



# Virtualisierung mit VMware

## NetApp Solutions

NetApp  
May 10, 2024

# Inhalt

- NetApp-Lösungen für die Virtualisierung mit VMware von Broadcom ..... 1
  - VMware Cloud Foundation ..... 1
  - Einführung in die Automatisierung für ONTAP und vSphere ..... 139
  - NetApp Hybrid-Multi-Cloud mit VMware Lösungen ..... 152
  - Anwendungsfälle für die VMware Hybrid-Multi-Cloud ..... 152
  - Virtual Desktops ..... 153
  - NetApp All-Flash SAN-Array mit VMware vSphere 8 ..... 194
  - Demos und Tutorials ..... 239

# NetApp-Lösungen für die Virtualisierung mit VMware von Broadcom

## 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

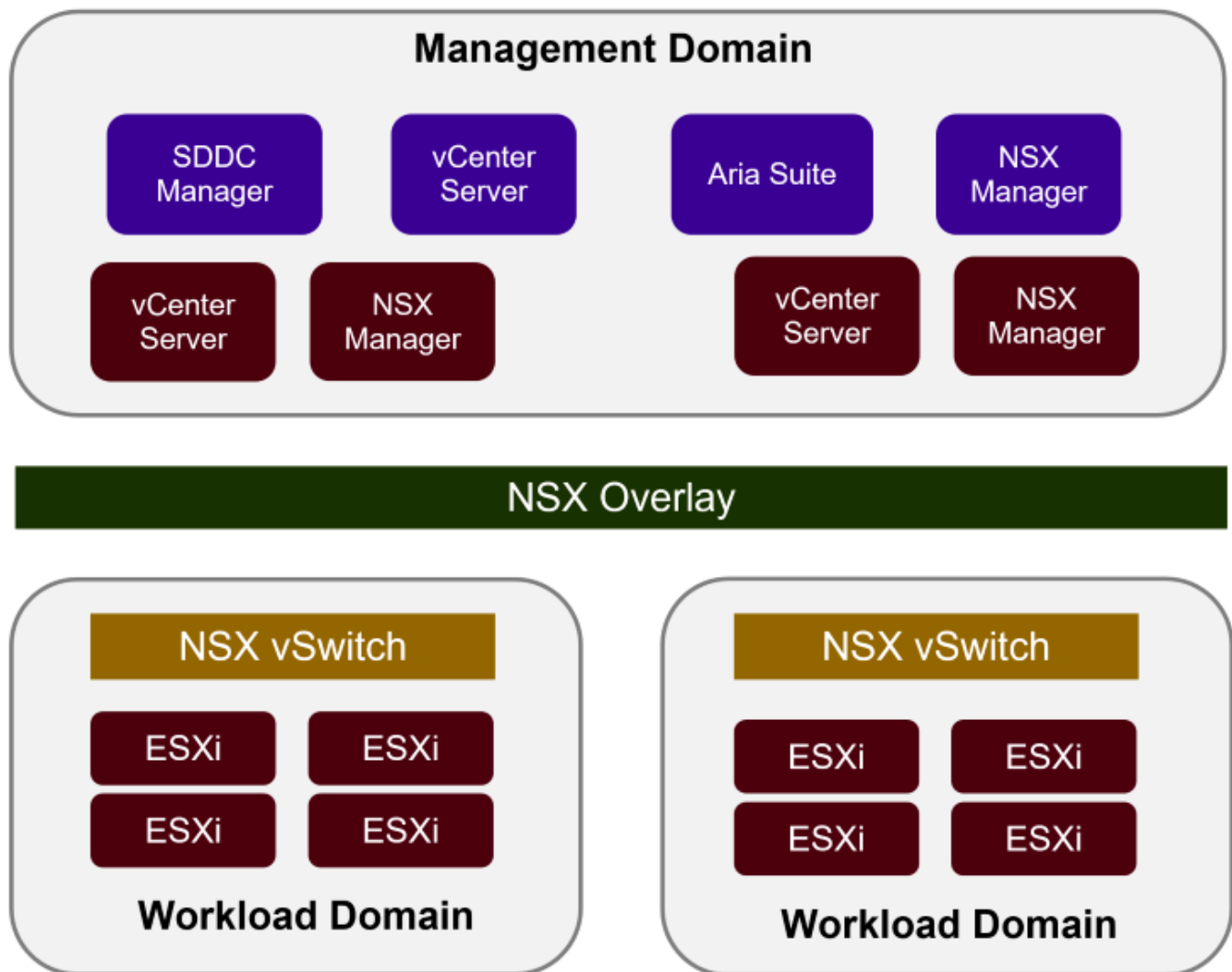
Die VCF mit NetApp ASA-Lösung besteht aus den folgenden Hauptkomponenten:

### 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.

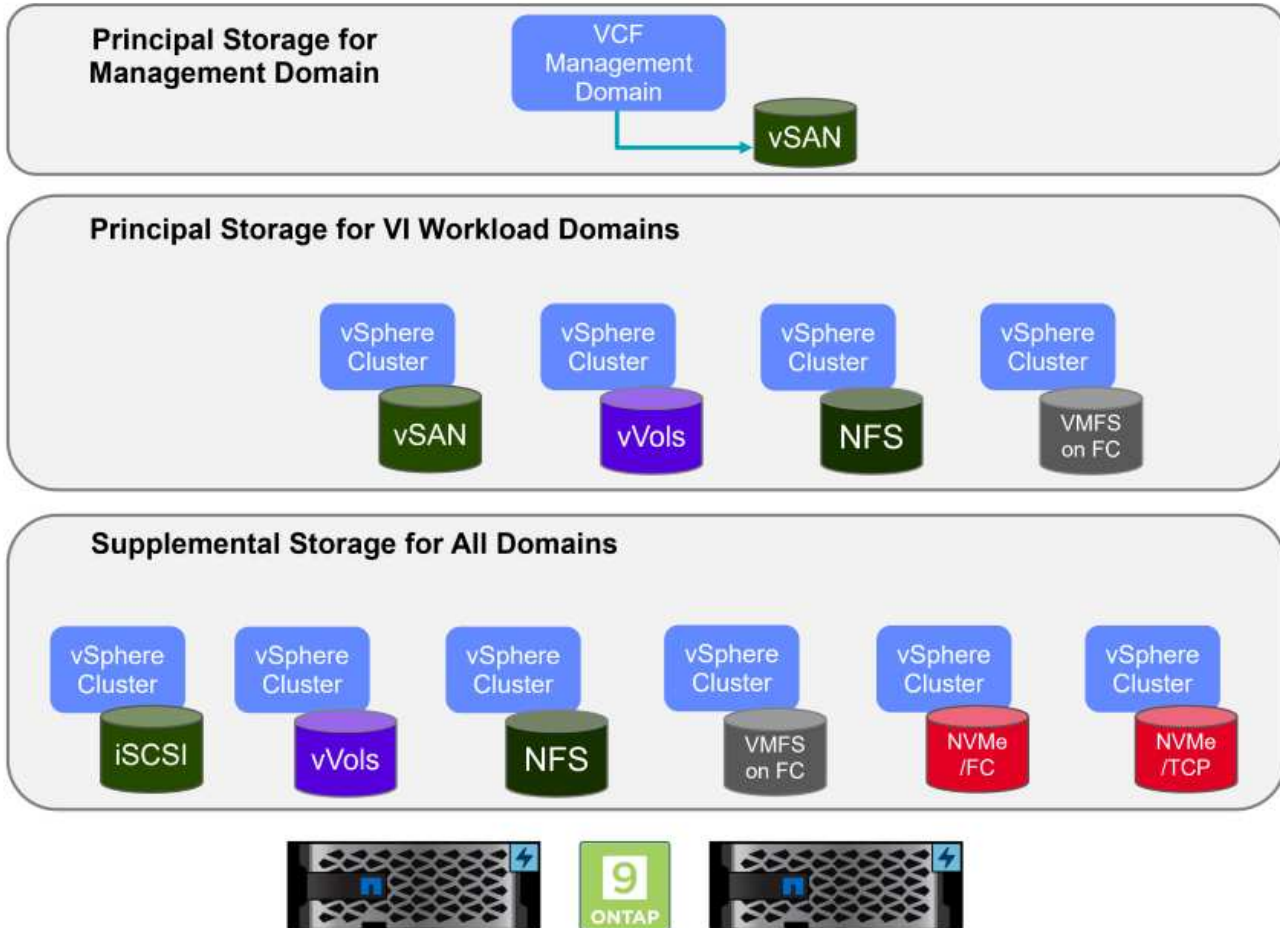


Weitere Informationen zur Architektur und Planung von VCF finden Sie unter "[Architekturmodelle und Workload-Domänen-Typen in VMware Cloud Foundation](#)".



## VCF Storage-Optionen

VMware unterteilt Speicheroptionen für VCF in **Principal** und **Supplemental** Speicher. Die VCF-Management-Domäne muss vSAN als Haupt-Speicher 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.

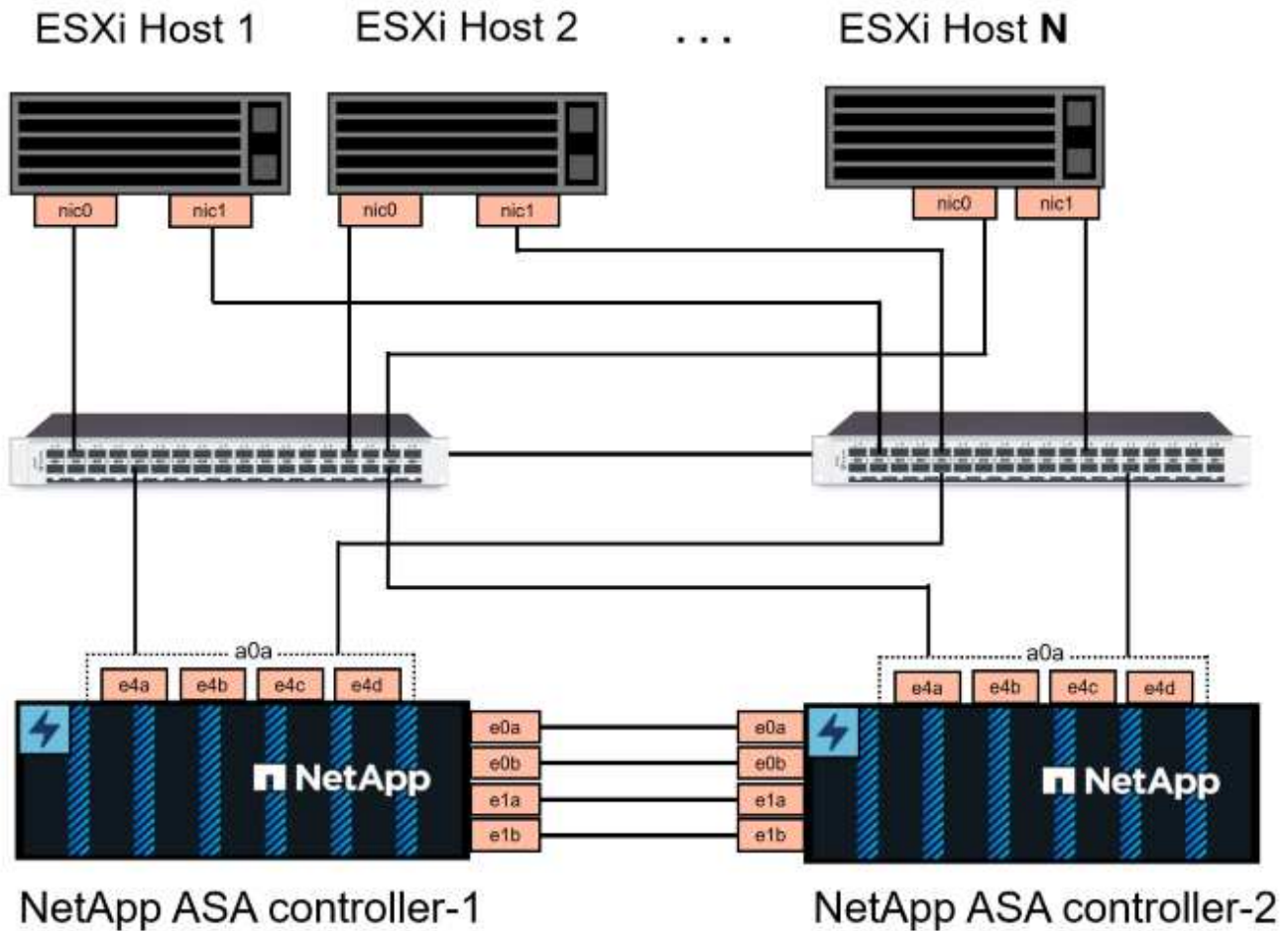
## Voraussetzungen

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:

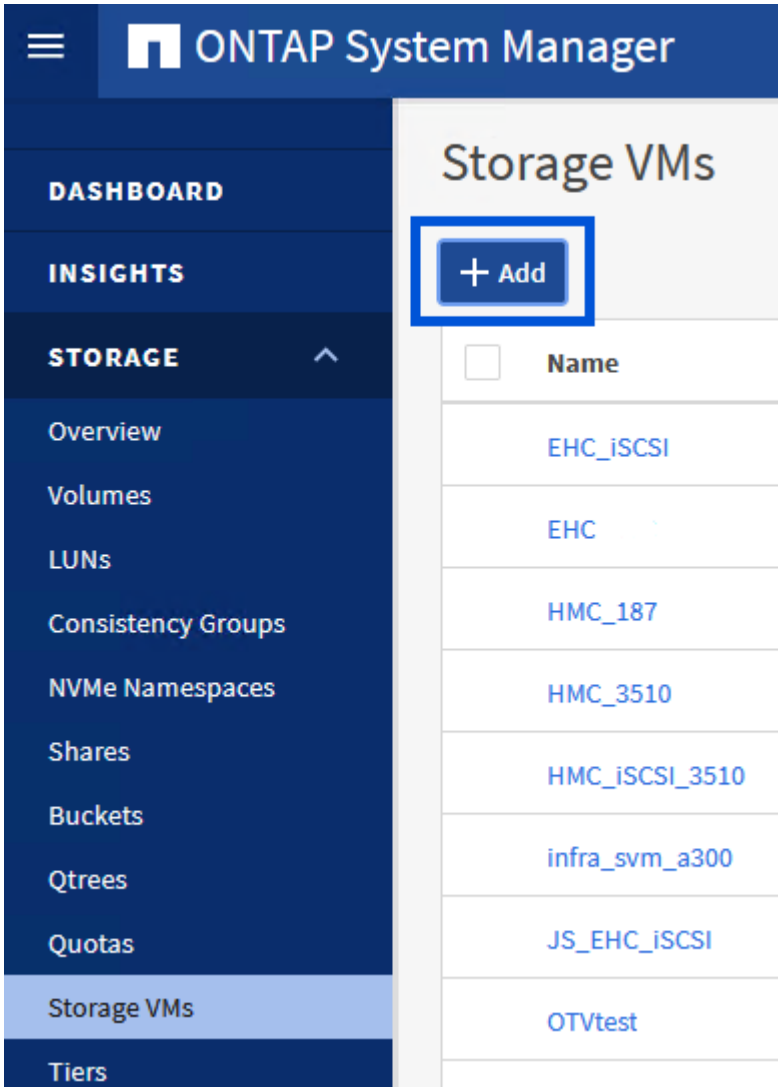
## **Erstellung der SVM und LIFs auf dem ONTAP Storage-System**

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

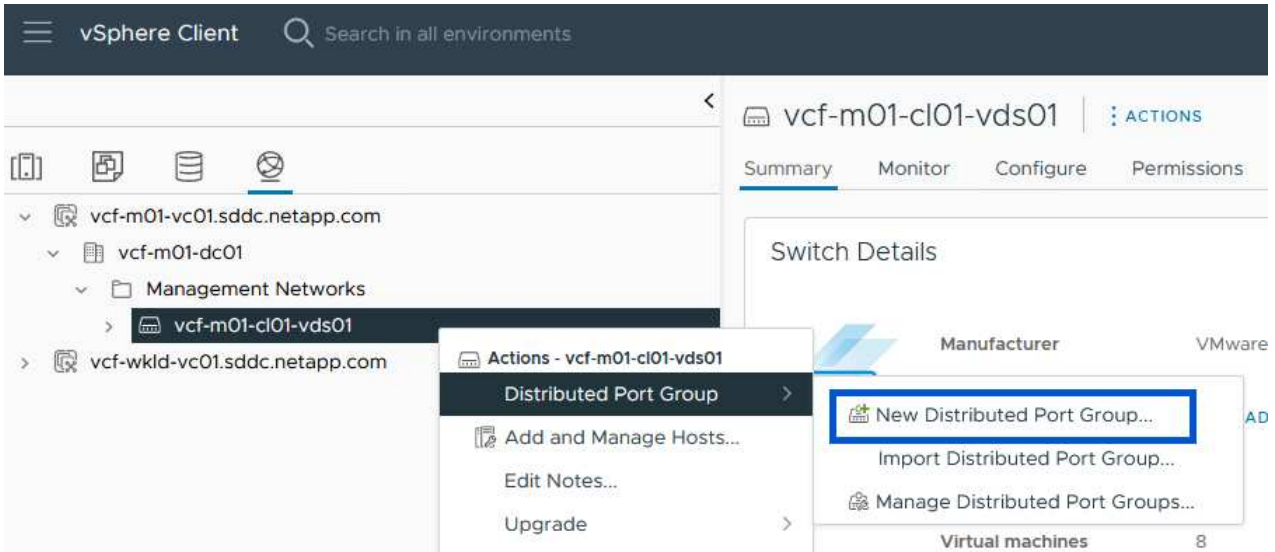
### Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein

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	
<input type="checkbox"/> Customize default policies configuration	

CANCEL BACK NEXT

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

The screenshot shows the vSphere Client interface. The top navigation bar includes the vSphere Client logo and a search bar. The main content area is divided into a left-hand navigation pane and a right-hand details pane. The left pane shows a tree view of the environment, with the following structure:

- 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 (highlighted)
        - vcf-m01-cl01-vds01
        - vcf-m01-cl01-vds01
        - vcf-m01-cl01-vds01
        - vcf-m01-cl01-vds01
- vcf-wkld-vc01.sddc.netapp.com

The right-hand pane displays the details for the selected port group, **vcf-m01-cl01-vds01-pg-iscsi-a**. The details are as follows:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	vcf-m01-cl01-vds01
Network protocol profile	--
Network resource pool	--
Hosts	4

An action menu is open over the selected port group, showing the following options:

- Actions - vcf-m01-cl01-vds01-pg-iscsi-a
- Edit Settings... (highlighted)
- 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	<b>Load balancing</b>	Route based on originating virtual por ▾
Advanced	<b>Network failure detection</b>	Link status only ▾
VLAN	<b>Notify switches</b>	Yes ▾
Security	<b>Failback</b>	Yes ▾
Traffic shaping		
<b>Teaming and failover</b>		
Monitoring	<b>Failover order</b> ⓘ	
Miscellaneous	<b>Active uplinks</b>	
	uplink1	
	<b>Standby uplinks</b>	
	<b>Unused uplinks</b>	
	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

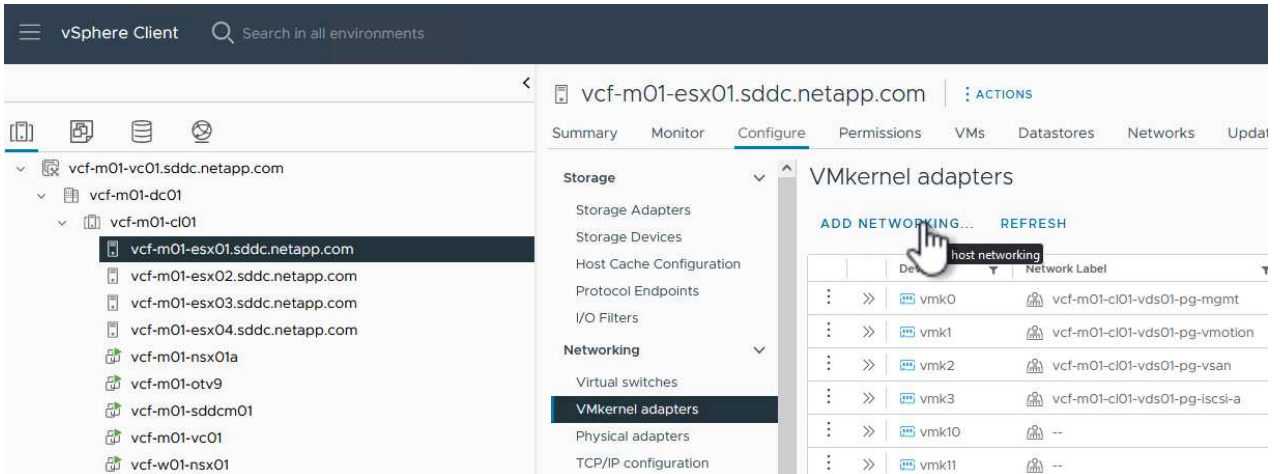
### Unused uplinks

uplink1

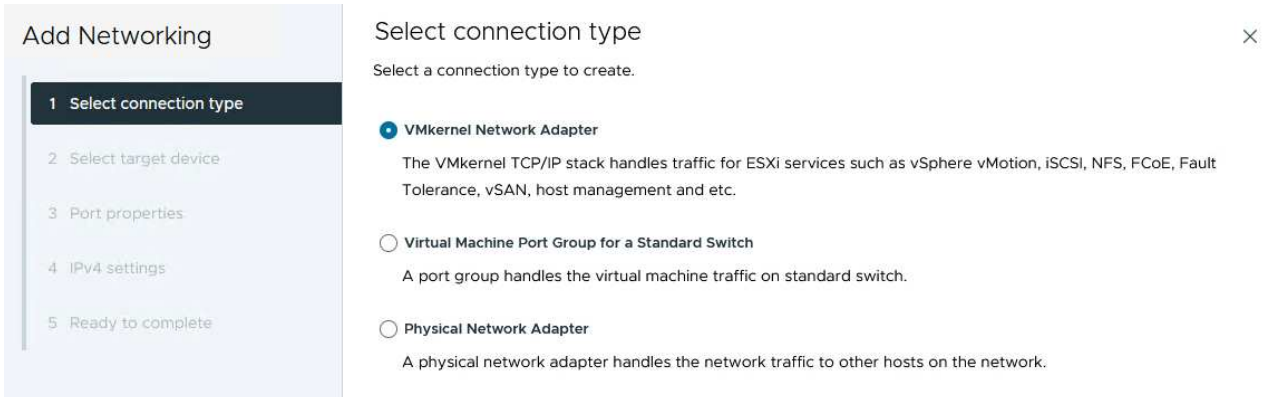
## Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

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

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically  
 Use static IPv4 settings

**IPv4 address**

**Subnet mask**

**Default gateway**  Override default gateway for this adapter

**DNS server addresses**

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

### Add Networking

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

### Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

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

Distributed switch vcf-m01-cl01-vds01
- ▼ Port properties

New port group vcf-m01-cl01-vds01-pg-iscsi-a (vcf-m01-cl01-vds01)

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.114 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

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

## **Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools**

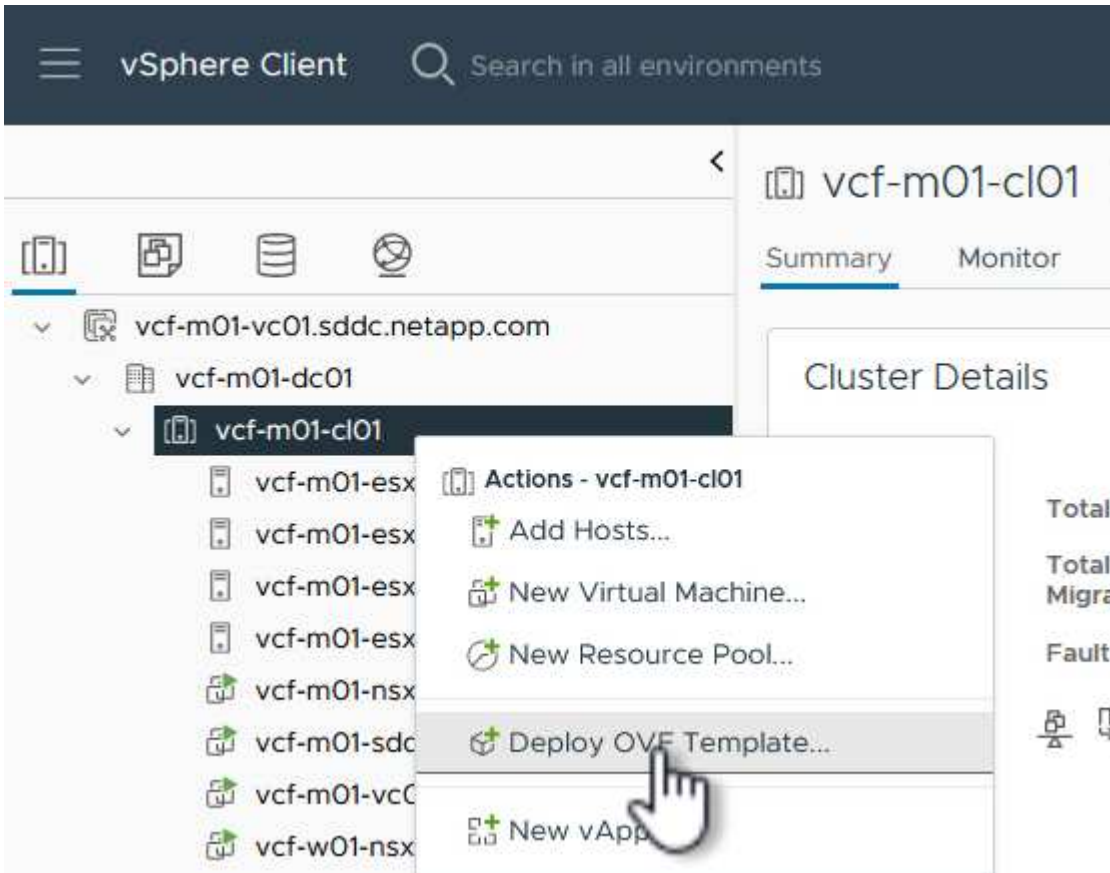
Die folgenden Schritte werden auf dem VCF-Management-Domänencluster unter Verwendung des vSphere-Clients durchgeführt und umfassen die Bereitstellung von OTV, die Erstellung eines VMFS-iSCSI-Datastore und die Migration von Management-VMs auf den neuen Datastore.

## Implementieren Sie ONTAP-Tools für VMware vSphere

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

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

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



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

## Deploy OVF Template

### 1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 Select storage

6 Ready to complete

## Select an OVF template

Select an OVF template from remote URL or local file system

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

URL

Local file

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

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

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

**6 Select storage**

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

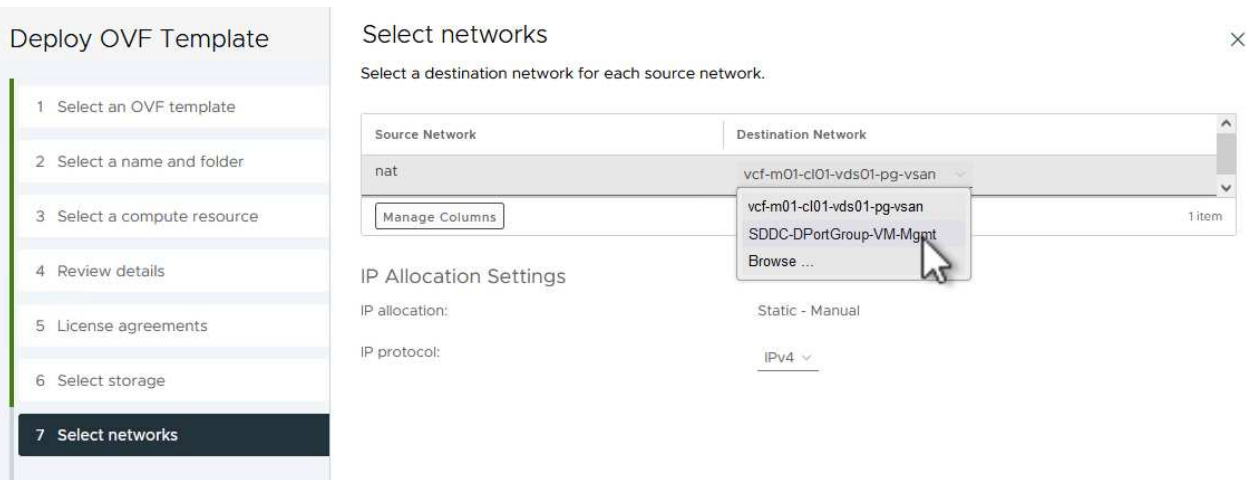
VM Storage Policy

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 5 items

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



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

- 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
<b>Application User Password (*)</b>	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="....."/>
<b>NTP Servers</b>	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"/>
<b>Maintenance User Password (*)</b>	Password to assign to maint user account.
	Password <input type="password" value="....."/>
	Confirm Password <input type="password" value="....."/>

## Deploy OVF Template

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

## Customize template

Configure vCenter or Enable VCF	5 settings
<b>Enable VMware Cloud Foundation (VCF)</b>	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>
<b>vCenter Server Address (*)</b>	Specify the IP address/hostname of an existing vCenter to register to. <input type="text" value="172.21.166.140"/>
<b>Port (*)</b>	Specify the HTTPS port of an existing vCenter to register to. <input type="text" value="443"/>
<b>Username (*)</b>	Specify the username of an existing vCenter to register to. <input type="text" value="administrator@vsphere.local"/>
<b>Password (*)</b>	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
<b>Host Name</b>	Specify the hostname for the appliance. (Leave blank if DHCP is desired) <input type="text" value="vcf-m01-otv9"/>
<b>IP Address</b>	Specify the IP address for the appliance. (Leave blank if DHCP is

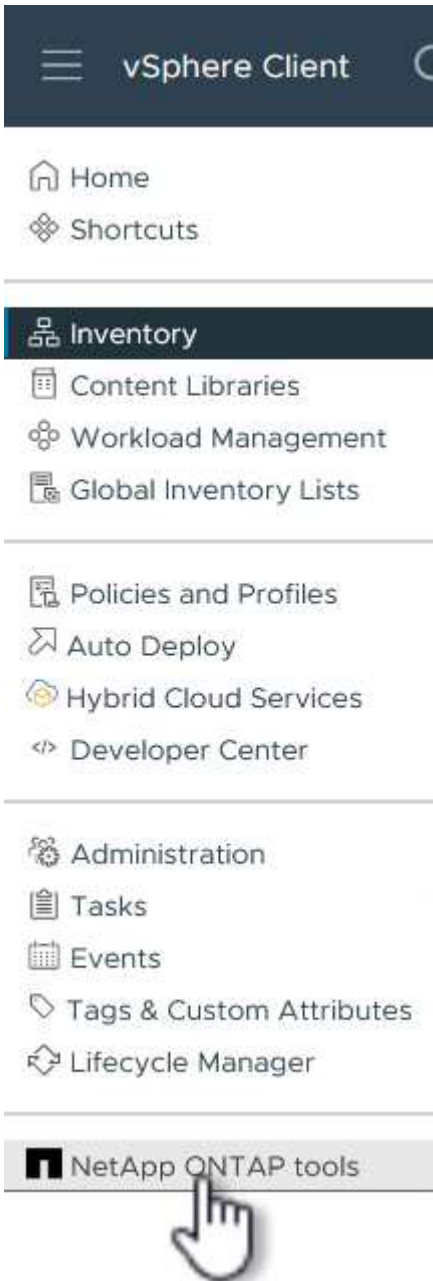
CANCEL BACK NEXT

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

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

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

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



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

vSphere Client Search in all environments

NetApp ONTAP tools INSTANCE 172.21.166.139:8443

Overview

Storage Systems

Storage capability profile

Storage Mapping

Settings


Reports

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

## ONTAP tools for VMware vSphere


Getting Started Traditional Dashboard vVols Dashboard


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



**Add Storage System**


Add storage systems to ONTAP tools for VMware vSphere.





**Provision Datastore**

Create traditional or vVols datastores.




[What's new?](#)  
September 4, 2023


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

**Resources**

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

**Next Steps**

 [View Dashboard](#)  
View and monitor the datastores in ONTAP tools for VMware vSphere.



 [Settings](#)  
Configure administrative settings such as credentials, alarm thresholds.

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



## Add Storage System

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

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


CANCEL

SAVE & ADD MORE

ADD 

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

## Add Storage System

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

vCenter server

vcf-m01-vc01.sddc.netapp.com

### Authorize Cluster Certificate

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

[Show certificate](#)

Do you want to trust this certificate?

NO

YES



CANCEL

SAVE & ADD MORE

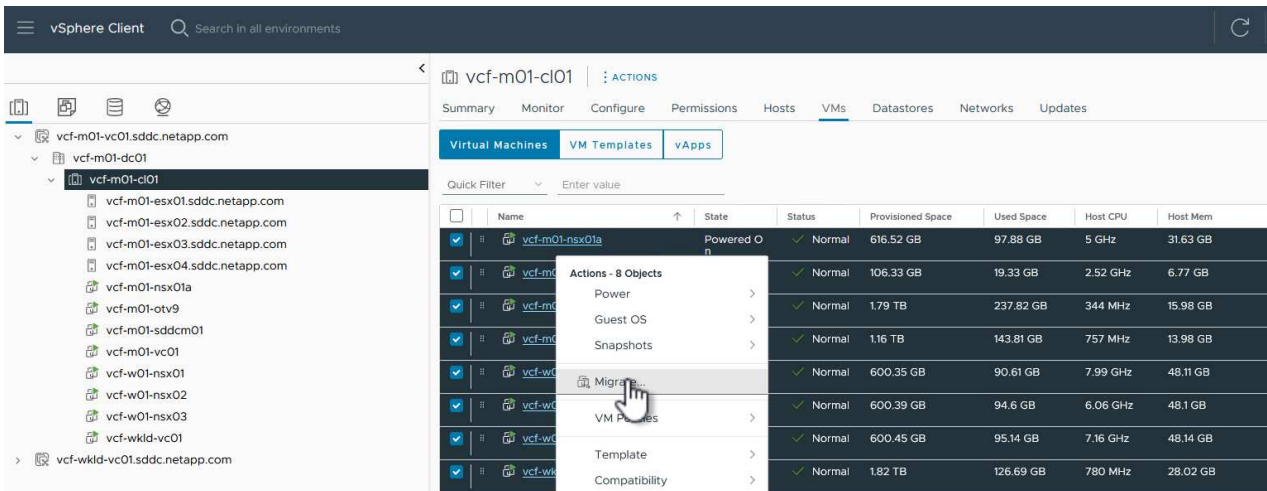
ADD

## Migration von Management-VM's auf iSCSI-Datenspeicher

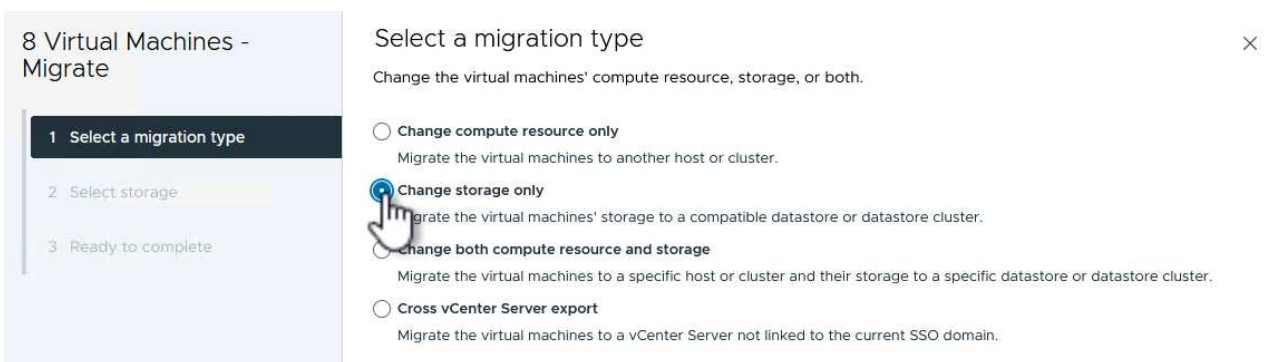
In Fällen, in denen es bevorzugt wird, ONTAP Storage zum Schutz der VCF Management-VM zu verwenden, kann vMotion zur Migration der VMs zum neu erstellten iSCSI-Datenspeicher verwendet werden.

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

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



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



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

## 8 Virtual Machines - Migrate

1 Select a migration type

2 Select storage

3 Ready to complete

### Select storage

Select the destination storage for the virtual machine migration.

**BATCH CONFIGURE** CONFIGURE PER DISK

Select virtual disk format Same format as source

VM Storage Policy Datastore Default

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free
<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

Manage Columns Items per page 10 2 items

#### Compatibility

✓ Compatibility checks succeeded.

CANCEL

BACK

NEXT

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

Task Name	Target	Status	Details
Relocate virtual machine	<a href="#">vcf-w01-nsx03</a>	38%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-wkld-vc01</a>	42%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-otv9</a>	36%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-nsx01a</a>	49%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-w01-nsx02</a>	47%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-sddcm01</a>	39%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-w01-nsx01</a>	42%	Migrating Virtual Machine active state
Relocate virtual machine	<a href="#">vcf-m01-vc01</a>	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:

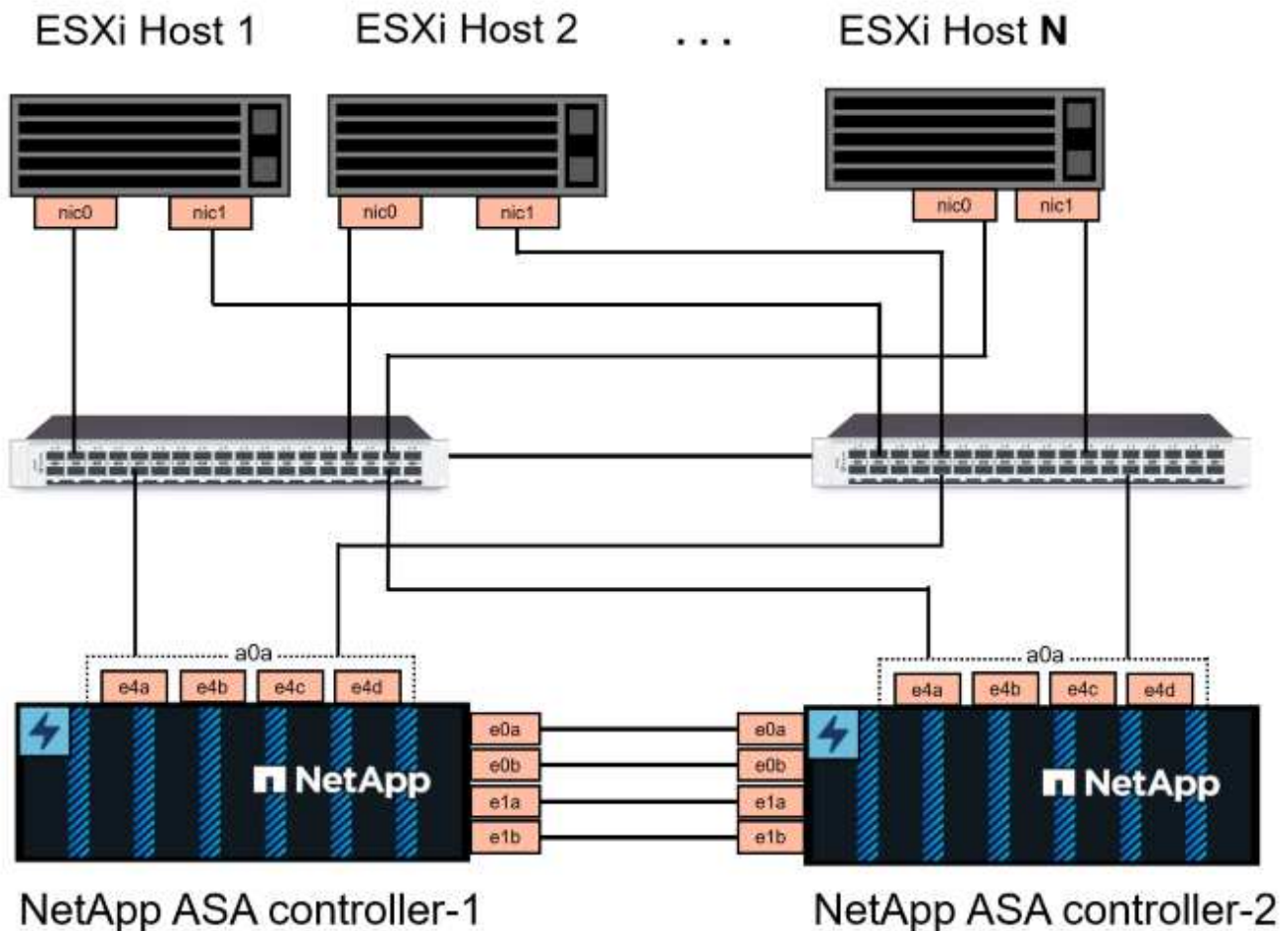
- Storage Virtual Machine (SVM) mit logischen Schnittstellen (LIFs) für iSCSI-Datenverkehr erstellen.
- Erstellen Sie verteilte Portgruppen für iSCSI-Netzwerke in der VI-Workload-Domäne.
- Erstellen Sie vmkernel-Adapter für iSCSI auf den ESXi-Hosts für die VI-Workload-Domäne.
- Implementieren Sie ONTAP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

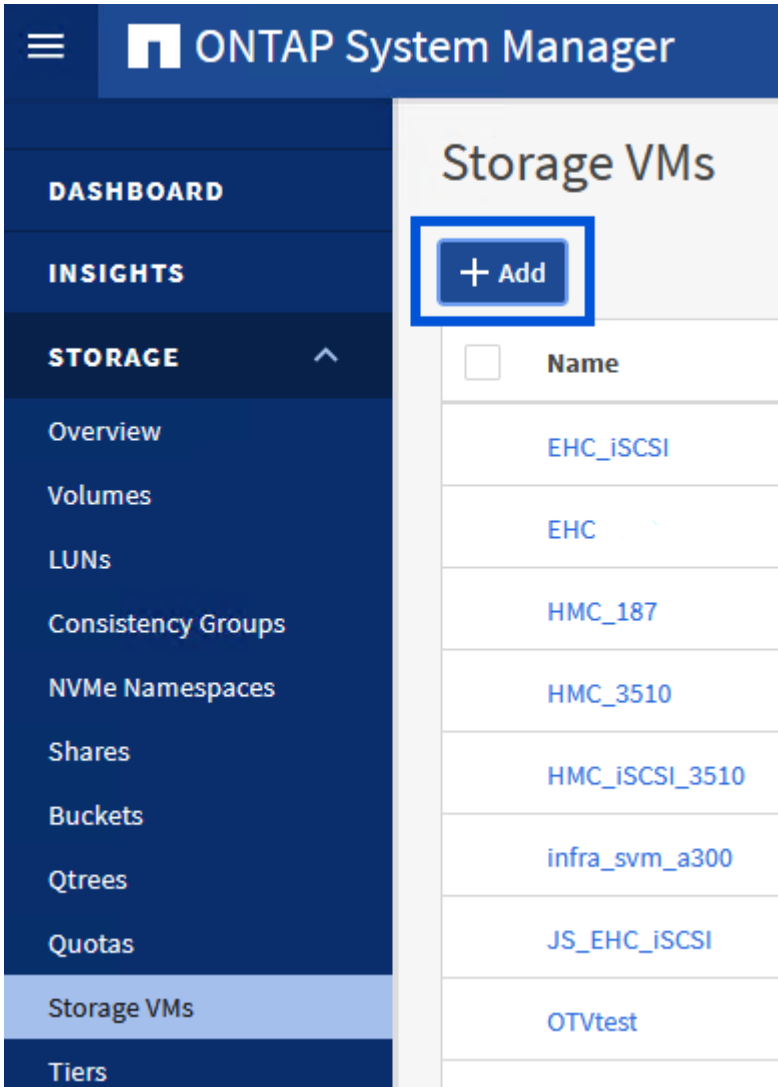
## **Erstellung der SVM und LIFs auf dem ONTAP Storage-System**

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

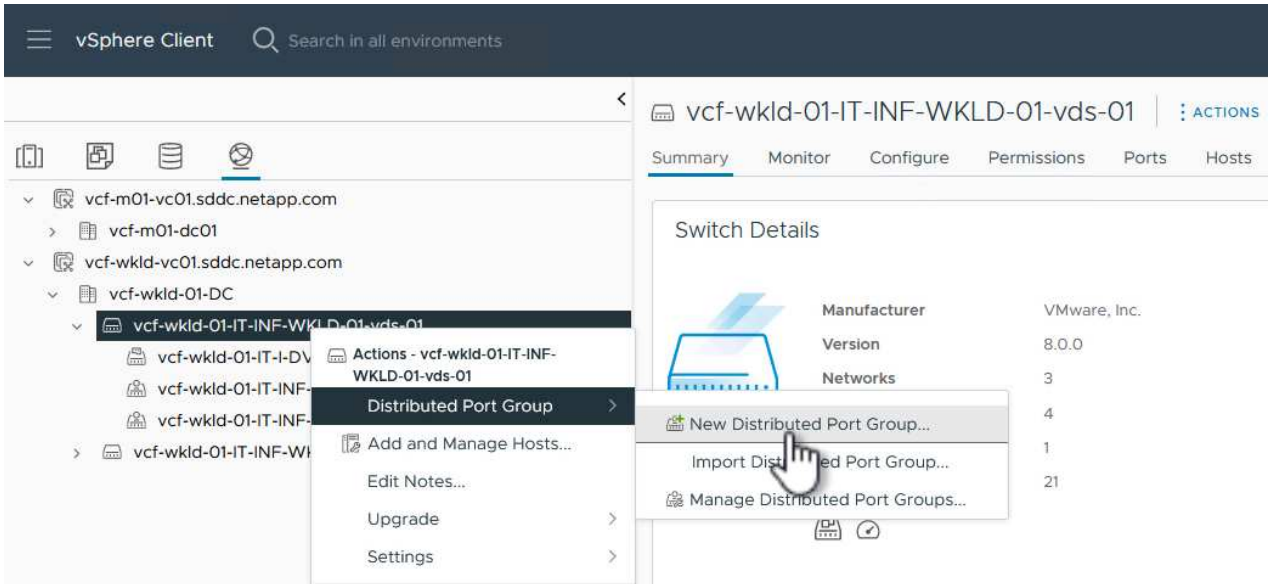
### Richten Sie das Netzwerk für iSCSI auf ESXi-Hosts ein

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	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

NEXT

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

The screenshot shows the vSphere Client interface. On the left, a tree view displays the environment structure, with the path **vcf-wkld-01-iscsi-a** selected. A context menu is open over this selection, showing options like **Actions - vcf-wkld-01-iscsi-a** and **Edit Settings...**. On the right, the **Distributed Port Group Details** panel is visible, showing the following configuration:

Port binding	Static binding
Port allocation	Elastic
VLAN ID	3374
Distributed switch	<a href="#">vcf-wkld-01-IT-INF-WKLD-01-vds-01</a>
Network protocol profile	--

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

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

General	<b>Load balancing</b>	<u>Route based on originating virtual por</u> ▾
Advanced	<b>Network failure detection</b>	<u>Link status only</u> ▾
VLAN	<b>Notify switches</b>	<u>Yes</u> ▾
Security	<b>Failback</b>	<u>Yes</u> ▾
Traffic shaping		
<b>Teaming and failover</b>		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

**Active uplinks**

uplink1

**Standby uplinks**

**Unused uplinks**

uplink2

CANCEL **OK**

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

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

General	<b>Load balancing</b>	<u>Route based on originating virtual por</u> ▾
Advanced	<b>Network failure detection</b>	<u>Link status only</u> ▾
VLAN	<b>Notify switches</b>	<u>Yes</u> ▾
Security	<b>Failback</b>	<u>Yes</u> ▾
Traffic shaping		
<b>Teaming and failover</b>		
Monitoring		
Miscellaneous		

Failover order ⓘ

MOVE UP MOVE DOWN

**Active uplinks**

uplink2

**Standby uplinks**

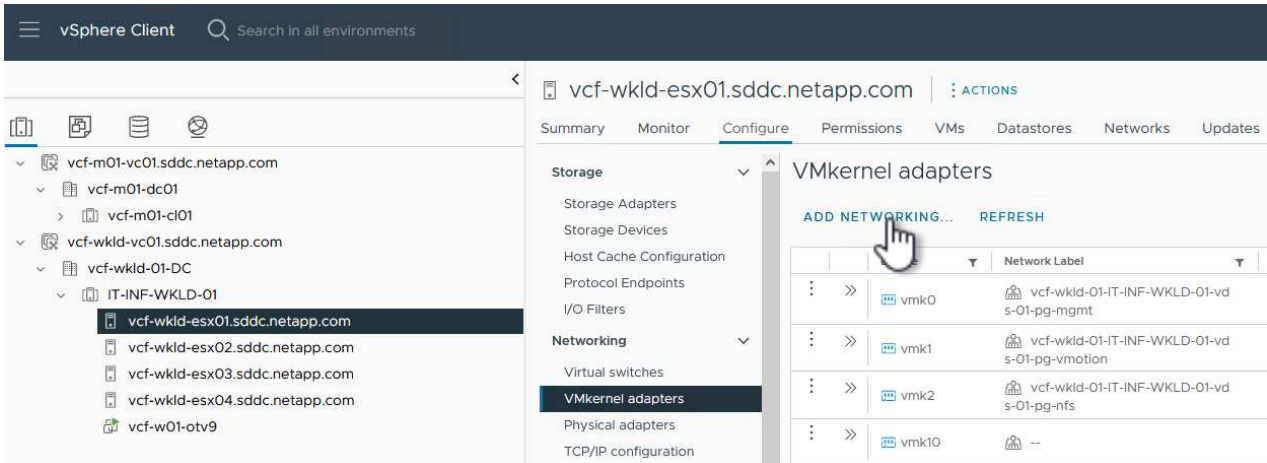
**Unused uplinks**

uplink1

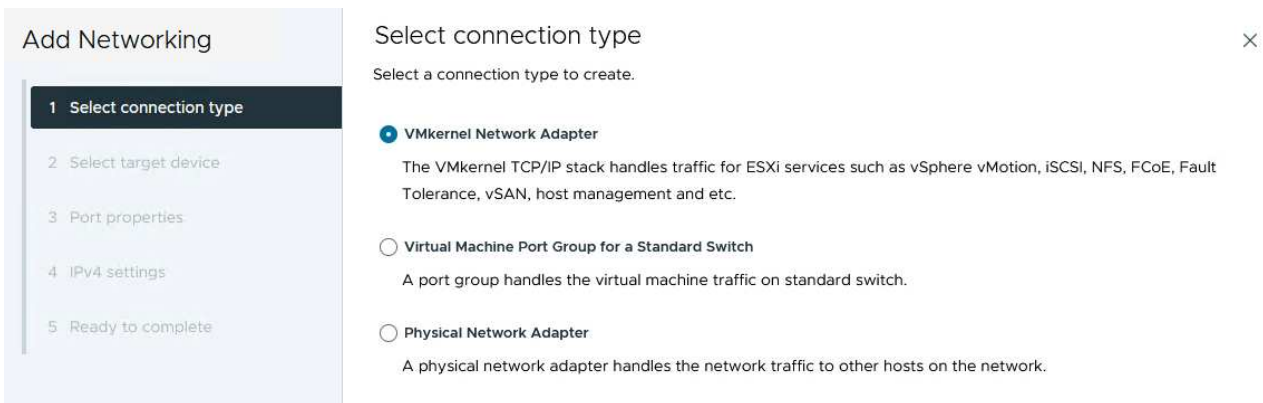
## Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

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



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



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

## Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete






## Select target device

Select a target device for the new connection.

