hostet, hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

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

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

Implementierungsschritte

Gehen Sie wie folgt vor, um eine VI-Workload-Domäne mit einem NFS-Datastore als Hauptspeicher bereitzustellen:

Netzwerk für ONTAP SVM überprüfen

Vergewissern Sie sich, dass die erforderlichen logischen Schnittstellen für das Netzwerk vorhanden sind, die NFS-Datenverkehr zwischen dem ONTAP Storage-Cluster und der VI Workload Domain transportieren.

1. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **Speicher-VMs** und klicken Sie auf die SVM, die für den NFS-Datenverkehr verwendet werden soll. Klicken Sie auf der Registerkarte **Übersicht** unter **NETZWERK-IP-SCHNITTSTELLEN** auf den numerischen Wert rechts von **NFS**. Überprüfen Sie in der Liste, ob die erforderlichen LIF-IP-Adressen aufgeführt sind.

The screenshot shows the ONTAP System Manager interface. The left sidebar 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 mit dem folgenden Befehl die LIFs, die einer SVM zugeordnet sind, über die ONTAP-CLI überprüfen:

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

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

```
vmkping <IP Address>
```

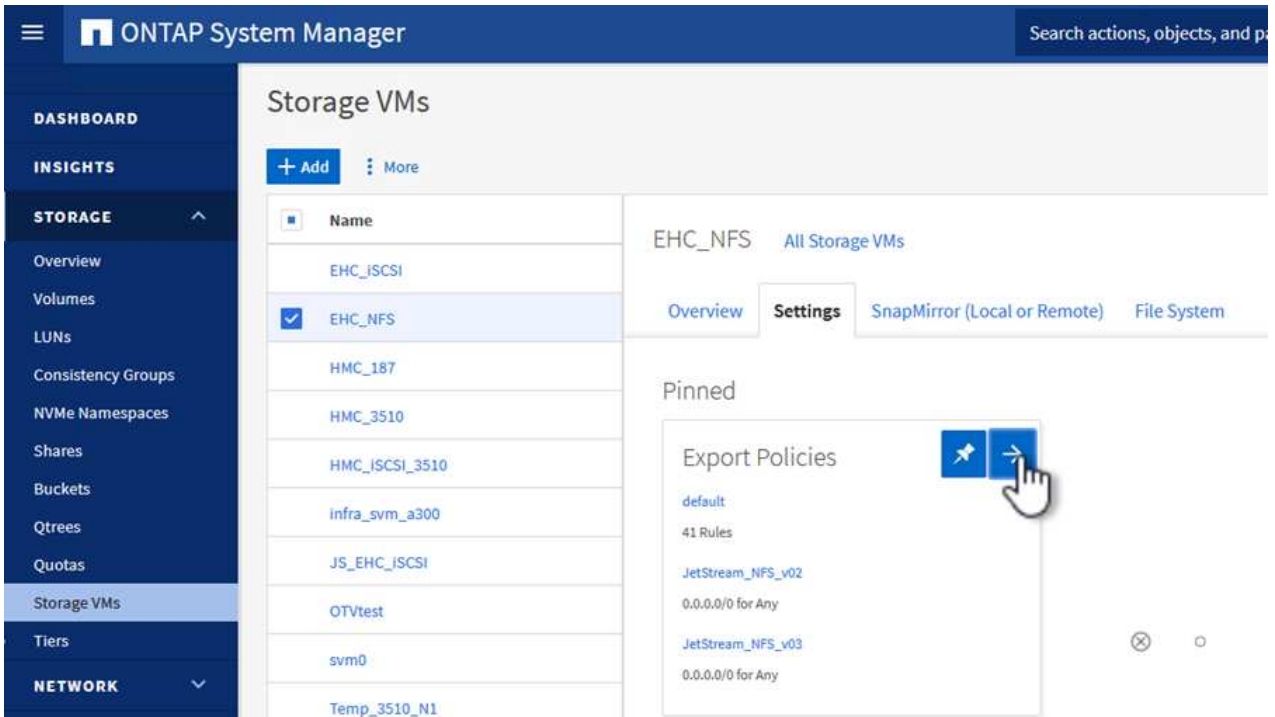


Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk zum NFS-Server routingfähig ist oder 2) eine LIF für das Managementnetzwerk zur SVM, die das NFS-Datastore-Volumen hostet, hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

Erstellen Sie eine Exportrichtlinie für die gemeinsame Nutzung von NFS-Volumen

Eine Richtlinie für den Export in ONTAP System Manager erstellen, um die Zugriffssteuerung für NFS Volumes zu definieren.

1. Klicken Sie im ONTAP System Manager im linken Menü auf **Speicher-VMs** und wählen Sie eine SVM aus der Liste aus.
2. Suchen Sie auf der Registerkarte **Settings Export Policies** und klicken Sie auf den Pfeil, um darauf zuzugreifen.



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

New export policy

NAME

WKLD_DM01

☒ Copy rules from existing policy

STORAGE VM

svm0

EXPORT POLICY

default

RULES

No data

+ Add



Add New Rules

Save

Cancel

4. Geben Sie die IP-Adressen, den IP-Adressbereich oder das Netzwerk ein, die Sie in die Regel aufnehmen möchten. Deaktivieren Sie die Kontrollkästchen **SMB/CIFS** und **FlexCache** und treffen Sie eine Auswahl für die unten stehenden Zugriffsdetails. Die Auswahl der UNIX-Felder ist für den ESXi-Hostzugriff ausreichend.

New Rule



CLIENT SPECIFICATION

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



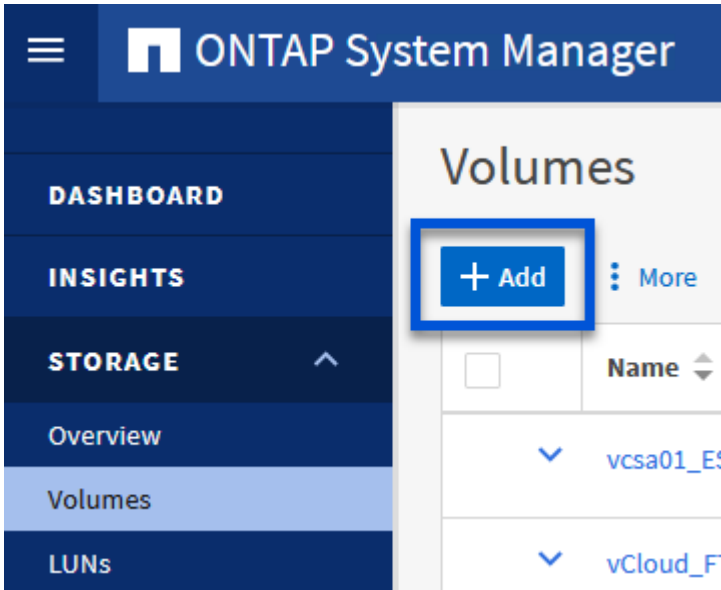
Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass die Exportrichtlinie das VCF-Managementnetzwerk umfasst, damit die Validierung fortgesetzt werden kann.

- Nachdem alle Regeln eingegeben wurden, klicken Sie auf die Schaltfläche **Speichern**, um die neue Exportrichtlinie zu speichern.
- Alternativ können Sie Richtlinien und Regeln für den Export in der ONTAP CLI erstellen. Weitere Informationen finden Sie in den Schritten zum Erstellen einer Exportrichtlinie und zum Hinzufügen von Regeln in der ONTAP-Dokumentation.
 - Verwenden Sie die ONTAP-CLI für ["Erstellen Sie eine Exportrichtlinie"](#).
 - Verwenden Sie die ONTAP-CLI für ["Fügen Sie eine Regel zu einer Exportrichtlinie hinzu"](#).

Erstellen Sie ein NFS-Volume

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

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



2. Fügen Sie einen Namen für das Volume hinzu, füllen Sie die gewünschte Kapazität aus und wählen Sie die Storage-VM aus, die das Volume hosten soll. Klicken Sie auf **Weitere Optionen**, um fortzufahren.