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

Quick Filter

Enter value

	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

Manage Columns 5 items

CANCEL

BACK

NEXT

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

## Add Networking

1 Select connection type

2 Select target device

3 Port properties

4 IPv4 settings

5 Ready to complete

## Port properties

Specify VMkernel port settings.

Network label

MTU

TCP/IP stack

### Available services

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

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

### Add Networking

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

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically  
 Use static IPv4 settings

**IPv4 address**

**Subnet mask**

**Default gateway**  Override default gateway for this adapter

**DNS server addresses**

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

### Add Networking

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

### Ready to complete

Review your selections before finishing the wizard

- ▼ Select target device

Distributed port group vcf-wkld-01-iscsi-a

Distributed switch vcf-wkld-01-IT-INF-WKLD-01-vds-01
- ▼ Port properties

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

MTU 9000

vMotion Disabled

Provisioning Disabled

Fault Tolerance logging Disabled

Management Disabled

vSphere Replication Disabled

vSphere Replication NFC Disabled

vSAN Disabled

vSAN Witness Disabled

vSphere Backup NFC Disabled

NVMe over TCP Disabled

NVMe over RDMA Disabled
- ▼ IPv4 settings

IPv4 address 172.21.118.127 (static)

Subnet mask 255.255.255.0

CANCEL
BACK
FINISH

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



## Implementieren und konfigurieren Sie den Speicher mit den ONTAP-Tools

Die folgenden Schritte werden auf dem VCF-Management-Domänencluster mithilfe des vSphere-Clients durchgeführt. Dazu gehören die 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.

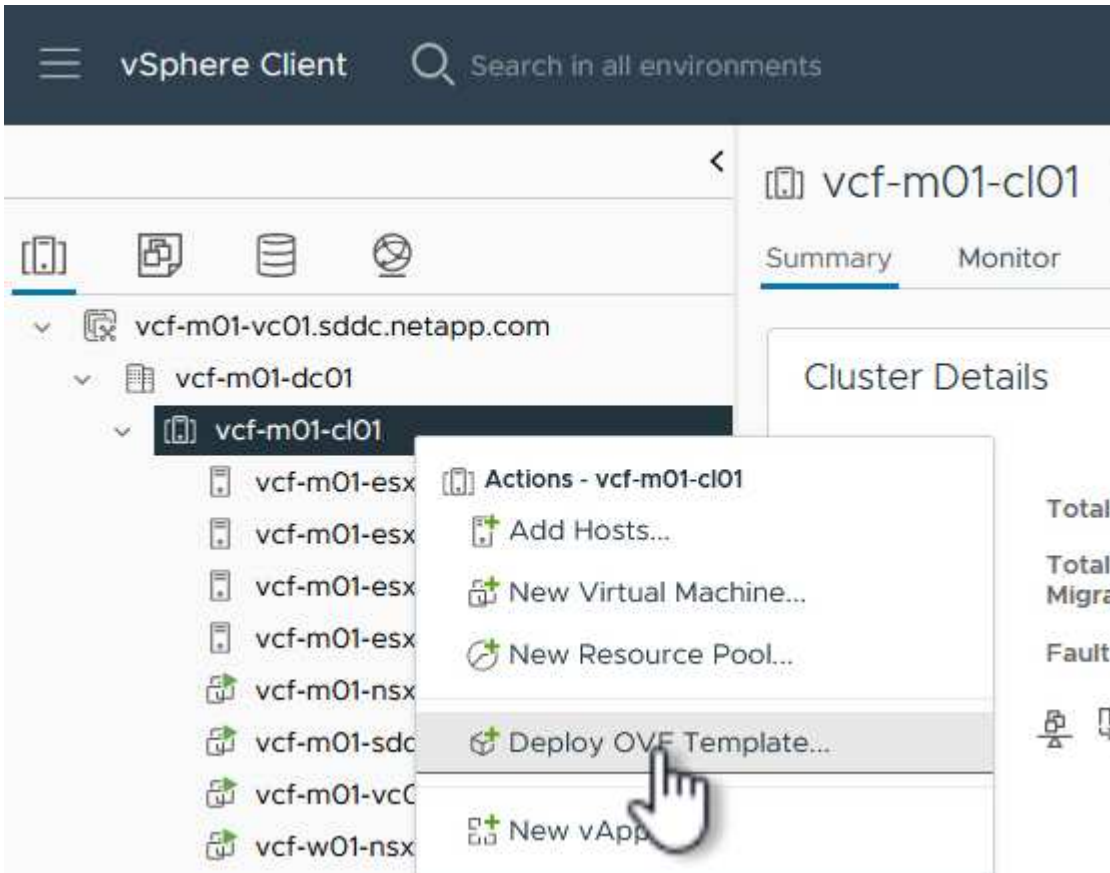
Weitere Informationen zum Implementieren und Verwenden von ONTAP Tools in einer Umgebung mit mehreren vCenter finden Sie unter ["Voraussetzungen für die Registrierung von ONTAP-Tools in einer Umgebung mit mehreren vCenter-Servern"](#).

## 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

Local file

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

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

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

**6 Select storage**

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format

As defined in the VM storage policy ▾

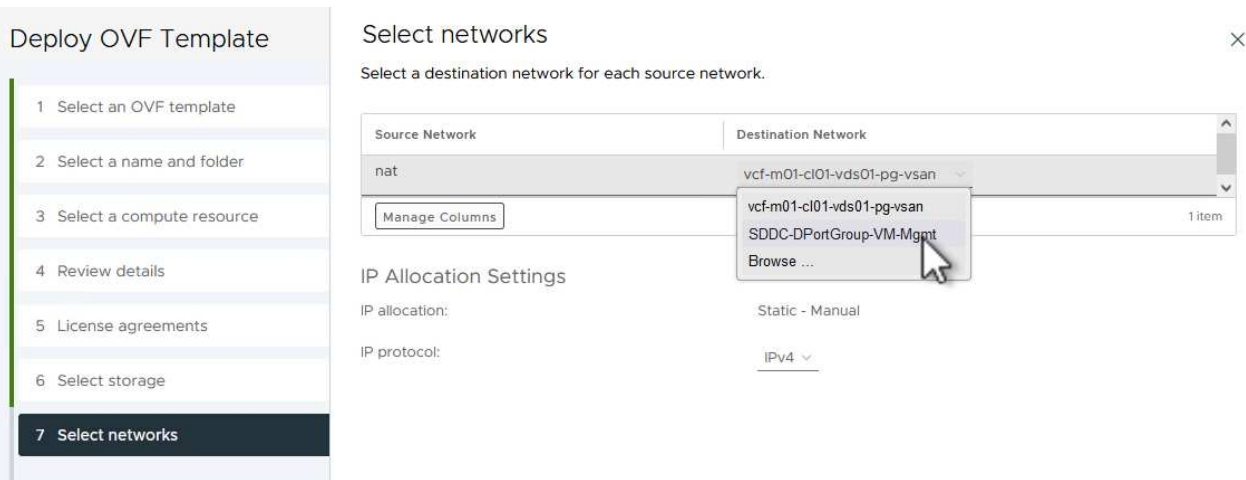
VM Storage Policy

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	vcf-m01-c01-ds-vsan01	--	999.97 GB	7.17 TB	225.72 GB	▼
<input type="radio"/>	vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
<input type="radio"/>	vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page 10 5 items

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



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

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

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

## Deploy OVF Template

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

## Customize template

Customize the deployment properties of this software solution.

! 2 properties have invalid values X

System Configuration		4 settings
<b>Application User Password (*)</b>	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	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>
<b>NTP Servers</b>	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	
<b>Maintenance User Password (*)</b>	Password to assign to maint user account.	
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>

## Deploy OVF Template

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

## Customize template

! 2 properties have invalid values X

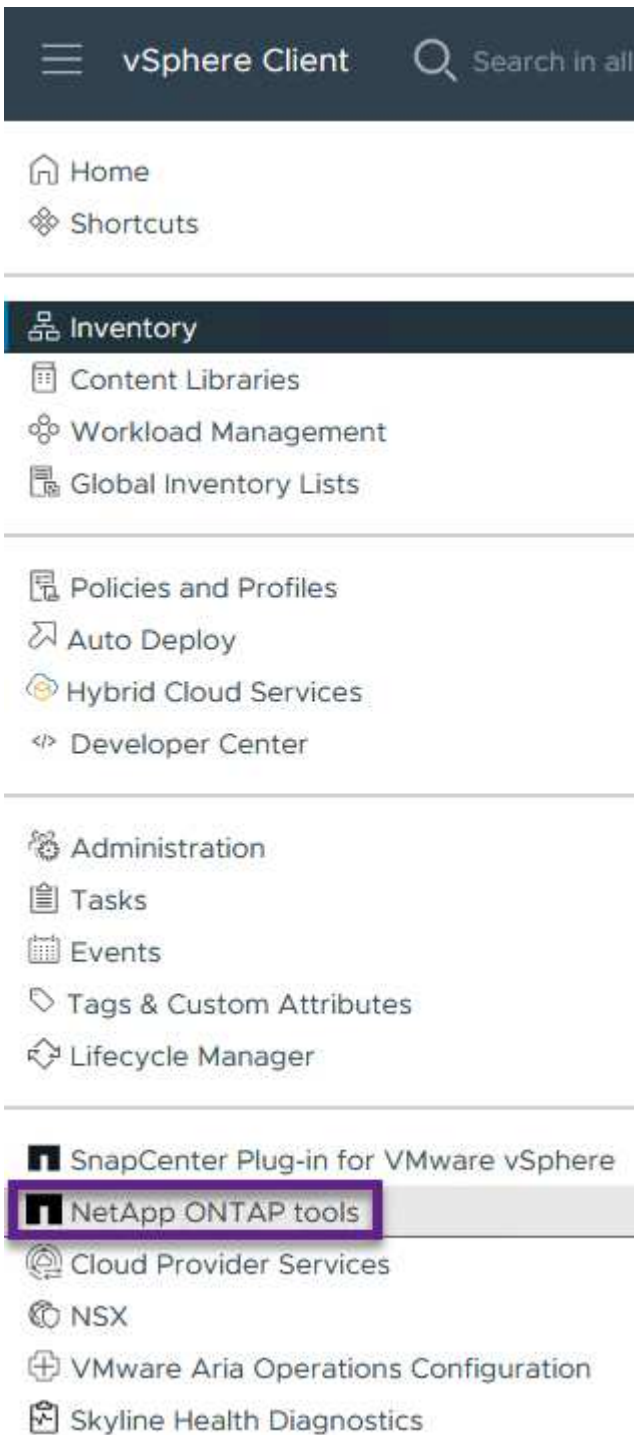
Configure vCenter or Enable vCenter		3 settings
<b>Enable VMware Cloud Foundation (VCF)</b>	vCenter server and user details are ignored when VCF is enabled. <input type="checkbox"/>	
<b>vCenter Server Address (*)</b>	Specify the IP address/hostname of an existing vCenter to register to. cf-wkld-vc01.sddc.netapp.com	
<b>Port (*)</b>	Specify the HTTPS port of an existing vCenter to register to. 443	
<b>Username (*)</b>	Specify the username of an existing vCenter to register to. administrator@vsphere.local	
<b>Password (*)</b>	Specify the password of an existing vCenter to register to.	
	Password	..... <span>👁</span>
	Confirm Password	..... <span>👁</span>
Network Properties		8 settings
<b>Host Name</b>	Specify the hostname for the appliance. (Leave blank if DHCP is desired) vcf-w01-otv9	
<b>IP Address</b>	Specify the IP address for the appliance. (Leave blank if DHCP is desired)	

CANCEL BACK NEXT

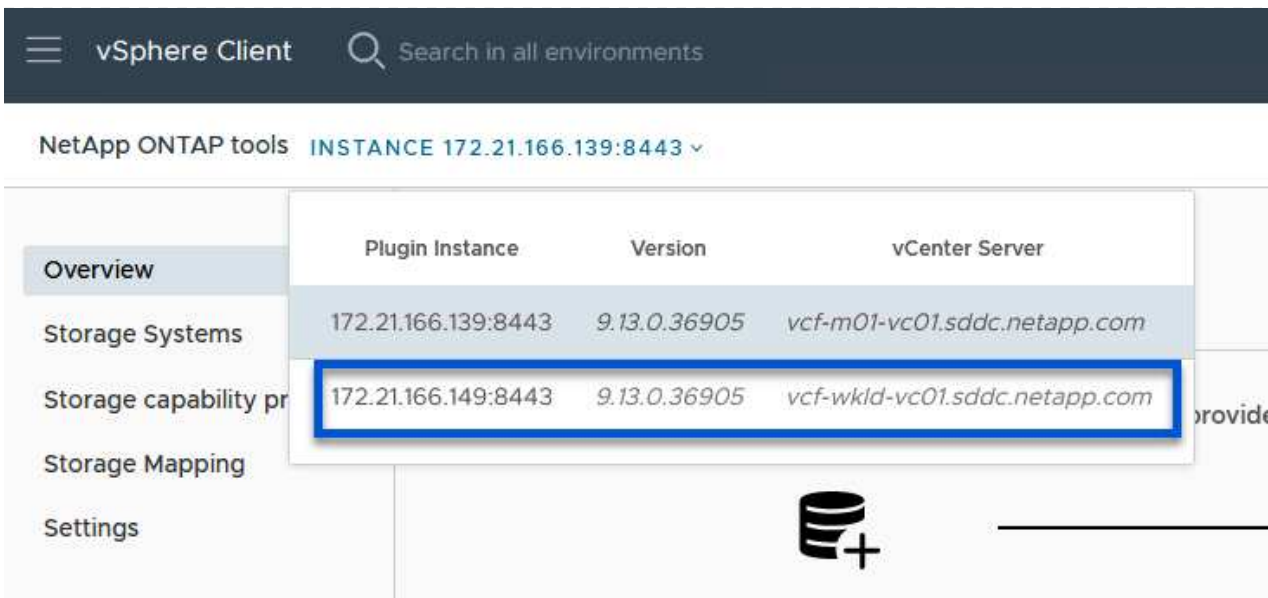
9. Überprüfen Sie alle Informationen auf der Seite bereit zur Fertigstellung, und klicken Sie auf Fertig stellen, um mit der Bereitstellung der OTV-Appliance zu beginnen.

## Fügen Sie ONTAP Tools ein Storage-System hinzu.

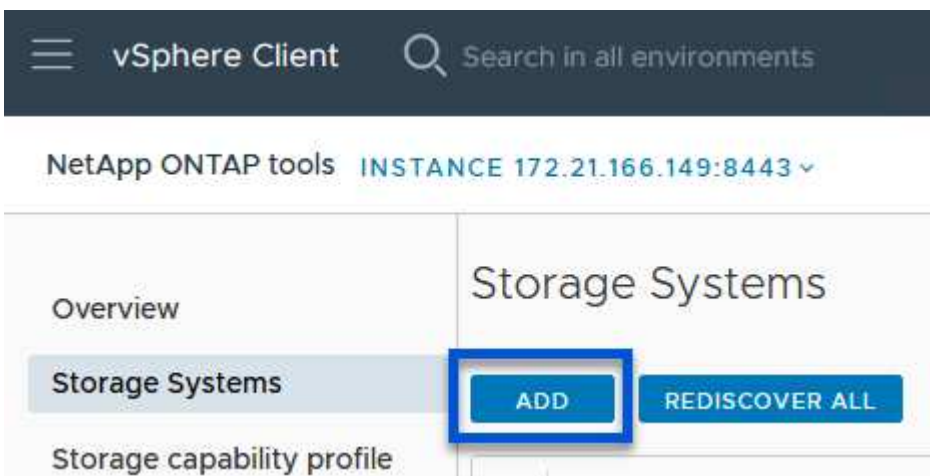
1. Greifen Sie auf die NetApp ONTAP-Tools zu, indem Sie sie im Hauptmenü des vSphere-Clients auswählen.



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.



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



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



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

## Add Storage System

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

vCenter server	<input type="text" value="vcf-m01-vc01.sddc.netapp.com"/> ▾
Name or IP address:	<input type="text" value="172.16.9.25"/>
Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="••••••••"/>
Port:	<input type="text" value="443"/>

Advanced options 

ONTAP Cluster Certificate:  Automatically fetch  Manually upload

CANCEL

SAVE & ADD MORE

ADD

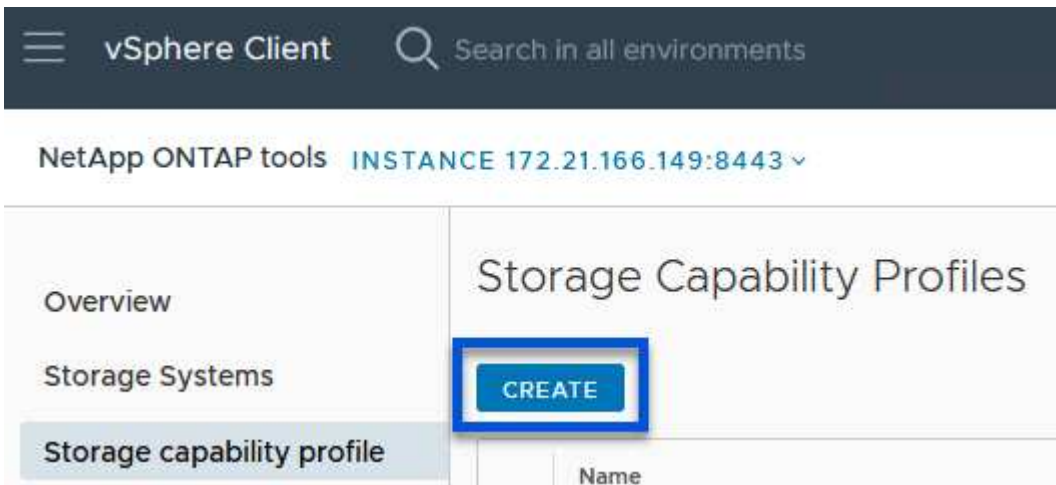


## Erstellen Sie in ONTAP-Tools ein Storage-Funktionsprofil

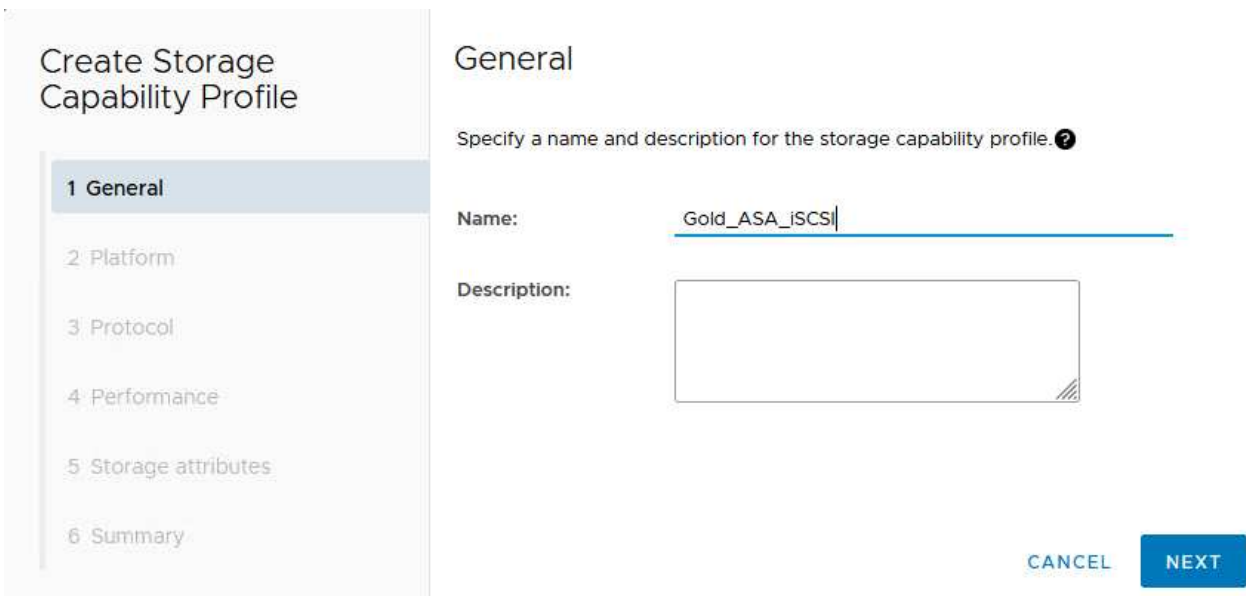
Storage-Funktionsprofile beschreiben die Funktionen eines Storage-Arrays oder Storage-Systems. Sie umfassen Definitionen zur Servicequalität und werden zur Auswahl von Storage-Systemen verwendet, die die im Profil definierten Parameter erfüllen. Eines der zur Verfügung gestellten Profile kann verwendet 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 in the 'General' step. On the left, a sidebar lists the steps: '1 General', '2 Platform', '3 Protocol', '4 Performance', '5 Storage attributes', and '6 Summary'. The 'General' step is selected. The main area contains the following fields: 'Name:' with the value 'Gold\_ASA\_iSCSI' entered, and 'Description:' with an empty text area. Below the fields, there are two buttons: 'CANCEL' and 'NEXT'. The 'NEXT' button is highlighted in blue.

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Protocol

Protocol:

Any

Any

FCP

iSCSI

NVMe/FC

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

\_\_\_\_\_

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

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

## Summary

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

CANCEL

BACK

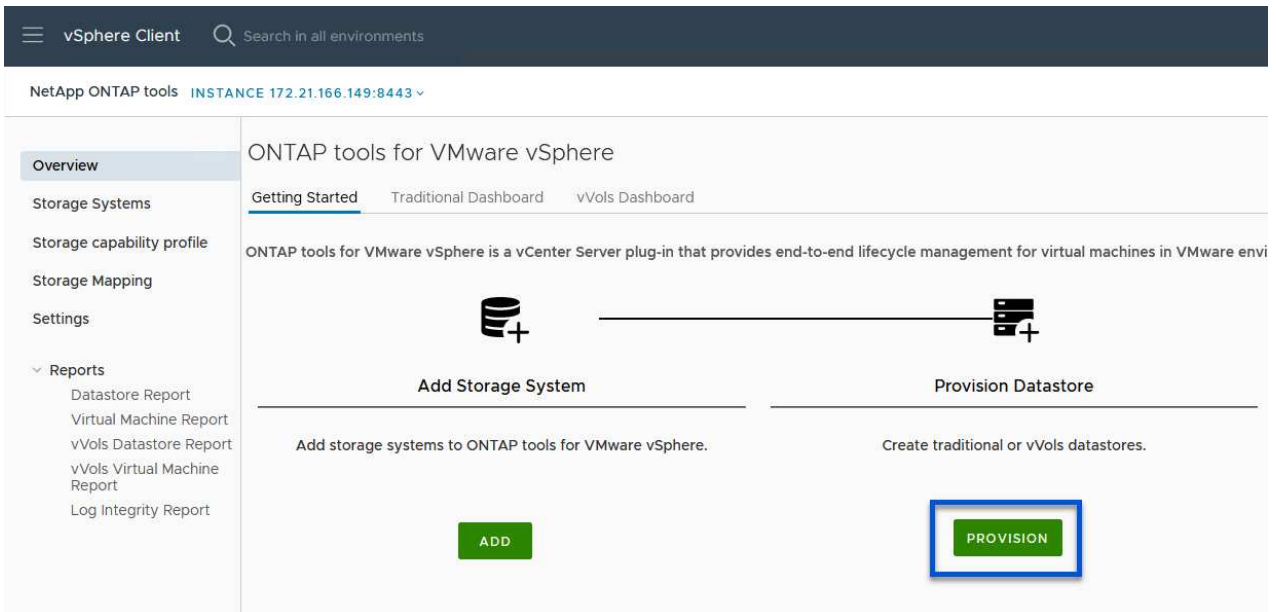
FINISH



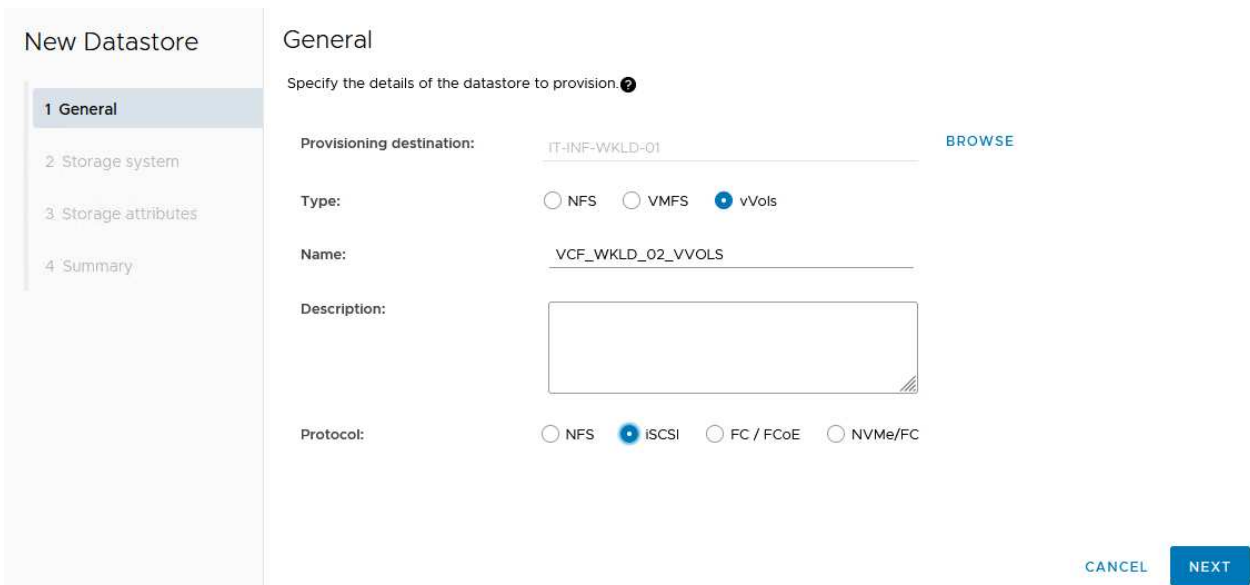
## Erstellen Sie einen VVols-Datstore in ONTAP Tools

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

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



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



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

## New Datastore

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

### Storage system

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

Storage capability profiles:

- AFF\_Encrypted\_Min50\_ASA\_A
- FAS\_Default
- FAS\_Max20
- Custom profiles
- ASA\_Gold\_iSCSI

Storage system: ntaphci-a300e9u25 (172.16.9.25)

Storage VM: VCF\_iSCSI

CANCEL BACK NEXT

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

## New Datastore

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

### Storage attributes

Specify the storage details for provisioning the datastore.

Volumes:  Create new volumes  Select volumes

Create new volumes

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

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

CANCEL BACK NEXT

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

### New Datastore

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

### Summary

Datastore type: vVols  
 Protocol: iSCSI  
 Storage capability profile: ASA\_Gold\_iSCSI

**Storage system details**

Storage system: ntaphcl-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

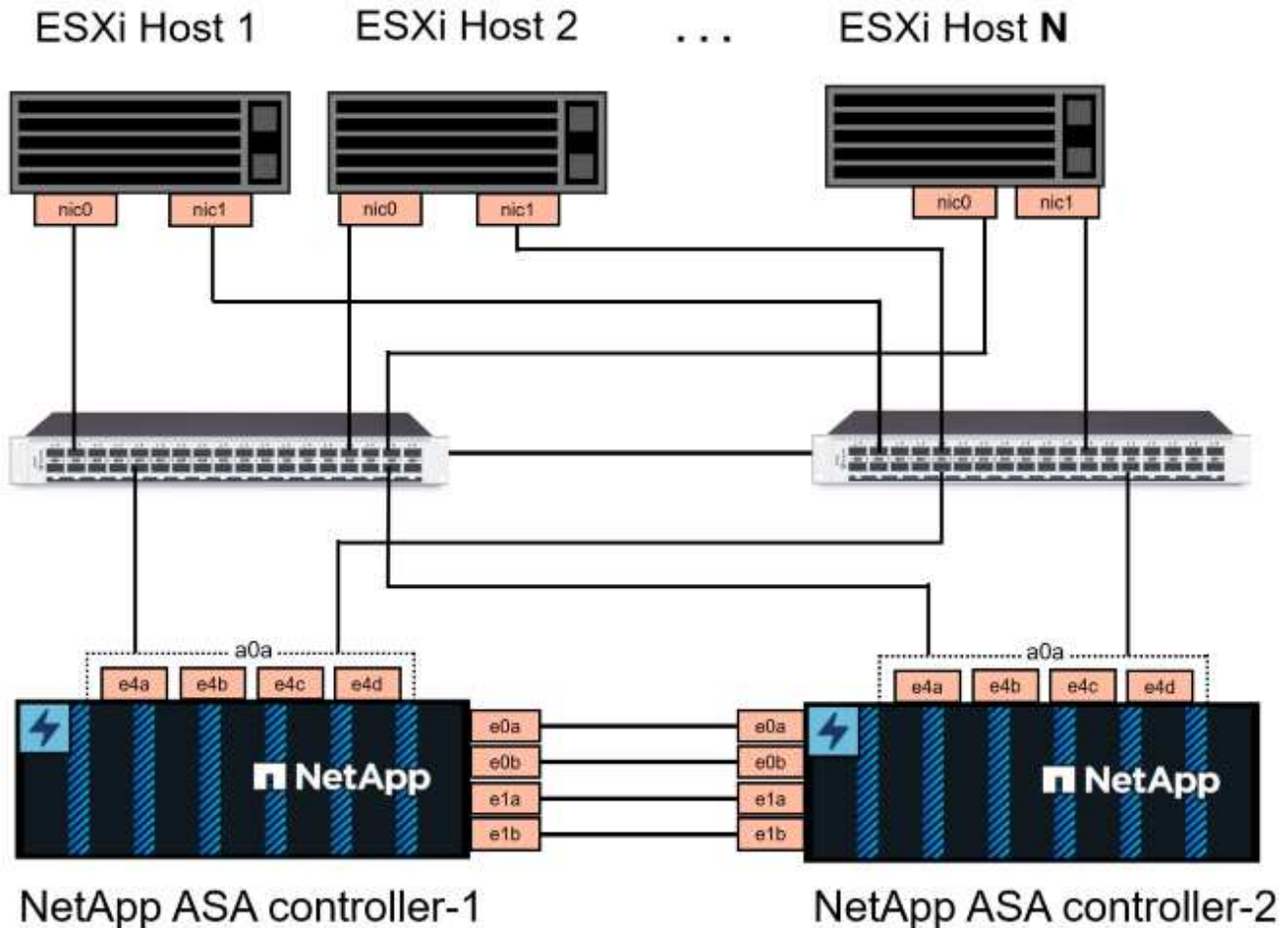
#### Voraussetzungen

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.



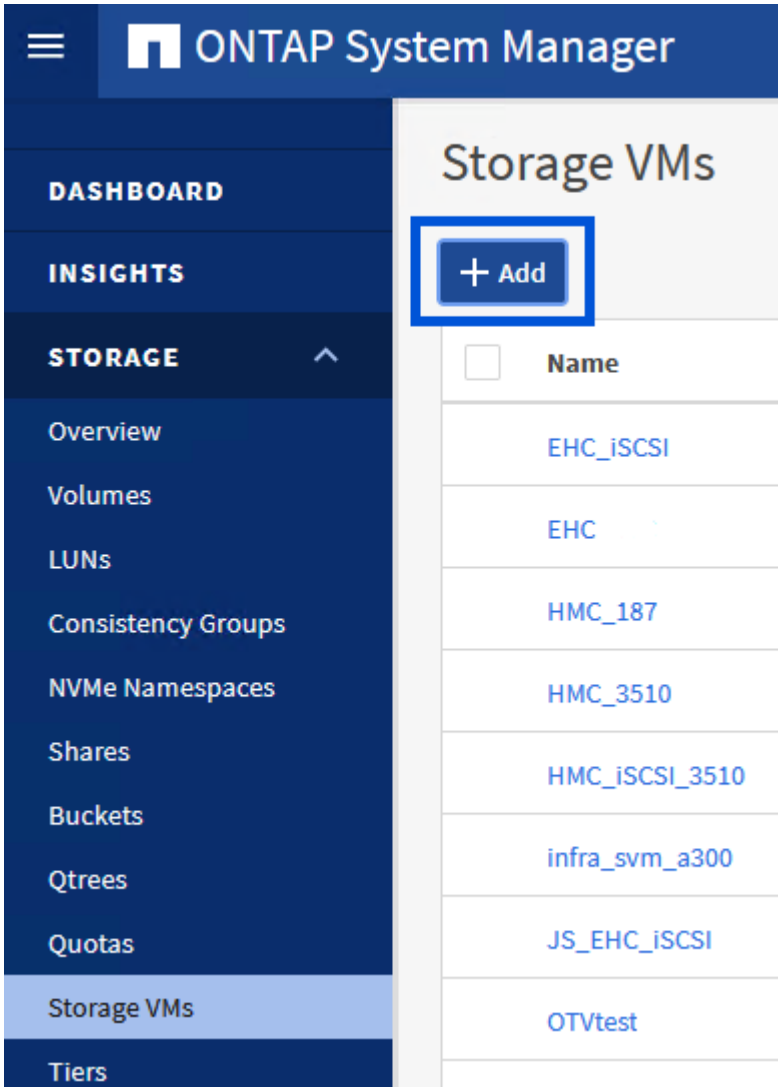
## **Erstellung von SVMs, LIFs und NVMe Namespace auf dem ONTAP Storage-System**

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-Namespaces

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

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

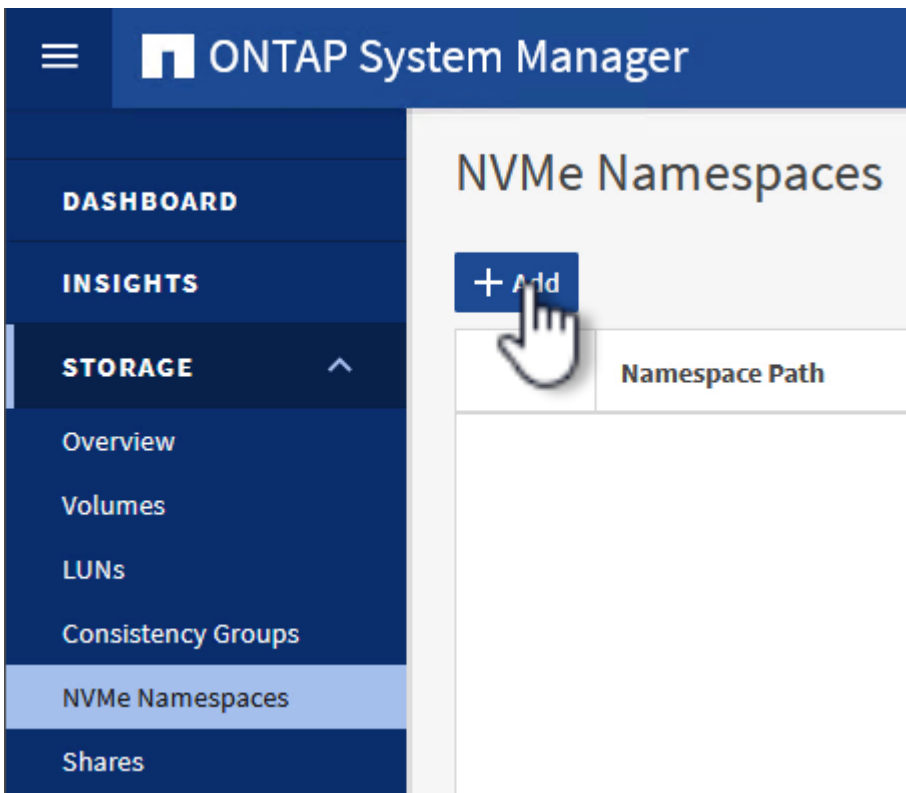
1. Öffnen Sie eine SSH-Sitzung mit einem ESXi-Host im Cluster, um dessen NQN zu erhalten. Verwenden Sie den folgenden Befehl aus der CLI:

```
esxcli nvme info get
```

Es sollte eine Ausgabe ähnlich der folgenden angezeigt werden:

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

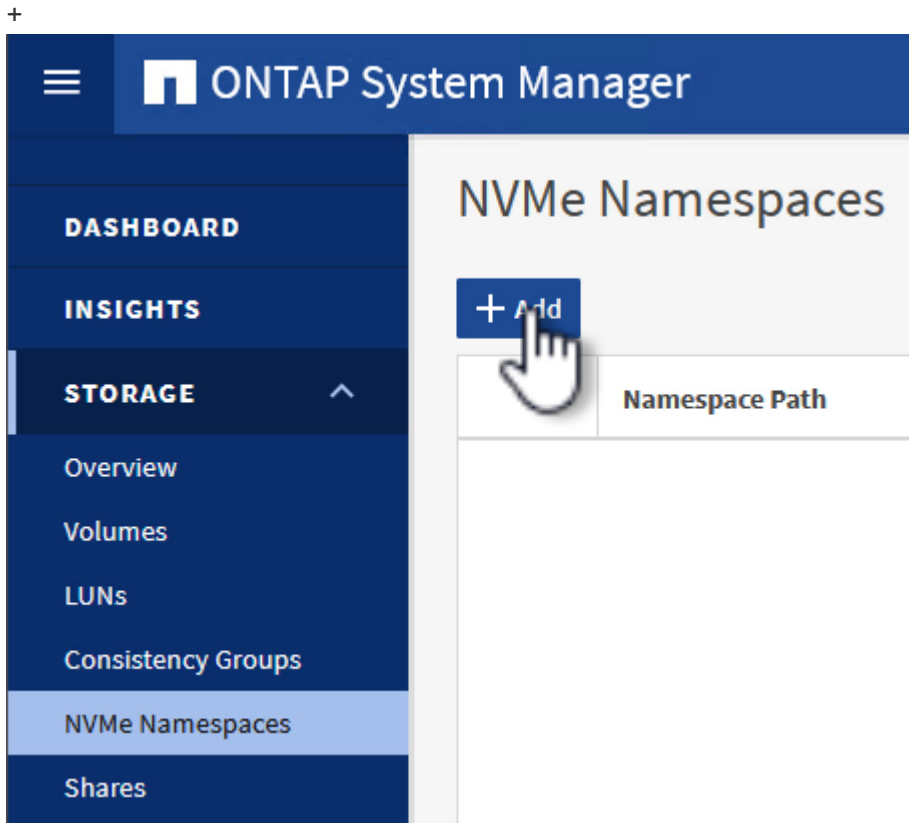
2. Notieren Sie die NQN für jeden ESXi-Host im Cluster
3. Navigieren Sie im ONTAP-Systemmanager im linken Menü zu **NVMe Namespaces** und klicken Sie auf **+ Hinzufügen**, um zu starten.



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

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

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



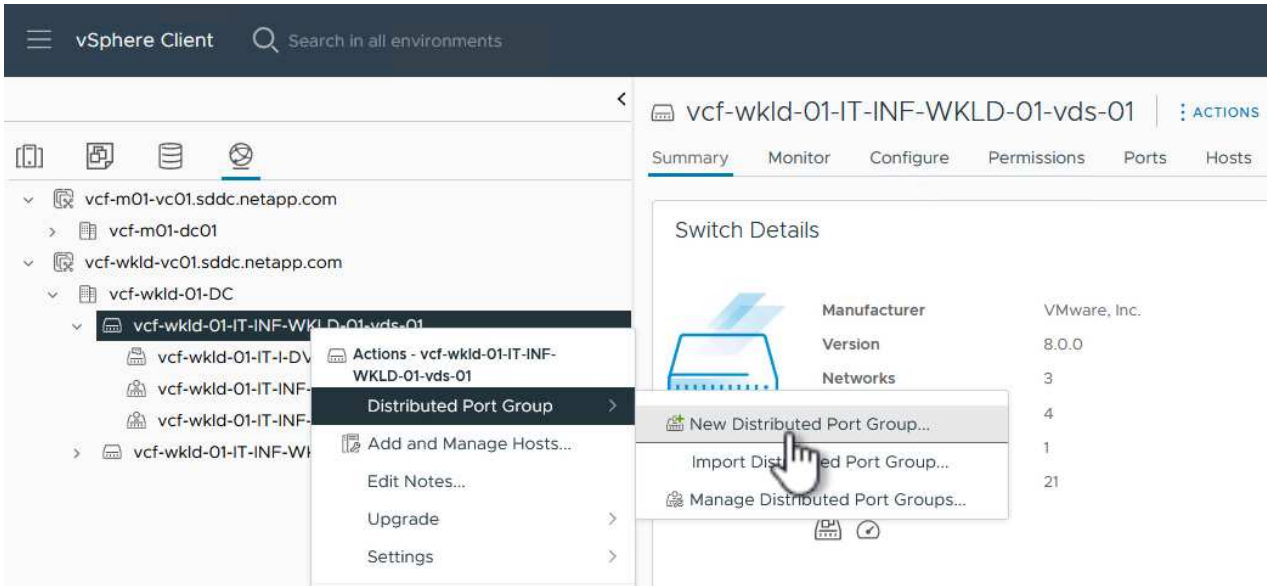
### Richten Sie Netzwerk- und NVMe-Softwareadapter auf ESXi-Hosts ein

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

## Verteilte Portgruppen für NVMe/TCP-Datenverkehr erstellen

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

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



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



## New Distributed Port Group

1 Name and location

2 **Configure settings**

3 Ready to complete

### Configure settings

Set general properties of the new port group.

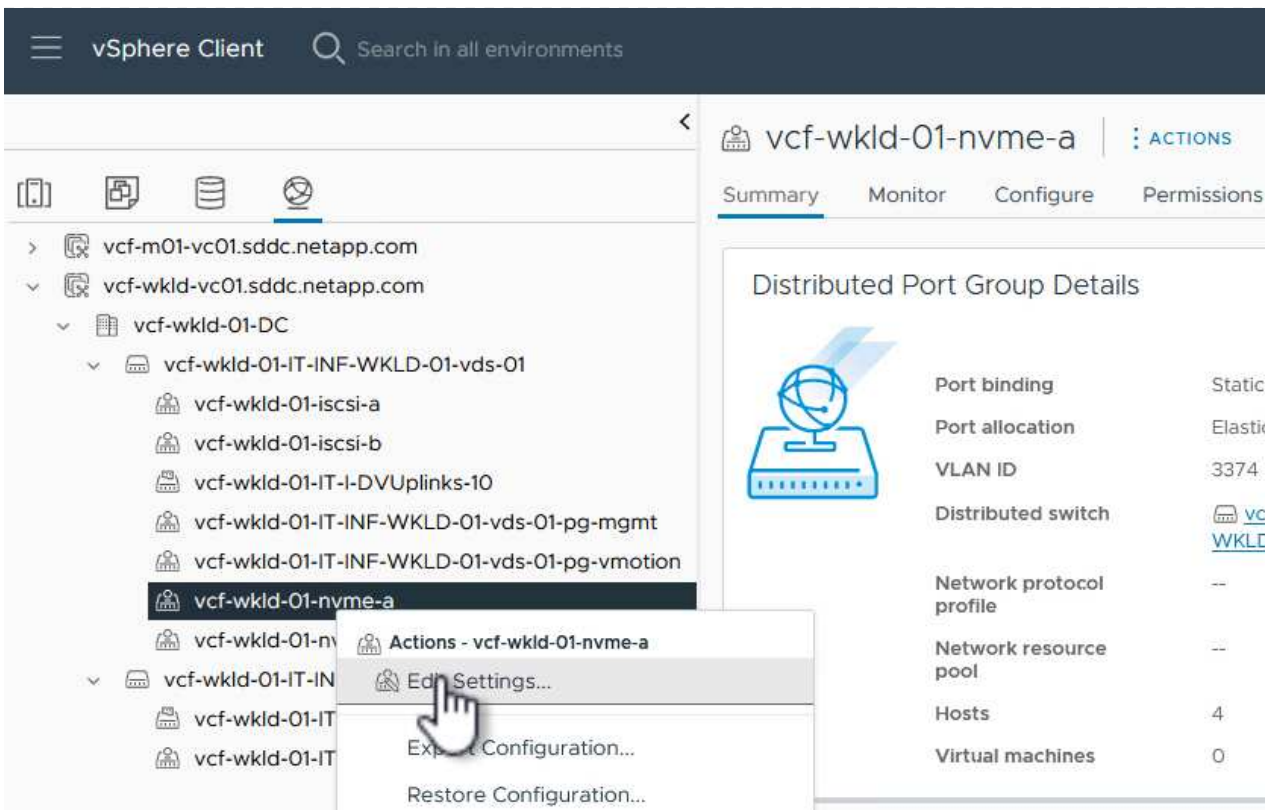
Port binding	Static binding
Port allocation	Elastic <span>?</span>
Number of ports	8
Network resource pool	(default)
VLAN	
VLAN type	VLAN
VLAN ID	3374
Advanced	
<input type="checkbox"/> Customize default policies configuration	

CANCEL

BACK

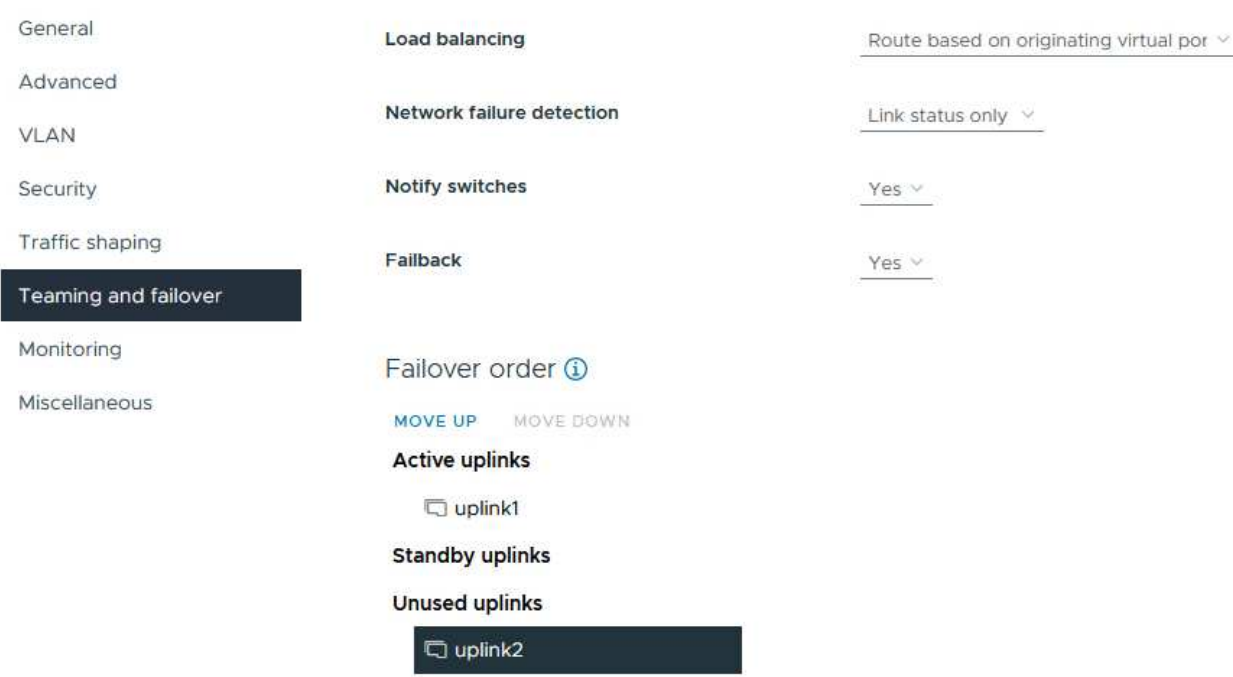
NEXT

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



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

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



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

## Mal Uplink1 zu unbenutzten Uplinks.

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

General

Advanced

VLAN

Security

Traffic shaping

**Teaming and fallover**

Monitoring

Miscellaneous

**Load balancing**

Route based on originating virtual por

**Network failure detection**

Link status only

**Notify switches**

Yes

**Failback**

Yes

Failover order 

[MOVE UP](#) [MOVE DOWN](#)

**Active uplinks**

 uplink2

**Standby uplinks**

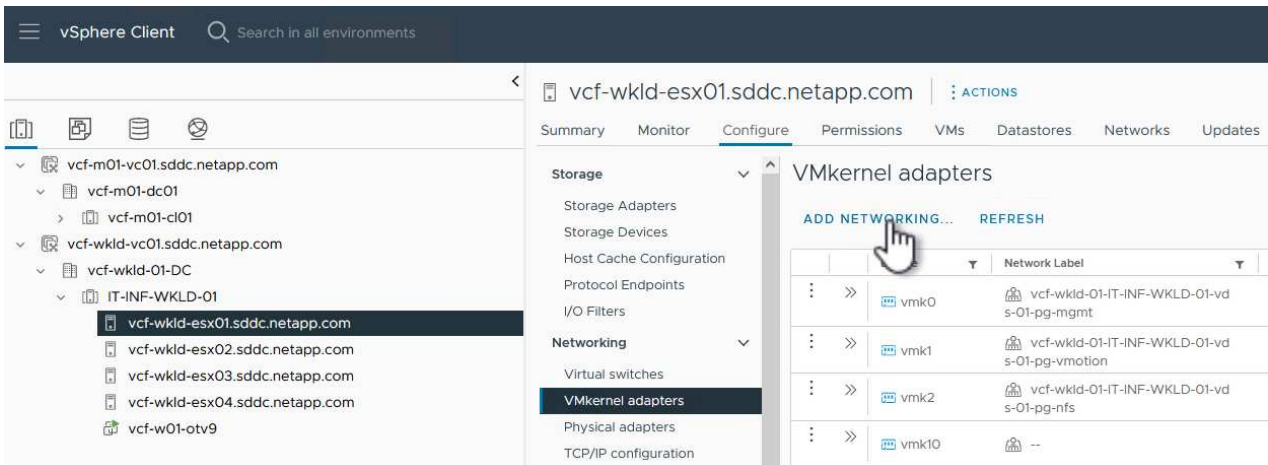
**Unused uplinks**

 uplink1

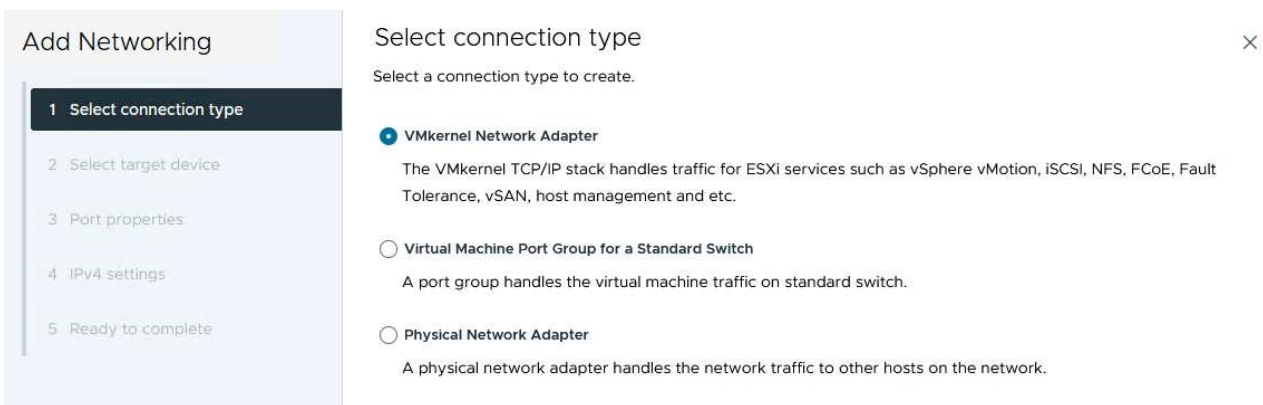
## Erstellen Sie VMkernel-Adapter auf jedem ESXi-Host

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

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



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



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

## Add Networking

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



## Select target device

Select a target device for the new connection.

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

Quick Filter

Enter value

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

Manage Columns 7 Items

CANCEL

BACK

NEXT

Packages

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

### Add Networking

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

### Port properties

Specify VMkernel port settings.

**Network label**

**MTU**

**TCP/IP stack**

**Available services**

**Enabled services**

<input checked="" type="checkbox"/> vMotion	<input type="checkbox"/> vSphere Replication NFC	<input type="checkbox"/> NVMe over RDMA
<input type="checkbox"/> Provisioning	<input type="checkbox"/> vSAN	
<input type="checkbox"/> Fault Tolerance logging	<input type="checkbox"/> vSAN Witness	
<input type="checkbox"/> Management	<input type="checkbox"/> vSphere Backup NFC	
<input type="checkbox"/> vSphere Replication	<input checked="" type="checkbox"/> NVMe over TCP	

CANCEL BACK NEXT

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

### Add Networking

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

### IPv4 settings

Specify VMkernel IPv4 settings.

Obtain IPv4 settings automatically

Use static IPv4 settings

**IPv4 address**

**Subnet mask**

**Default gateway**  Override default gateway for this adapter

**DNS server addresses**

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

## Add Networking

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

## Ready to complete

Review your selections before finishing the wizard

### ▼ Select target device

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

### ▼ Port properties

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

### ▼ IPv4 settings

IPv4 address	172.21.118.191 (static)
Subnet mask	255.255.255.0

CANCEL

BACK

FINISH

Packages

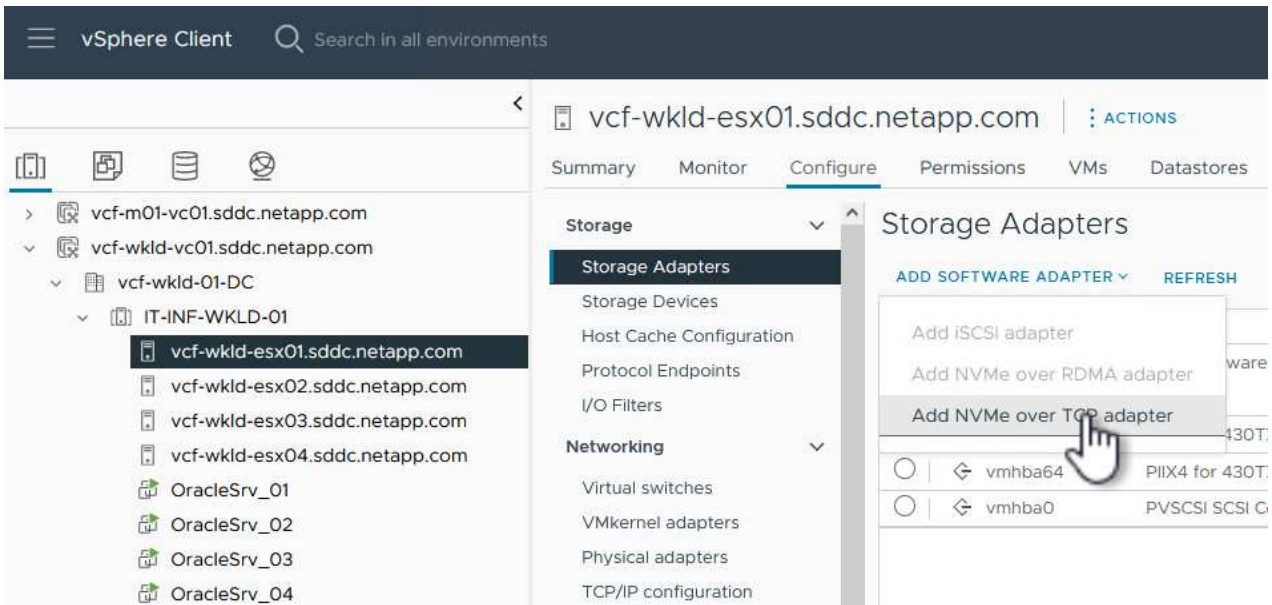
7. Wiederholen Sie diesen Vorgang, um einen VMkernel Adapter für das zweite iSCSI-Netzwerk zu erstellen.

## Fügen Sie einen NVMe-over-TCP-Adapter hinzu

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

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

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



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

Add Software NVMe over TCP adapter

vcf-wkld-esx01.sddc.netapp.com

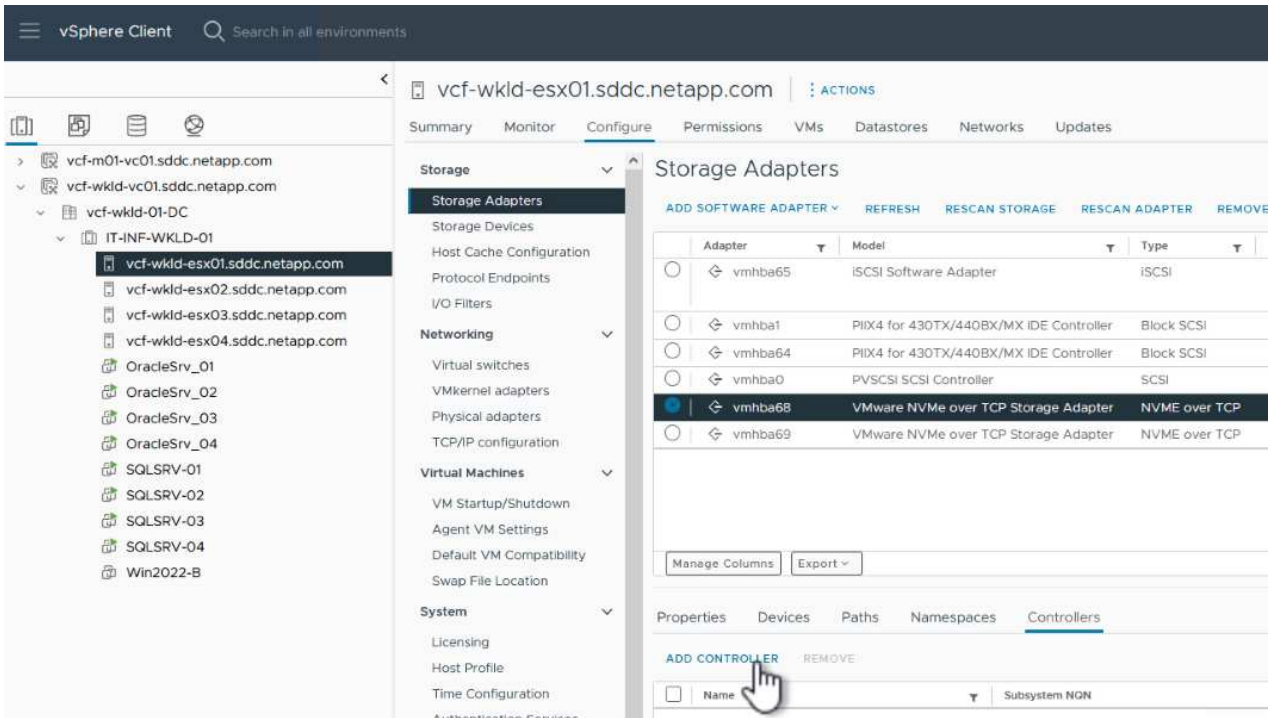
Enable software NVMe adapter on the selected physical network adapter.

Physical Network Adapter





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



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

## Add controller | vmhba68



Automatically

Manually

Host NQN

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

COPY

IP

1

172.21.118.189

Enter IPv4 / IPv6 address

Central discovery controller

Port Number

Range more from 0

Digest parameter

Header digest

Data digest

DISCOVER CONTROLLERS

2

Select which controller to connect

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

Manage Columns 4 items

3

4

OK

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

## Storage Adapters

ADD SOFTWARE ADAPTER ▾ REFRESH RESCAN STORAGE RESCAN ADAPTER REMOVE

Adapter	Model	Type	Status	Identifier	Targets	Devices	Paths
vmhba65	iSCSI Software Adapter	iSCSI	Online	iscsi_vmk(iqn.1998-01.com.vmware:vcf-wkld-esx01.sddc.net app.com:794177624:65)	4	2	8
vmhba1	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	1	1	1
vmhba64	PIIX4 for 430TX/440BX/MX IDE Controller	Block SCSI	Unknown	--	0	0	0
vmhba0	PVSCSI SCSI Controller	SCSI	Unknown	--	3	3	3
vmhba68	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	1	1	1
vmhba69	VMware NVMe over TCP Storage Adapter	NVME over TCP	Online	--	0	0	0

Manage Columns Export ▾ 6 items

Properties **Devices** Paths Namespaces Controllers

REFRESH ATTACH DETACH RENAME

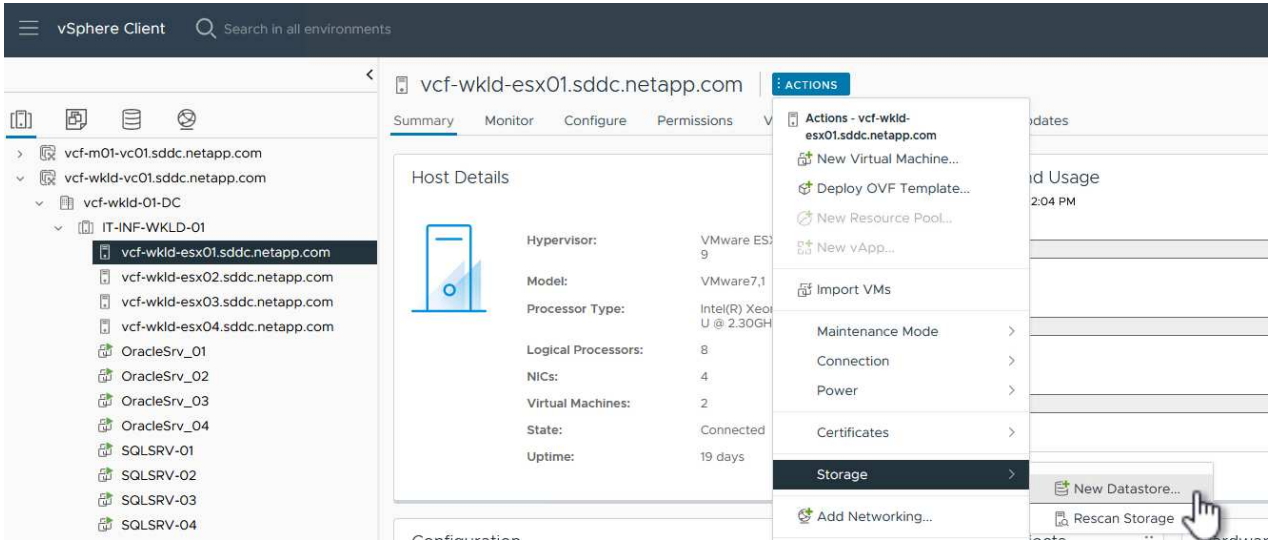
Name	LUN	Type	Capacity	Datastore	Operational State	Hardware Acceleration	Drive Type	Transport
NVMe TCP Disk (uuid.929a6a9045764784 9146e09d6e55b076)	0	disk	3.00 TB	Not Consumed	Attached	Supported	Flash	TCPTRAN: RT

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

## NVMe over TCP Datastore implementieren

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

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



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

## New Datastore

1 Type

2 Name and device selection

3 VMFS version

4 Partition configuration

5 Ready to complete

## Name and device selection

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

Name

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

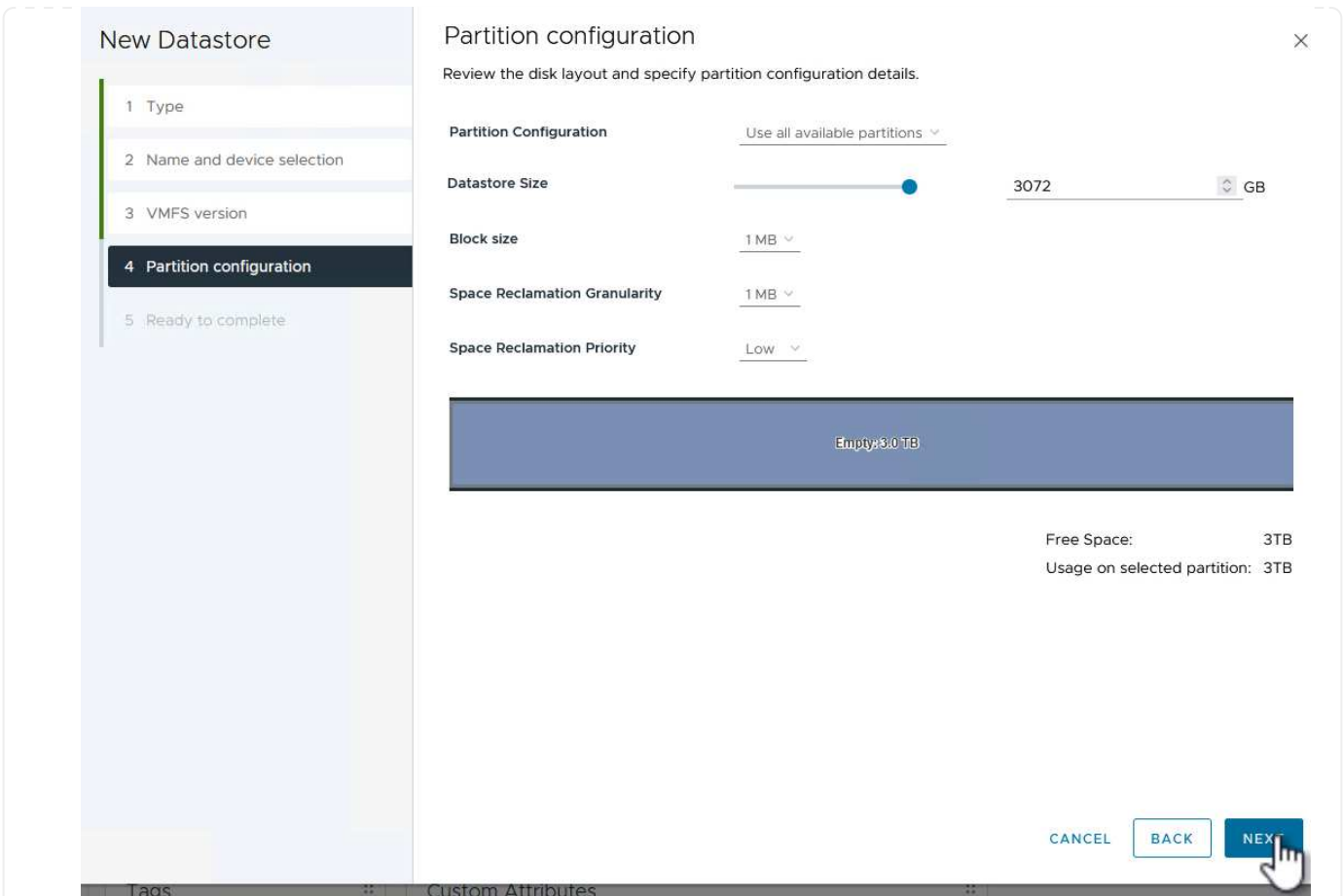
Manage Columns Export 3 items

CANCEL

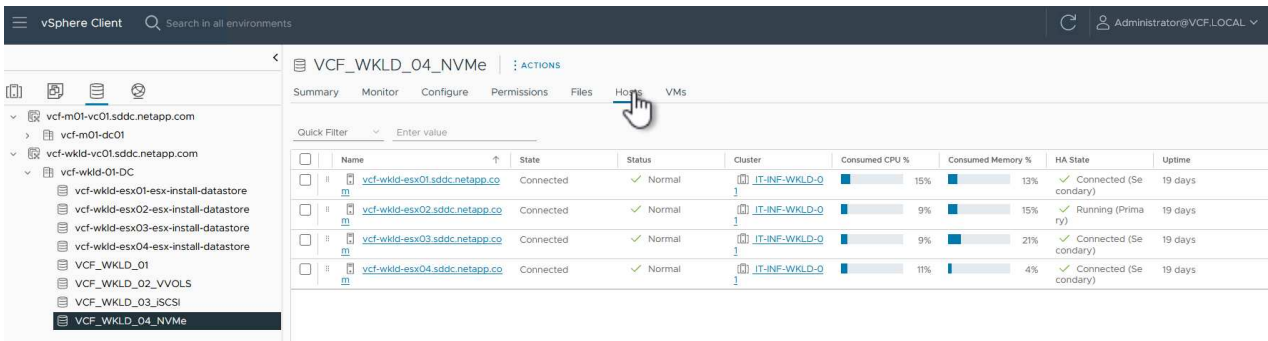
BACK

NEXT

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



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



## Weitere Informationen

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

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

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

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

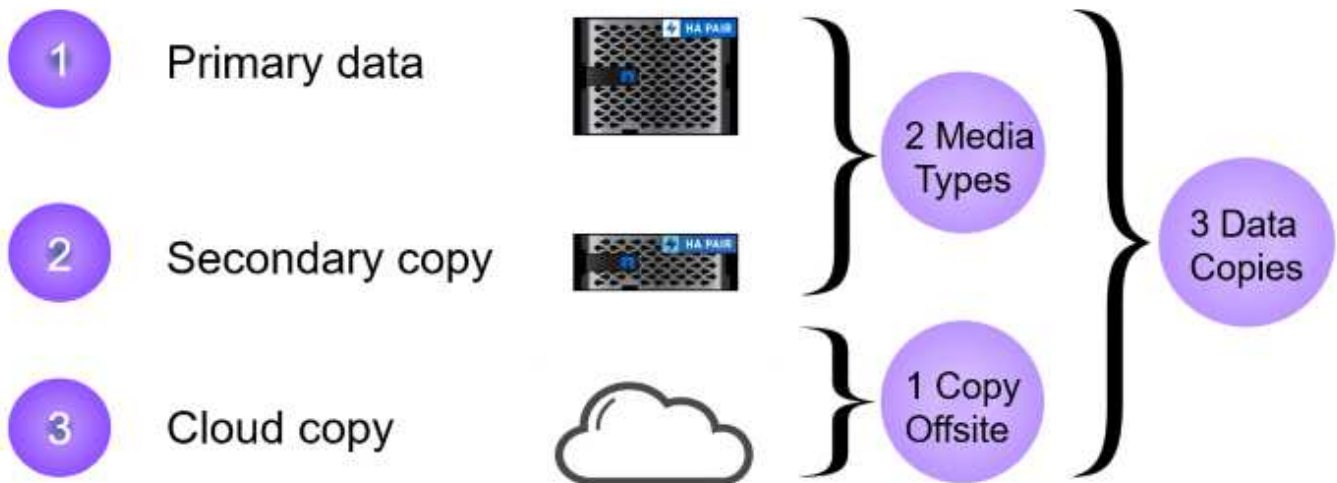
Dieses Szenario erfordert die folgenden Komponenten und Konfigurationen:

- 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:

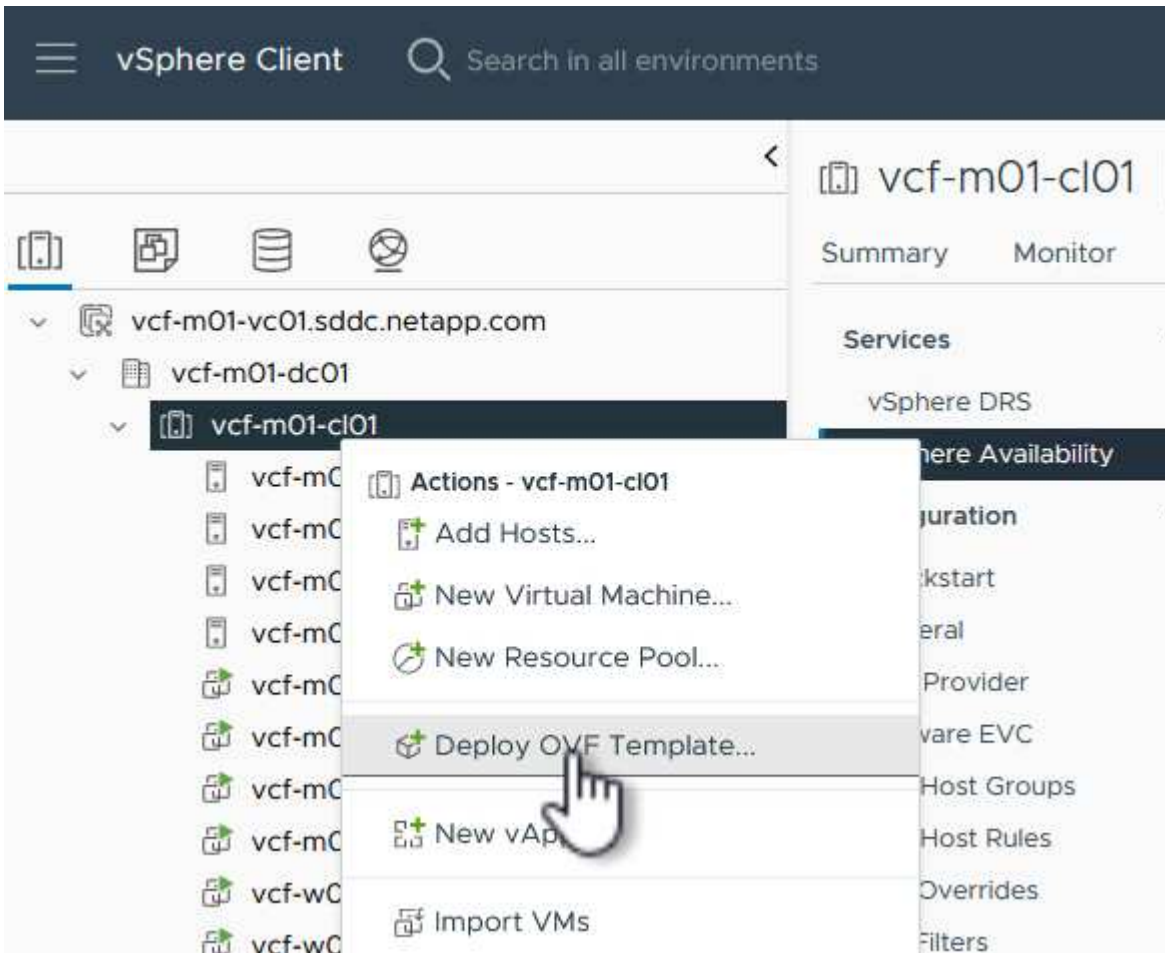


## Implementieren Sie das SnapCenter Plug-in für VMware vSphere

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.OP2-240310\_1514.ova

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

## Deploy OVF Template

1 Select an OVF template

2 Select a name and folder

3 Select a compute resource

4 Review details

5 License agreements

6 Select storage

7 Select networks

8 Customize template

9 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine ⓘ

Select virtual disk format Thin Provision ▾

VM Storage Policy Datastore Default ▾

Disable Storage DRS for this virtual machine

Name	Storage Compatibility	Capacity	Provisioned	Free	
mgmt_01_iscsi	--	3 TB	3.71 TB	2.5 TB	▼
vcf-m01-cl01-ds-vsant01	--	999.97 GB	49.16 GB	957.54 GB	▼
vcf-m01-esx01-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
vcf-m01-esx02-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
vcf-m01-esx03-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼
vcf-m01-esx04-esx-install-datastore	--	25.75 GB	4.56 GB	21.19 GB	▼

Manage Columns Items per page: 10 6 items

### Compatibility

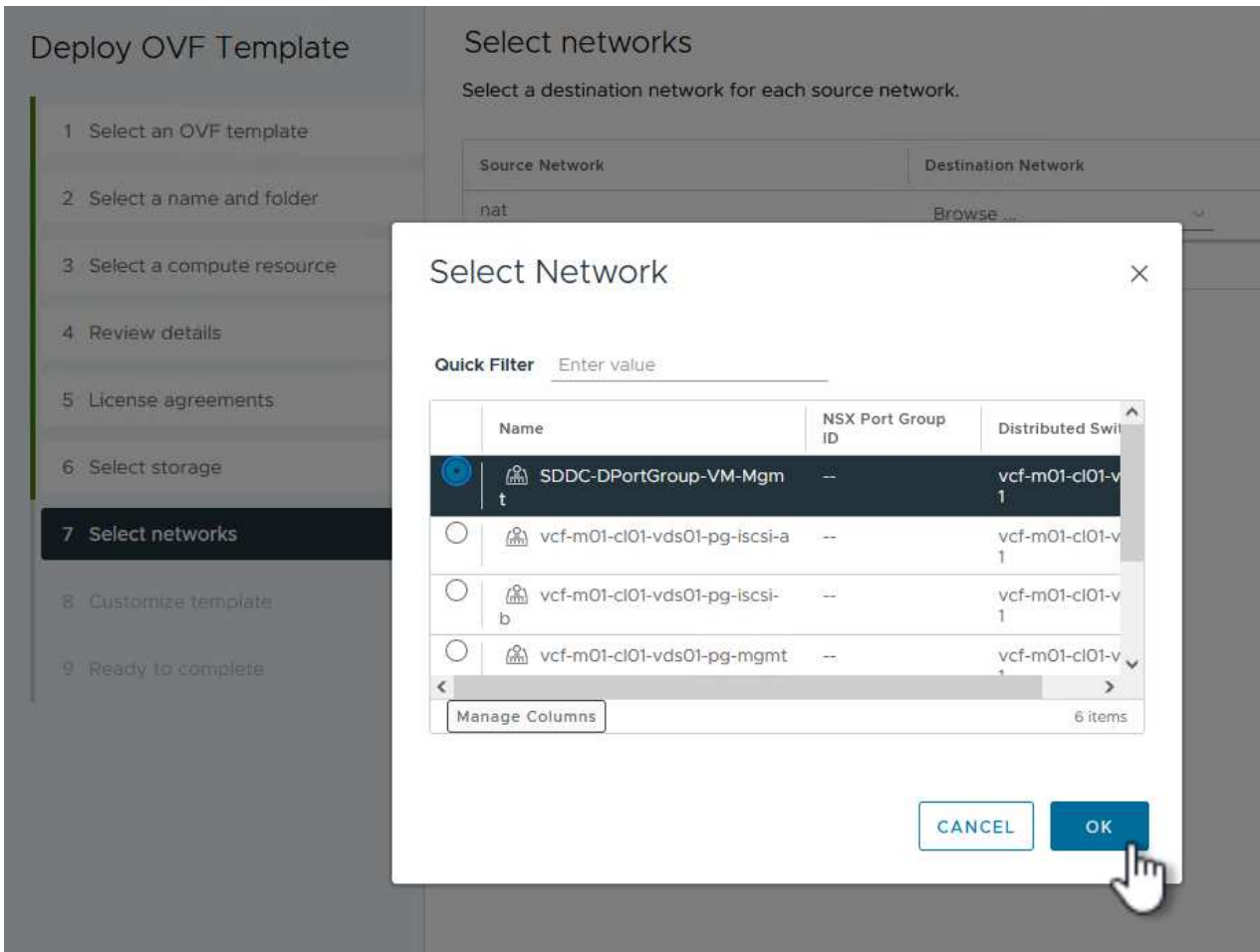
✓ Compatibility checks succeeded.

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.

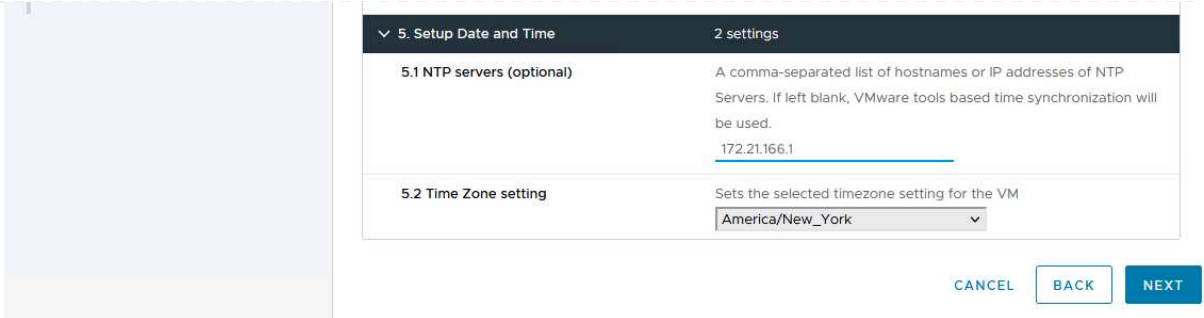
<b>1. Register to existing vCenter</b>		4 settings
1.1 vCenter Name(FQDN) or IP Address	<input type="text" value="cf-wkld-vc01.sddc.netapp.com"/>	
1.2 vCenter username	<input type="text" value="administrator@vcf.local"/>	
1.3 vCenter password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
1.4 vCenter port	<input type="text" value="443"/>	
<b>2. Create SCV Credentials</b>		2 settings
2.1 Username	<input type="text" value="admin"/>	
2.2 Password	Password	<input type="password" value="....."/>
	Confirm Password	<input type="password" value="....."/>
<b>3. System Configuration</b>		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

<b>4.2 Setup IPv4 Network Properties</b>		6 settings
4.2.1 IPv4 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.148"/>	
4.2.2 IPv4 Netmask	Subnet to use on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="255.255.255.0"/>	
4.2.3 IPv4 Gateway	Gateway on the deployed network. (Leave blank if DHCP is desired) <input type="text" value="172.21.166.1"/>	
4.2.4 IPv4 Primary DNS	Primary DNS server's IP address. (Leave blank if DHCP is desired) <input type="text" value="10.61.185.231"/>	
4.2.5 IPv4 Secondary DNS	Secondary DNS server's IP address. (optional - Leave blank if DHCP is desired) <input type="text" value="10.61.186.231"/>	
4.2.6 IPv4 Search Domains (optional)	Comma separated list of search domain names to use when resolving host names. (Leave blank if DHCP is desired) <input type="text" value="netapp.com,sddc.netapp.com"/>	
<b>3.3 Setup IPv6 Network Properties</b>		6 settings
4.3.1 IPv6 Address	IP address for the appliance. (Leave blank if DHCP is desired) <input type="text"/>	
4.3.2 IPv6 PrefixLen	Prefix length to use on the deployed network. (Leave blank if DHCP is desired) <input type="text"/>	

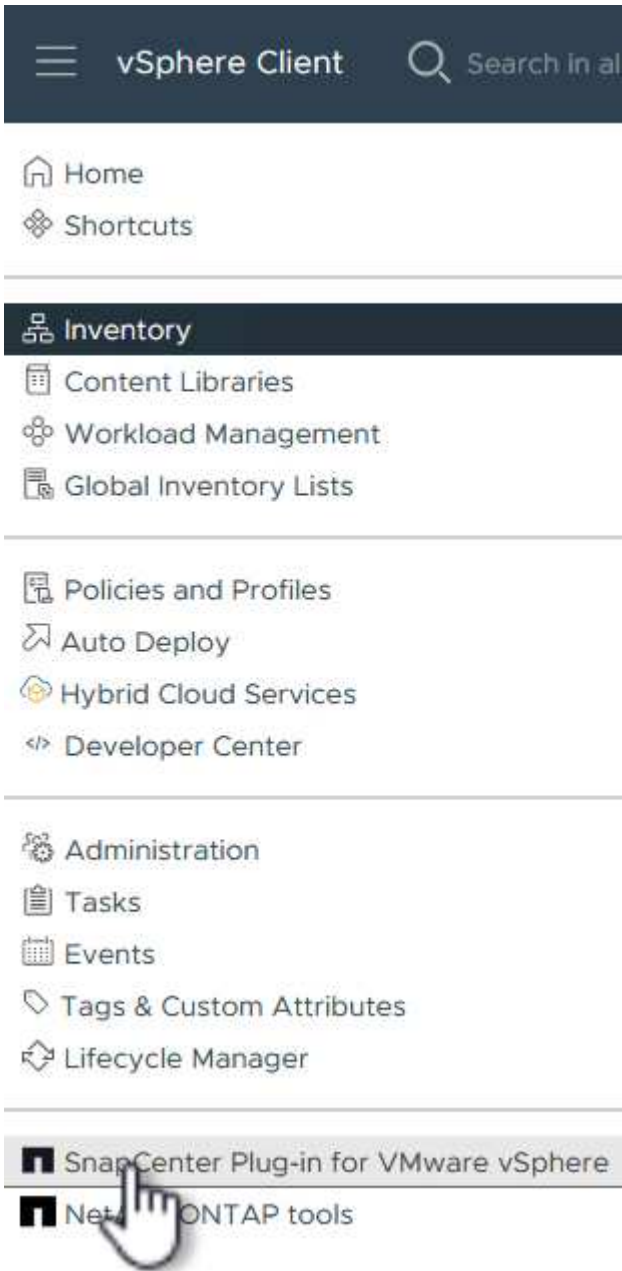


10. Überprüfen Sie abschließend auf der Seite **bereit zur Fertigstellung** alle Einstellungen und klicken Sie auf Fertig stellen, um die Bereitstellung zu starten.