Add Volume



NAME

VCF_WKLD_01

CAPACITY

5



TiB



STORAGE VM

EHC_NFS



Export via NFS

More Options

Cancel


Save

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

Access Permissions

☒ Export via NFS

GRANT ACCESS TO HOST



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, 172.21.2

+



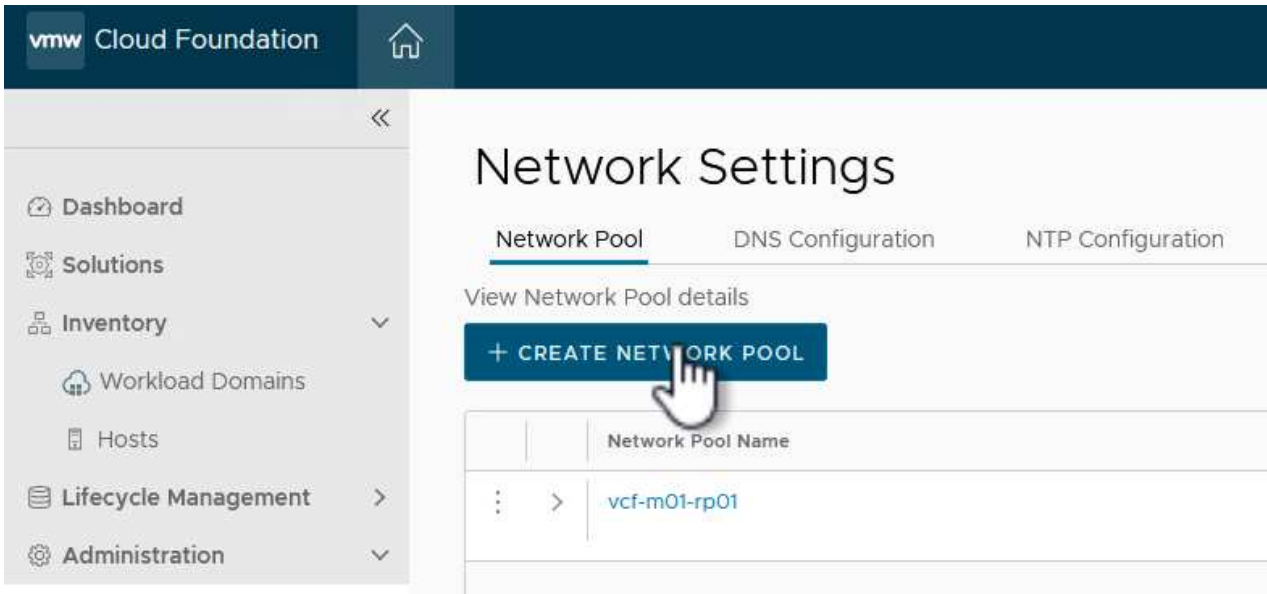
Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk zum NFS-Server routingfähig ist oder 2) eine LIF für das Managementnetzwerk zur SVM, die das NFS-Datastore-Volumen hostet, hinzugefügt wurde, um sicherzustellen, dass die Validierung fortgesetzt werden kann.

1. Alternativ können ONTAP Volumes auch über die ONTAP CLI erstellt werden. Weitere Informationen finden Sie im ["lun erstellen"](#) In der Dokumentation zu ONTAP-Befehlen.