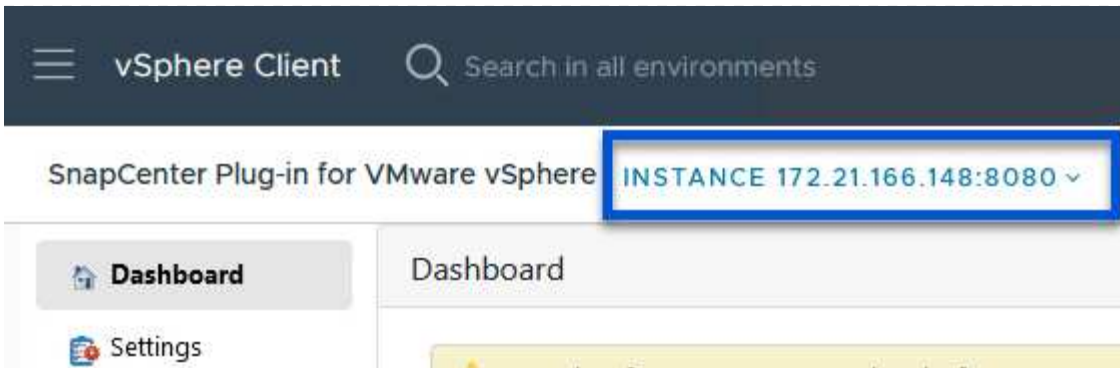
## Fügen Sie dem SCV Speichersysteme hinzu

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

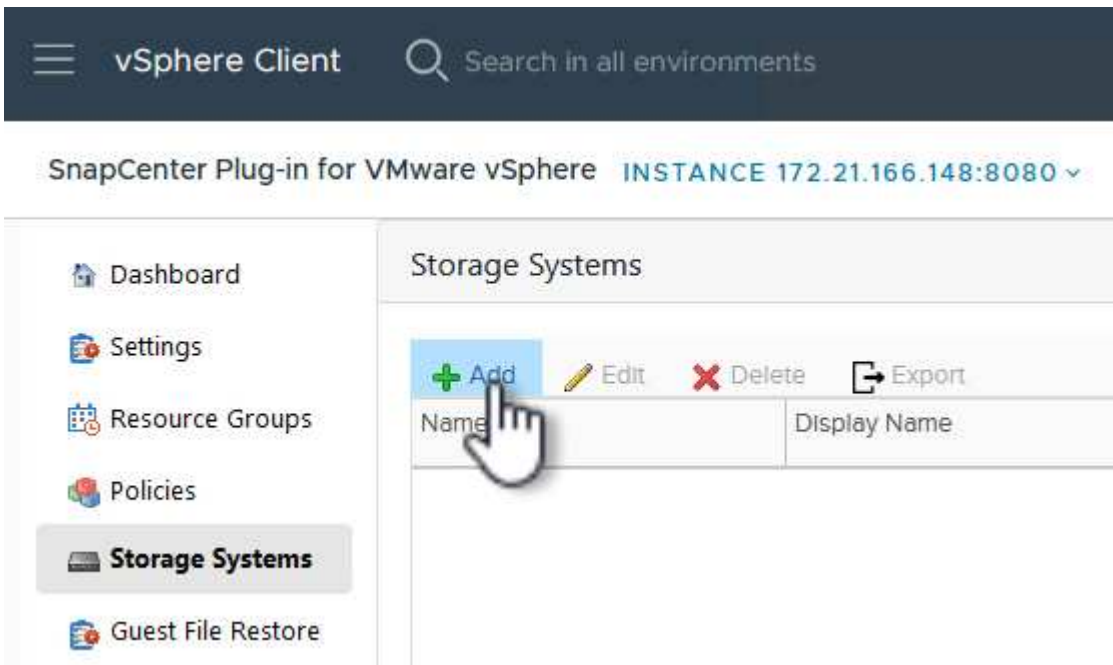
1. Auf SCV kann über das Hauptmenü im vSphere Client zugegriffen werden.



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



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



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

## Add Storage System



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

### Event Management System(EMS) & AutoSupport Setting

- Log Snapcenter server events to syslog
- Send AutoSupport Notification for failed operation to storage system

CANCEL

ADD



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

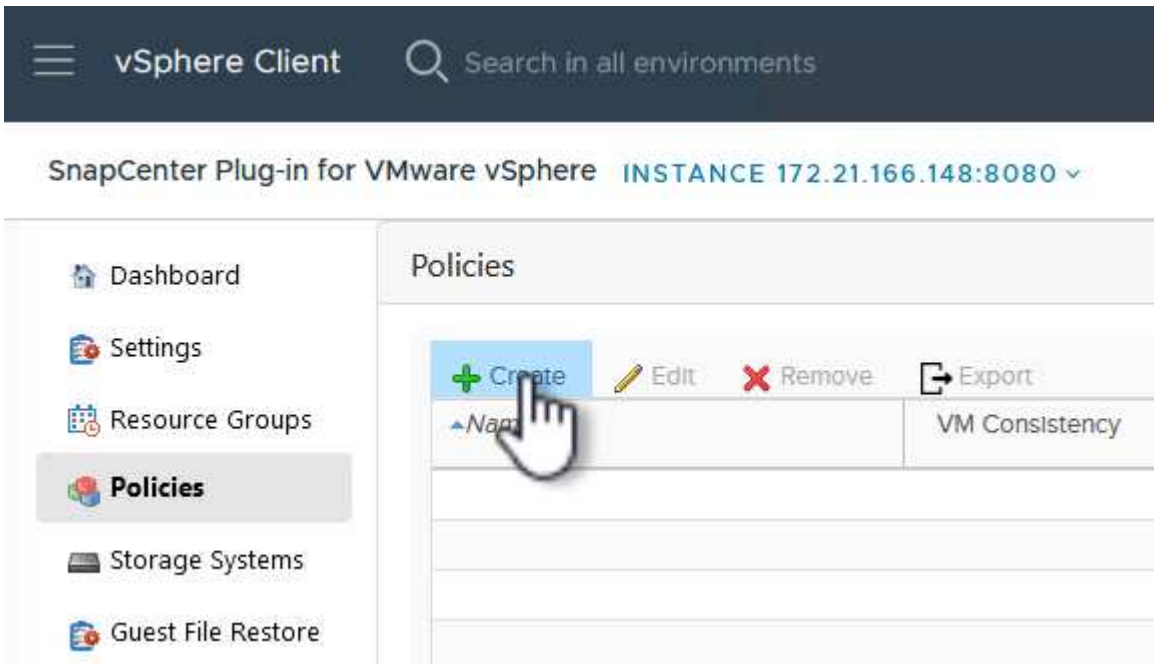


## Konfigurieren Sie Backup-Richtlinien in SCV

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**

**Description**

**Frequency**

**Locking Period**  Enable Snapshot Locking ⓘ

**Retention**   ⓘ

**Replication**  Update SnapMirror after backup ⓘ  
 Update SnapVault after backup ⓘ

Snapshot label

**Advanced** ▾  VM consistency ⓘ  
 Include datastores with independent disks

**Scripts** ⓘ

CANCEL

ADD

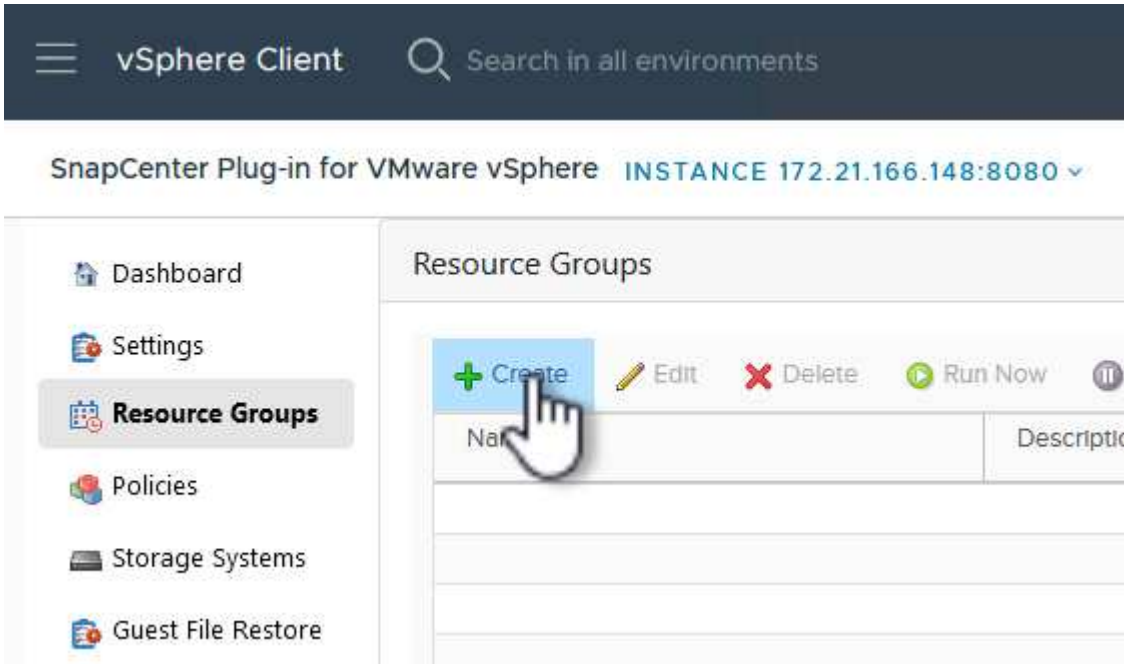


## Erstellen Sie Ressourcengruppen in SCV

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

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

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



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



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

## Create Resource Group

1. General info & notification

2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Scope: Virtual Machines

Parent entity: VCF\_WKLD\_03\_iSCSI

Enter available entity name

Available entities

OracleSrv\_01  
OracleSrv\_02  
OracleSrv\_03  
OracleSrv\_04

Selected entities

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

BACK

NEXT

FINISH

CANCEL

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

## Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

3. Spanning disks

4. Policies

5. Schedules

6. Summary

Always exclude all spanning datastores

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

Always include all spanning datastores

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

Manually select the spanning datastores to be included ⓘ

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

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

BACK

NEXT

FINISH

CANCEL

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



## Create Resource Group

✓ 1. General info & notification

✓ 2. Resource

✓ 3. Spanning disks

✓ 4. Policies

5. Schedules

6. Summary

Daily\_Snapmi... ▼

Type Daily

Every 1 Day(s)

Starting 04/04/2024

At 04 45 PM

BACK

NEXT

FINISH

CANCEL

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

## Create Resource Group

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

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

BACK

NEXT

**FINISH**

CANCEL

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

vSphere Client

SnapCenter Plug-in for VMware vSphere **INSTANCE 172.21.166.148:8080** ▾

Dashboard

Settings

**Resource Groups**

Policies

Storage Systems

Guest File Restore

»

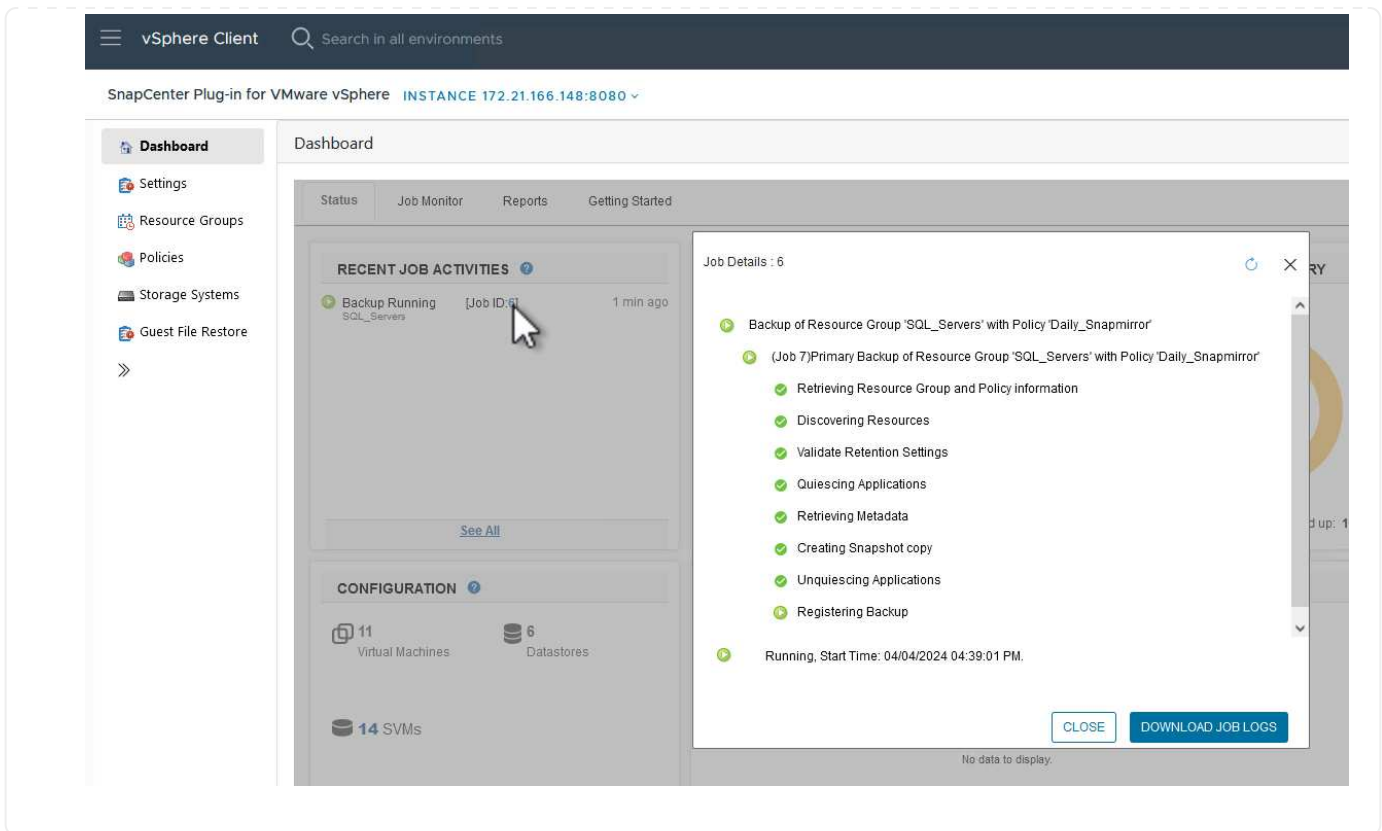
### Resource Groups

[+ Create](#) [✎ Edit](#) [✖ Delete](#) [▶ Run Now](#) [⏸ Suspend](#) [▶ Resume](#) [📄 Export](#)

Name	Description	Pol...
SQL_Servers		Daily_

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





## Stellen Sie VMs, VMDKs und Dateien mit SCV wieder her

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

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

VVol VMs können auf dem ursprünglichen Host wiederhergestellt werden.

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

VMDKs in vVol VMs können im ursprünglichen Datenspeicher wiederhergestellt werden.

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

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

## Stellen Sie VMs mit dem SnapCenter Plug-in wieder her

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

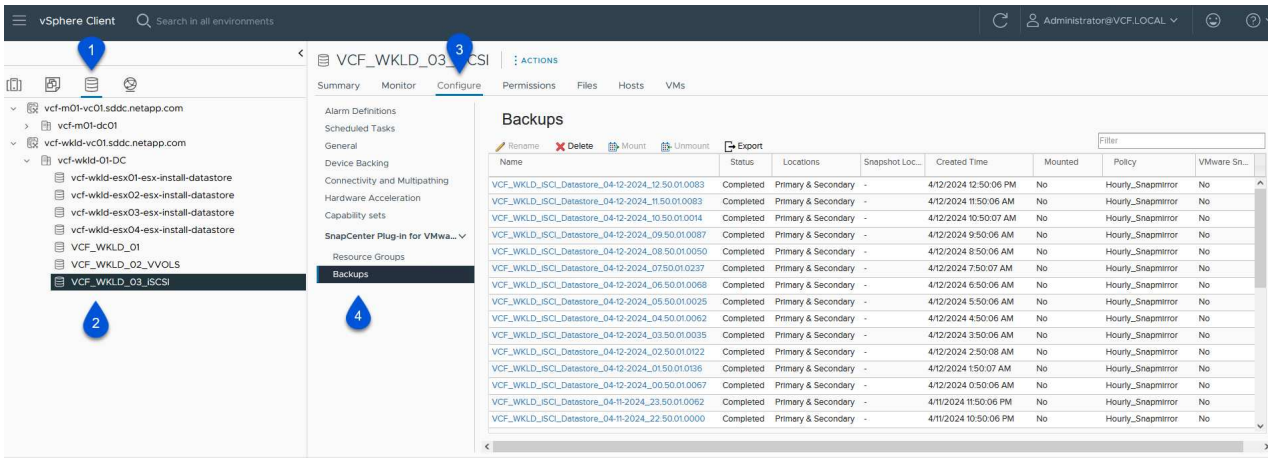
1. Navigieren Sie zu der VM, die im vSphere-Client wiederhergestellt werden soll, klicken Sie mit der rechten Maustaste, und navigieren Sie zu **SnapCenter-Plug-in für VMware vSphere**. Wählen Sie im Untermenü \* Restore\* aus.

The screenshot displays the vSphere Client interface. On the left, a tree view shows the inventory structure: vcf-m01-vc01.sddc.netapp.com > vcf-m01-dc01 > vcf-wkld-vc01.sc > vcf-wkld-01-D > IT-INF-WK > OracleSrv\_04. The 'Actions - OracleSrv\_04' context menu is open, listing various operations. The 'Restore' option is highlighted, and a sub-menu is visible with 'File Restore' selected. The main panel shows the 'Summary' tab for OracleSrv\_04, displaying hardware specifications: 4 CPU(s), 22 MHz used; 32 GB, 0 GB memory active; 100 GB | Thin Provision VCF\_WKLD\_03\_ISCSI. A 'Recent Tasks' table is partially visible at the bottom left.

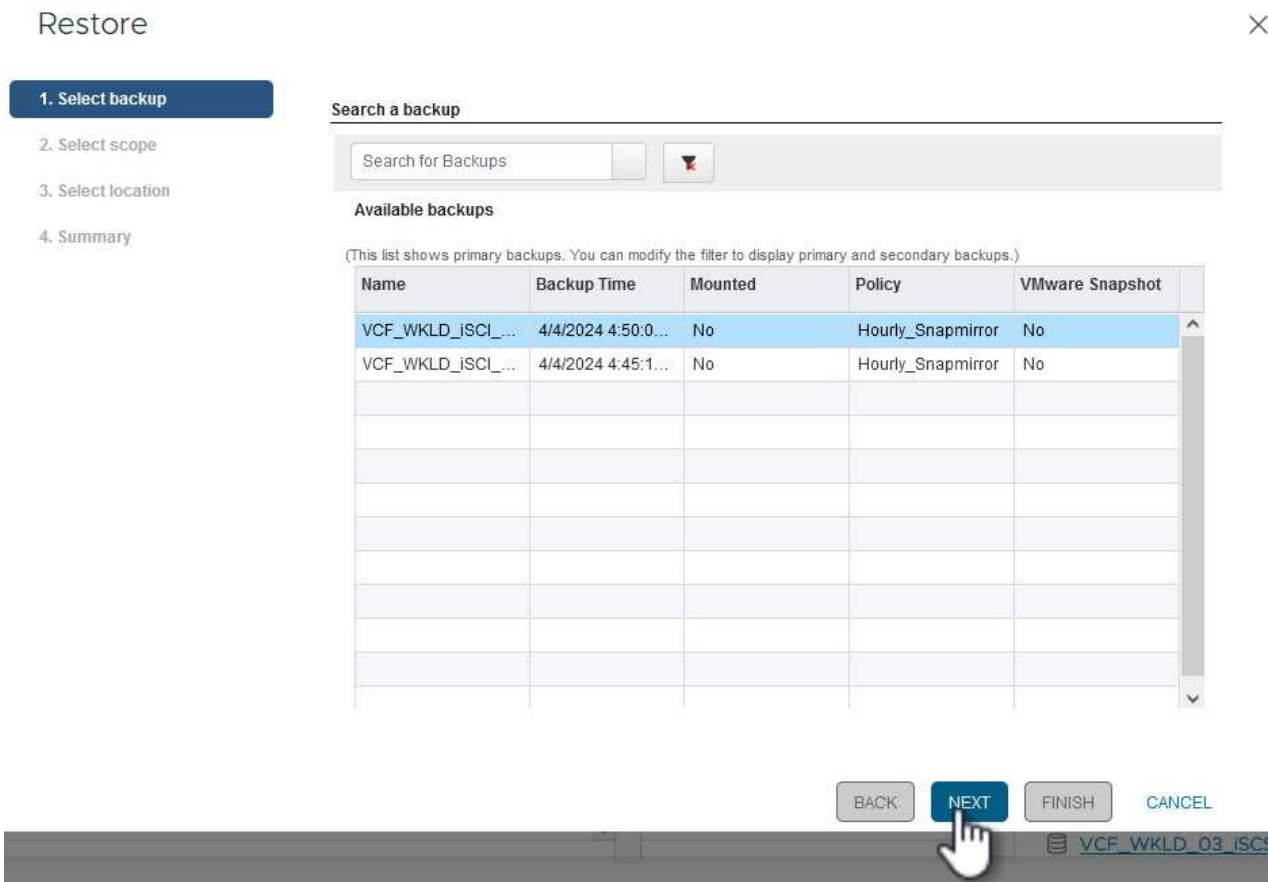
Task Name



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



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



3. Füllen Sie auf der Seite **Bereich auswählen** alle erforderlichen Felder aus:

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

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

Restore

1. Select backup

2. Select scope

3. Select location

4. Summary

Restore scope: Entire virtual machine

Restart VM:

Restore Location:

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

Destination vCenter Server: 172.21.166.143

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

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

VM name after restore: OracleSrv\_04\_restored

Select Datastore: VCF\_WKLD\_03\_ISCSI

BACK NEXT FINISH CANCEL

VCF\_WKLD\_03\_ISCSI

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

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

## Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- 3. Select location**
- 4. Summary

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

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

## Restore

- ✓ 1. Select backup
- ✓ 2. Select scope
- ✓ 3. Select location
- 4. Summary**

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



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

BACK

NEXT

**FINISH**

CANCEL

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

- Dashboard
- Settings
- Resource Groups
- Policies
- Storage Systems
- Guest File Restore
- >>

Dashboard

Status Job Monitor Reports Getting Started

RECENT JOB ACTIVITIES

- Restore Running [Job ID:18] 1 min ago  
VCF\_WKLD\_ISCI\_Datastore\_04-04-2024...
- Backup Successful [Job ID:15] 8 min ago  
VCF\_WKLD\_ISCI\_Datastore
- Backup Successful [Job ID:12] 13 min ago  
VCF\_WKLD\_ISCI\_Datastore
- Backup Successful [Job ID:9] 13 min ago  
SQL\_Servers
- Backup Successful [Job ID:6] 19 min ago  
SQL\_Servers

[See All](#)

CONFIGURATION

11 Virtual Machines    6 Datastores

14 SVMs

2 Resource Groups    2 Backup Policies

Job Details : 18

- Restoring backup with name: VCF\_WKLD\_ISCI\_Datastore\_04-04-2024\_16:50:00.0940
- Preparing for Restore: Retrieving Backup metadata from Repository.
- Pre Restore
- Restore

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

CLOSE DOWNLOAD JOB LOGS

No data to display.

Recent Tasks Alarms

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

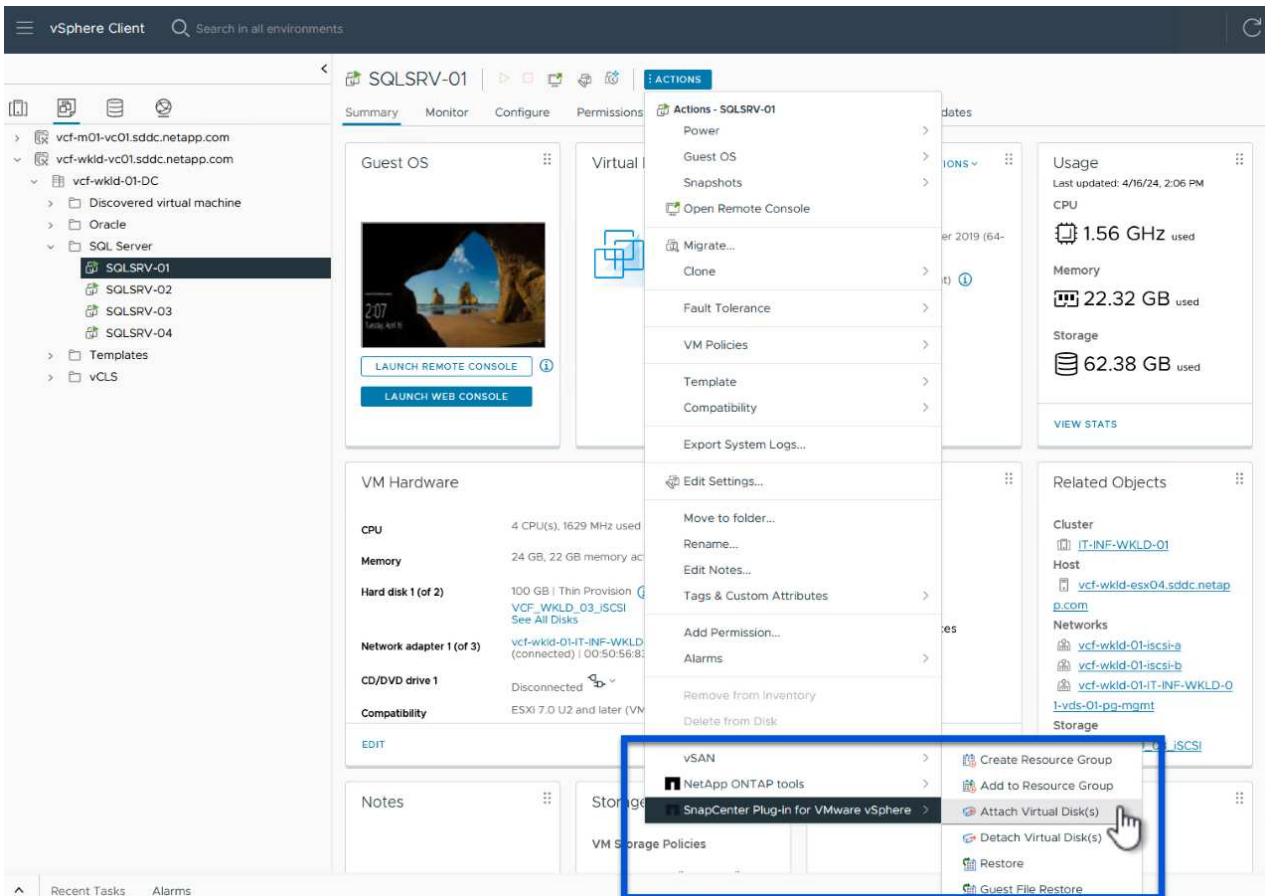
Manage Columns Running More Tasks

## Stellen Sie VMDKs mit dem SnapCenter Plug-in wieder her

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

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

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



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



# Attach Virtual Disk(s)



Click here to attach to alternate VM

## Backup

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

Name	Backup Time	Mounted	Policy	VMware Snapshot
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218	4/17/2024 9:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223	4/17/2024 8:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204	4/17/2024 7:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194	4/17/2024 6:50:00 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245	4/17/2024 5:50:01 AM	No	Hourly_Snapmirror	No
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231	4/17/2024 4:50:01 AM	No	Hourly_Snapmirror	No

## Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

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

# Attach Virtual Disk(s)



Click here to attach to alternate VM

## Backup

(This list shows primary backups)

Name
VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0218
VCF_WKLD_iSCSI_Datastore_04-17-2024_08.50.01.0223
VCF_WKLD_iSCSI_Datastore_04-17-2024_07.50.01.0204
VCF_WKLD_iSCSI_Datastore_04-17-2024_06.50.01.0194
VCF_WKLD_iSCSI_Datastore_04-17-2024_05.50.01.0245
VCF_WKLD_iSCSI_Datastore_04-17-2024_04.50.01.0231

## Select disks

Virtual disk	Location
<input type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01.vmdk	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...
<input checked="" type="checkbox"/> [VCF_WKLD_03_iSCSI] SQLSRV-01/SQLSRV-01_1.v...	Primary:VCF_iSCSI:VCF_WKLD_03_iSCSI:VCF_WKLD_iSCSI_Datastore_04-17-2024_09.50.01.0...

Time range

From

Hour  Minute  Second

To

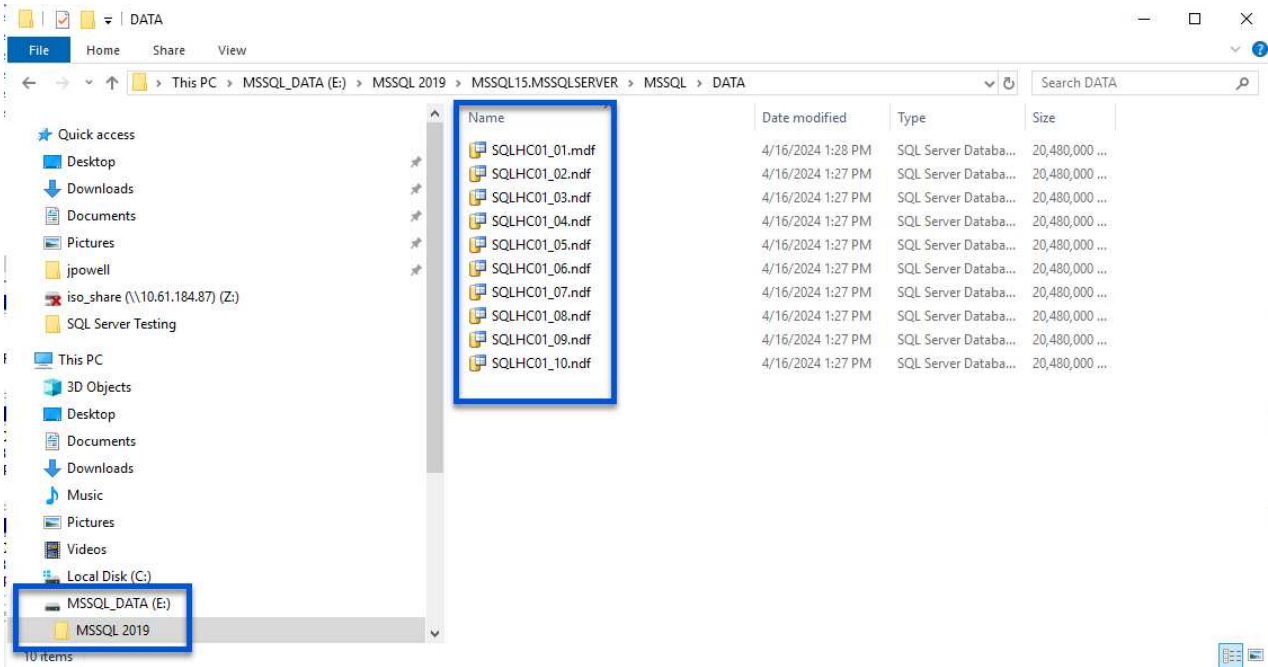
Hour  Minute  Second

VMware snapshot

Mounted

Location

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



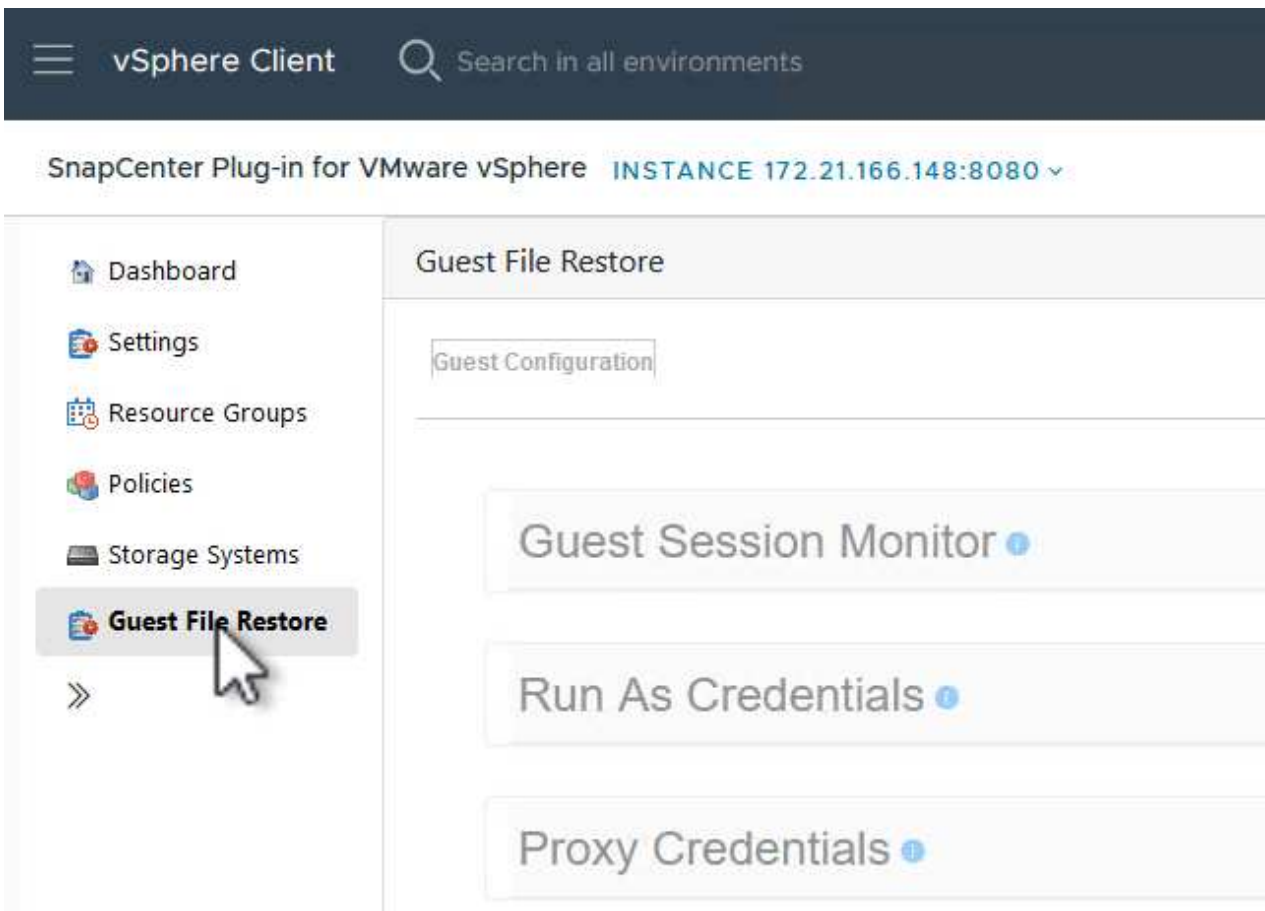
## Wiederherstellung des Gastdateisystems mit dem SnapCenter Plug-in

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

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

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

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



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

## Run As Credentials



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



<input type="button" value="CANCEL"/>	<input type="button" value="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

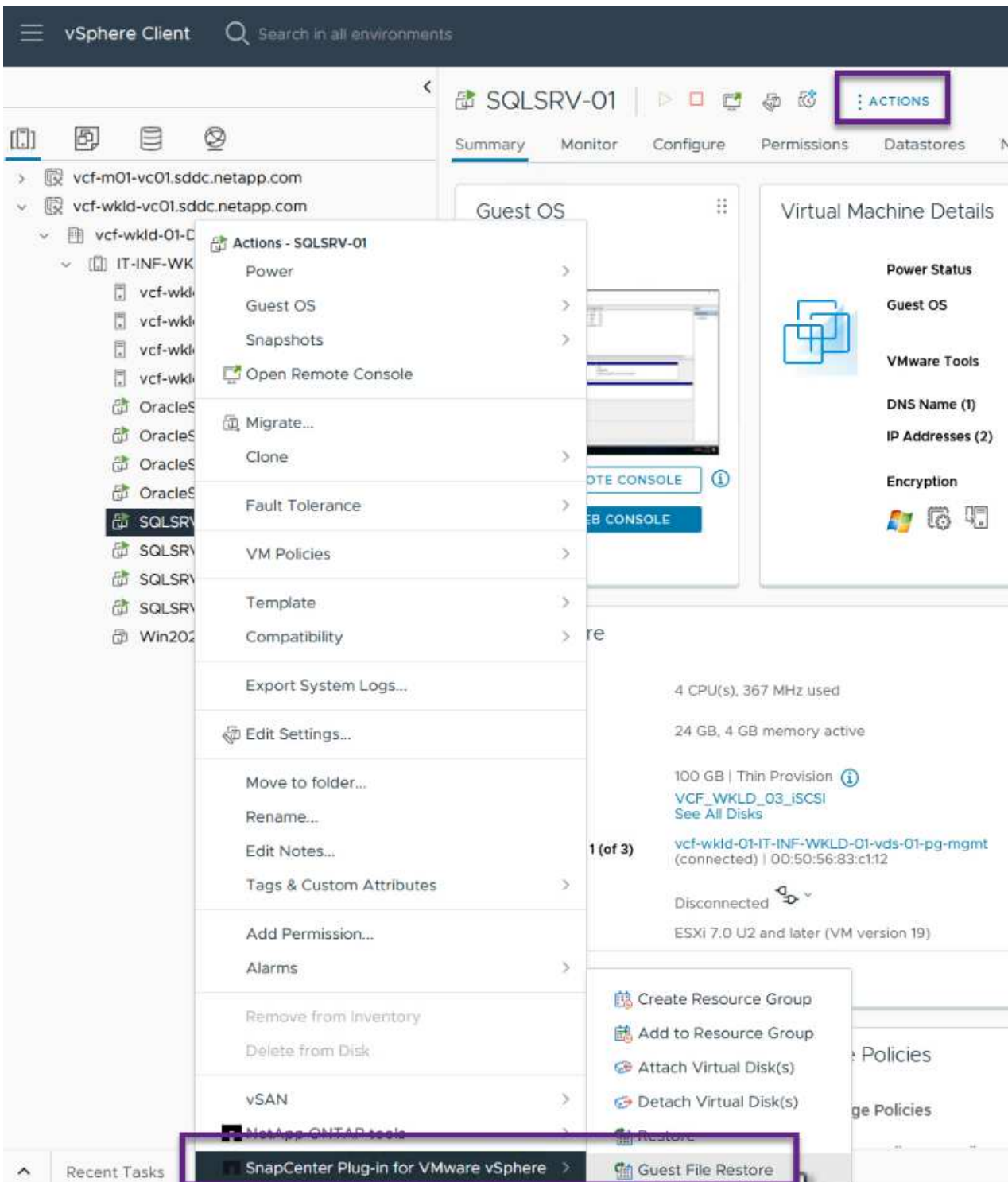
Search by Virtual Machine name

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.



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

## Guest File Restore



### 1. Restore Scope

#### 2. Guest Details

#### 3. Summary

Backup Name	Start Time	End Time
SQL_Servers_04-16-2024_13.52.3...	4/16/2024 1:52:34 PM	4/16/2024 1:52:40 PM
VCF_WKLD_iscsi_Datastore_04-1...	4/16/2024 1:50:01 PM	4/16/2024 1:50:08 PM

VMDK
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01.vmdk
[VCF_WKLD_03_iscsi] SQLSRV-01/SQLSRV-01_1.vmdk

Locations
Primary:VCF_iscsi:VCF_WKLD_03_iscsi:SQL_Servers_04-16-2024_13.52.34.0329
Secondary:svm_iscsi:VCF_WKLD_03_iscsi_dest:SQL_Servers_04-16-2024_13.52.34.0329

BACK NEXT FINISH CANCEL



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

## Guest File Restore



### 1. Restore Scope

### 2. Guest Details

### 3. Summary

#### Use Guest VM

Guest File Restore operation will attach disk to guest VM

Run As Name	Username	Authentication Mode
Administrator	administrator	WINDOWS

#### Use Guest File Restore proxy VM

#### Send email notification

Email send from:

Email send to:

Email subject:

BACK

NEXT

FINISH

CANCEL

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

The screenshot shows the vSphere Client interface for the SnapCenter Plug-in for VMware vSphere. The main content area displays the 'Guest File Restore' configuration page. Below the configuration, there is a 'Guest Session Monitor' table with the following data:

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_JCSI](sc-202404161419...	E:\	23h:58m	

Below the table, there are sections for 'Run As Credentials' and 'Proxy Credentials', both with expandable dropdown menus.

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



## Guest File Browse



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



E:\MSSQL 2019

	Name	Size	
<input type="checkbox"/>	MSSQL15.MSSQLSERVER		^
			v

Selected 0 Files / 1 Directory

Name	Path	Size	Delete	
MSSQL 2019	E:\MSSQL 2019			^
				v

### Select Restore Location



Select address family for UNC path:

IPv4

IPv6

**Either Files to Restore or Restore Location is not selected!**

CANCEL

RESTORE

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-Datstores als Haupt-Storage sowie eine Reihe zusätzlicher Storage-Optionen abgedeckt.

## **Anwendungsfälle**

Anwendungsfälle in dieser Dokumentation:

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

## **Zielgruppe**

Diese Lösung ist für folgende Personen gedacht:

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

## **Technologischer Überblick**

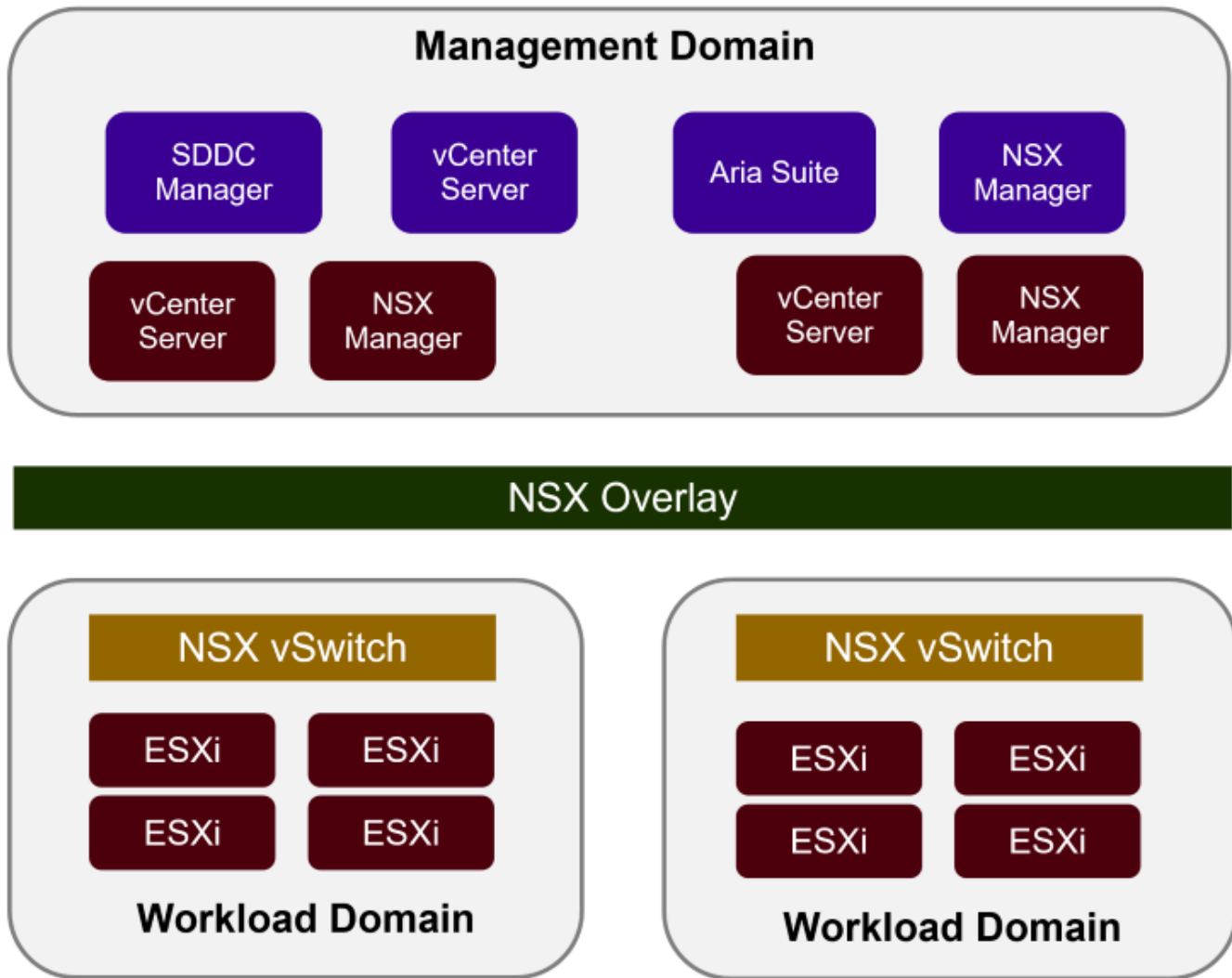
Die VCF mit NetApp AFF-Lösung besteht aus den folgenden Hauptkomponenten:

### **VMware Cloud Foundation**

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

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

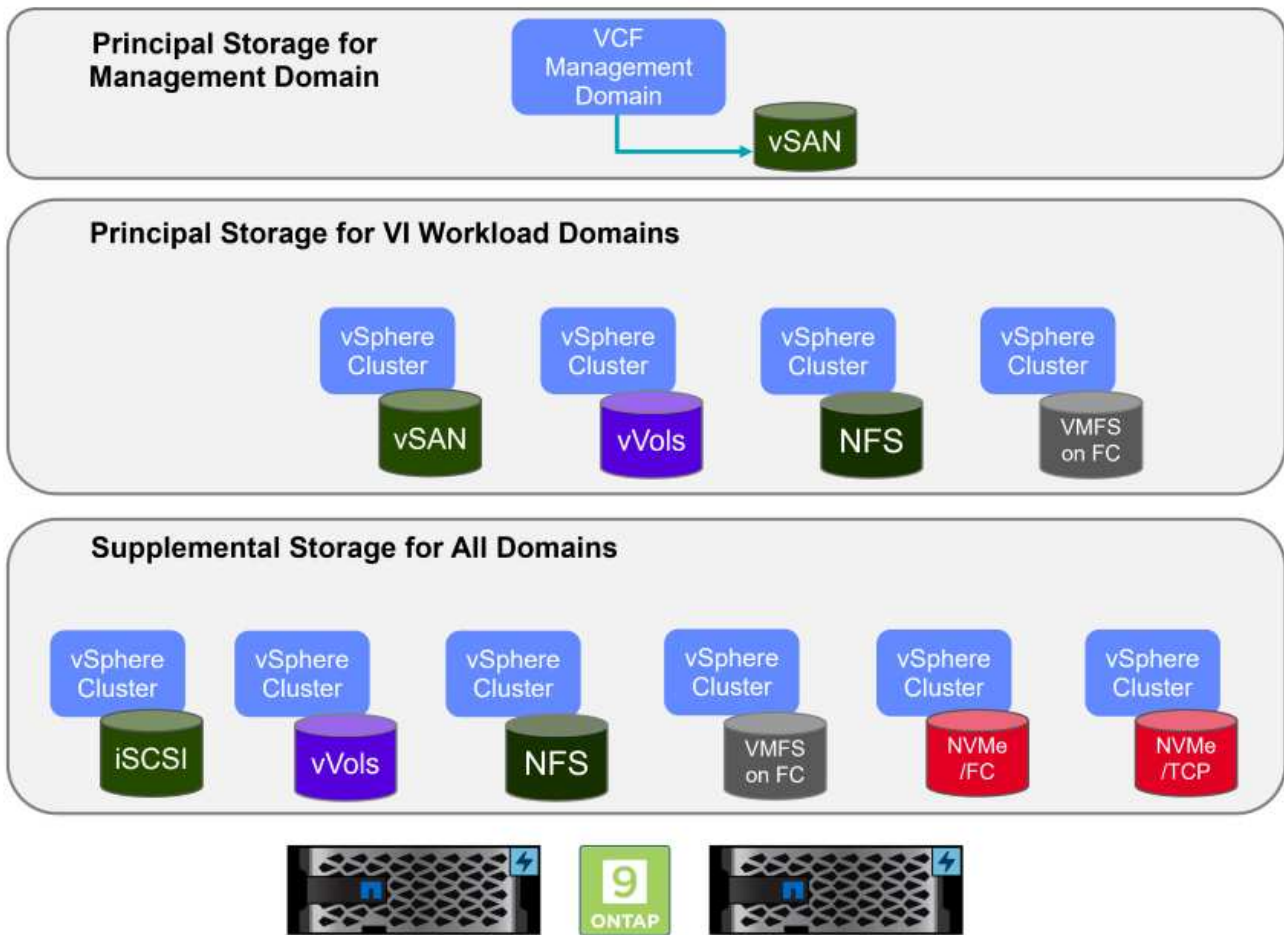
VCF besteht aus einer einzelnen Management-Domäne und bis zu 24 VI-Workload-Domänen, die jeweils eine Einheit für applikationsfähige Infrastrukturen darstellen. Eine Workload-Domäne besteht aus einem oder mehreren vSphere Clustern, die von einer einzelnen vCenter Instanz gemanagt werden.



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

### VCF Storage-Optionen

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



### Hauptspeicher für Workload-Domänen

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

### Ergänzender Speicher für Management- und Workload-Domänen

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

Zusätzliche Dokumentationsressourcen für VMware Cloud Foundation:

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

### Rein Flash-basierte Storage-Arrays von NetApp

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

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

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

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

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

### NetApp ONTAP Tools für VMware vSphere

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

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

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

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

### Lösungsüberblick

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

Szenarien in dieser Dokumentation:

- **Konfigurieren und verwenden Sie einen NFS-Datastore als Hauptspeicher während der VI-Workload-Domänen-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 contains a navigation menu with categories: DASHBOARD, INSIGHTS, STORAGE (expanded), and NETWORK. Under STORAGE, 'Storage VMs' is selected. The main area displays a list of Storage VMs with 'EHC\_NFS' selected. To the right, the 'Overview' tab for 'EHC\_NFS' is active, showing 'All Storage VMs'. Below this, the 'NETWORK IP INTERFACES' section is visible, with 'NFS' selected and a count of '7'. A list of IP addresses is shown, with '172.21.118.163' and '172.21.118.164' highlighted by blue boxes.

Alternativ können Sie mit dem folgenden Befehl die LIFs, die einer SVM zugeordnet sind, über die ONTAP-CLI überprüfen:

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

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

```
vmkping <IP Address>
```



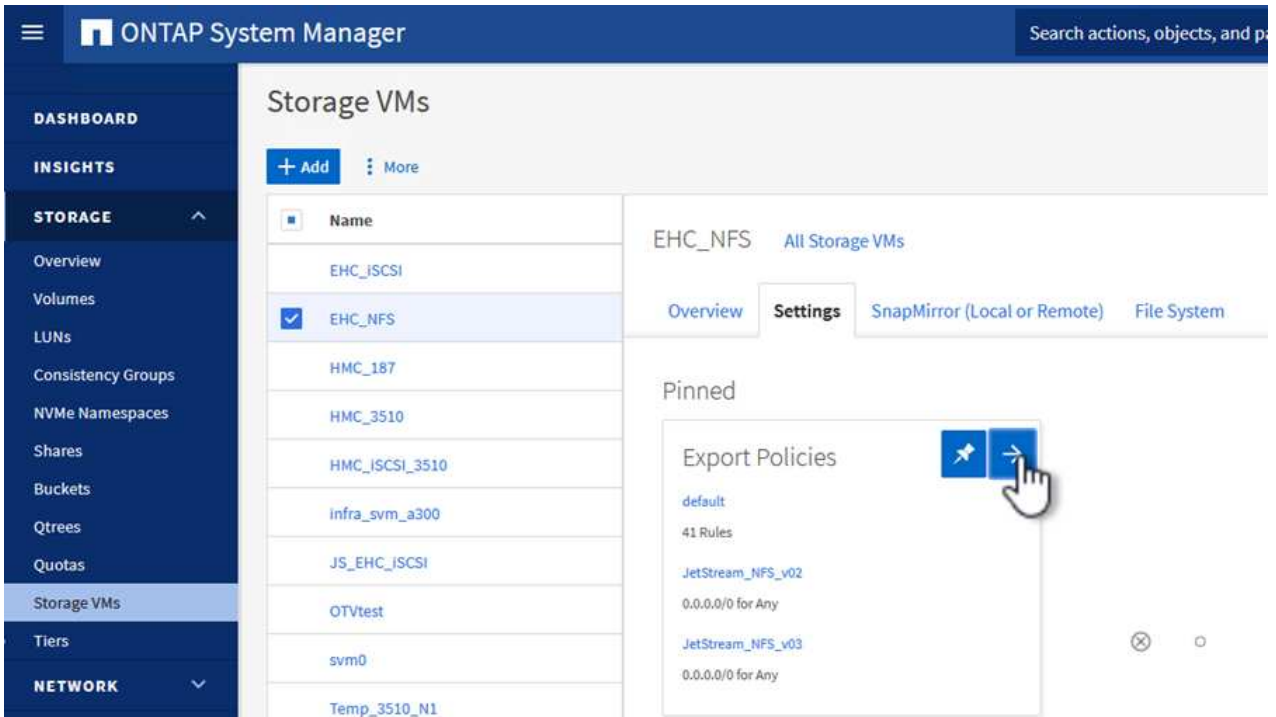


Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk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

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

Eine Richtlinie für den Export in ONTAP System Manager erstellen, um die Zugriffssteuerung für NFS-Volumen 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



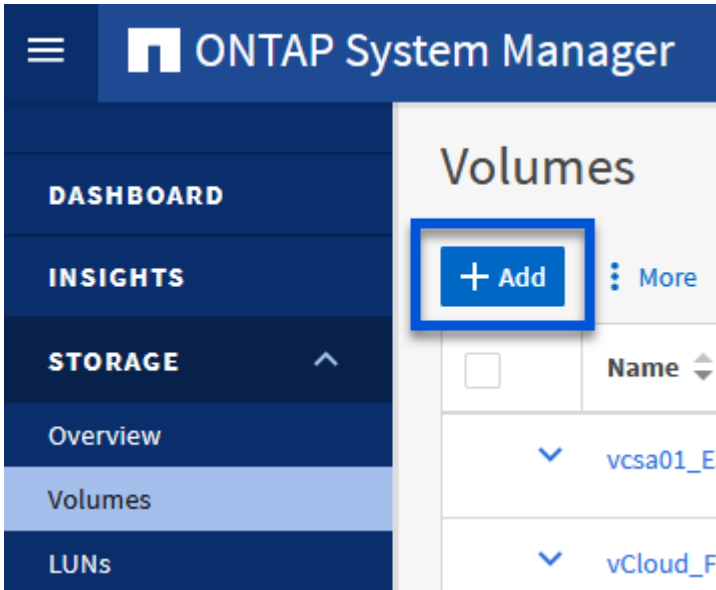
Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass die Exportrichtlinie das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

default 

JetStream\_NFS\_v04  
Clients : 0.0.0.0/0 | Access protocols : Any

NFSmountTest01  
3 rules

NFSmountTestReno01  
Clients : 0.0.0.0/0 | Access protocols : Any

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

TestEnv\_VPN  
Clients : 172.21.254.0/24 | Access protocols : Any

VCF\_WKLD  
2 rules

WKLD\_DM01  
2 rules

Wkld01\_NFS  
Clients : 172.21.252.205, 172.21.252.206, 172.21.252.207, 172.21.252.208

+



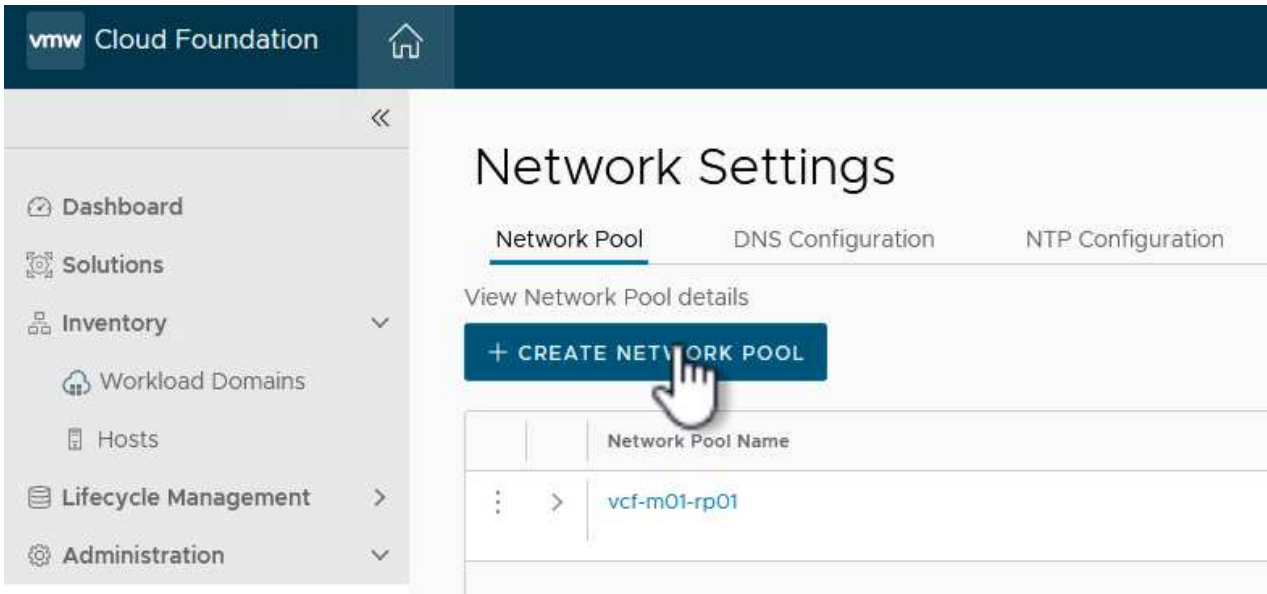
Bei der Bereitstellung einer VI-Workload-Domäne validiert VCF die Verbindung zum NFS-Server. Dies erfolgt mithilfe des Management-Adapters auf den ESXi Hosts, bevor ein zusätzlicher vmkernel-Adapter mit der NFS-IP-Adresse hinzugefügt wird. Daher muss sichergestellt werden, dass 1) das Managementnetzwerk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

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

## Netzwerkpool im SDDC Manager erstellen

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

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



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



The screenshot shows the VMware Cloud Foundation interface for creating a Network Pool. The page is titled "Network Settings" and "Create Network Pool". The "Network Pool Name" is "NFS\_NPOOL". The "Network Type" is set to "NFS".

**NFS Network Information**

VLAN ID	3374
MTU	9000
Network	172.21.118.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.118.1

**Included IP Address Ranges**

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

172.21.118.145	To	172.21.118.148	REMOVE
xxx.xxx.xxx.xxx	To	xxx.xxx.xxx.xxx	ADD

**vMotion Network Information**

VLAN ID	3423
MTU	9000
Network	172.21.167.0
Subnet Mask	255.255.255.0
Default Gateway	172.21.167.1

**Included IP Address Ranges**

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

172.21.167.121	To	172.21.167.124	REMOVE
xxx.xxx.xxx.xxx	To	xxx.xxx.xxx.xxx	ADD

At the bottom, there are "CANCEL" and "SAVE" buttons.

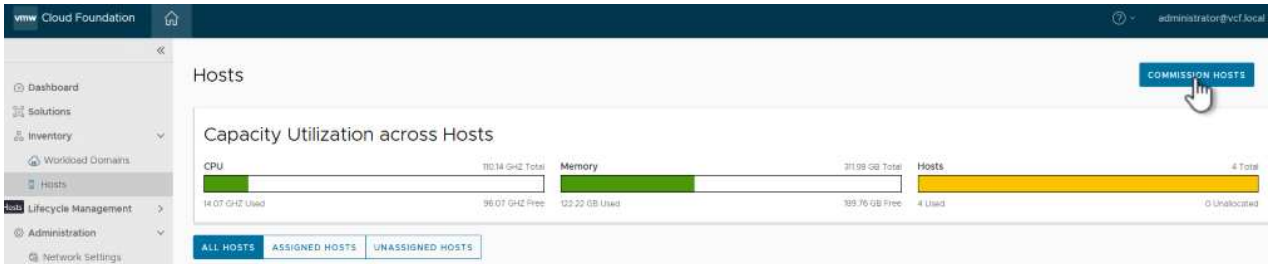
3. Klicken Sie auf die Schaltfläche **Speichern**, um die Erstellung des Netzwerkpools abzuschließen.

## Provisionswirte

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

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

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



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

## Checklist

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

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

CANCEL

PROCEED

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

## 1 Host Addition and Validation

2 Review

## Add Hosts

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

Add new  Import

Host FQDN

Storage Type  vSAN  NFS  VMFS on FC  vVol

Network Pool Name

User Name

Password

ADD

## Hosts Added

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

REMOVE

Confirm all Finger Prints

VALIDATE ALL

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

1 hosts

CANCEL

NEXT

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

## Hosts Added

✔ Host Validated Successfully. ✕

REMOVE  Confirm all Finger Prints (i) VALIDATE ALL

<input checked="" type="checkbox"/>	FGDN	Network Pool	IP Address	Confirm FingerPrint	Validation Status
<input checked="" type="checkbox"/>	vcf-wkld-esx04.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.138	<span style="color: green;">✔</span> SHA256:9Kg+9nQaE4SQkOMsQPON/k5gZB9zyKN+6CBPmXsvLBc	<span style="color: green;">✔</span> Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx03.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.137	<span style="color: green;">✔</span> SHA256:nPX4/mei/2zmLJHfmPwbk6zhapoUxV2lOwZDPFH+z0	<span style="color: green;">✔</span> Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx02.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.136	<span style="color: green;">✔</span> SHA256:AMhyR60OpTQ1YYq0DJhqVbj/M/GvrQaqUy7Ce+M4lWY	<span style="color: green;">✔</span> Valid
<input checked="" type="checkbox"/>	vcf-wkld-esx01.sddc.netapp.com	NFS_NP01 <span style="font-size: 0.8em;">(i)</span>	172.21.166.135	<span style="color: green;">✔</span> SHA256:CKbsinfEOG+ +z/lpFUoFDI2tLuYFZ47WicVDp6vEQM	<span style="color: green;">✔</span> Valid

CANCEL NEXT

- Überprüfen Sie die Liste der Hosts, die beauftragt werden sollen, und klicken Sie auf die Schaltfläche **Provision**, um den Prozess zu starten. Überwachen Sie den Inbetriebnahmeprozess im SDDC-Manager im Aufgabenbereich.

## Commission Hosts

1 Host Addition and Validation

2 **Review**

## Review

Skip failed hosts during commissioning   On

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

CANCEL

BACK

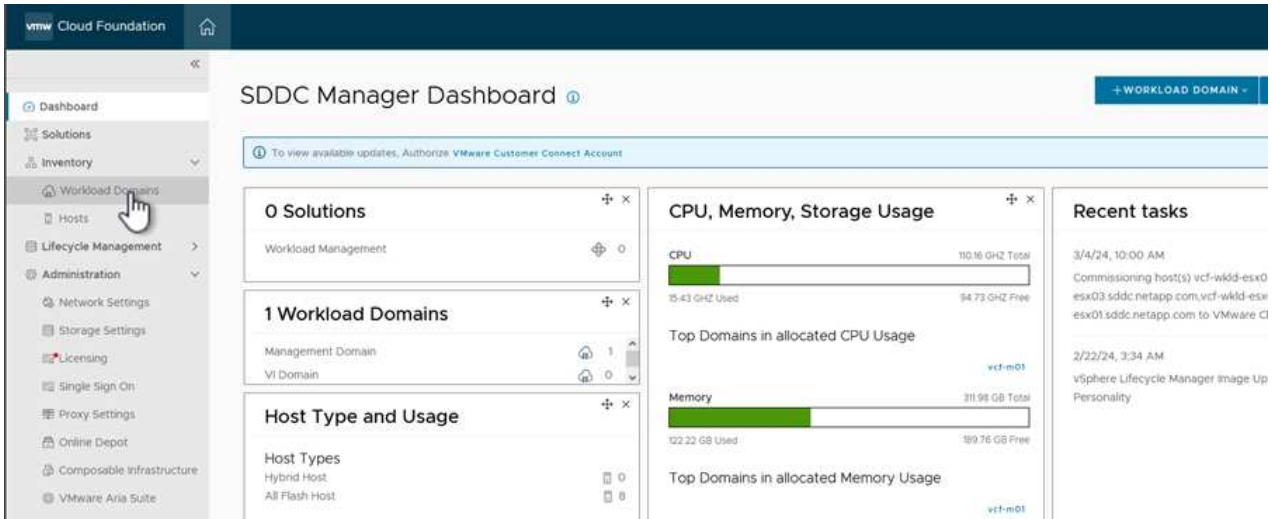
COMMISSION

## Implementieren Sie VI Workload Domain

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

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

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



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

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

+

# VI Configuration

## 1 General Info

2 Cluster

3 Compute

4 Networking

5 Host Selection

6 NFS Storage

7 Switch Configuration

8 License

9 Review

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

The screenshot shows the VI Configuration Wizard with the 'NFS Storage' step selected. The configuration details are as follows:

NFS Storage	
<b>NFS Share Details</b>	
Datastore Name ⓘ	VCF_WKLD_01
Folder ⓘ	/VCF_WKLD_01
NFS Server IP Address ⓘ	172.21.118.163

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



### VI Configuration

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

### Review

General	
Virtual Infrastructure Name	vcf-wkld-01
Organization Name	it-inf
SSO Domain Option	Joining Management SSO Domain
Cluster	
Cluster Name	IT-INF-WKLD-01
Compute	
vCenter IP Address	172.21.166.143
vCenter DNS Name	vcf-wkld-vc01.sddc.netapp.com
vCenter Subnet Mask	255.255.255.0
vCenter Default Gateway	172.21.166.1
Networking	
NSX Manager Instance Option	Creating new NSX instance
NSX Manager Cluster IP	172.21.166.147
NSX Manager Cluster FQDN	vcf-w01-nsxc101.sddc.netapp.com
NSX Manager IP Addresses	172.21.166.144, 172.21.166.145, 172.21.166.146

CANCEL
BACK
FINISH

3. Überwachen Sie den Prozess und beheben Sie alle während des Prozesses auftretenden Validierungsprobleme.

### Installation des NetApp NFS Plug-ins für VMware VAAI

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

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

### Video-Demo für diese Lösung

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

## Einführung in die Automatisierung für ONTAP und vSphere

### VMware Automatisierung

Seit den ersten Tagen von VMware ESX ist die Automatisierung ein integraler Bestandteil des Managements von VMware Umgebungen. Die Möglichkeit, Infrastruktur als Code zu implementieren und Verfahren auf

private Cloud-Vorgänge auszuweiten, um Bedenken hinsichtlich Skalierbarkeit, Flexibilität, Self-Provisioning und Effizienz zu zerstreuen.

Die Automatisierung kann in die folgenden Kategorien eingeteilt werden:

- \* Bereitstellung virtueller Infrastrukturen\*
- **Betrieb der Gastmaschine**
- **Cloud-Betrieb**

Administratoren stehen im Hinblick auf die Automatisierung ihrer Infrastruktur viele Optionen zur Verfügung. Ob durch die Nutzung nativer vSphere Funktionen wie Host-Profile oder Anpassungsspezifikationen für Virtual Machines über verfügbare APIs auf den VMware Software-Komponenten, Betriebssystemen und NetApp Storage-Systemen verfügen - hier sind umfangreiche Dokumentationen und Anleitungen verfügbar.

Data ONTAP 8.0.1 und höher unterstützt bestimmte VMware vSphere APIs for Array Integration (VAAI)-Funktionen, wenn der ESX-Host ESX 4.1 oder höher ausführt. VAAI ist eine Reihe von APIs für die Kommunikation zwischen VMware vSphere ESXi Hosts und Storage-Geräten. Diese Funktionen helfen, Vorgänge vom ESX Host zum Storage-System zu verlagern und den Netzwerkdurchsatz zu steigern. Der ESX-Host aktiviert die Funktionen automatisch in der richtigen Umgebung. Sie können bestimmen, in welchem Umfang Ihr System VAAI-Funktionen verwendet, indem Sie die Statistiken in den VAAI-Zählern prüfen.

Der häufigste Ausgangspunkt für die Automatisierung der Implementierung einer VMware-Umgebung ist die Bereitstellung von Block- oder dateibasierten Datastores. Vor der Entwicklung der entsprechenden Automatisierung ist es wichtig, die Anforderungen der eigentlichen Aufgaben abzubilden.

Weitere Informationen zur Automatisierung von VMware-Umgebungen finden Sie in den folgenden Ressourcen:

- ["„NetApp Pub“"](#). NetApp Konfigurationsmanagement und Automatisierung:
- ["Ansible Galaxy Community für VMware"](#). Eine Sammlung von Ansible-Ressourcen für VMware.
- ["VMware {Code} Ressourcen"](#). Ressourcen, die zum entwickeln von Lösungen für das softwaredefinierte Datacenter erforderlich sind, einschließlich Foren, Designstandards, Beispielcode und Entwickler-Tools

## VSphere herkömmliche Block-Storage-Bereitstellung mit ONTAP

VMware vSphere unterstützt die folgenden VMFS-Datastore-Optionen, wobei die Unterstützung für das ONTAP-SAN-Protokoll angegeben ist.

VMFS-Datenspeicher-Optionen	Unterstützte ONTAP SAN-Protokolle
<a href="#">"Fibre Channel (FC)"</a>	ja
<a href="#">"Fibre Channel over Ethernet (FCoE)"</a>	ja
<a href="#">"iSCSI"</a>	ja
iSCSI-Erweiterungen für RDMA (iSER)	Nein
<a href="#">"NVMe over Fabric mit FC (NVMe/FC)"</a>	ja

VMFS-Datenspeicher-Optionen	Unterstützte ONTAP SAN-Protokolle
NVMe over Fabric mit RDMA over Converged Ethernet (NVMe/RoCE)	Nein



Wenn iSER- oder NVMe/RoCE-VMFS erforderlich ist, prüfen Sie SANtricity-basierte Storage-Systeme.

## VSphere VMFS Datastore – Fibre-Channel-Storage-Back-End mit ONTAP

### Über diese Aufgabe

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit ONTAP Fibre Channel (FC)-Storage behandelt.

Verwenden Sie eines der folgenden Skripte für die automatisierte Bereitstellung: [\[PowerShell\]](#), [\[Ansible\]](#), Oder [\[Terraform\]](#).

### Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- Ein ONTAP-Storage-System (FAS/AFF/CVO/ONTAP Select/ASA) mit ONTAP 9.8 oder höher
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ONTAP WWPN von Host-, Ziel- und SVM- sowie LUN-Informationen
- ["Das ausgefüllte FC-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- Informationen zu vSphere Hosts
  - VSphere 7.0 oder höher
- Fabric Switch(e)
  - Mit verbundenen ONTAP FC-Daten-Ports und vSphere-Hosts
  - Bei aktivierter N\_Port ID Virtualization (NPIV)
  - Erstellen Sie einen einzelnen Initiator-Zielbereich.
    - Erstellen Sie für jeden Initiator eine Zone (einzelne Initiatorzone).
    - Geben Sie für jede Zone ein Ziel an, das die logische ONTAP FC-Schnittstelle (WWPN) für die SVMs ist. Es sollten mindestens zwei logische Schnittstellen pro Node pro SVM vorhanden sein. Verwenden Sie den WWPN der physischen Ports nicht.
- Ein ONTAP Tool für Implementierung, Konfiguration und Einsatzbereitschaft von VMware vSphere

### Bereitstellung eines VMFS-Datenspeichers

Gehen Sie wie folgt vor, um einen VMFS-Datenspeicher bereitzustellen:

1. Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#)
2. Überprüfen Sie das ["FCP-Konfiguration wird unterstützt"](#).

## ONTAP Aufgaben

1. "Vergewissern Sie sich, dass Sie eine ONTAP-Lizenz für FCP haben."
  - a. Verwenden Sie die `system license show` Befehl zum Überprüfen, ob FCP aufgeführt ist.
  - b. Nutzung `license add -license-code <license code>` Um die Lizenz hinzuzufügen.
2. Vergewissern Sie sich, dass das FCP-Protokoll auf der SVM aktiviert ist.
  - a. "Überprüfen Sie das FCP auf einer vorhandenen SVM."
  - b. "Konfigurieren Sie das FCP für eine vorhandene SVM."
  - c. "Erstellen Sie mit dem FCP eine neue SVM."
3. Stellen Sie sicher, dass auf einer SVM logische FCP-Schnittstellen verfügbar sind.
  - a. Nutzung `Network Interface show` Um den FCP-Adapter zu überprüfen.
  - b. Wird mit der GUI eine SVM erstellt, gehören zu diesem Prozess logische Schnittstellen.
  - c. Verwenden Sie zum Umbenennen von Netzwerkschnittstellen `Network Interface modify`.
4. "Erstellen und Zuordnen einer LUN." Überspringen Sie diesen Schritt, wenn Sie ONTAP-Tools für VMware vSphere verwenden.

## Aufgaben für VMware vSphere

1. Die HBA-Treiber sind installiert. Von VMware unterstützte HBAs verfügen über Out-of-the-Box-Treiber, die im sichtbar sein sollten "[Informationen Zum Storage-Adapter](#)".
2. "[Stellen Sie einen VMFS-Datenspeicher mit ONTAP Tools bereit](#)".

## VSphere VMFS Datenspeicher – Fibre Channel over Ethernet Storage-Protokoll mit ONTAP

### Über diese Aufgabe

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit dem FCoE-Transportprotokoll (Fibre Channel over Ethernet) zu ONTAP Storage behandelt.

Verwenden Sie eines der folgenden Skripte für die automatisierte Bereitstellung: [\[PowerShell\]](#), [\[Ansible\]](#), Oder [\[Terraform\]](#).

### Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- Ein ONTAP Storage-System (FAS/AFF/CVO/ONTAP Select) mit ONTAP 9.8 oder höher
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- "[Eine unterstützte FCoE-Kombination](#)"
- "[Ein ausgefülltes Konfigurationsarbeitsblatt](#)"
- Anmeldedaten für vCenter Server
- Informationen zu vSphere Hosts
  - VSphere 7.0 oder höher
- Fabric Switch(e)
  - Mit ONTAP FC-Daten-Ports oder vSphere-Hosts verbunden

- Bei aktivierter N\_Port ID Virtualization (NPIV)
- Erstellen Sie einen einzelnen Initiator-Zielbereich.
- ["FC/FCoE-Zoning konfiguriert"](#)
- Netzwerk-Switch(e)
  - FCoE-Support
  - DCB-Support
  - ["Jumbo Frames für FCoE"](#)
- ONTAP Tool für VMware vSphere – implementiert, konfiguriert und betriebsbereit

### Bereitstellung eines VMFS-Datenspeichers

- Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#).
- ["Vergewissern Sie sich, dass die FCoE-Konfiguration unterstützt wird"](#).

### ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für FCP."](#)
  - a. Verwenden Sie die `system license show` Befehl zum Überprüfen, ob das FCP aufgeführt ist.
  - b. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. Vergewissern Sie sich, dass das FCP-Protokoll auf der SVM aktiviert ist.
  - a. ["Überprüfen Sie das FCP auf einer vorhandenen SVM."](#)
  - b. ["Konfigurieren Sie das FCP für eine vorhandene SVM."](#)
  - c. ["Erstellen Sie eine neue SVM mit dem FCP."](#)
3. Vergewissern Sie sich, dass auf der SVM logische FCP-Schnittstellen verfügbar sind.
  - a. Nutzung `Network Interface show` Um den FCP-Adapter zu überprüfen.
  - b. Wird mit der GUI eine SVM erstellt, sind logische Schnittstellen Teil dieses Prozesses.
  - c. Verwenden Sie zum Umbenennen der Netzwerkschnittstelle `Network Interface modify`.
4. ["Erstellen und Zuordnen einer LUN"](#); überspringen Sie diesen Schritt, wenn Sie ONTAP-Tools für VMware vSphere nutzen.

### Aufgaben für VMware vSphere

1. Vergewissern Sie sich, dass die HBA-Treiber installiert sind. Bei den von VMware unterstützten HBAs sind die Treiber Out-of-the-Box implementiert und sollten im sichtbar sein ["Informationen zu Storage-Adapttern"](#).
2. ["Stellen Sie einen VMFS-Datenspeicher mit ONTAP Tools bereit"](#).

### VSphere VMFS Datenspeicher – iSCSI-Storage-Back-End mit ONTAP

#### Über diese Aufgabe

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit ONTAP iSCSI-Speicher behandelt.

Verwenden Sie eines der folgenden Skripte für die automatisierte Bereitstellung: [\[PowerShell\]](#), [\[Ansible\]](#), Oder [\[Terraform\]](#).

## Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- Ein ONTAP-Storage-System (FAS/AFF/CVO/ONTAP Select/ASA) mit ONTAP 9.8 oder höher
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ONTAP Netzwerkport, SVM und LUN-Informationen für iSCSI
- ["Ein ausgefülltes iSCSI-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- Informationen zu vSphere Hosts
  - VSphere 7.0 oder höher
- IP-Informationen zum iSCSI VMkernel Adapter
- Netzwerk-Switch(e)
  - Mit Netzwerk-Daten-Ports des ONTAP Systems und verbundenen vSphere Hosts
  - Für iSCSI konfigurierte VLANs
  - (Optional) Link Aggregation konfiguriert für ONTAP Netzwerkdatenports
- ONTAP Tool für VMware vSphere – implementiert, konfiguriert und betriebsbereit

## Schritte

1. Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#).
2. ["Vergewissern Sie sich, dass die iSCSI-Konfiguration unterstützt wird."](#)
3. Führen Sie die folgenden Aufgaben für ONTAP und vSphere aus.

## ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für iSCSI"](#).
  - a. Verwenden Sie die `system license show` Befehl, um zu überprüfen, ob iSCSI aufgeführt ist.
  - b. Nutzung `license add -license-code <license code>` Um die Lizenz hinzuzufügen.
2. ["Vergewissern Sie sich, dass das iSCSI-Protokoll auf der SVM aktiviert ist."](#)
3. Vergewissern Sie sich, dass auf der SVM logische iSCSI-Netzwerk-Schnittstellen verfügbar sind.



Wenn über die GUI eine SVM erstellt wird, werden auch iSCSI-Netzwerkschnittstellen erstellt.

4. Verwenden Sie die `network interface` Befehl zum Anzeigen oder Ändern der Netzwerkschnittstelle.



Es werden zwei iSCSI-Netzwerkschnittstellen pro Node empfohlen.

5. ["Erstellen Sie eine iSCSI-Netzwerkschnittstelle."](#) Sie können die Service-Richtlinie für Standarddatenblöcke verwenden.
6. ["Überprüfen Sie, ob der Daten-iscsi-Service in der Service-Richtlinie enthalten ist."](#) Verwenden Sie können `network interface service-policy show` Zu überprüfen.
7. ["Vergewissern Sie sich, dass Jumbo Frames aktiviert sind."](#)

8. "Erstellen und Zuordnen der LUN." Überspringen Sie diesen Schritt, wenn Sie ONTAP-Tools für VMware vSphere verwenden. Wiederholen Sie diesen Schritt für jede LUN.

### Aufgaben für VMware vSphere

1. Stellen Sie sicher, dass mindestens eine NIC für das iSCSI-VLAN verfügbar ist. Zwei NICs werden bevorzugt, um eine bessere Performance und Fehlertoleranz zu schaffen.
2. "Ermitteln Sie die Anzahl der physischen NICs, die auf dem vSphere-Host verfügbar sind."
3. "Konfigurieren Sie den iSCSI-Initiator." Ein typischer Anwendungsfall ist ein Software-iSCSI-Initiator.
4. "Stellen Sie sicher, dass der TCPIP-Stack für iSCSI verfügbar ist".
5. "Vergewissern Sie sich, dass iSCSI-Portgruppen verfügbar sind".
  - In der Regel verwenden wir einen einzelnen virtuellen Switch mit mehreren Uplink-Ports.
  - Verwenden Sie 1:1-Adapterzuordnung.
6. Vergewissern Sie sich, dass die iSCSI-VMkernel-Adapter für die Anzahl der NICs aktiviert sind und IP-Adressen zugewiesen sind.
7. "Binden Sie den iSCSI-Software-Adapter an die iSCSI-VMkernel-Adapter."
8. "Stellen Sie den VMFS-Datenspeicher mit ONTAP Tools bereit". Wiederholen Sie diesen Schritt für alle Datenspeicher.
9. "Prüfen Sie, ob die Hardware-Beschleunigung unterstützt wird."

### Was kommt als Nächstes?

Nach Abschluss dieser Aufgaben kann der VMFS-Datenspeicher für die Bereitstellung von Virtual Machines genutzt werden.

### Ansible Playbook

```
## Disclaimer: Sample script for reference purpose only.

- hosts: '{{ vsphere_host }}'
  name: Play for vSphere iSCSI Configuration
  connection: local
  gather_facts: false
  tasks:
    # Generate Session ID for vCenter
    - name: Generate a Session ID for vCenter
      uri:
        url: "https://{{ vcenter_hostname }}/rest/com/vmware/cis/session"
        validate_certs: false
        method: POST
        user: "{{ vcenter_username }}"
        password: "{{ vcenter_password }}"
        force_basic_auth: yes
        return_content: yes
      register: vclogin
```

```

# Generate Session ID for ONTAP tools with vCenter
- name: Generate a Session ID for ONTAP tools with vCenter
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/security/user/login"
    validate_certs: false
    method: POST
    return_content: yes
    body_format: json
    body:
      vcenterUserName: "{{ vcenter_username }}"
      vcenterPassword: "{{ vcenter_password }}"
  register: login

# Get existing registered ONTAP Cluster info with ONTAP tools
- name: Get ONTAP Cluster info from ONTAP tools
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters"
    validate_certs: false
    method: Get
    return_content: yes
    headers:
      vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  register: clusterinfo

- name: Get ONTAP Cluster ID
  set_fact:
    ontap_cluster_id: "{{ clusterinfo.json |
json_query(clusteridquery) }}"
  vars:
    clusteridquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='Cluster'].id | [0]"

- name: Get ONTAP SVM ID
  set_fact:
    ontap_svm_id: "{{ clusterinfo.json | json_query(svmidquery) }}"
  vars:
    svmidquery: "records[?ipAddress == '{{ netapp_hostname }}' &&
type=='SVM' && name == '{{ svm_name }}'].id | [0]"

- name: Get Aggregate detail
  uri:
    url: "https://{{ ontap_tools_ip
}}:8143/api/rest/2.0/storage/clusters/{{ ontap_svm_id }}/aggregates"
    validate_certs: false

```



```

method: GET
return_content: yes
headers:
  vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  cluster-id: "{{ ontap_svm_id }}"
when: ontap_svm_id != ''
register: aggrinfo

- name: Select Aggregate with max free capacity
set_fact:
  aggr_name: "{{ aggrinfo.json | json_query(aggrquery) }}"
vars:
  aggrquery: "max_by(records, &freeCapacity).name"

- name: Convert datastore size in MB
set_fact:
  datastoreSizeInMB: "{{ iscsi_datastore_size |
human_to_bytes/1024/1024 | int }}"

- name: Get vSphere Cluster Info
uri:
  url: "https://{{ vcenter_hostname }}/api/vcenter/cluster?names={{
vsphere_cluster }}"
  validate_certs: false
  method: GET
  return_content: yes
  body_format: json
  headers:
    vmware-api-session-id: "{{ vclogin.json.value }}"
when: vsphere_cluster != ''
register: vcenterclusterid

- name: Create iSCSI VMFS-6 Datastore with ONTAP tools
uri:
  url: "https://{{ ontap_tools_ip
}}:8143/api/rest/3.0/admin/datastore"
  validate_certs: false
  method: POST
  return_content: yes
  status_code: [200]
  body_format: json
  body:
    traditionalDatastoreRequest:
      name: "{{ iscsi_datastore_name }}"
      datastoreType: VMFS
      protocol: ISCSI

```

```

    spaceReserve: Thin
    clusterID: "{{ ontap_cluster_id }}"
    svmID: "{{ ontap_svm_id }}"
    targetMoref: ClusterComputeResource:{{
vcenterclusterid.json[0].cluster }}
    datastoreSizeInMB: "{{ datastoreSizeInMB | int }}"
    vmfsFileSystem: VMFS6
    aggrName: "{{ aggr_name }}"
    existingFlexVolName: ""
    volumeStyle: FLEXVOL
    datastoreClusterMoref: ""
  headers:
    vmware-api-session-id: "{{ login.json.vmwareApiSessionId }}"
  when: ontap_cluster_id != '' and ontap_svm_id != '' and aggr_name !=
''
  register: result
  changed_when: result.status == 200

```

## VSphere VMFS Datastore – NVMe/FC mit ONTAP

### Über diese Aufgabe

In diesem Abschnitt wird die Erstellung eines VMFS-Datenspeichers mit ONTAP-Storage mithilfe von NVMe/FC beschrieben.

Verwenden Sie eines der folgenden Skripte für die automatisierte Bereitstellung: [\[PowerShell\]](#), [\[Ansible\]](#), Oder [\[Terraform\]](#).

### Was Sie brauchen

- Erforderliche Grundkenntnisse für das Management von vSphere Umgebungen und ONTAP
- ["Grundkenntnisse von NVMe/FC"](#).
- Ein ONTAP-Storage-System (FAS/AFF/CVO/ONTAP Select/ASA) mit ONTAP 9.8 oder höher
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID und Passwort)
- ONTAP WWPN für Host-, Ziel- und SVMs- sowie LUN-Informationen
- ["Ein ausgefülltes FC-Konfigurationsarbeitsblatt"](#)
- VCenter Server
- Informationen zu vSphere-Hosts (vSphere 7.0 oder höher)
- Fabric Switch(e)
  - Mit ONTAP FC-Daten-Ports und vSphere-Hosts verbunden.
  - Bei aktivierter N\_Port ID Virtualization (NPIV).
  - Erstellen einer Zielzone für einen einzelnen Initiator
  - Erstellen Sie für jeden Initiator eine Zone (einzelne Initiatorzone).
  - Geben Sie für jede Zone ein Ziel an, das die logische ONTAP FC-Schnittstelle (WWPN) für die SVMs ist. Es sollten mindestens zwei logische Schnittstellen pro Node pro SVM vorhanden sein. Verwenden

Sie den WWPN von physischen Ports nicht.

### Bereitstellung von VMFS-Datenspeichern

1. Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#).
2. ["Vergewissern Sie sich, dass die NVMe/FC-Konfiguration unterstützt wird."](#)

### ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für FCP."](#)Verwenden Sie die `system license show` Befehl und Prüfung, ob `NVMe_of` aufgeführt ist. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. Vergewissern Sie sich, dass das NVMe-Protokoll auf der SVM aktiviert ist.
  - a. ["Konfigurieren Sie SVMs für NVMe."](#)
3. Stellen Sie sicher, dass auf den SVMs logische NVMe/FC-Schnittstellen verfügbar sind.
  - a. Nutzung `Network Interface show` Um den FCP-Adapter zu überprüfen.
  - b. Wird mit der GUI eine SVM erstellt, gehören zu diesem Prozess logische Schnittstellen.
  - c. Verwenden Sie zum Umbenennen der Netzwerkschnittstelle den Befehl `Network Interface modify`.
4. ["NVMe Namespace und Subsystem erstellen"](#)

### Aufgaben für VMware vSphere

1. Vergewissern Sie sich, dass die HBA-Treiber installiert sind. Die von VMware unterstützten HBAs verfügen über die Out-of-the-Box-Treiber und sollten bei sichtbar sein ["Informationen Zum Storage-Adapter"](#)
2. ["Führen Sie die Installation des vSphere Host-NVMe-Treibers und Validierungsaufgaben durch"](#)
3. ["Erstellen eines VMFS-Datenspeichers"](#)

## VSphere herkömmliche File Storage-Bereitstellung mit ONTAP

VMware vSphere unterstützt folgende NFS-Protokolle: Beide unterstützen ONTAP.

- ["NFS-Version 3"](#)
- ["NFS-Version 4.1"](#)

Wenn Sie Hilfe bei der Auswahl der richtigen NFS-Version für vSphere benötigen, prüfen Sie die Version ["Diesen Vergleich der NFS Client-Versionen"](#).

### Referenz

["VSphere Datastore- und Protokollfunktionen: NFS"](#)

### VSphere NFS Datastore - Version 3 mit ONTAP

#### Über diese Aufgabe

Erstellung von NFS-Data-Version-3-Datenspeichern mit ONTAP-NAS-Storage

Verwenden Sie eines der folgenden Skripte für die automatisierte Bereitstellung: [\[PowerShell\]](#), [\[Ansible\]](#), Oder [\[Terraform\]](#).

## Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und ONTAP
- Ein ONTAP Storage-System (FAS/AFF/CVO/ONTAP Select/Cloud-Volume-Service/Azure NetApp Files) mit ONTAP 9.8 oder höher
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID, Passwort)
- ONTAP Netzwerkport, SVM und LUN-Informationen für NFS
  - ["Ein ausgefülltes NFS-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- VSphere Host(s)-Informationen für vSphere 7.0 oder höher
- IP-Informationen für den NFS VMkernel Adapter
- Netzwerk-Switch(e)
  - Mit Netzwerk-Daten-Ports des ONTAP Systems und verbundenen vSphere Hosts
  - Für NFS konfigurierte VLANs
  - (Optional) Link Aggregation konfiguriert für ONTAP Netzwerkdatenports
- ONTAP Tool für VMware vSphere – implementiert, konfiguriert und betriebsbereit

## Schritte

- Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\)"](#)
  - ["Vergewissern Sie sich, dass die NFS-Konfiguration unterstützt wird."](#)
- Führen Sie die folgenden Aufgaben für ONTAP und vSphere aus.

## ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für NFS."](#)
  - a. Verwenden Sie die `system license show` Führen Sie einen Befehl aus und überprüfen Sie, ob NFS aufgelistet ist.
  - b. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. ["Folgen Sie dem NFS-Konfigurations-Workflow."](#)

## Aufgaben für VMware vSphere

["Folgen Sie dem Workflow der NFS Client-Konfiguration für vSphere."](#)

## Referenz

["VSphere Datastore- und Protokollfunktionen: NFS"](#)

## Was kommt als Nächstes?

Nach Abschluss dieser Aufgaben kann der NFS-Datenspeicher zur Bereitstellung von Virtual Machines genutzt werden.

## VSphere NFS Datastore - Version 4.1 mit ONTAP

## Über diese Aufgabe

In diesem Abschnitt wird die Erstellung eines NFS-Version 4.1-Datenspeichers mit ONTAP-NAS-Speicher beschrieben.

Verwenden Sie eines der folgenden Skripte für die automatisierte Bereitstellung: [\[PowerShell\]](#), [\[Ansible\]](#), Oder [\[Terraform\]](#).

## Was Sie brauchen

- Grundkenntnisse für das Management einer vSphere Umgebung und einer ONTAP
- ONTAP-Storage-System (FAS/AFF/CVO/ONTAP Select/Cloud-Volume-Service/Azure NetApp-Dateien) mit ONTAP 9.8 oder höher
- ONTAP-Anmeldedaten (SVM-Name, Benutzer-ID, Passwort)
- ONTAP Netzwerkport, SVM und LUN-Informationen für NFS
- ["Ein ausgefülltes NFS-Konfigurationsarbeitsblatt"](#)
- Anmeldedaten für vCenter Server
- VSphere-Host(s)-Informationen vSphere 7.0 oder höher
- IP-Informationen für den NFS VMkernel Adapter
- Netzwerk-Switch(e)
  - Mit ONTAP System-Netzwerk-Daten-Ports, vSphere-Hosts und verbunden
  - Für NFS konfigurierte VLANs
  - (Optional) Link Aggregation konfiguriert für ONTAP Netzwerkdatenports
- ONTAP Tools für VMware vSphere Implementierung, Konfiguration und Einsatzbereitschaft

## Schritte

- Prüfen Sie die Kompatibilität mit dem ["Interoperabilitäts-Matrix-Tool \(IMT\):"](#)
  - ["Vergewissern Sie sich, dass die NFS-Konfiguration unterstützt wird."](#)
- Führen Sie die im Folgenden aufgeführten ONTAP- und vSphere-Aufgaben aus.

## ONTAP Aufgaben

1. ["Überprüfen Sie die ONTAP Lizenz für NFS"](#)
  - a. Einsatz `the system license show` Befehl zum Überprüfen, ob NFS aufgelistet ist.
  - b. Nutzung `license add -license-code <license code>` Um eine Lizenz hinzuzufügen.
2. ["Folgen Sie dem NFS-Konfigurations-Workflow"](#)

## Aufgaben für VMware vSphere

["Folgen Sie dem NFS Client Configuration für vSphere Workflow."](#)

## Was kommt als Nächstes?

Nach Abschluss dieser Aufgaben kann der NFS-Datenspeicher zur Bereitstellung von Virtual Machines genutzt werden.