Netzwerkpool im SDDC Manager erstellen

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

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



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

vmw Cloud Foundation

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 NameNFS_NP01

Network Type

vSAN

☒ NFS

iSCSI

☒ vMotion

NFS Network Information

VLAN ID3374

MTU9000

Network172.21.118.0

Subnet Mask255.255.255.0

Default Gateway172.21.118.1

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 ID3423

MTU9000

Network172.21.167.0

Subnet Mask255.255.255.0

Default Gateway172.21.167.1

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

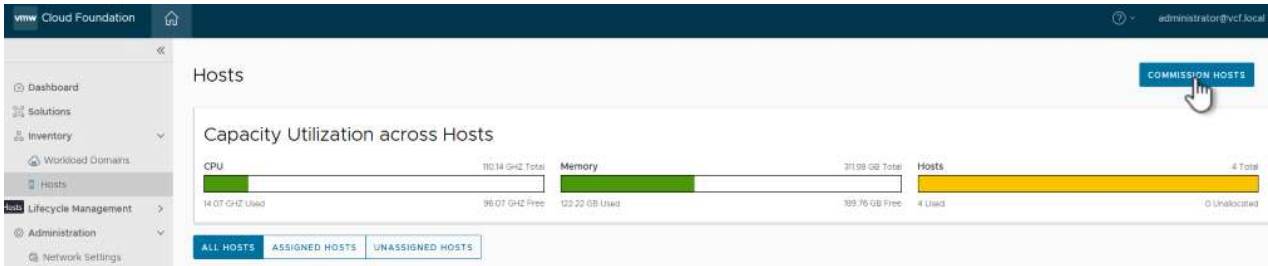
3. Klicken Sie auf die Schaltfläche **Speichern**, um die Erstellung des Netzwerkpools abzuschließen.

Provisionswirte

Bevor ESXi-Hosts als Workload-Domäne bereitgestellt werden können, müssen sie dem Bestand des SDDC-Managers hinzugefügt werden. Dazu gehören die Bereitstellung der erforderlichen Informationen, die bestandende Validierung und der Beginn des Inbetriebnahmeprozesses.

Weitere Informationen finden Sie unter "[Provisionswirte](#)" Im VCF-Administrationshandbuch.

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



2. Die erste Seite ist eine Checkliste für Voraussetzungen. Markieren Sie alle Voraussetzungen, und aktivieren Sie alle Kontrollkästchen, um fortzufahren.

Checklist

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

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

CANCEL

PROCEED

3. Füllen Sie im Fenster **Host Addition and Validation** die Felder **Host FQDN**, **Storage Type**, **Network Pool** aus, die die für die Workload-Domain zu verwendenden vMotion- und NFS-Speicher-IP-Adressen sowie die Anmeldeinformationen für den Zugriff auf den ESXi-Host enthalten. Klicken Sie auf **Add**, um den Host zur Gruppe der zu validierenden Hosts hinzuzufügen.

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	<input checked="" type="checkbox"/> Not Validated

1 hosts

CANCEL

NEXT

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

Hosts Added

✓ Host Validated Successfully.

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-esx04.sddc.netapp.com	NFS_NP01	172.21.166.138	✓ SHA256:9Kg+9 nQaE4SQkOMs QPON/ k5gZB9zyKN+6 CBPmXsvLBc	✓ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01	172.21.166.137	✓ SHA256:nPX4/ mei/ 2zmLJHfmPwbk 6zhapoUxV2IO wZDPFH+zo	✓ Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01	172.21.166.136	✓ SHA256:AMhyR 60OpTQ1YYq0 DJhqVbj/M/ GvrQaqUy7Ce+ M4IWY	✓ Valid
<input checked="" type="checkbox"/>	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 Hosts, die beauftragt werden sollen, und klicken Sie auf die Schaltfläche **Provision**, um den Prozess zu starten. Überwachen Sie den Inbetriebnahmeprozess im SDDC-Manager im Aufgabenbereich.



Commission Hosts

1 Host Addition and Validation

2 Review

Review

Skip failed hosts during commissioning ⓘ ☒ On

Validated Host(s)

vcf-wkld-esx04.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.138 Storage Type: NFS
vcf-wkld-esx03.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.137 Storage Type: NFS
vcf-wkld-esx02.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.136 Storage Type: NFS
vcf-wkld-esx01.sddc.netapp.com	Network Pool Name: NFS_NP01 IP Address: 172.21.166.135 Storage Type: NFS