# NetApp Hybrid-Multi-Cloud mit VMware Lösungen

## Anwendungsfälle für die VMware Hybrid-Multi-Cloud

### Anwendungsfälle für NetApp Hybrid-Multi-Cloud mit VMware

Ein Überblick über die Anwendungsfälle, die für DIE IT-Abteilung bei der Planung von Hybrid-Cloud- oder Cloud-First-Implementierungen von Bedeutung sind

#### Gängige Anwendungsfälle

Anwendungsfälle:

- Disaster Recovery,
- Hosting von Workloads während der Rechenzentrumswartung, \* schneller Burst, in dem zusätzliche Ressourcen über die im lokalen Rechenzentrum bereitgestellten Ressourcen erforderlich sind,
- VMware-Site-Erweiterung,
- Schnelle Migration in die Cloud,
- Entwicklung/Test und
- Modernisierung von Applikationen mithilfe von zusätzlichen Cloud-Technologien

In der gesamten Dokumentation werden die Referenzen für Cloud-Workloads anhand der VMware Anwendungsfälle detailliert beschrieben. Anwendungsfälle sind:

- Schutz (sowohl Disaster Recovery als auch Backup/Restore)
- Migrieren
- Erweitern

#### In DER IT-Entwicklung

Die meisten Unternehmen befinden sich auf dem Weg zur Transformation und Modernisierung. Im Rahmen dieses Prozesses versuchen Unternehmen, ihre vorhandenen VMware Investitionen zu nutzen und gleichzeitig von den Vorteilen der Cloud zu profitieren und Möglichkeiten für eine nahtlose Migration zu entdecken. Durch diesen Ansatz würde sich ihre Modernisierungsbemühungen sehr vereinfachen, da sich die Daten bereits in der Cloud befinden.

Die einfachste Antwort auf dieses Szenario sind die Angebote von VMware in jedem Hyperscaler. Wie bei NetApp Cloud Volumes bietet VMware eine Möglichkeit, lokale VMware Umgebungen in jede Cloud zu verschieben oder zu erweitern. So können Sie vorhandene Ressourcen, Fachkenntnisse und Tools weiterhin nutzen, während Sie Workloads nativ in der Cloud ausführen. Das verringert die Risiken, da keine Serviceunterbrechungen oder IP-Änderungen erforderlich sind. Das IT-Team kann so unter Verwendung vorhandener Fachkenntnisse und Tools vor Ort Verfahren. Dies ermöglicht beschleunigte Cloud-Migrationen und einen viel reibungsloseren Übergang zu einer Hybrid Multi Cloud Architektur.

#### Bedeutung von zusätzlichen NFS-Storage-Optionen

Während VMware in jeder Cloud seinen Kunden einzigartige Hybrid-Funktionen bietet, haben begrenzte zusätzliche NFS-Storage-Optionen den Nutzen für Unternehmen mit Storage-lastigen Workloads eingeschränkt. Da Storage direkt an Hosts gebunden ist, besteht die einzige Möglichkeit zur Skalierung von Storage darin, weitere Hosts hinzuzufügen. Die Kosten können bei Storage-intensiven Workloads um 35 bis 40

% oder mehr gesenkt werden. Diese Workloads erfordern nur zusätzlichen Storage und keine zusätzliche Leistung. Aber das bedeutet, dass zusätzliche Hosts bezahlt werden.

Betrachten wir das folgende Szenario:

Ein Kunde benötigt nur fünf Hosts für CPU und Arbeitsspeicher, hat aber hohe Storage-Anforderungen und benötigt 12 Hosts, um die Storage-Anforderungen zu erfüllen. Diese Anforderung kippt letztlich in Richtung Finanzskalierung, indem sie zusätzliche Leistung kaufen müssen, wenn sie nur den Storage erhöhen müssen.

Wenn Sie Cloud-Einführung und -Migrationen planen, ist es immer wichtig, den besten Ansatz zu bewerten und den einfachsten Weg zu gehen, der die Gesamtinvestitionen reduziert. Der gängigste und einfachste Ansatz für jede Applikationsmigration besteht in Rehosting (auch bekannt als „Lift and Shift“), in dem keine Virtual Machine (VM) oder Datenkonvertierung vorhanden ist. NetApp Cloud Volumes mit dem softwaredefinierten Datacenter (SDDC) von VMware und ergänzen vSAN und bieten eine einfache „Lift-and-Shift“-Option.

## Virtual Desktops

### Virtual Desktop Services (VDS)

#### TR-4861: Hybrid Cloud VDI mit Virtual Desktop Service

Suresh ThopPay, NetApp

Der NetApp Virtual Desktop Service (VDS) orchestriert die Remote Desktop Services (RDS) in führenden Public Clouds sowie auf Private Clouds. VDS unterstützt Windows Virtual Desktop (WVD) unter Microsoft Azure. VDS automatisiert viele Aufgaben, die nach der Implementierung von WVD oder RDS ausgeführt werden müssen, einschließlich der Einrichtung von SMB-Dateifreigaben (für Benutzerprofile, gemeinsam genutzte Daten und das Benutzer-Home-Laufwerk) sowie der Aktivierung von Windows-Funktionen, Applikations- und Agent-Installation, Firewall sowie Richtlinien usw.

Benutzer nutzen VDS für dedizierte Desktops, Shared Desktops und Remote-Applikationen. VDS bietet skriptbasierte Ereignisse zur Automatisierung des Anwendungsmanagements für Desktops und verringert die Anzahl der zu verwaltenden Images.

VDS bietet ein zentrales Management-Portal für den Umgang mit Implementierungen über Public und Private Cloud-Umgebungen hinweg.

#### Mehrwert Für Den Kunden

Die explosionsartige Zunahme der Mitarbeiter an Remote-Standorten im Jahr 2020 hat die Anforderungen an Business Continuity geändert. IT-Abteilungen stehen bei der schnellen Bereitstellung virtueller Desktops vor neuen Herausforderungen. Sie müssen daher flexible Lösungen bei der Bereitstellung, Remote-Management und die TCO-Vorteile einer Hybrid Cloud benötigen, was die Bereitstellung von On-Premises- und Cloud-Ressourcen vereinfacht. Sie benötigen eine Hybrid-Cloud-Lösung mit folgenden Vorteilen:

- Adressiert die Realität des Post-COVID-Arbeitsbereichs, um flexible Arbeitsmodelle mit globaler Dynamik zu ermöglichen
- Schichtarbeit wird ermöglicht, indem die Bereitstellung von Arbeitsumgebungen für alle Mitarbeiter vereinfacht und beschleunigt wird, von Task Workers bis hin zu Power Usern

- Mobilisiert Ihre Mitarbeiter, indem Sie umfassende, sichere VDI-Ressourcen bereitstellen, unabhängig vom physischen Standort
- Vereinfachte Hybrid-Cloud-Implementierung
- Automatisiert und vereinfacht das Management zur Risikominimierung

### **Anwendungsfälle**

Mit einer hybriden VDI mit NetApp VDS können Service-Provider und Virtual Desktop-Administratoren der Enterprise-Klasse Ressourcen problemlos auf andere Cloud-Umgebungen erweitern, ohne ihre Benutzer zu beeinträchtigen. Das Vorhandensein von On-Premises-Ressourcen ermöglicht eine bessere Kontrolle von Ressourcen und bietet umfassende Auswahl an Optionen (Computing, GPU, Storage und Netzwerk) zur Erfüllung der Anforderungen.

Diese Lösung trifft auf folgende Anwendungsfälle zu:

- Wechsel zur Cloud aufgrund von rasant anstiegenderem Bedarf an Remote-Desktops und -Applikationen
- Reduzieren der TCO für lange ausgeführte Remote-Desktops und Applikationen, indem sie lokal mit Flash-Storage- und GPU-Ressourcen gehostet werden
- Einfaches Management von Remote-Desktops und -Applikationen in Cloud-Umgebungen
- Erleben Sie Remote-Desktops und -Applikationen mit einem Software-as-a-Service-Modell mit On-Premises-Ressourcen

### **Zielgruppe**

Die Zielgruppe für die Lösung umfasst die folgenden Gruppen:

- EUC-/VDI-Architekten, die die Anforderungen an ein hybrides VDS verstehen möchten
- NetApp Partner, die Kunden bei ihren Remote-Desktop- und -Applikationsanforderungen unterstützen möchten
- Vorhandene NetApp HCI Kunden, die Remote-Desktop- und -Applikationsanforderungen erfüllen möchten

### **NetApp Virtual Desktop Service – Überblick**

NetApp bietet viele Cloud-Services an, darunter die schnelle Bereitstellung von Virtual Desktop mit WVD oder Remote-Applikationen und die schnelle Integration mit Azure NetApp Files.

Üblicherweise dauert die Bereitstellung und Bereitstellung von Remote Desktop Services für Kunden Wochen. Abgesehen von der Provisionierung kann es schwierig sein, Applikationen, Benutzerprofile, gemeinsam genutzte Daten und Gruppenrichtlinienobjekte zu managen, um Richtlinien durchzusetzen. Firewall-Regeln können die Komplexität erhöhen und erfordern eigene Kenntnisse und Tools.

Mit dem Microsoft Azure Windows Virtual Desktop Service übernimmt Microsoft die Wartung der Komponenten von Remote Desktop Services, sodass Kunden sich auf die Bereitstellung von Workspaces in der Cloud konzentrieren können. Kunden müssen den gesamten Stack bereitstellen und managen, für den das Management von VDI-Umgebungen besondere Fähigkeiten erforderlich sind.

Mit VDS können Kunden virtuelle Desktops schnell implementieren, ohne sich Gedanken darüber machen zu müssen, wo Komponenten wie Broker, Gateways, Agents usw. installiert werden müssen. Kunden, die die

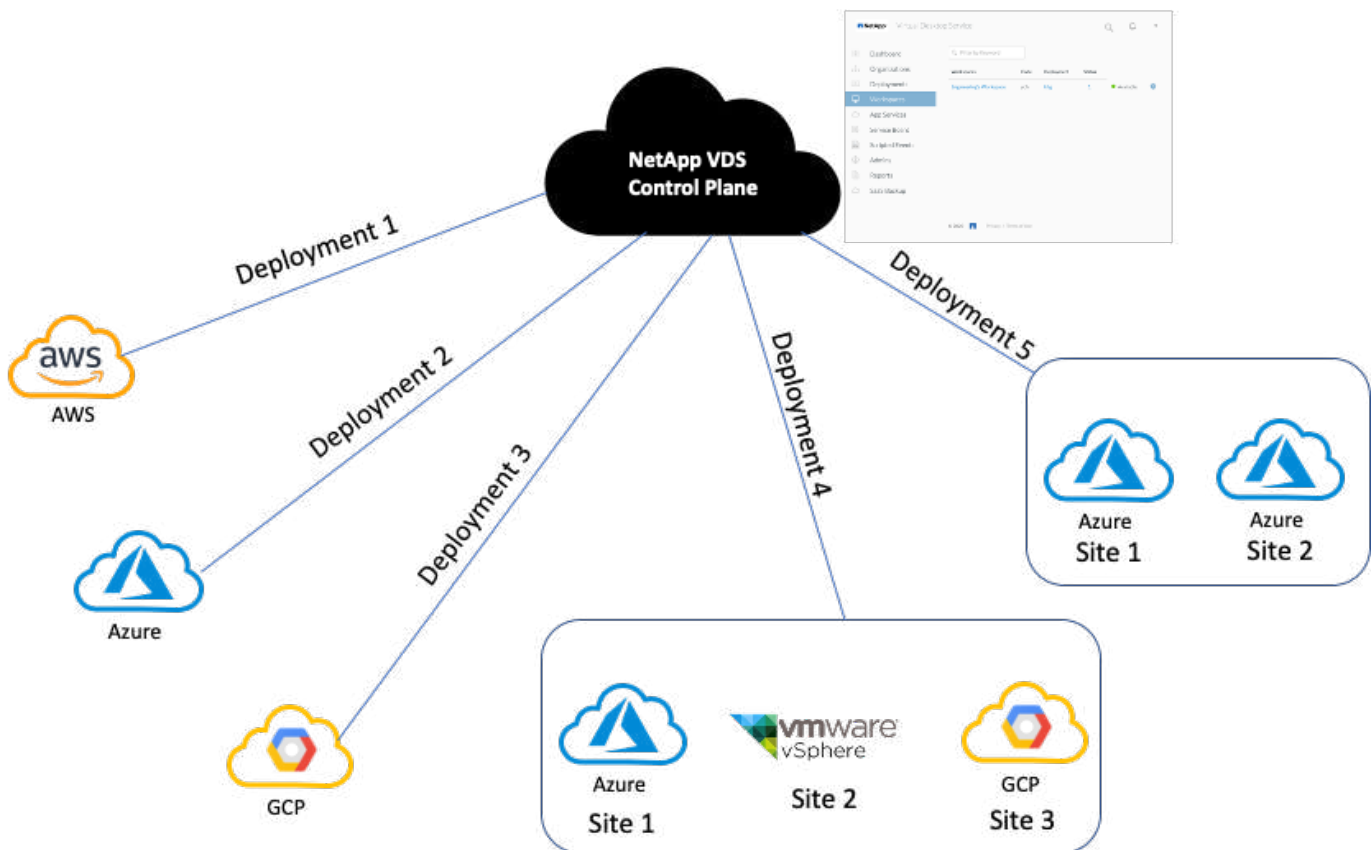


vollständige Kontrolle über ihre Umgebung benötigen, können mit einem Professional Services Team zusammenarbeiten, um ihre Ziele zu erreichen. Kunden nutzen VDS als Service und können sich somit auf ihre wichtigsten geschäftlichen Herausforderungen konzentrieren.

NetApp VDS ist ein Software-as-a-Service-Angebot für das zentrale Management mehrerer Implementierungen in AWS, Azure, GCP oder Private Cloud-Umgebungen. Microsoft Windows Virtual Desktop ist nur auf Microsoft Azure verfügbar. NetApp VDS orchestriert Microsoft Remote Desktop Services in anderen Umgebungen.

Microsoft bietet Multisession unter Windows 10 ausschließlich für Windows Virtual Desktop-Umgebungen auf Azure an. Die Authentifizierung und Identität werden durch die Virtual Desktop-Technologie gehandhabt. WVD erfordert Azure Active Directory Synchronisiert (mit AD Connect) mit Active Directory und Session-VMs, die mit Active Directory verbunden sind. RDS erfordert Active Directory für die Benutzeridentität und Authentifizierung, während VM-Domänen beitreten und verwalten.

Die folgende Abbildung zeigt eine Beispieltopologie für die Implementierung.

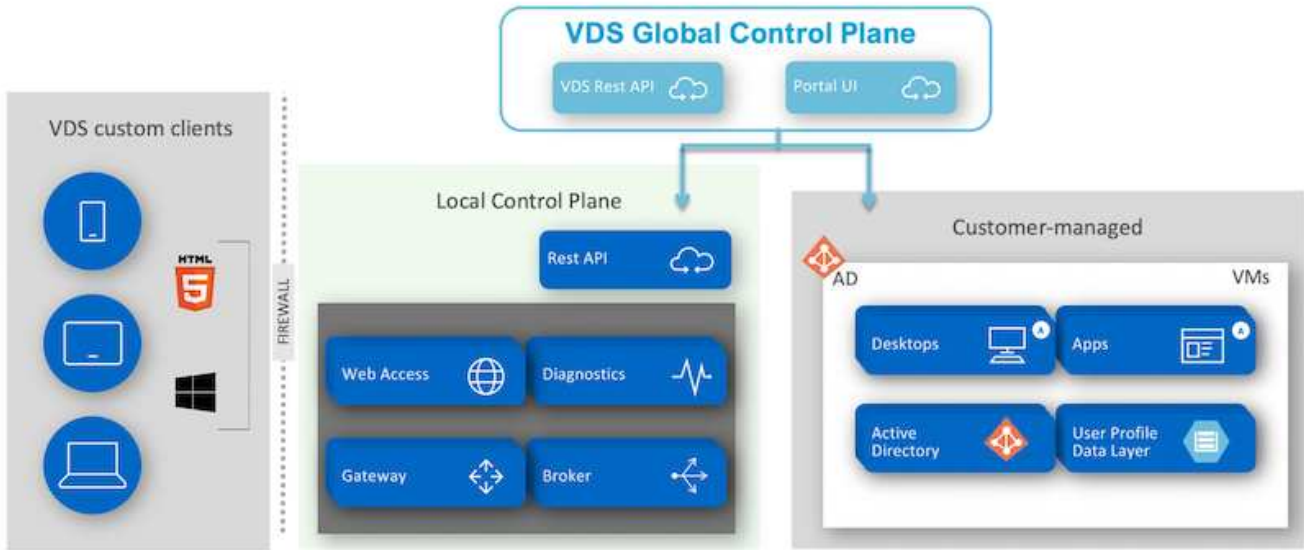


Jede Bereitstellung ist mit einer Active Directory-Domäne verknüpft und stellt den Clients einen Zugriffspunkt für Arbeitsbereiche und Anwendungen zur Verfügung. Ein Service-Provider oder Unternehmen mit mehreren Active Directory-Domänen verfügt in der Regel über mehr Implementierungen. Eine einzelne Active Directory-Domäne, die mehrere Regionen umfasst, verfügt normalerweise über eine einzige Implementierung mit mehreren Standorten.

Für WVD in Azure bietet Microsoft eine Plattform als Service, die von NetApp VDS verbraucht wird. Für andere Umgebungen orchestriert NetApp VDS die Implementierung und Konfiguration von Microsoft Remote Desktop Services. NetApp VDS unterstützt sowohl WVD Classic ALS auch WVD ARM und kann auch für ein Upgrade vorhandener Versionen verwendet werden.

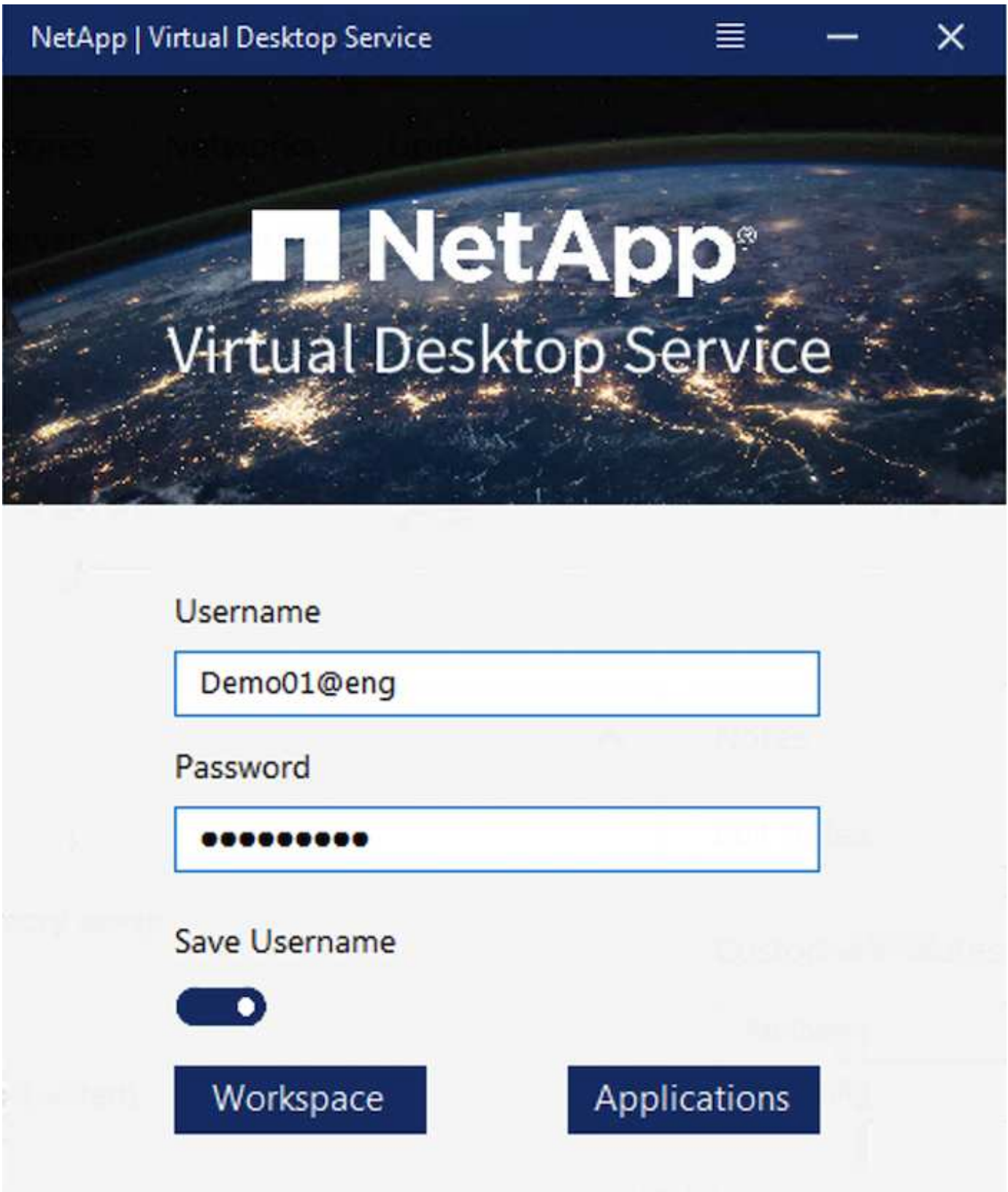
Jede Implementierung verfügt über eigene Plattform-Services, die aus Cloud Workspace Manager (REST-API-

Endpunkt), einem HTML 5 Gateway (Verbindung zu VMs über ein VDS-Managementportal), RDS Gateways (Access Point für Clients) und einem Domain Controller bestehen. Die folgende Abbildung zeigt die VDS Control Plane Architektur für die Implementierung von RDS.



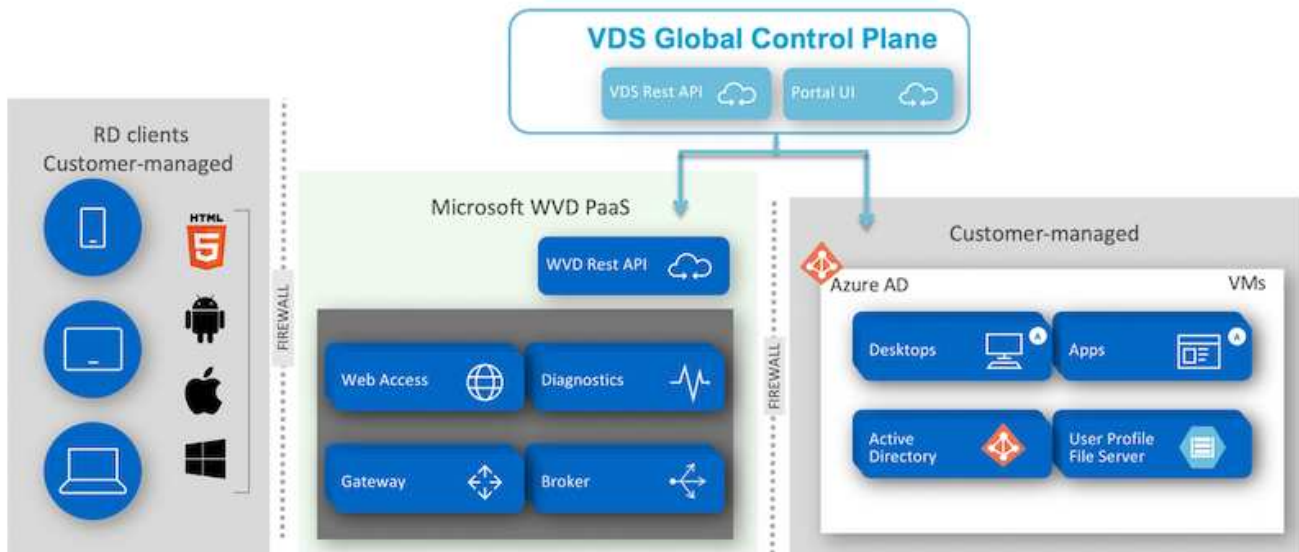
Bei RDS-Implementierungen ist der Zugriff auf NetApp VDS über Windows und Browser mithilfe der Client-Software möglich, die angepasst werden kann und das Kundenlogo und -Bilder enthält. Basierend auf den Benutzeranmeldeinformationen bietet es Benutzern Zugriff auf genehmigte Arbeitsbereiche und Anwendungen. Es müssen keine Gateway-Details konfiguriert werden.

Die folgende Abbildung zeigt den NetApp VDS Client.



In der Azure WVD-Implementierung übernimmt Microsoft den Zugriffspunkt für die Clients und kann von einem Microsoft WVD-Client genutzt werden, der nativ für verschiedene Betriebssysteme verfügbar ist. Sie ist auch über ein webbasiertes Portal zugänglich. Die Konfiguration der Client-Software muss vom Group Policy Object (GPO) oder auf andere Weise vom Kunden bevorzugt werden.

Die folgende Abbildung zeigt die VDS Control Plane Architecture für Azure WVD-Implementierungen.



Neben der Implementierung und Konfiguration der erforderlichen Komponenten übernimmt NetApp VDS auch das Management von Benutzern, das Applikations-Management, die Skalierung von Ressourcen und die Optimierung.

NetApp VDS kann Benutzer erstellen oder bestehenden Benutzerkonten Zugriff auf Cloud-Workspace oder Applikationsservices gewähren. Das Portal kann auch für das Zurücksetzen von Kennwörtern und die Delegierung der Verwaltung einer Teilmenge von Komponenten verwendet werden. Helpdesk-Administratoren oder Level-3-Techniker können Benutzersitzungen zur Fehlerbehebung Schatten stellen oder eine Verbindung zu Servern innerhalb des Portals herstellen.

NetApp VDS kann die von Ihnen erstellten Bildvorlagen verwenden oder vorhandene vom Markt für die Cloud-basierte Bereitstellung nutzen. Um die Anzahl der zu managenden Images zu verringern, können Sie ein Basis-Image verwenden. Weitere Applikationen, die Sie benötigen, können Sie über das zur Verfügung gestellte Framework bereitstellen. Dazu gehören sämtliche Befehlszeilen-Tools wie Chocolatey, MSIX App-Attached, PowerShell usw. Sogar benutzerdefinierte Skripts können als Teil von Ereignissen des Maschinellen Lebenszyklus verwendet werden.

### Übersicht über NetApp HCI

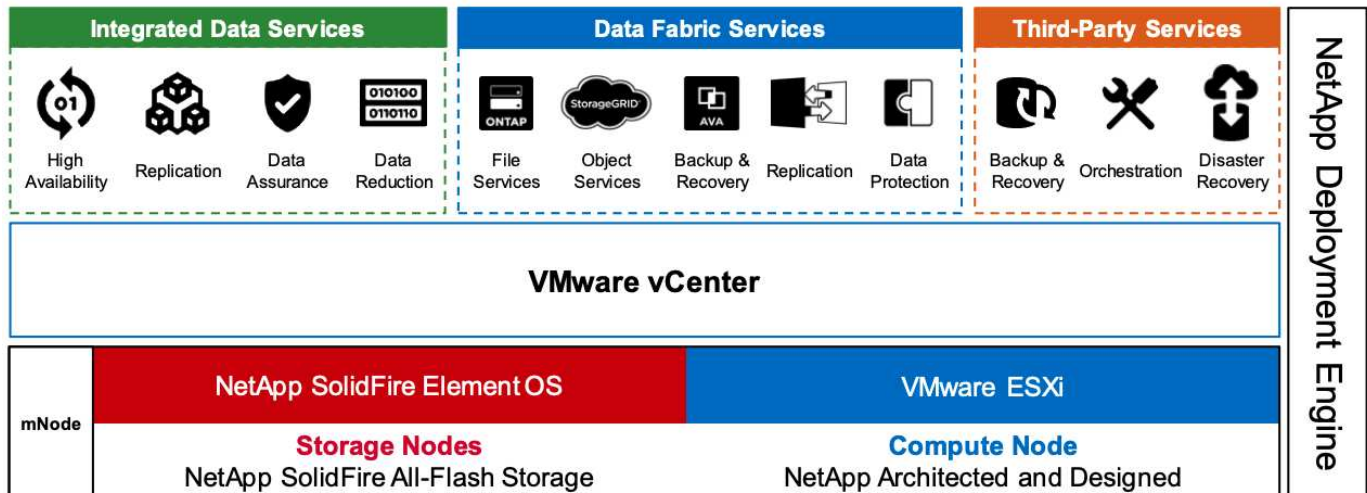
NetApp HCI ist eine Hybrid-Cloud-Infrastruktur, die aus einer Kombination von Storage- und Compute-Nodes besteht. Und ist je nach Modell als Einheit mit zwei oder einem Rack erhältlich. Die zur Implementierung von VMs erforderliche Installation und Konfiguration werden mithilfe der NetApp Deployment Engine (nde) automatisiert. Compute-Cluster werden mit VMware vCenter gemanagt, während Storage-Cluster mit dem via nde bereitgestellten vCenter Plug-in gemanagt werden. Als Teil der nde wird zudem eine Management-VM namens mNode bereitgestellt.

NetApp HCI übernimmt folgende Funktionen:

- Versionsupgrades
- Übermittlung von Ereignissen per Push an vCenter
- vCenter Plug-in-Management
- Ein VPN-Tunnel zur Unterstützung



- Den NetApp Active IQ Collector
- Die Erweiterung von NetApp Cloud Services auf On-Premises-Systeme (ermöglicht eine Hybrid-Cloud-Infrastruktur). In der folgenden Abbildung sind die HCI Komponenten dargestellt.



## Storage-Nodes

Storage-Nodes sind als Rack-Einheit in halber oder in voller Breite verfügbar. Zuerst sind mindestens vier Storage-Nodes erforderlich und ein Cluster kann auf bis zu 40 Nodes erweitert werden. Ein Storage-Cluster kann über mehrere Compute-Cluster hinweg gemeinsam genutzt werden. Alle Storage-Nodes verfügen zur Verbesserung der Schreib-Performance über einen Cache-Controller. Ein einzelner Node bietet entweder 50.000 oder 100.000 IOPS mit einer Blockgröße von 4 KB.

Auf NetApp HCI Storage-Nodes wird die NetApp Element Software ausgeführt. Diese begrenzt-, maximal- und Burst-QoS-Limits. Das Storage-Cluster unterstützt eine Kombination aus Storage-Nodes, wobei ein Storage-Node jedoch ein Drittel der Gesamtkapazität nicht überschreiten darf.

## Compute-Nodes



NetApp unterstützt seinen Storage, der mit den im aufgeführten Computing-Servern verbunden ist "[VMware Compatability Guide](#)".

Compute-Nodes sind in halber Breite, voller Breite und zwei Höheneinheiten verfügbar. Der NetApp HCI H410C und der H610C arbeiten mit skalierbaren Intel Skylake-Prozessoren. Der H615C arbeitet mit skalierbaren Intel Cascade Lake Prozessoren der zweiten Generation. Es sind zwei Compute-Modelle mit GPUs verfügbar: Der H610C enthält zwei NVIDIA M10-Karten und der H615C enthält drei NVIDIA T4-Karten.



Die NVIDIA T4 enthält 40 RT-Cores, die die für das Echtzeit-Ray-Tracing erforderliche Rechenleistung liefern. Das von Designern und Ingenieuren häufig verwendete Server-Modell kann jetzt auch von Künstlern verwendet werden, um fotorealistic Bilder zu erstellen, bei denen das Licht von Oberflächen wie im wirklichen Leben von den Oberflächen abstrahlt. Diese RTX-fähige GPU erzeugt eine Echtzeit-Ray-Tracing-Performance von bis zu fünf GIGA-Rays pro Sekunde. In Kombination mit der Quadro Virtual Data Center Workstation-Software (Quadro VDWS) ermöglicht es die NVIDIA T4 Künstlern, an jedem Standort und auf jedem Gerät fotorealistic Designs mit exakten Schatten, Reflexionen und Brechungen zu gestalten.

Tensor Cores ermöglichen die Ausführung von Deep-Learning-Inferenz-Workloads. Wenn sie diese Workloads ausführen, kann ein NVIDIA T4 mit Quadro VDWS bis zu 25-mal schneller als eine VM, die von einem rein CPU-basierten Server angetrieben wird. Ein NetApp H615C mit drei NVIDIA T4-Karten in einer Rack-Einheit ist eine ideale Lösung für Grafik- und rechenintensive Workloads.

In der folgenden Abbildung werden NVIDIA-GPU-Karten aufgeführt und deren Funktionen miteinander verglichen.

NVIDIA GPUs Recommended for Virtualization				Available on NetApp HCI H615C	Available on NetApp HCI H610C	
	V100S	RTX 8000	RTX 6000	T4	M10	P6
GPU	1 NVIDIA Volta	1 NVIDIA Turing	1 NVIDIA Turing	1 NVIDIA Turing	4 NVIDIA Maxwell	1 NVIDIA Pascal
CUDA Cores	5,120	4,608	4,608	2,560	2,560 (640 per GPU)	2,048
Tensor Cores	640	576	576	320	—	—
RT Cores	—	72	72	40	—	—
Guaranteed QoS (GPU Scheduler)	✓	✓	✓	✓	—	✓
Live Migration	✓	✓	✓	✓	✓	✓
Multi-vGPU	✓	✓	✓	✓	✓	✓
Memory Size	32/16 GB HBM2	48 GB GDDR6	24 GB GDDR6	16 GB GDDR6	32 GB GDDR5 (8 GB per GPU)	16 GB GDDR5
vGPU Profiles	1 GB, 2 GB, 4 GB, 8 GB, 16 GB, 32 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 16 GB, 24 GB, 48 GB	1 GB, 2 GB, 3 GB, 4 GB, 6 GB, 8 GB, 12 GB, 24 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB	0.5 GB, 1 GB, 2 GB, 4 GB, 8 GB	1 GB, 2 GB, 4 GB, 8 GB, 16 GB
Form Factor	PCIe 3.0 dual slot and SXM2	PCIe 3.0 dual slot	PCIe 3.0 dual slot	PCIe 3.0 single slot	PCIe 3.0 dual slot	MXM (blade servers)
Power	250 W /300 W (SXM2)	250 W	250 W	70 W	225 W	90 W
Thermal	passive	passive	passive	passive	passive	bare board
vGPU Software Support	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer	Quadro vDWS, GRID vPC, GRID vApps	Quadro vDWS, GRID vPC, GRID vApps, vComputeServer
Use Case	Ultra-high-end rendering, simulation, 3D design with Quadro vDWS; ideal upgrade path for V100	High-end rendering, 3D design and creative workflows with Quadro vDWS	Mid-range to high-end rendering, 3D design and creative workflows with Quadro vDWS	Entry-level to high-end 3D design and engineering workflows with Quadro vDWS. High-density, low power GPU acceleration for knowledge workers with NVIDIA GRID software.	Knowledge workers using modern productivity apps and Windows 10 requiring best density and total cost of ownership (TCO), multimonitor support with NVIDIA GRID vPC/vApps	For customers requiring GPUs in a blade server form factor; ideal upgrade path for M6

M10 GPU bleibt die beste TCO-Lösung für Knowledge-Worker-Anwendungsfälle. Die T4 ist jedoch eine hervorragende Alternative, wenn beispielsweise im Unternehmen eine einheitliche GPU verwendet werden soll, die sich für verschiedene Anwendungsfälle eignet, beispielsweise für virtuelle Workstations, Grafikleistung, interaktives Echtzeit-Rendern und Inferenz. Dank der T4 können DIE IT-TECHNIKER die GPU-Ressourcen zur Durchführung unterschiedlicher Workloads nutzen—beispielsweise um tagsüber VDI und nachts Compute-Workloads auszuführen.

Der H610C Compute-Node ist zwei Höheneinheiten groß. Der H615C ist eine Höheneinheit groß und verbraucht weniger Strom. Der H615C unterstützt H.264 und H.265 (High Efficiency Video Coding [HEVC]) 4:4:4-Codierung und -Dekodierung. Er unterstützt auch den zunehmend Mainstream VP9-Dekoder. Selbst das von YouTube bereitgestellte WebM-Container-Paket verwendet den VP9-Codec für Videos.

Die Anzahl der Nodes in einem Compute-Cluster wird von VMware vorgegeben und beträgt derzeit 96 Nodes mit VMware vSphere 7.0 Update 1. Die Kombination verschiedener Compute-Node-Modelle in einem Cluster wird unterstützt, wenn Enhanced vMotion Compatibility (EVC) aktiviert ist.

### NVIDIA-Lizenzierung

Bei Verwendung eines H610C oder H615C muss die Lizenz für die GPU von einem dafür autorisierten NVIDIA-Partner erworben werden. NVIDIA-Partner finden Sie mit dem **"PARTNERFINDER"**. Suche nach Kompetenzen wie Virtual GPU (vGPU) oder Tesla

Die NVIDIA vGPU-Software ist in vier Editionen verfügbar:

- NVIDIA GRID Virtual PC (GRID vPC)
- NVIDIA GRID Virtual Applikationen (GRID vApps)
- NVIDIA Quadro Virtual Data Center Workstation (Quadro VDWS)
- NVIDIA Virtual ComputeServer (vComputeServer)

## GRID Virtual PC

Dieses Produkt ist ideal für Benutzer, die einen virtuellen Desktop benötigen, der eine hohe Benutzerfreundlichkeit für Microsoft Windows Applikationen, Browser, HD-Video und Unterstützung für mehrere Monitore bietet. NVIDIA GRID Virtual PC bietet ein natives Arbeiten in einer virtuellen Umgebung, sodass Sie alle PC-Applikationen ohne jede Einschränkung ausführen können.

## GRID Virtual Applikationen

GRID vApps richten sich an Unternehmen, die einen RDSH (Remote Desktop Session Host) oder andere Applikations-Streaming- oder sitzungsbasierte Lösungen einsetzen. Auf Windows-Servern gehostete RDSH-Desktops, auf denen Microsoft Windows-Applikationen ohne Leistungseinschränkungen laufen, werden von GRID vApps ebenfalls unterstützt.

## Quadro Virtual Data Center Workstation

Diese Edition eignet sich ideal für große und anspruchsvolle Designer, die leistungsstarke Anwendungen zur Erstellung von 3D-Inhalten wie Dassault CATIA, SOLIDWORKS, 3DEXCITE, Siemens NX, PTC Creo, Schlumberger Petrel oder Autodesk Maya. NVIDIA Quadro VDWS ermöglicht es Nutzern, überall und auf jedem Gerät auf ihre professionellen Grafik-Applikationen mit vollständigen Funktionen und Performance zuzugreifen.

## NVIDIA Virtual ComputeServer

In vielen Unternehmen werden rechenintensive Server-Workloads wie künstliche Intelligenz (KI), Deep Learning (DL) und Data Science ausgeführt. In diesen Einsatzbereichen virtualisiert die NVIDIA vComputeServer-Software die NVIDIA-GPU, die rechenintensive Server-Workloads mit Funktionen wie Fehlerkorrektur-Code, Page Retirement, Peer-to-Peer über NVLink und Multi-vGPU beschleunigt.



Eine Quadro VDWS-Lizenz berechtigt Sie zur Nutzung VON GRID vPC und NVIDIA vComputeServer.

## Einsatz

NetApp VDS kann mithilfe einer Setup-Applikation, die basierend auf der erforderlichen Codebase verfügbar ist, in Microsoft Azure implementiert werden. Die aktuelle Version ist verfügbar ["Hier"](#) Und die Vorversion des bevorstehenden Produkts ist verfügbar ["Hier"](#).

Siehe ["Dieses Video"](#) Anleitungen zur Implementierung.



# NetApp Virtual Desktop Service

## Deployment & AD Connect

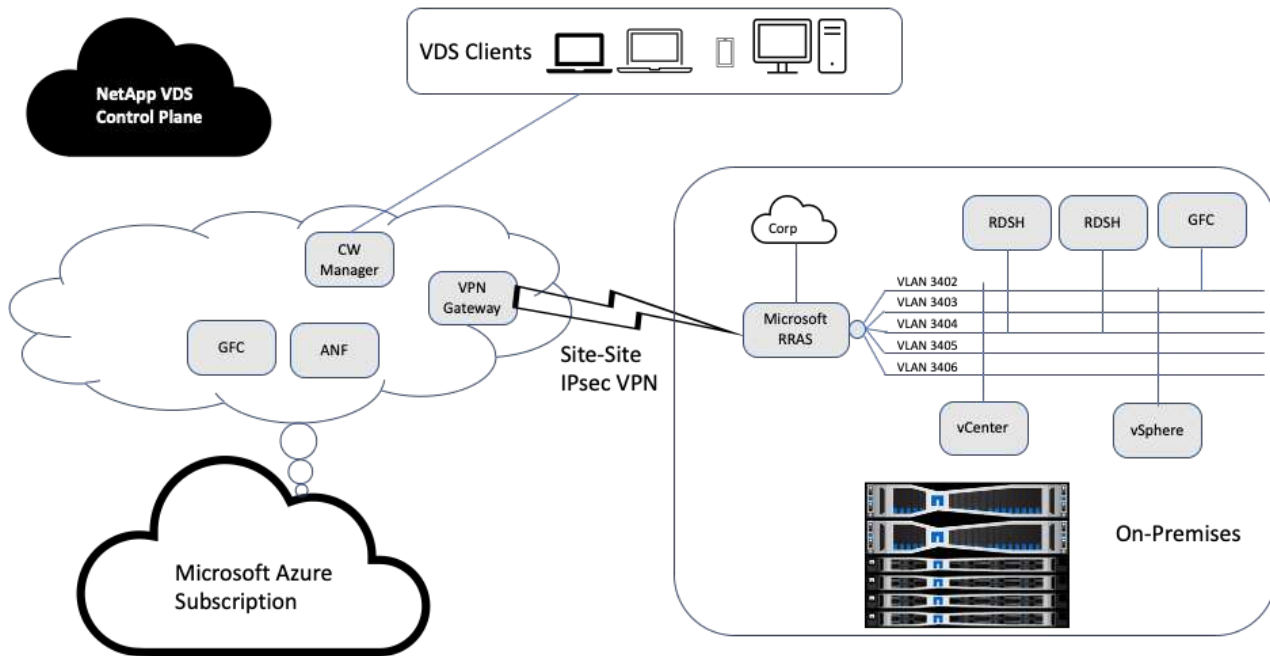
Toby vanRoojen  
Product Marketing Manager  
June, 2020

### Hybrid Cloud-Umgebung

Der NetApp Virtual Desktop Service kann bei der Konnektivität zwischen lokalen Ressourcen und Cloud-Ressourcen auf den lokalen Storage erweitert werden. Unternehmen können die Verbindung zu Microsoft Azure über Express Route oder eine IPsec-VPN-Verbindung zwischen Standorten herstellen. Sie können auch Verbindungen zu anderen Clouds auf ähnliche Weise erstellen, entweder über eine dedizierte Verbindung oder über einen IPsec VPN-Tunnel.

Für die Lösungsvalidierung verwendeten wir die in der folgenden Abbildung dargestellte Umgebung.





Vor Ort hatten wir mehrere VLANs für das Management, Hosts zur Remote-Desktop-Session usw. Sie befanden sich im Subnetz 172.21.146-150.0/24 und wurden mithilfe des Microsoft Remote Routing Access Service an das Unternehmensnetzwerk weitergeleitet. Außerdem haben wir folgende Aufgaben ausgeführt:

1. Wir haben die öffentliche IP des Microsoft Routing and Remote Access Servers (RRAS; identifiziert mit IPchicken.com) festgestellt.
2. Wir haben eine Ressource für Virtual Network Gateway (Routing-basiertes VPN) auf Azure Subscription erstellt.
3. Wir haben die Verbindung erstellt, die die lokale Netzwerk-Gateway-Adresse für die öffentliche IP des Microsoft RRAS-Servers bereitstellt.
4. Wir haben die VPN-Konfiguration auf RRAS abgeschlossen, um eine virtuelle Schnittstelle mit vorgemeinsamer Authentifizierung zu erstellen, die bei der Erstellung des VPN-Gateways bereitgestellt wurde. Bei korrekter Konfiguration sollte sich das VPN im Status „Verbunden“ befinden. Anstelle von Microsoft RRAS können Sie auch pfSense oder andere relevante Tools verwenden, um den Site-to-Site IPsec VPN-Tunnel zu erstellen. Da es sich um eine Routingbasierte handelt, wird der Datenverkehr anhand der konfigurierten Subnetze umgeleitet.

Microsoft Azure Active Directory bietet Identitätsauthentifizierung basierend auf OAuth. Für die Authentifizierung von Enterprise-Clients ist in der Regel eine NTLM- oder Kerberos-basierte Authentifizierung erforderlich. Microsoft Azure Active Directory-Domänendienste führen Passwort-Hash-Synchronisierung zwischen Azure Active Directory und lokalen Domänencontrollern mithilfe von ADConnect durch.

Für diese Hybrid VDS-Lösungvalidierung wurde zunächst in Microsoft Azure implementiert und dann noch ein zusätzlicher Standort mit vSphere hinzugefügt. Der Vorteil bei diesem Ansatz besteht darin, dass Plattformservices in Microsoft Azure implementiert und anschließend über das Portal ohne weiteres gesichert wurden. Auf Services kann von überall aus problemlos zugegriffen werden, selbst wenn die Site-Site-VPN-Verbindung nicht verfügbar ist.

Zum Hinzufügen einer weiteren Site haben wir ein Tool namens DCConfig verwendet. Die Verknüpfung zur

Anwendung ist auf dem Desktop der VM des Cloud Workspace Manager (CWMgr) verfügbar. Nachdem diese Anwendung gestartet wurde, navigieren Sie zur Registerkarte „DataCenter Sites“, fügen Sie den neuen Datacenter-Standort hinzu, und geben Sie die erforderlichen Informationen wie unten gezeigt ein. Die URL verweist auf die vCenter IP. Stellen Sie sicher, dass die CWMgr VM mit vCenter kommunizieren kann, bevor Sie die Konfiguration hinzufügen.