CANCEL

BACK

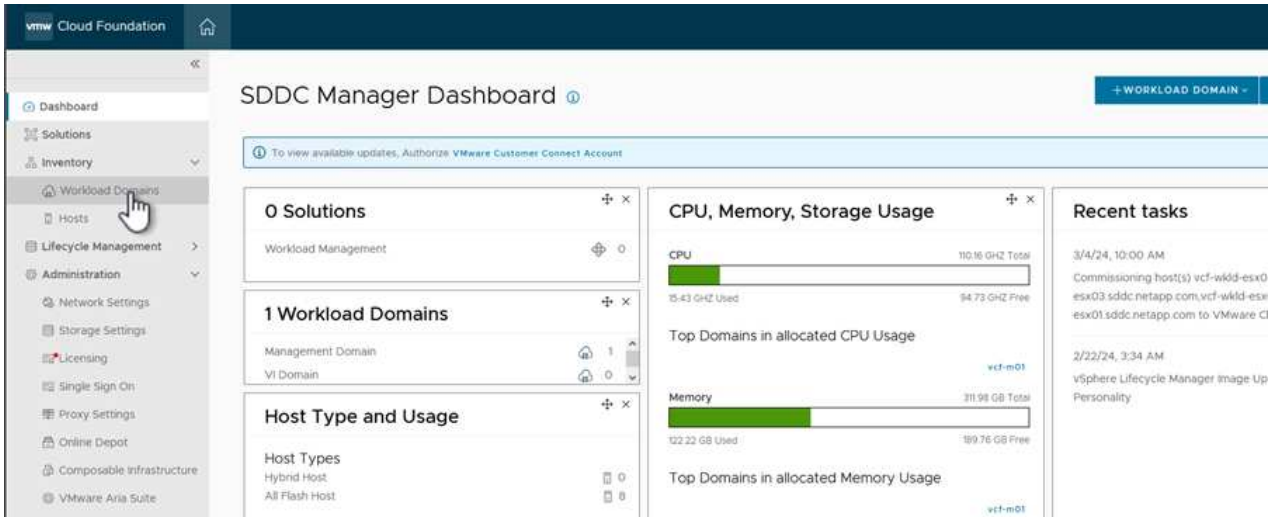
COMMISSION

Implementieren Sie VI Workload Domain

Die Implementierung von VI-Workload-Domänen erfolgt über die Schnittstelle des VCF Cloud Manager. Hier werden nur die Schritte in Bezug auf die Speicherkonfiguration dargestellt.

Schritt-für-Schritt-Anweisungen zur Bereitstellung einer VI-Workload-Domäne finden Sie unter ["Stellen Sie eine VI-Workload-Domäne über die SDDC Manager-Benutzeroberfläche bereit"](#).

1. Klicken Sie im SDDC Manager Dashboard auf **+ Workload Domain** in der oberen rechten Ecke, um eine neue Workload Domain zu erstellen.



2. Füllen Sie im VI Configuration Wizard die Abschnitte für **Allgemeine Informationen**, **Cluster**, **Datenverarbeitung**, **Netzwerk** und **Host Selection** nach Bedarf aus.

Informationen zum Ausfüllen der im VI-Konfigurationsassistenten erforderlichen Informationen finden Sie unter ["Stellen Sie eine VI-Workload-Domäne über die SDDC Manager-Benutzeroberfläche bereit"](#).

+

VI Configuration

1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

7 Switch Configuration

8 License

9 Review

1. Füllen Sie im Abschnitt NFS-Storage den Datenspeichernamen, den Ordner-Bereitstellungspunkt des NFS-Volume und die IP-Adresse der logischen Schnittstelle des ONTAP NFS-Storage VM aus.

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 Configuration Wizard die Schritte Switch Configuration und License aus, und klicken Sie dann auf **Finish**, um die Erstellung der Workload Domain zu starten.

VI Configuration

- 1 General Info
- 2 Cluster
- 3 Compute
- 4 Networking
- 5 Host Selection
- 6 NFS Storage
- 7 Switch Configuration
- 8 License
- 9 Review**

Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nxsci01.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 beheben Sie alle während des Prozesses auftretenden Validierungsprobleme.

Installation des NetApp NFS Plug-ins für VMware VAAI

Das NetApp-NFS-Plug-in für VMware VAAI integriert die auf dem ESXi-Host installierten VMware Virtual Disk Libraries und bietet höhere Performance-Klonvorgänge, die schneller abgeschlossen werden können. Dies wird empfohlen, wenn Sie ONTAP Storage-Systeme mit VMware vSphere verwenden.

Schritt-für-Schritt-Anweisungen zum Bereitstellen des NetApp-NFS-Plug-ins für VMware VAAI finden Sie unter ["Installation des NetApp NFS Plug-ins für VMware VAAI"](#).

Video-Demo für diese Lösung

[NFS-Datenspeicher als Principal Storage für VCF Workload Domains](#)

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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