Stellen Sie sicher, dass vSphere PowerCLI 5.1 auf CloudWorkspace Manager installiert ist, um die Kommunikation mit VMware vSphere Umgebung zu ermöglichen.

Die folgende Abbildung zeigt die Konfiguration des Datacenter-Standorts vor Ort.

The screenshot displays the 'DataCenter Sites' configuration page. On the left, a table lists existing sites:

DataCenter Site	Type	Is Primary	DataCenter Site Detail
Site 1	AzureRM	<input checked="" type="checkbox"/>	
Site 2	vSphere	<input type="checkbox"/>	

Below the table, a red message reads: "To delete DataCenter Site(s), Select it and right click to delete".

The right-hand side of the interface shows the configuration for 'Site 2':

- DataCenter Site:** Site 2
- Hypervisor:** vSphere
- General Settings:**
  - Local VM Account:** Username: Administrator, Password: [masked]
  - Hypervisor Account:** Username: Administrator@vsphere, Password: [masked]
  - URL:** https://172.21.146.150/sdk/
  - VM Name Prefix:** [empty]
  - Max Concurrent Create Server:** 20
  - Subnet Mask:** 255.255.255.0
  - Default Gateway:** 172.21.148.250
  - Is Primary Hypervisor?:**  Yes  No
  - Must Set IpAddress Of VMs:**  Yes  No
- DNS:**
  - Primary DNS:** 10.67.78.11
  - Secondary DNS:** [empty]
  - Set DNS Address:**  Yes  No
- VSphere:**
  - Data Center:** NetApp-HCI-Datacenter
  - Cluster:** [empty]
  - Resource Pool:** [empty]
  - Host Name:** [empty]
  - VM Folder:** VDS
  - Max VMs In Datastore:** -1
  - Min HD Free Space In Datastore GB:** -1
  - Min Ram Free GB:** -1

At the bottom, there are checkboxes for "Exclude VSphere DataStore" and "Exclude VSphere ResourcePools".

Beachten Sie, dass Filteroptionen für Computing-Ressourcen auf Basis des jeweiligen Clusters, Host-Namens oder freien RAM-Speicherplatzes verfügbar sind. Die Filteroptionen für Storage-Ressourcen beinhalten den minimalen freien Speicherplatz auf Datastores oder die maximale Anzahl von VMs pro Datenspeicher. Datastores können mit regulären Ausdrücken ausgeschlossen werden. Klicken Sie auf die Schaltfläche Speichern, um die Konfiguration zu speichern.

Um die Konfiguration zu validieren, klicken Sie auf die Schaltfläche Test oder klicken Sie auf Hypervisor laden und prüfen Sie die Dropdown-Liste unter vSphere. Er sollte mit entsprechenden Werten gefüllt werden. Es empfiehlt sich, den primären Hypervisor für den Standard-Bereitstellungsstandort auf „Ja“ gesetzt zu lassen.

Die auf VMware vSphere erstellten VM-Vorlagen werden als Sammlungen auf VDS verwendet. Provisioning-Sammlungen haben zwei Formen: Shared IT und VDI. Der Sammeltyp für Shared Provisioning wird für Remote Desktop Services verwendet, bei denen eine einzelne Ressourcenrichtlinie auf alle Server angewendet wird. Der VDI-Typ wird für WVD-Instanzen verwendet, denen die Ressourcenrichtlinie individuell zugewiesen wird. Den Servern in einer Bereitstellungssammlung kann eine der folgenden drei Rollen zugewiesen werden:

- **TSDATA.** Kombination von Terminal Services und Data Server-Rolle.
- **TS.** Terminaldienste (Session Host).
- **\* DATA.\*** File Server oder Database Server. Wenn Sie die Serverrolle definieren, müssen Sie die VM-Vorlage und den Storage (Datenspeicher) auswählen. Der ausgewählte Datenspeicher kann auf einen bestimmten Datenspeicher beschränkt werden. Alternativ kann die am wenigsten genutzte Option verwendet werden, bei der der Datenspeicher basierend auf der Datennutzung ausgewählt wird.

Jede Implementierung verfügt über Standardeinstellungen für VM-Ressourcen für die Cloud-Ressourcenzuweisung basierend auf „aktiven Benutzern“, „Feste“, „Serverlast“ oder „Benutzeranzahl“.

#### Belastungstest mit einem Server mit Login VSI

Der NetApp Virtual Desktop Service verwendet das Microsoft Remote Desktop Protocol für den Zugriff auf virtuelle Desktop-Sitzungen und -Applikationen. Das Login VSI Tool bestimmt die maximale Anzahl an Benutzern, die auf einem bestimmten Servermodell gehostet werden können. Login VSI simuliert Benutzeranmeldung in bestimmten Intervallen und führt Benutzervorgänge wie das Öffnen von Dokumenten, Lesen und Komprimieren von Mails, Arbeiten mit Excel und PowerPoint, Drucken von Dokumenten, Komprimieren von Dateien und das Erstellen zufälliger Pausen durch. Er misst dann Reaktionszeiten. Die Reaktionszeit der Benutzer ist bei niedriger Server-Auslastung gering und erhöht sich, wenn mehr Benutzersitzungen hinzugefügt werden. Login VSI bestimmt den Basisplan basierend auf den ersten Benutzeranmeldesessions und meldet die maximale Benutzersitzung, wenn die Benutzerantwort 2 Sekunden von der Baseline entfernt ist.

Der NetApp Virtual Desktop Service verwendet das Microsoft Remote Desktop Protocol, um auf die virtuelle Desktop-Session und Applikationen zuzugreifen. Um die maximale Anzahl von Benutzern zu bestimmen, die auf einem bestimmten Servermodell gehostet werden können, haben wir das Login VSI-Tool verwendet. Login VSI simuliert Benutzeranmeldung in bestimmten Intervallen und führt Benutzervorgänge durch, wie z. B. das Öffnen von Dokumenten, Lesen und Komprimieren von Mails, Arbeiten mit Excel und PowerPoint, Drucken von Dokumenten, Komprimieren von Dateien, Zufallspausen usw. Er misst auch Reaktionszeiten. Die Reaktionszeit der Benutzer ist bei niedriger Server-Auslastung gering und erhöht sich, wenn mehr Benutzersitzungen hinzugefügt werden. Login VSI bestimmt den Basisplan basierend auf den ersten Benutzeranmeldesessions und meldet die maximalen Benutzersitzungen, wenn die Benutzerantwort 2 Sekunden von der Baseline entfernt ist.

Die folgende Tabelle enthält die Hardware, die für diese Validierung verwendet wird.

Modell	Zählen	Beschreibung
NetApp HCI H610C	4	Drei in einem Cluster für Launchers, AD, DHCP und so weiter. Ein Server für Auslastungstests.
NetApp HCI H615C	1	2x24C Intel Xeon Gold 6282 @2,1 GHz. 1,5 TB RAM:

Die folgende Tabelle enthält die für diese Validierung verwendete Software.

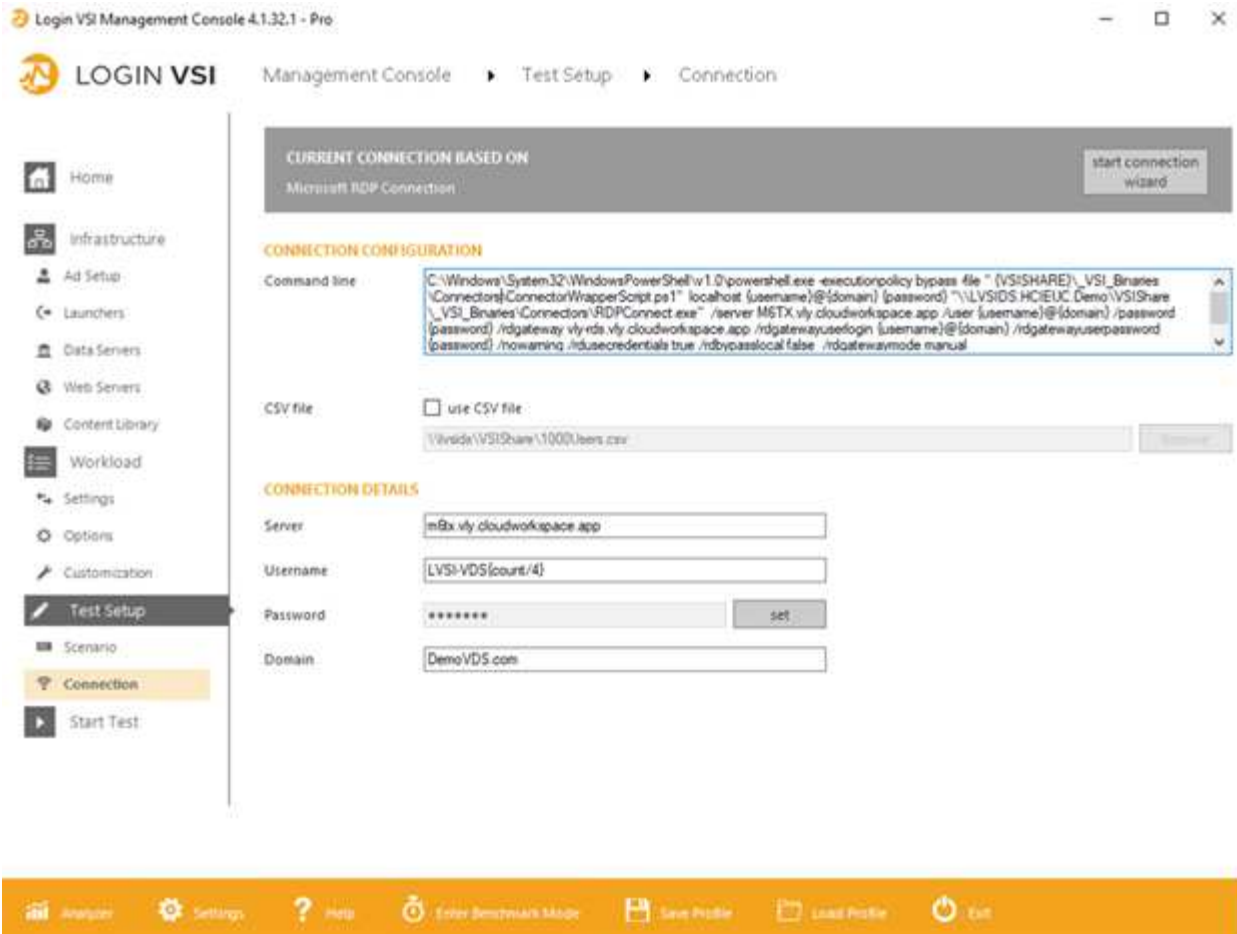
<b>Produkt</b>	<b>Beschreibung</b>
NetApp VDS 5.4	Orchestrierung
VM-Vorlage Windows 2019 1809	Server-Betriebssystem für RDSH
Login VSI	4.1.32.1
VMware vSphere 6.7, Update 3	Hypervisor
VMware vCenter 6.7 Update 3f	VMware Management Tool

Die Login VSI-Testergebnisse lauten wie folgt:

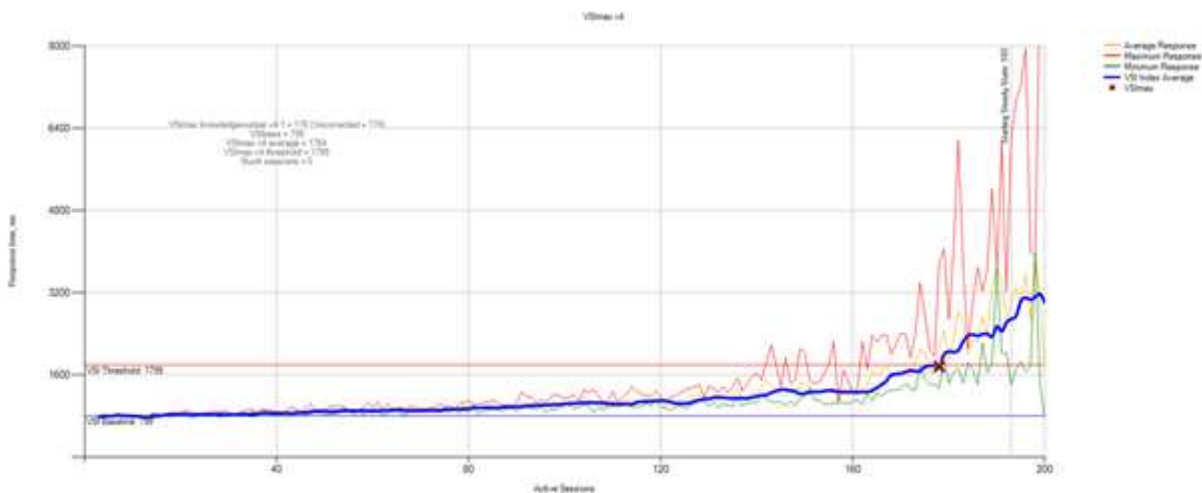
<b>Modell</b>	<b>VM-Konfiguration</b>	<b>Login VSI-Baseline</b>	<b>Login VSI max</b>
H610C	8 vCPUs, 48 GB RAM, 75 GB Festplatte, 8 Q vGPU-Profil	799	178
H615C	12 vCPUs, 128 GB RAM, 75 GB Festplatte	763	272

Da die Sub-NUMA-Grenzen und das Hyper-Threading berücksichtigt wurden, hängen die acht VMs, die für VM-Tests und -Konfiguration ausgewählt wurden, von den Kernen ab, die auf dem Host verfügbar sind.

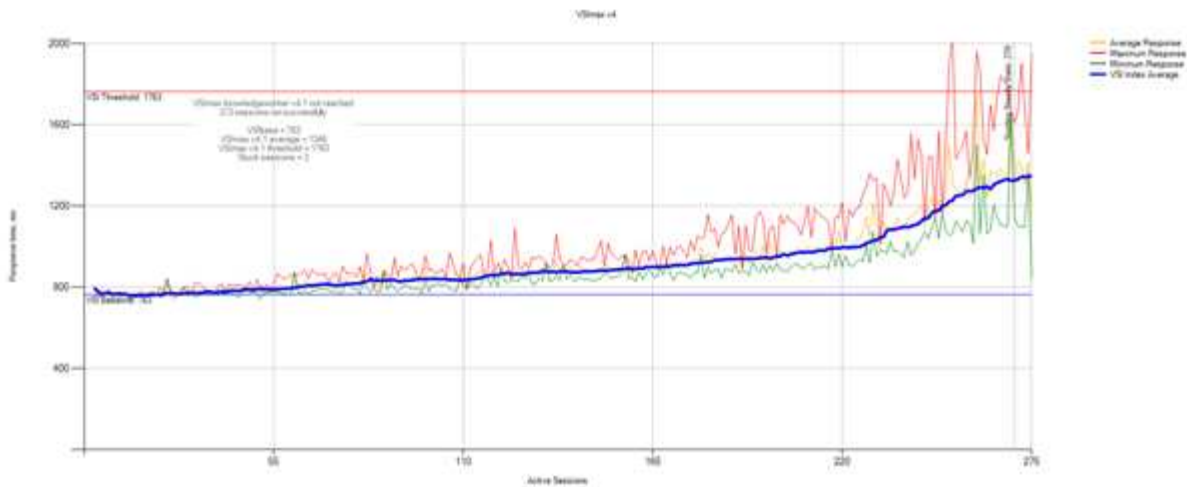
Wir haben auf dem H610C 10 Launcher VMs verwendet, die das RDP-Protokoll verwendet haben, um eine Verbindung zur Benutzersitzung herzustellen. Die folgende Abbildung zeigt die Login VSI-Verbindungsinformationen.



Die folgende Abbildung zeigt die Login VSI Reaktionszeit gegenüber den aktiven Sitzungen für den H610C.



In der folgenden Abbildung wird die Login VSI Reaktionszeit im Vergleich zu aktiven Sitzungen für den H615C angezeigt.



Die Performance-Kennzahlen von Cloud Insights während der H615C Login VSI Tests für den vSphere Host und VMs werden in der folgenden Abbildung dargestellt.



## Management Portal

Das Portal der NetApp VDS Cloud Workspace Management Suite ist verfügbar ["Hier"](#) Und die bevorstehende Version steht zur Verfügung ["Hier"](#).

Das Portal ermöglicht das zentrale Management verschiedener VDS-Implementierungen, darunter Standorte für On-Premises-Benutzer, administrative Benutzer, den Applikationskatalog und skriptbasierte Ereignisse. Das Portal wird auch von administrativen Benutzern für die manuelle Bereitstellung von Anwendungen verwendet, falls erforderlich, und für die Verbindung mit Maschinen zur Fehlerbehebung.

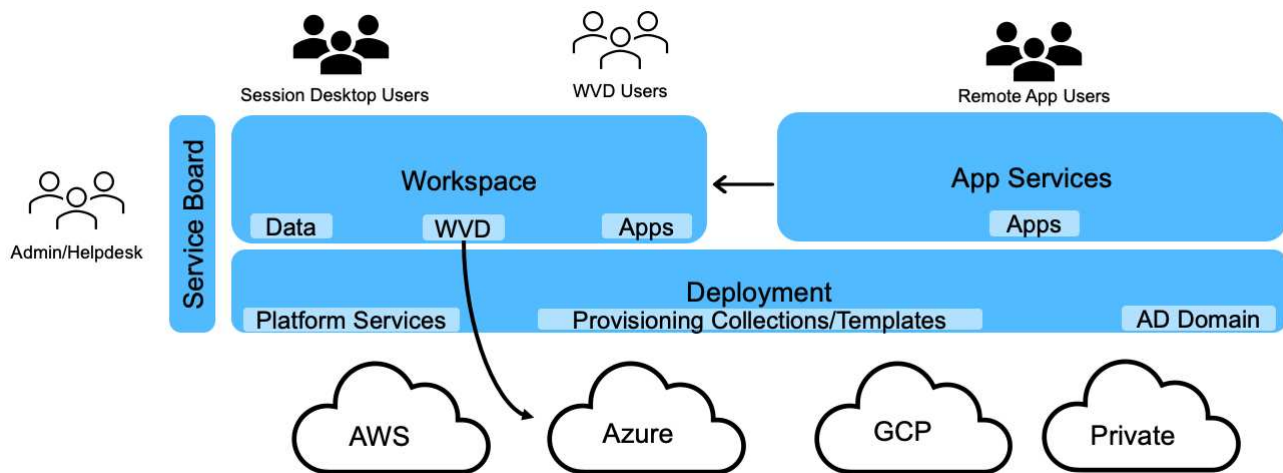
Über dieses Portal können Service-Provider ihren eigenen Channel-Partner hinzufügen, damit sie ihre eigenen Kunden verwalten können.

## Benutzerverwaltung

NetApp VDS verwendet Azure Active Directory für die Identitätsauthentifizierung und Azure Active Directory Domain Services für NTLM/Kerberos-Authentifizierung. Das ADConnect Tool kann verwendet werden, um eine On-Prem Active Directory Domain mit Azure Active Directory zu synchronisieren.

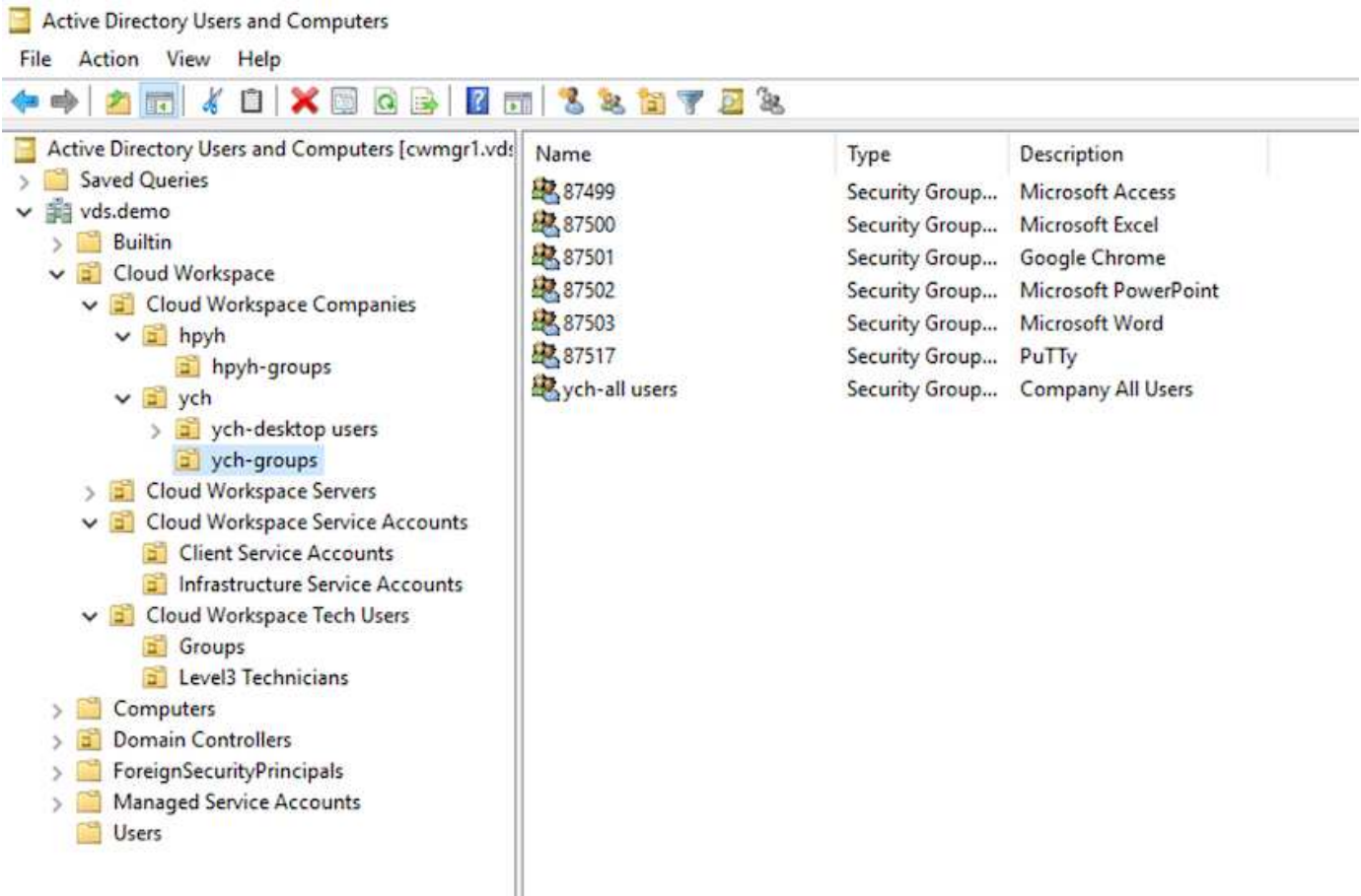
Neue Benutzer können aus dem Portal hinzugefügt werden, oder Sie können Cloud Workspace für bestehende Benutzer aktivieren. Die Berechtigungen für Arbeitsbereiche und Anwendungsdienste können von einzelnen Benutzern oder Gruppen gesteuert werden. Über das Managementportal können Verwaltungsbenutzer definiert werden, um Berechtigungen für das Portal, die Arbeitsbereiche usw. zu kontrollieren.

Die folgende Abbildung zeigt die Benutzerverwaltung im NetApp VDS.



Jeder Workspace befindet sich in einer eigenen Active Directory-Organisationseinheit (OU) unter der OU des Cloud Workspace, wie in der folgenden Abbildung dargestellt.





Weitere Informationen finden Sie unter "[Dieses Video](#)" Auf Benutzerberechtigungen und Benutzermanagement in NetApp VDS.

Wenn eine Active Directory-Gruppe als CRAUserGroup definiert ist, die einen API-Aufruf für das Rechenzentrum verwendet, werden alle Benutzer in dieser Gruppe zur Verwaltung über die Benutzeroberfläche in den CloudWorkspace importiert. Wenn der Cloud-Arbeitsbereich für den Benutzer aktiviert ist, erstellt VDS Home-Ordner für Benutzer, Einstellungsberechtigungen, Aktualisierungen von Benutzereigenschaften usw.

Wenn VDI-Benutzer aktiviert ist, erstellt VDS einen RDS-Rechner für einzelne Sitzungen, der diesem Benutzer zugewiesen ist. Sie werden zur Bereitstellung der Vorlage und des Datastores aufgefordert.



Security Settings

VDI User Enabled  Mobile Drive Enabled

Hypervisor Template  
Windows20192899ver1

Storage Type  
D502

Account Expiration Enabled  Local Drive Access Enabled

Force Password Reset at Next Login  Wake On Demand Enabled

Multi-factor Auth Enabled

Update

### Workspace-Management

Ein Workspace besteht aus einer Desktop-Umgebung. Dieser kann Remote-Desktop-Sitzungen nutzen, die lokal oder in einer beliebigen unterstützten Cloud-Umgebung gehostet werden. Mit Microsoft Azure kann die Desktop-Umgebung mit Windows Virtual Desktops persistent sein. Jeder Arbeitsbereich ist einer bestimmten Organisation oder einem bestimmten Client zugeordnet. Optionen, die beim Erstellen eines neuen Arbeitsbereichs verfügbar sind, sind in der folgenden Abbildung zu sehen.

## New Workspace

Client & Settings
Choose Applications
Add Users
Review & Provision

Select a Client [Add](#)

No Clients Added.

**Workspace Settings**

Company Name

Primary Notification Email

**Application Settings**

Enable Remote App

Enable App Locker

Enable Application Usage Tracking

**Device Settings**

Disable Printing Access

Enable Workspace User Data Storage

**Security Settings**

Require Complex User Password

Enable MFA for All Users

Permit Access To Task Manager

Cancel
Continue



Jeder Arbeitsbereich ist mit einer bestimmten Bereitstellung verknüpft.

Arbeitsbereiche enthalten zugehörige Apps und App-Services, freigegebene Datenordner, Server und eine WVD-Instanz. Jeder Workspace kann Sicherheitsoptionen kontrollieren, wie beispielsweise Passwortkomplexität, Multi-Faktor-Authentifizierung, Dateiaudits usw. durchgesetzt werden.

Arbeitsbereiche können den Workload-Zeitplan zum Einschalten zusätzlicher Server steuern, die Anzahl der Benutzer pro Server begrenzen oder den Zeitplan für die Ressourcen festlegen, die für einen bestimmten Zeitraum verfügbar sind (immer ein/aus). Die Ressourcen können auch so konfiguriert werden, dass sie bei Bedarf aktiviert werden können.

Der Arbeitsbereich kann bei Bedarf die Standardeinstellungen der VM-Ressourcen für die Implementierung außer Kraft setzen. Für WVD können WVD-Hostpools (die Session-Hosts und App-Gruppen enthalten) und WVD-Workspaces auch über das Portal der Cloud Workspace Management Suite gemanagt werden. Weitere Informationen über den WVD-Host-Pool finden Sie hier ["Video"](#).

### Applikationsmanagement

Task Worker können schnell eine Anwendung aus der Liste der ihnen zur Verfügung gestellten Anwendungen starten. App Services veröffentlichen Anwendungen von den Remote Desktop Services-Sitzungshosts. Mit WVD bieten Anwendungsgruppen ähnliche Funktionen aus Windows 10-Hostpools mit mehreren Sitzungen.

Für Büromitarbeiter bis hin zu Power-Usern können die Applikationen, die sie benötigen, manuell über eine Service-Platine bereitgestellt werden. Sie können aber mithilfe der skriptbasierten Ereignisfunktion im NetApp

VDS automatisch bereitgestellt werden.

Weitere Informationen finden Sie im ["NetApp Application Berechtigungsseite"](#).

#### ONTAP-Funktionen für Virtual Desktop Service

Die folgenden ONTAP Funktionen machen es zu einer attraktiven Wahl für einen virtuellen Desktop-Service.

- **Scale-out-Dateisystem.** ONTAP FlexGroup-Volumes können auf mehr als 20 PB groß sein und mehr als 400 Milliarden Dateien in einem Single Namespace enthalten. Das Cluster kann bis zu 24 Storage-Nodes enthalten, jedes mit einer flexiblen Anzahl von Netzwerkschnittstellenkarten, je nach verwendetem Modell.

Die virtuellen Desktops und Home-Ordner der Benutzer, Container mit Benutzerprofilen, gemeinsam genutzte Daten können je nach Bedarf erweitert werden, ohne die Dateisystem-Einschränkungen zu bedenken.

- **Dateisystemanalyse.** mit dem XCP-Tool erhalten Sie Einblicke in gemeinsam genutzte Daten. Mit ONTAP 9.8+ und ActiveIQ Unified Manager können Kunden Dateimetadaten einfach abfragen und abrufen und inaktive Daten identifizieren.
- \* Cloud-Tiering\* ermöglicht die Migration kalter Daten zu einem Objektspeicher in der Cloud oder zu jedem S3-kompatiblen Storage im Datacenter.
- **Dateiversionen.** Benutzer können Dateien wiederherstellen, die durch NetApp ONTAP Snapshot-Kopien geschützt sind. ONTAP Snapshot Kopien sind sehr platzsparend, da sie nur geänderte Blöcke aufzeichnen.
- **Global Namespace.** die ONTAP FlexCache-Technologie ermöglicht das Remote-Caching von File Storage und vereinfacht das Management gemeinsam genutzter Daten an verschiedenen Standorten mit ONTAP Storage-Systemen.
- **Unterstützung für sichere Mandantenfähigkeit.** Ein einziger physischer Storage Cluster kann als mehrere virtuelle Storage Arrays mit jeweils eigenen Volumes, Storage-Protokollen, logischen Netzwerkschnittstellen, Identitäts- und Authentifizierungsdomäne, Management-Benutzern usw. bereitgestellt werden. Auf diese Weise können Sie das Storage-Array für mehrere Geschäftseinheiten oder Umgebungen nutzen, beispielsweise für Tests, Entwicklung und Produktion.

Um Performance zu garantieren, können Sie mittels anpassungsfähiger QoS Performance-Level auf Basis von belegtem oder zugewiesenem Speicherplatz festlegen und die Storage-Kapazität mittels Quoten steuern.

- **VMware Integration.** ONTAP Tools für VMware vSphere bietet ein vCenter Plug-in zur Bereitstellung von Datastores, Implementierung von vSphere Host Best Practices und Überwachung von ONTAP Ressourcen.

ONTAP unterstützt vStorage APIs zur Array Integration (VAAI) zur Auslagerung von SCSI-/Dateivorgängen auf das Storage Array. ONTAP unterstützt auch vStorage APIs for Storage Awareness (VASA) und Virtual Volumes für Block- und Dateiprotokolle.

Das SnapCenter Plug-in für VMware vSphere ermöglicht mithilfe der Snapshot Funktion in einem Storage Array das Sichern und Wiederherstellen von Virtual Machines.

ActiveIQ Unified Manager bietet End-to-End-Sichtbarkeit des Storage-Netzwerks in einer vSphere-Umgebung. Administratoren können problemlos alle Latenzprobleme identifizieren, die in virtuellen Desktop-Umgebungen, die auf ONTAP gehostet werden, auftreten können.

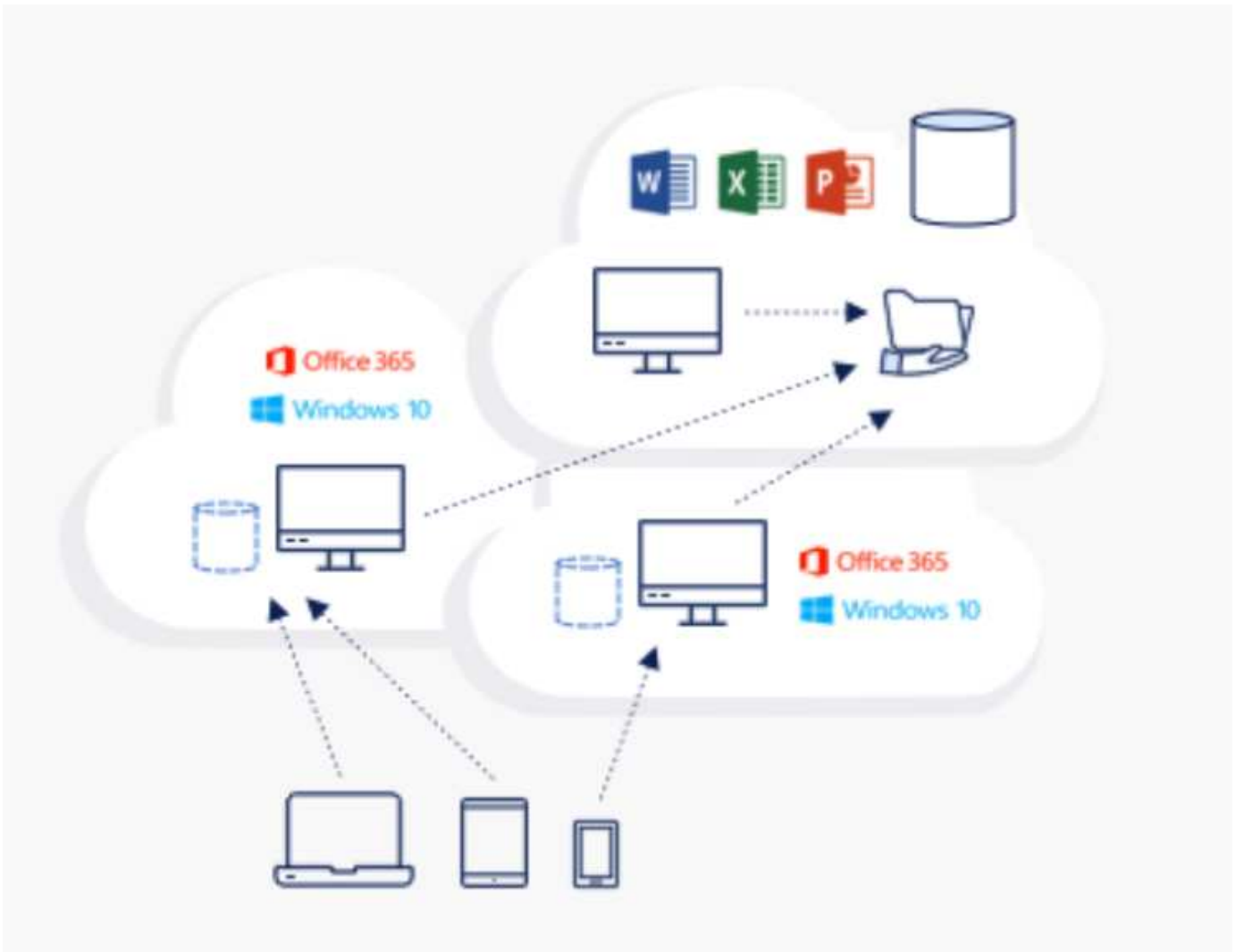
- **Einhaltung der Sicherheitsvorschriften** mit ActiveIQ Unified Manager können Sie mehrere ONTAP-Systeme mit Warnmeldungen auf Richtlinienverstöße überwachen.
- \* Multi-Protokoll-Unterstützung.\* ONTAP unterstützt Block (iSCSI, FC, FCoE und NVMe/FC), Datei (NFSv3, NFSv4.1, SMB2.x und SMB3.x) und Storage-Protokolle für Objekte (S3).
- **Automatisierungsunterstützung** ONTAP bietet REST-API, Ansible und PowerShell-Module zur Automatisierung von Aufgaben mit dem VDS-Verwaltungsportal.

## Datenmanagement

Im Rahmen der Bereitstellung können Sie die File-Services-Methode auswählen, um das Benutzerprofil, die gemeinsam genutzten Daten und den Ordner Home Drive zu hosten. Es stehen File Server, Azure Files oder Azure NetApp Files zur Verfügung. Nach der Implementierung können Sie diese Option jedoch mit dem Command Center-Tool ändern, um auf eine beliebige SMB-Freigabe zu verweisen. "[Das Hosting mit NetApp ONTAP bietet verschiedene Vorteile](#)". Informationen zum Ändern der SMB-Freigabe finden Sie unter "[Datenebene Ändern](#)".

## Globaler Datei-Cache

Wenn Benutzer sich über mehrere Standorte innerhalb eines globalen Namespace verteilen, kann Global File Cache die Latenz für häufig genutzte Daten verringern. Die globale Dateicache-Bereitstellung kann mithilfe einer Bereitstellungssammlung und skriptgesteuerter Ereignisse automatisiert werden. Global File Cache wickelt die Lese- und Schreib-Caches lokal ab und unterhält Dateisperren über mehrere Speicherorte hinweg. Global File Cache kann mit allen SMB-File-Servern einschließlich Azure NetApp Files eingesetzt werden.



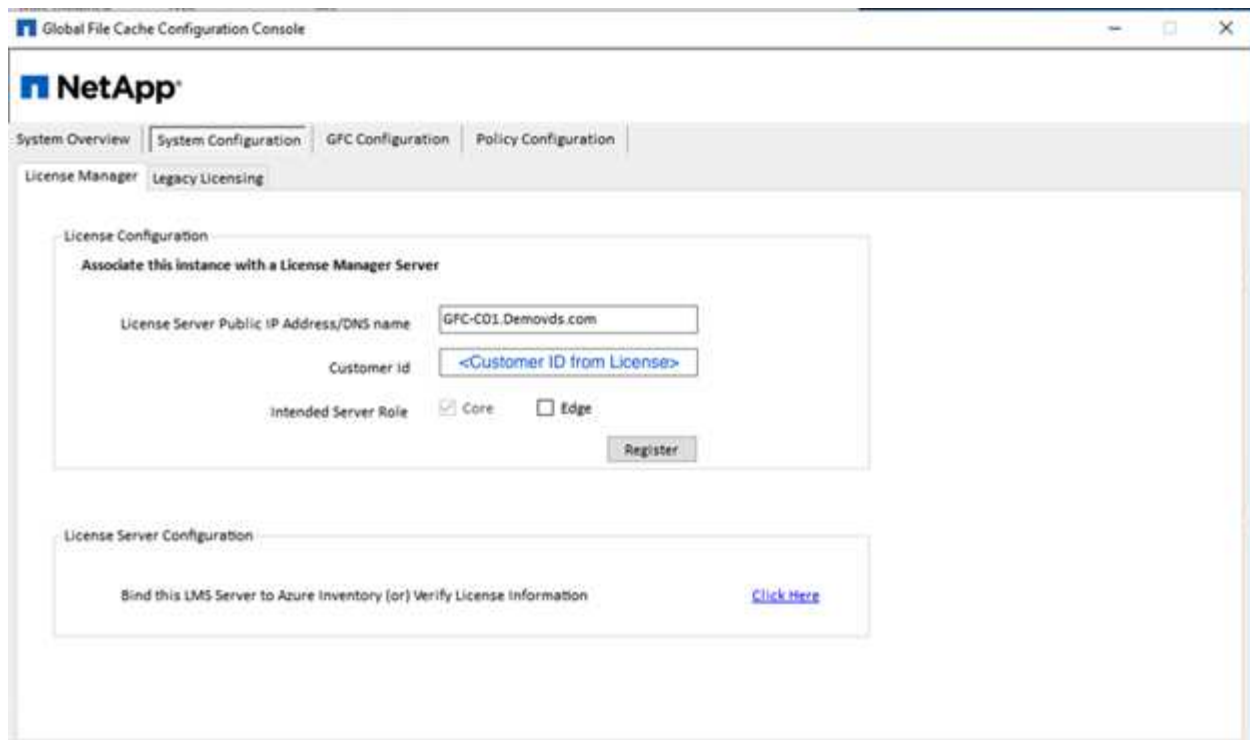
Global File Cache erfordert Folgendes:

- Management-Server (Lizenzverwaltungsserver)
- Kern
- Edge mit genügend Festplattenkapazität, um die Daten im Cache zu speichern

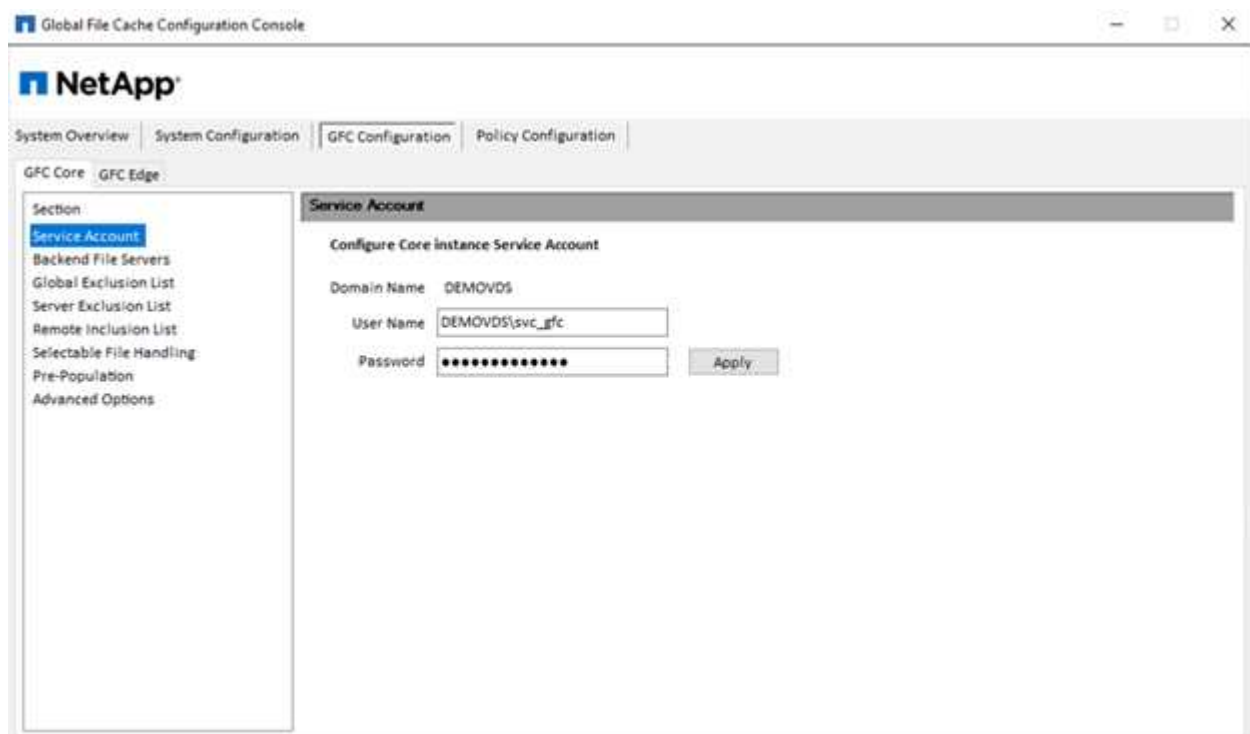
Informationen zum Herunterladen der Software und zur Berechnung der Festplatten-Cache-Kapazität für Edge finden Sie im "[GFC-Dokumentation](#)".

Für unsere Validierung haben wir die Kern- und Management-Ressourcen in Azure auf derselben VM und Edge-Ressourcen in NetApp HCI implementiert. Beachten Sie bitte, dass der Core-Bereich der Datenzugriff mit hohen Datenmengen erforderlich ist und der Edge eine Untergruppe des Kerns ist. Nach der Installation der Software müssen Sie vor der Verwendung die Lizenz aktivieren. Um das zu tun, führen Sie folgende Schritte aus:

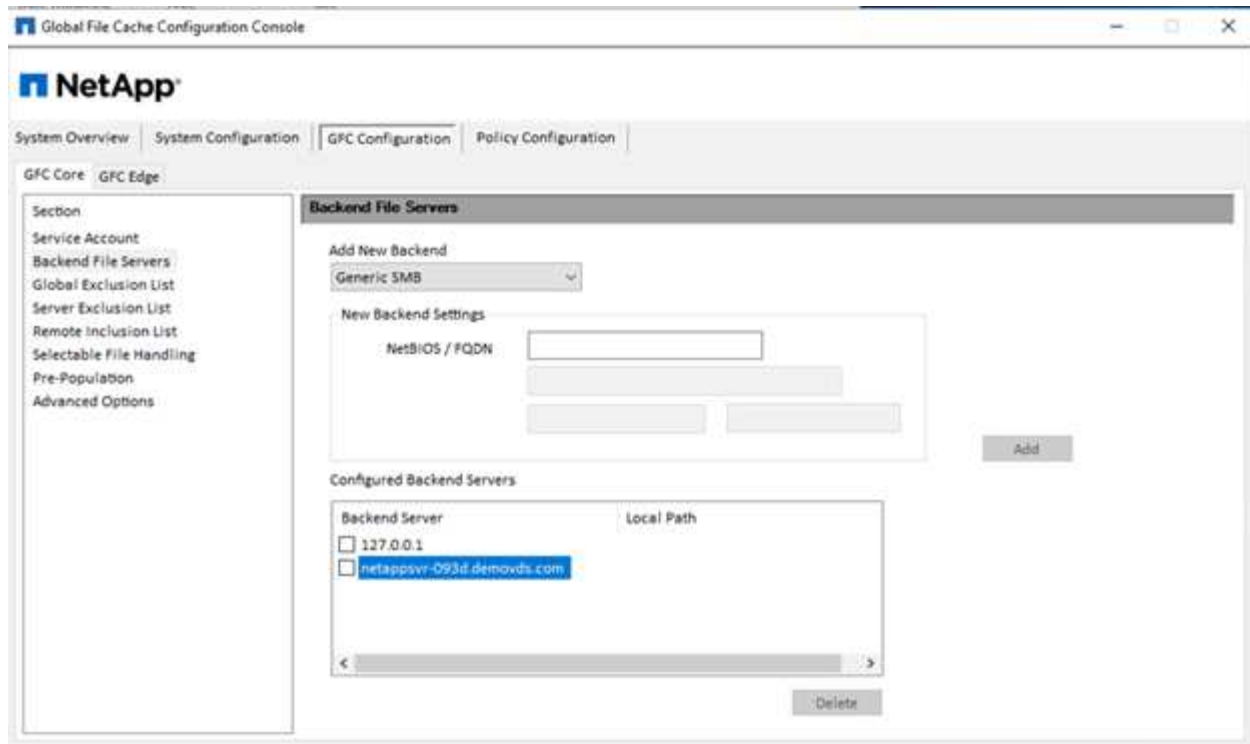
1. Verwenden Sie im Abschnitt Lizenzkonfiguration den Link [Klicken Sie hier](#), um die Lizenzaktivierung abzuschließen. Dann registrieren Sie den Kern.



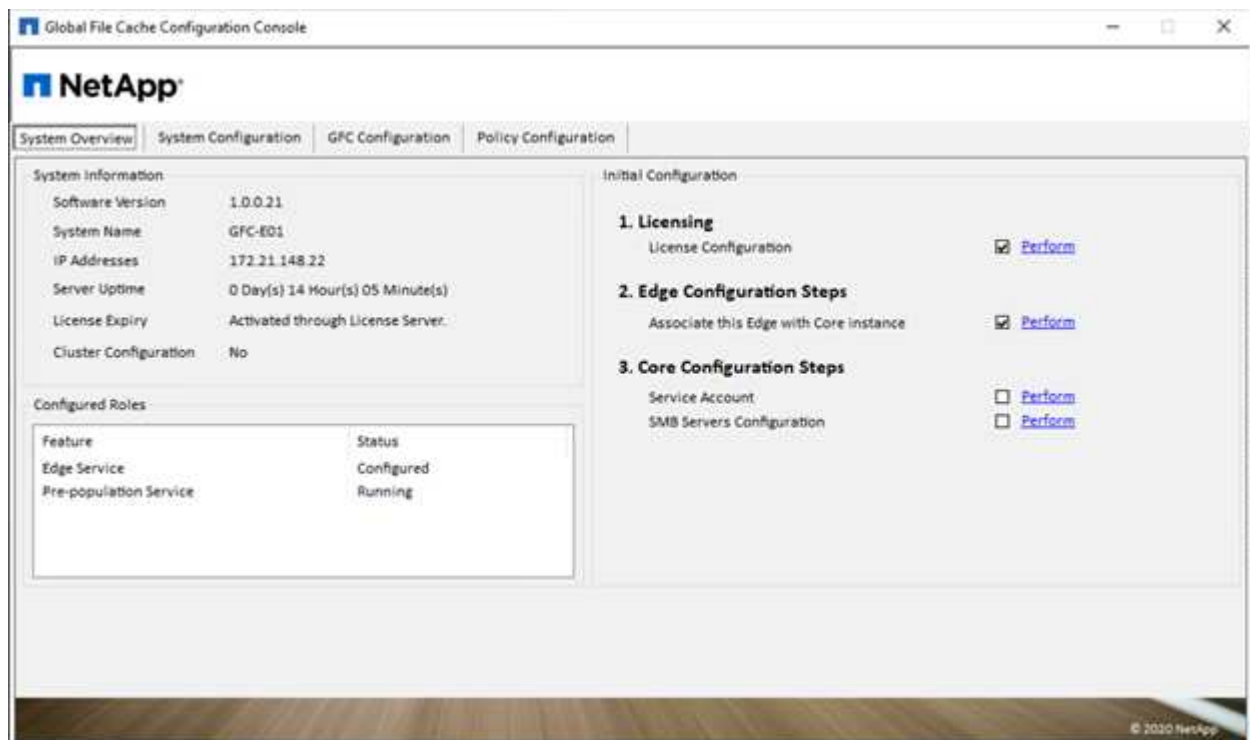
2. Geben Sie das Servicekonto an, das für den Global File Cache verwendet werden soll. Informationen zu den erforderlichen Berechtigungen für dieses Konto finden Sie im "[GFC-Dokumentation](#)".



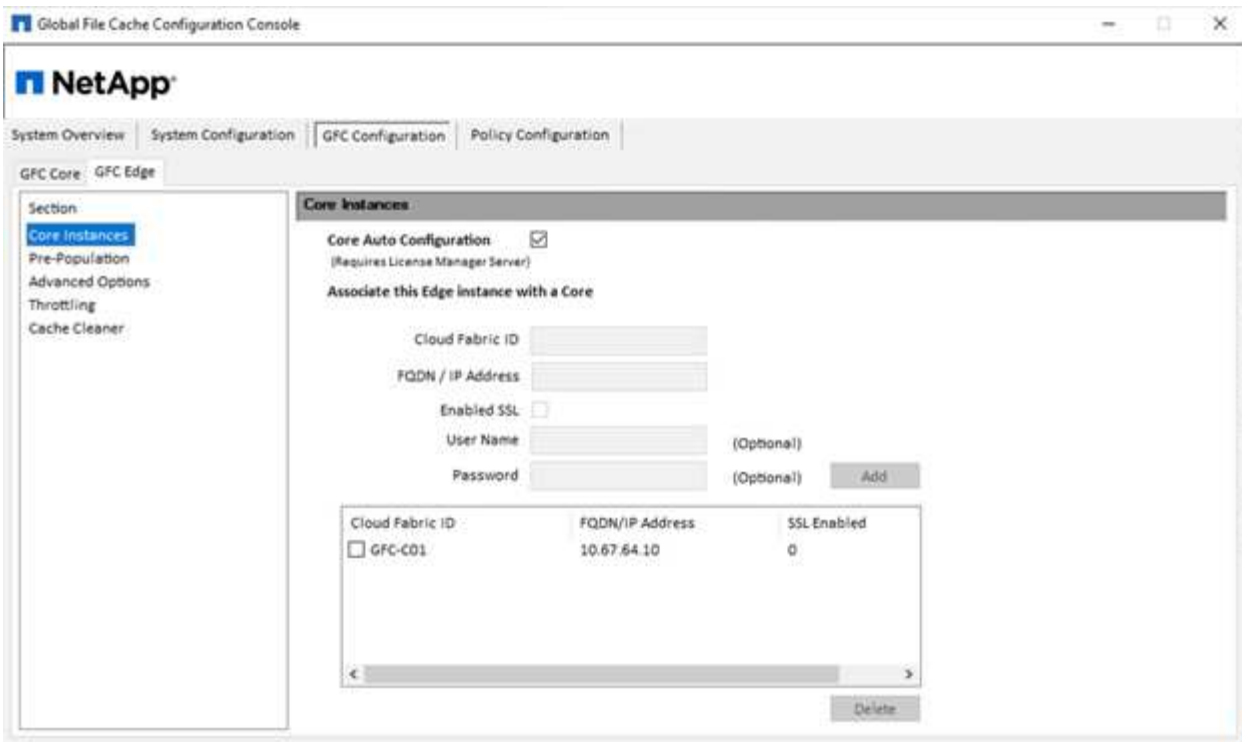
3. Fügen Sie einen neuen Back-End-Dateiserver hinzu und geben Sie den Namen oder die IP des Dateiservers an.



4. Am Rand muss das Cache-Laufwerk den Laufwerksbuchstaben D. haben Wenn dies nicht der Fall ist, verwenden Sie diskpart.exe, um das Volume auszuwählen und den Laufwerksbuchstaben zu ändern. Mit dem Lizenzserver als Edge registrieren.

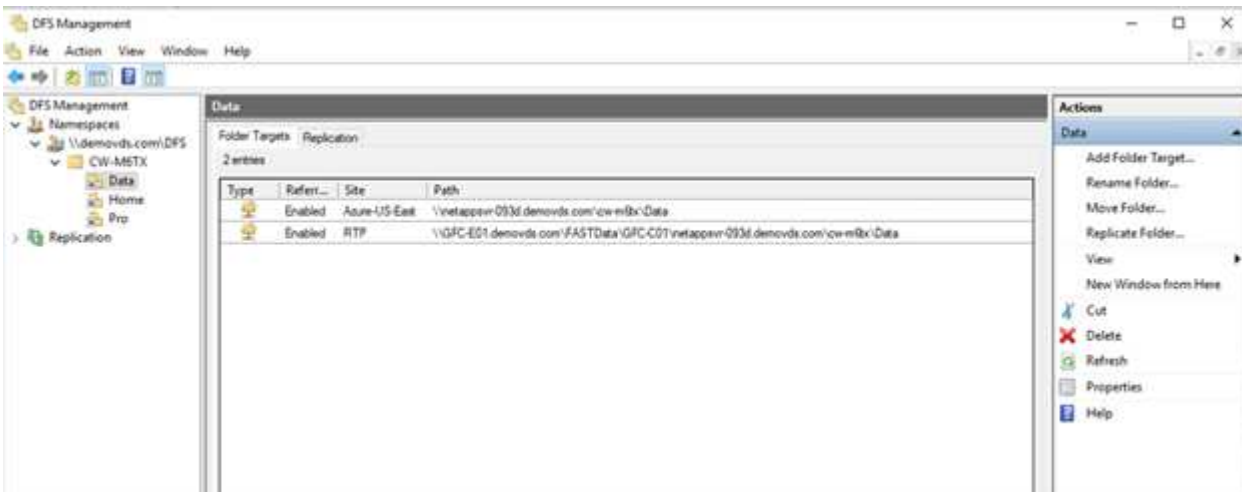


Wenn die automatische Kernkonfiguration aktiviert ist, werden die Kerninformationen automatisch vom Lizenzverwaltungsserver abgerufen.



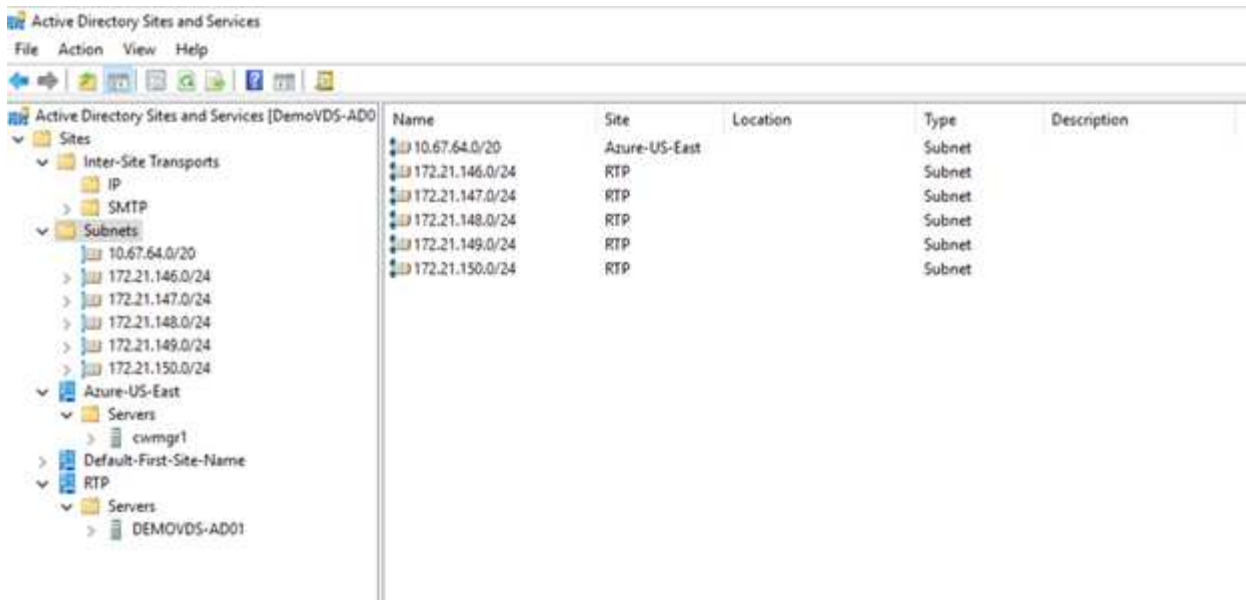
Von jedem Client-Rechner aus können die Administratoren, die zum Zugriff auf den Share auf dem Dateiserver verwendet wurden, über GFC Edge mithilfe von UNC Path auf ihn zugreifen \\<edge server name>\FASTDATA\<core server name>\<backend file server name>\<share name>. Administratoren können diesen Pfad in das Benutzerlogonskript oder GPO einschließen, um zu erreichen, dass Benutzer am Edge-Standort ihre Zuordnung vorantreiben.

Um Benutzern weltweit einen transparenten Zugriff zu bieten, kann ein Administrator das Microsoft Distributed Filesystem (DFS) mit Links auf File Server Shares und Edge-Standorte einrichten.

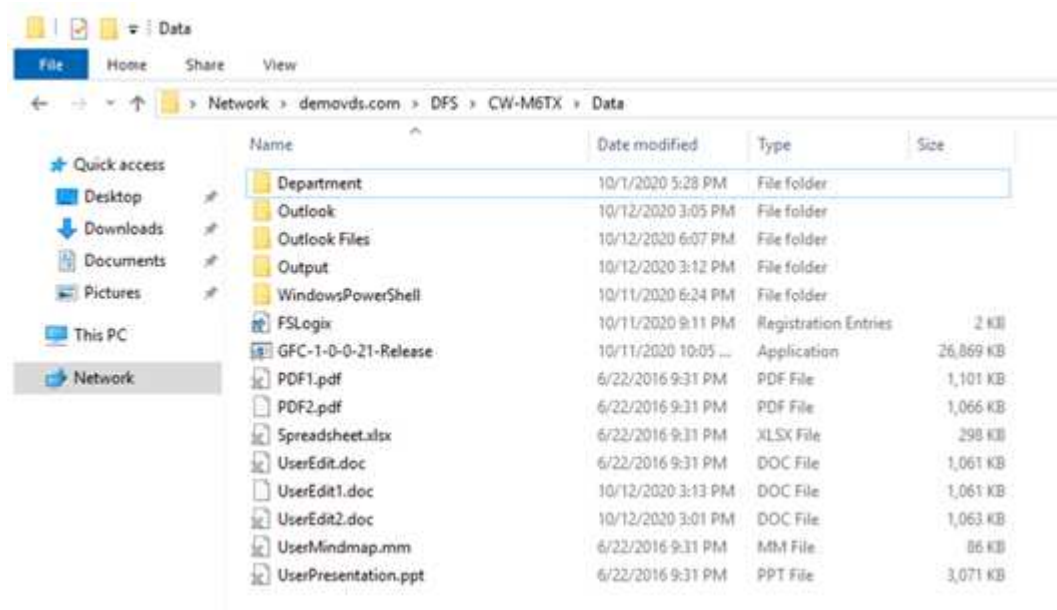


Wenn sich Benutzer basierend auf den Subnetzen anmelden, die der Site zugeordnet sind, wird der entsprechende Link vom DFS-Client zum Zugriff auf die Daten verwendet.

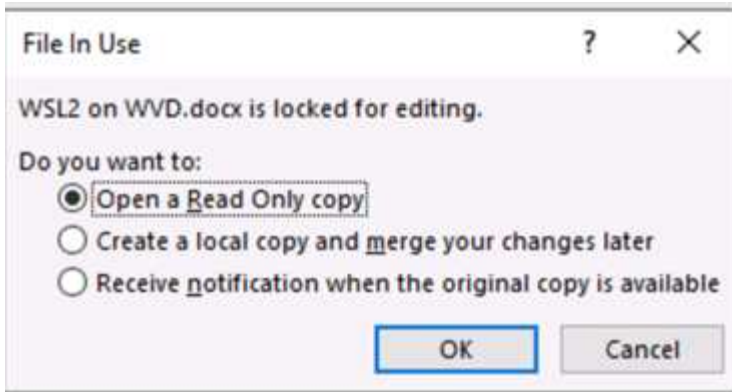




Die Dateisymbole ändern sich je nach dem Cache einer Datei. Dateien, die nicht im Cache gespeichert sind, haben in der linken unteren Ecke des Symbols ein graues X. Nachdem ein Benutzer an einem Edge-Standort auf eine Datei zugreift, wird diese Datei im Cache gespeichert und das Symbol ändert sich.



Wenn eine Datei geöffnet ist und ein anderer Benutzer versucht, dieselbe Datei von einem Randort aus zu öffnen, wird der Benutzer mit der folgenden Auswahl aufgefordert:



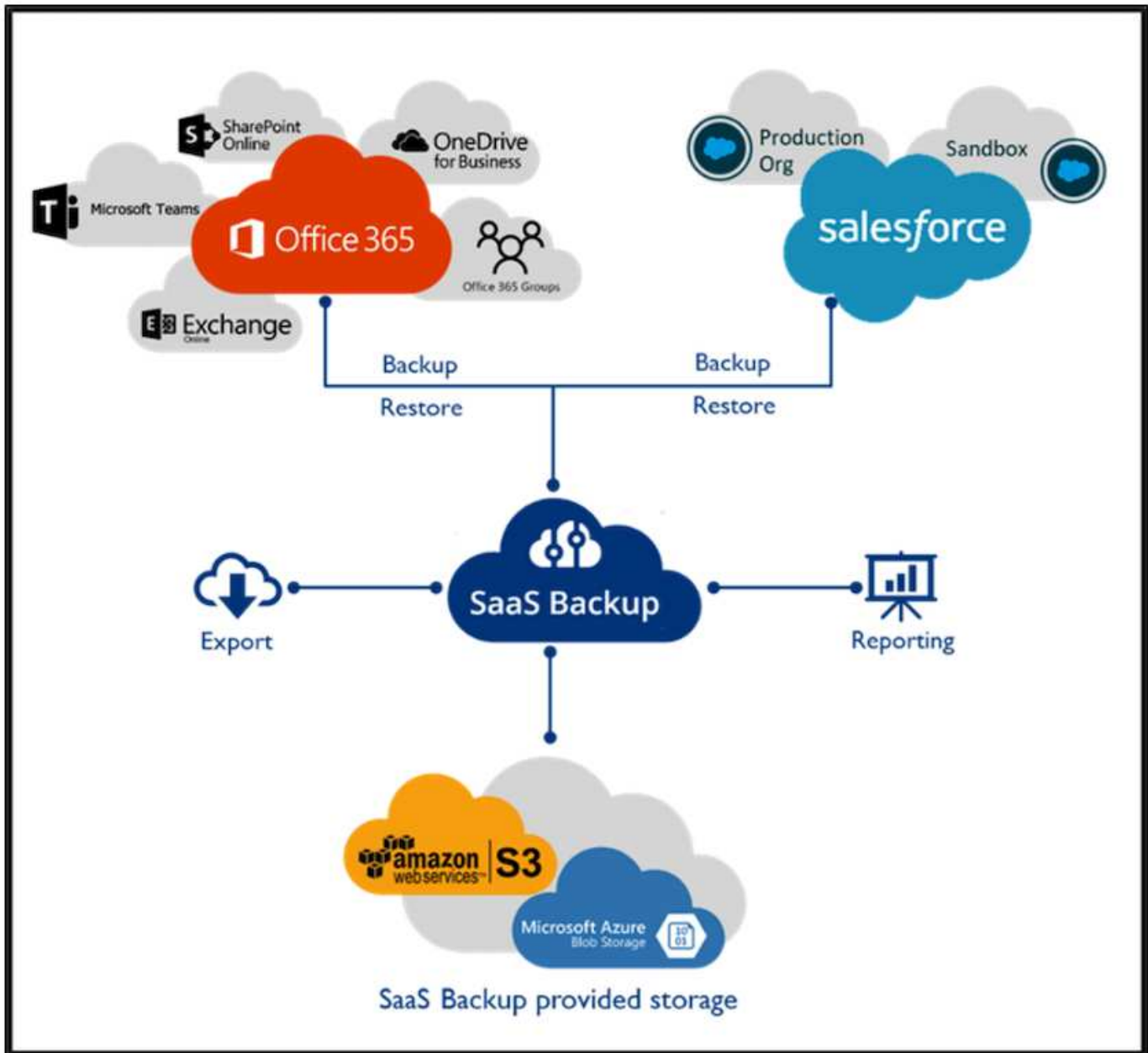
Wenn der Benutzer die Option zum Erhalt einer Benachrichtigung wählt, wenn die Originalversion verfügbar ist, wird der Benutzer wie folgt benachrichtigt:



Weitere Informationen finden Sie unter ["Video zu Talon und Azure NetApp Files Deployment"](#).

## SaaS-Backup

NetApp VDS bietet die Datensicherung für Salesforce und Microsoft Office 365, einschließlich Exchange, SharePoint und Microsoft OneDrive. Die folgende Abbildung zeigt, wie NetApp VDS SaaS Backup für diese Datenservices bereitstellt.



Eine Demonstration zur Datensicherung von Microsoft Office 365 finden Sie unter ["Dieses Video"](#).

Eine Demonstration der Salesforce-Datensicherung finden Sie unter ["Dieses Video"](#).

### Betriebsmanagement

Mit NetApp VDS können Administratoren Aufgaben an andere delegieren. Sie können Verbindungen zu bereitgestellten Servern herstellen, um Fehler zu beheben, Protokolle anzuzeigen und Audit-Berichte auszuführen. Die Unterstützung von Kunden, Helpdesk-Techniker oder Technikern der Stufe 3 kann bei Bedarf Benutzersitzungen im Schatten stellen, Prozesslisten anzeigen und Prozesse abtöten.

Informationen zu VDS-Logfiles finden Sie im ["Seite „Fehlerbehebung bei fehlgeschlagenen VDA-Aktionen“"](#).

Weitere Informationen zu den erforderlichen Mindestberechtigungen finden Sie im ["Seite VDA-Komponenten und Berechtigungen"](#).

Wenn Sie einen Server manuell klonen möchten, lesen Sie die ["Seite Klonen von Virtual Machines"](#).

Informationen zur automatischen Vergrößerung der VM-Festplattenkapazität finden Sie im ["Feature-Seite „Automatische Vergrößerung des Festplattenspeicherplatz“"](#).

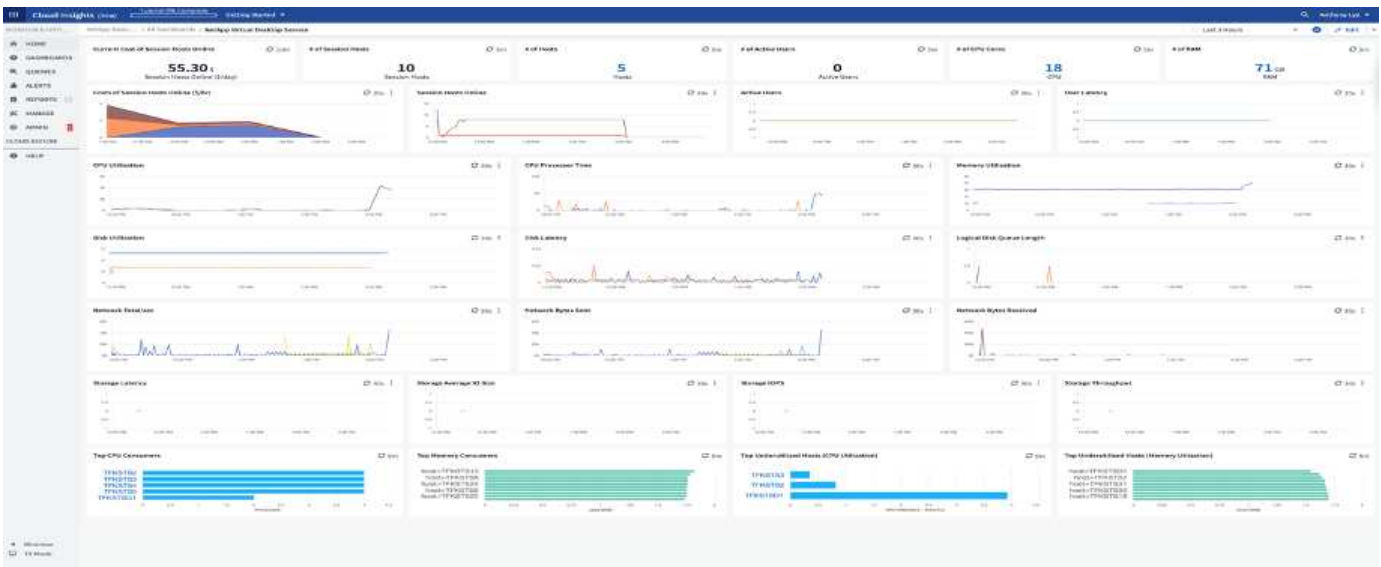
Informationen zur Identifizierung der Gateway-Adresse für die manuelle Konfiguration des Clients finden Sie im ["Anforderungen für Endbenutzer"](#).

## Einblicke in die Cloud

NetApp Cloud Insights ist ein webbasiertes Monitoring Tool, mit dem Sie den vollständigen Überblick über Infrastrukturen und Applikationen erhalten, die auf NetApp und anderen Infrastrukturkomponenten von Drittanbietern ausgeführt werden. Cloud Insights unterstützt sowohl Private Cloud- als auch Public Clouds für Monitoring, Fehlerbehebung und Optimierung von Ressourcen.

Nur die Erfassungseinheit-VM (kann Windows oder Linux sein) muss in einer privaten Cloud installiert werden, um Kennzahlen von Datensammlern zu sammeln, ohne dass Agenten erforderlich sind. Agenten-basierte Datensammler ermöglichen es Ihnen, benutzerdefinierte Metriken von Windows Performance Monitor oder von beliebigen Eingabemaagenten, die Telegraf unterstützt, zu holen.

Die folgende Abbildung zeigt das Cloud Insights VDS Dashboard.



Weitere Informationen zu NetApp Cloud Insights finden Sie unter ["Dieses Video"](#).

## Tools und Protokolle

### DCCConfig-Tool

Das DCCconfig-Tool unterstützt die folgenden Hypervisor-Optionen zum Hinzufügen einer Site:

DataCenter Site

DataCenter Site

Hypervisor

Cancel New Save

Load Hypervisor Test

Select Hypervisor

- Aws
- AzureClassic
- AzureRM
- ComputeEngine
- HyperV
- ProfitBricks
- vCloud
- vCloudRest
- vSphere
- XenServer

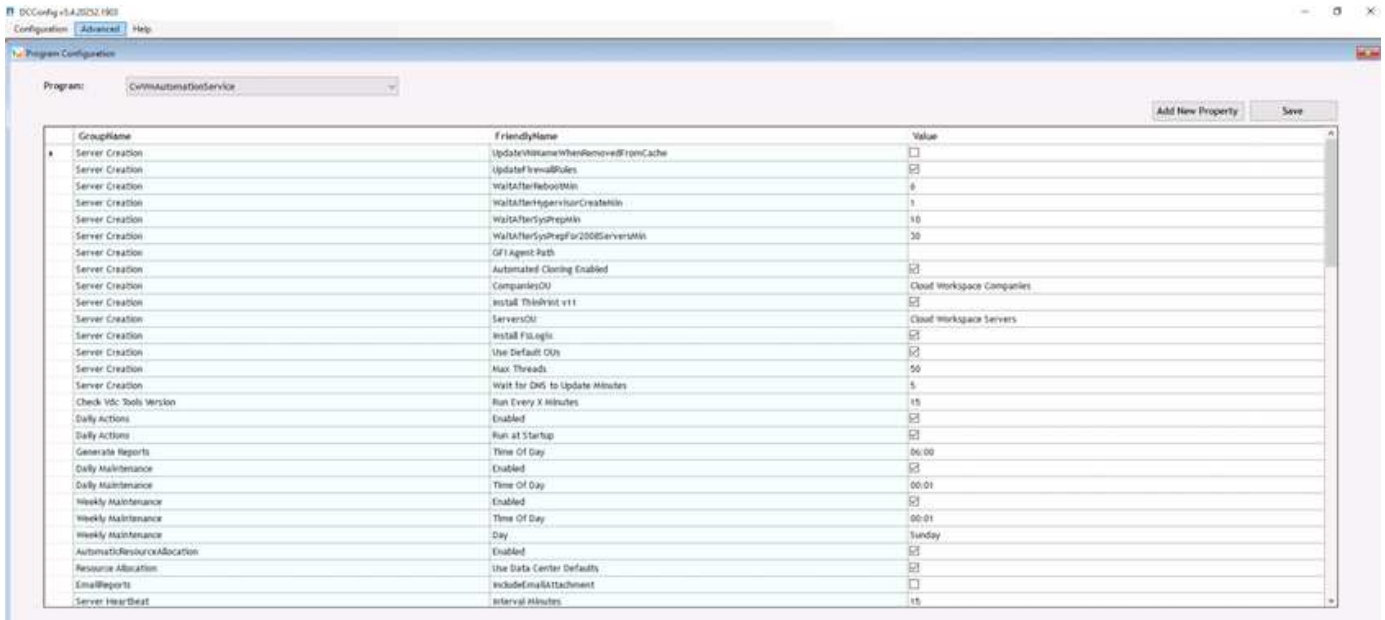
Configuration

DataCenter Accounts Email DatabaseConnection Exclude DataCenter Sites Product Keys Static IpAddress Drive Mapping

Save

	Description	DriveLetter
	Shared Data	P
	FTP	F
▶	User Home	H

Workspace-spezifische Laufwerksbuchstaben-Zuordnung für gemeinsam genutzte Daten kann über GPO bearbeitet werden. Professional Services oder das Support-Team können über die Registerkarte „Advanced“ Einstellungen wie Active Directory-Organisationsnamen, die Option zum Aktivieren oder Deaktivieren der Bereitstellung von FSLogix, verschiedene Zeitlimits usw. anpassen.

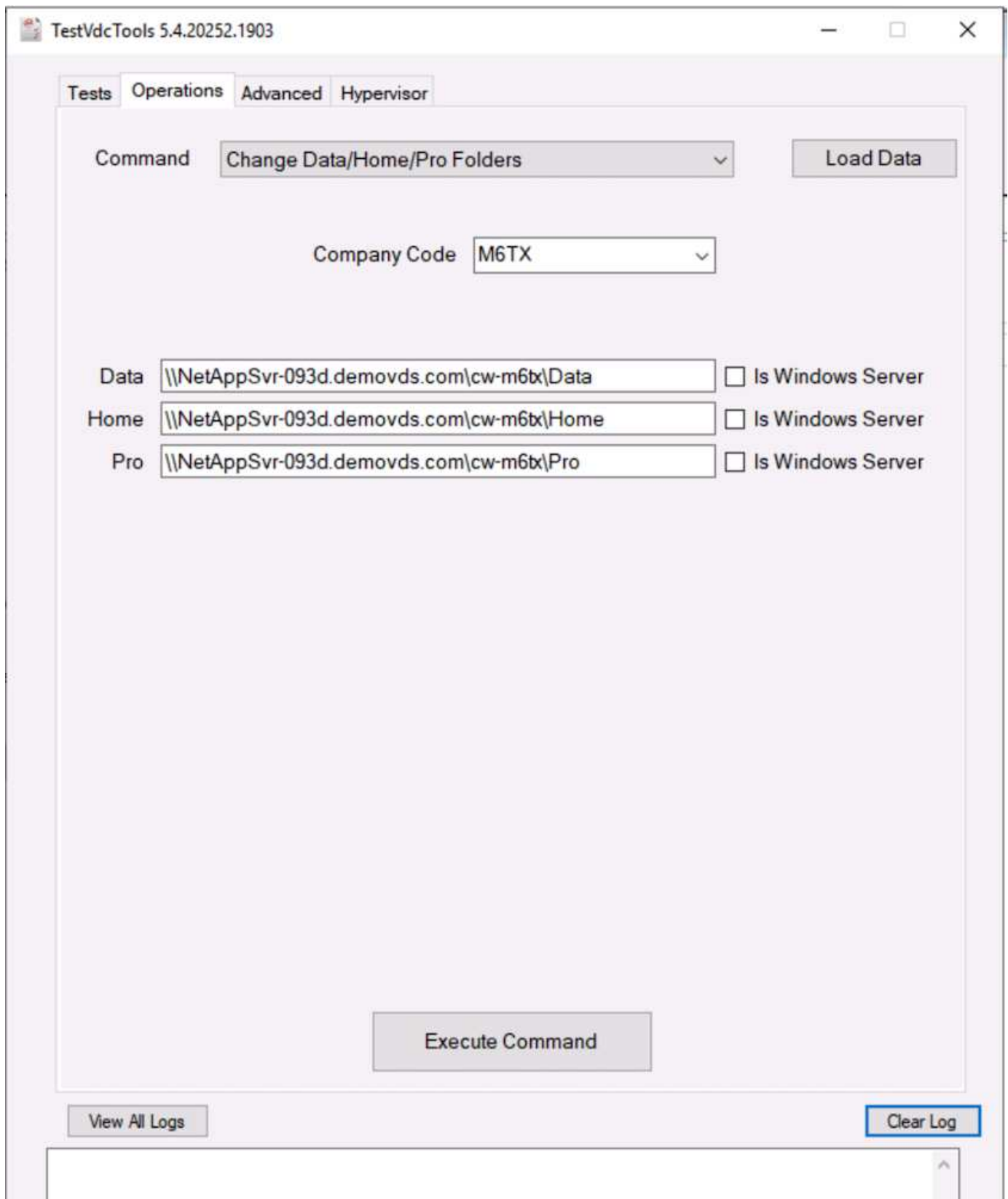


## Command Center (zuvor als TestVdc-Tools bekannt)

Informationen zum Starten von Command Center und der erforderlichen Rolle finden Sie im "[Command Center – Übersicht](#)".

Sie können folgende Vorgänge durchführen:

- Ändern Sie den SMB-Pfad für einen Arbeitsbereich.



- Ändern Sie die Site für die Provisioning-Sammlung.

Tests Operations **Advanced** Hypervisor

Command Edit Provisioning Collection

Load Data

Provisioning Collection Windows2019

Description On vSphere Site 2

Share Drive P

Minimum Cache Level 1

Operating System Windows Server 2019

Collection Type Shared

	Data Center Site	Role	Template	Storage
▶	Site 2	TSDData	Windows2019	DS01
*				







Execute Command

View All Logs

Clear Log

### Log-Dateien



Name	Date modified	Type	Size
 CwAgent	9/19/2020 12:35 PM	File folder	
 CWAutomationService	9/19/2020 12:34 PM	File folder	
 CWManagerX	9/19/2020 12:53 PM	File folder	
 CwVmAutomationService	9/19/2020 12:34 PM	File folder	
 TestVdcTools	9/22/2020 8:20 PM	File folder	
 report	9/19/2020 12:18 PM	Executable Jar File	705 KB

Prüfen "[Automatisierungsprotokolle](#)" Finden Sie weitere Informationen.

### Überlegungen zu GPUs

GPUs werden normalerweise für die Grafikkvisualisierung (Rendering) verwendet, indem repetitive Rechenberechnungen durchgeführt werden. Diese sich wiederholende Computing-Funktion wird häufig für KI- und Deep-Learning-Anwendungsfälle eingesetzt.

Für grafikintensive Anwendungen bietet Microsoft Azure die NV Serie auf Basis der NVIDIA Tesla M60 Karte mit einem bis vier GPUs pro VM an. Jede NVIDIA Tesla M60 Karte verfügt über zwei Maxwell-basierte GPUs mit jeweils 8 GB GDDR5-Speicher und insgesamt 16 GB.



Eine NVIDIA-Lizenz ist in der NV Serie enthalten.


TechPowerUp GPU-Z 2.36.0


Graphics Card | Sensors | Advanced | Validation

Name: NVIDIA Tesla M60 [Lookup](#)

GPU: GM204 Revision: FF

Technology: 28 nm Die Size: 398 mm<sup>2</sup>

Release Date: Aug 30, 2015 Transistors: 5200M 

BIOS Version: 84.04.85.00.03   UEFI

Subvendor: NVIDIA Device ID: 10DE 13F2 - 10DE 115E

ROPs/TMUs: 64 / 128 Bus Interface: PCI ?

Shaders: 2048 Unified DirectX Support: 12 (12\_1)

Pixel Fillrate: 75.4 GPixel/s Texture Fillrate: 150.8 GTexel/s

Memory Type: GDDR5 (Hynix) Bus Width: 256 bit

Memory Size: 8192 MB Bandwidth: 160.4 GB/s

Driver Version: 27.21.14.5257 (NVIDIA 452.57) / 2016

Driver Date: Oct 22, 2020 Digital Signature: WHQL

GPU Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz

Default Clock: 557 MHz Memory: 1253 MHz Boost: 1178 MHz

NVIDIA SLI: Disabled

Computing  OpenCL  CUDA  DirectCompute  DirectML

Technologies  Vulkan  Ray Tracing  PhysX  OpenGL 4.6

NVIDIA Tesla M60 [Close](#)

Bei NetApp HCI enthält die H615C GPU drei NVIDIA Tesla T4-Karten. Jede NVIDIA Tesla T4-Karte verfügt über eine Turing-basierte GPU mit 16 GB GDDR6-Speicher. Wenn sie in einer VMware vSphere Umgebung verwendet werden, können Virtual Machines die GPU gemeinsam nutzen, wobei jede VM einen dedizierten Frame-Puffer-Speicher hat. Die GPUs auf dem NetApp HCI H615C sind für Ray-Tracing verfügbar, um realistische Bilder einschließlich Lichtreflexionen herzustellen. Bitte beachten Sie, dass Sie einen NVIDIA-

Lizenzserver mit einer Lizenz für GPU-Funktionen benötigen.

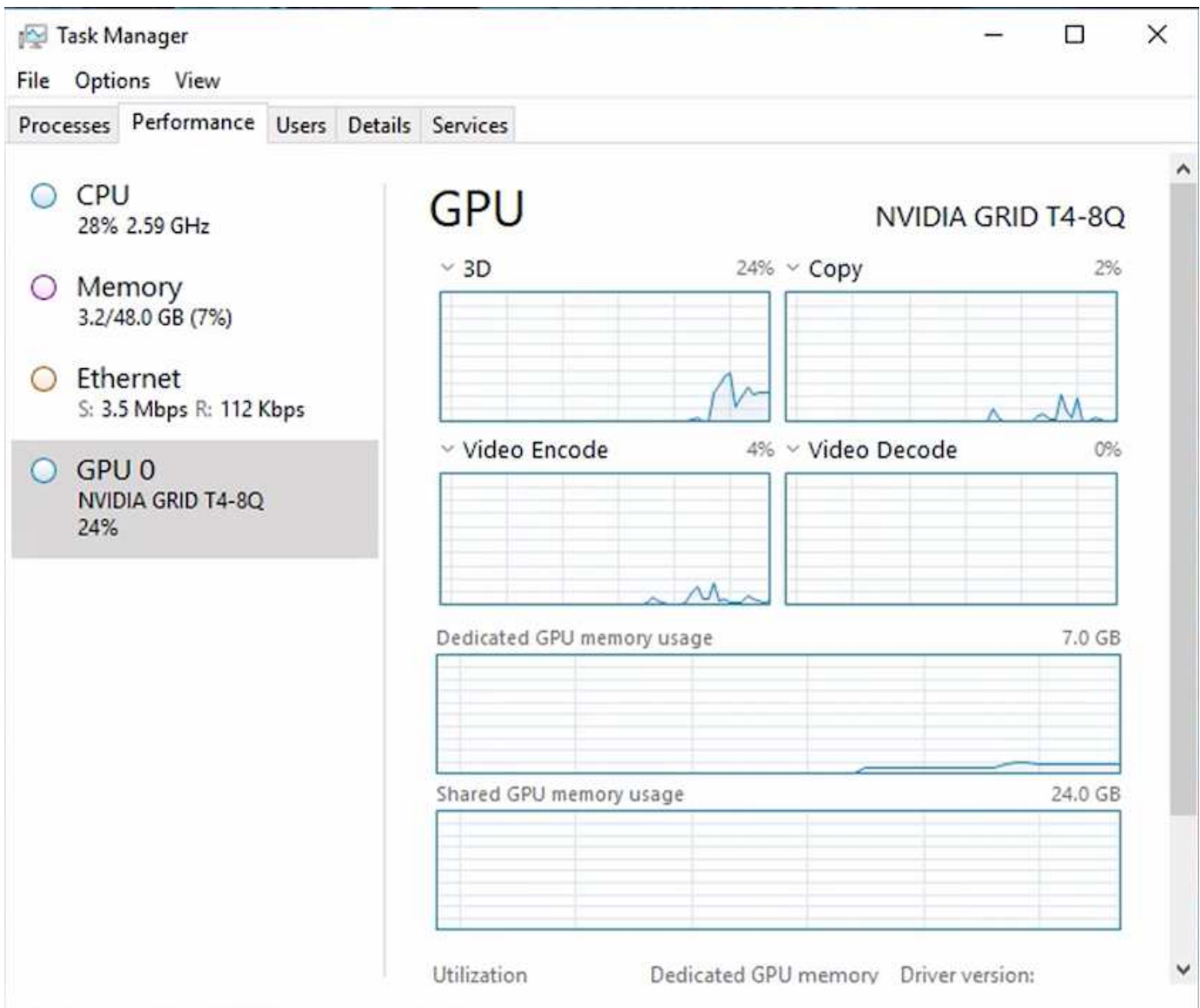
The screenshot shows the TechPowerUp GPU-Z 2.36.0 application window. The 'Graphics Card' tab is selected, displaying detailed information about the NVIDIA GRID T4-8Q GPU. The interface includes a top navigation bar with tabs for 'Graphics Card', 'Sensors', 'Advanced', and 'Validation'. The main content area is organized into a grid of fields and sections. The GPU name is 'NVIDIA GRID T4-8Q', and the GPU core is 'TU104'. The technology is '12 nm' and the die size is '545 mm²'. The release date is 'Sep 13, 2018' and the transistor count is '13600M'. The BIOS version is '0.00.00.00.00'. The subvendor is 'NVIDIA' and the device ID is '10DE 1EB8 - 10DE 130F'. The bus interface is 'PCI'. The memory type is 'GDDR6' and the memory size is '8192 MB'. The driver version is '27.21.14.5257 (NVIDIA 452.57) / 2016' and the driver date is 'Oct 22, 2020'. The GPU clock is '585 MHz' and the memory clock is '0 MHz'. The NVIDIA SLI is 'Disabled'. The computing technologies are 'OpenCL', 'CUDA', 'DirectCompute', and 'DirectML'. The technologies are 'Vulkan', 'Ray Tracing', 'PhysX', and 'OpenGL 4.6'. The NVIDIA logo is visible on the right side of the window. A 'Close' button is located at the bottom right of the window.

Field	Value
Name	NVIDIA GRID T4-8Q
GPU	TU104
Revision	A1
Technology	12 nm
Die Size	545 mm <sup>2</sup>
Release Date	Sep 13, 2018
Transistors	13600M
BIOS Version	0.00.00.00.00
Subvendor	NVIDIA
Device ID	10DE 1EB8 - 10DE 130F
ROPs/TMUs	8 / 160
Bus Interface	PCI
Shaders	2560 Unified
DirectX Support	12 (12_2)
Pixel Fillrate	4.7 GPixel/s
Texture Fillrate	93.6 GTexel/s
Memory Type	GDDR6
Bus Width	256 bit
Memory Size	8192 MB
Bandwidth	Unknown
Driver Version	27.21.14.5257 (NVIDIA 452.57) / 2016
Driver Date	Oct 22, 2020
Digital Signature	WHQL
GPU Clock	585 MHz
Memory	0 MHz
Shader	N/A
Default Clock	585 MHz
Memory	0 MHz
Shader	N/A
NVIDIA SLI	Disabled
Computing	<input checked="" type="checkbox"/> OpenCL <input checked="" type="checkbox"/> CUDA <input checked="" type="checkbox"/> DirectCompute <input type="checkbox"/> DirectML
Technologies	<input checked="" type="checkbox"/> Vulkan <input checked="" type="checkbox"/> Ray Tracing <input type="checkbox"/> PhysX <input checked="" type="checkbox"/> OpenGL 4.6

Um die GPU zu verwenden, müssen Sie den entsprechenden Treiber installieren, der vom NVIDIA-Lizenzportal heruntergeladen werden kann. In einer Azure-Umgebung ist der NVIDIA-Treiber als GPU-Treiber-Erweiterung verfügbar. Als Nächstes müssen die Gruppenrichtlinien im folgenden Screenshot aktualisiert







Um sicherzustellen, dass die Virtual Machine in der NetApp HCI H615C mit Virtual Desktop Service implementiert wird, definieren Sie eine Site mit der vCenter Cluster-Ressource, die H615C Hosts enthält. Die VM-Vorlage muss das erforderliche vGPU-Profil aufweisen.

In Shared-Umgebungen mit mehreren Sitzungen sollten mehrere homogene vGPU-Profile zugewiesen werden. Bei professionellen High-End-Grafikapplikationen ist es jedoch besser, jede VM dediziert einem Benutzer zu haben, um VMs voneinander zu isolieren.

Der GPU-Prozessor kann durch eine QoS-Richtlinie gesteuert werden, und jedes vGPU-Profil kann über dedizierte Frame-Puffer verfügen. Der Encoder und der Decoder werden jedoch für jede Karte freigegeben. Die Platzierung eines vGPU-Profiles auf einer GPU-Karte wird von der GPU-Zuweisungsrichtlinie des vSphere Hosts gesteuert, die die Performance (Spread VMs) oder die Konsolidierung (Gruppen-VMs) hervorheben kann.

#### Lösungen für die Branche

Grafikarbeitsplätze werden typischerweise in Branchen eingesetzt, zum Beispiel Fertigung, Gesundheitswesen, Energie, Medien und Unterhaltung, Bildung, Und so weiter. Häufig ist die Mobilität für grafikintensive Applikationen eingeschränkt.

Um das Problem der Mobilität zu lösen, bieten Virtual Desktop Services eine Desktop-Umgebung für alle Arten von Mitarbeitern, von Task Workers bis hin zu Experteneinsätzen, die Hardware-Ressourcen in der Cloud oder mit NetApp HCI verwenden, einschließlich Optionen für flexible GPU-Konfigurationen. MIT VDS können Benutzer von überall aus mit Laptops, Tablets und anderen mobilen Geräten auf ihre Arbeitsumgebung zugreifen.

Zur Ausführung von Produktions-Workloads mit Software wie ANSYS Fluent, ANSYS Mechanical, Autodesk AutoCAD, Autodesk Inventor, Autodesk 3ds Max, Dassault Systèmes SOLIDWORKS, Dassault Systèmes CATIA, PTC Creo, Siemens PLM NX usw., Die in verschiedenen Clouds verfügbaren GPUs (Stand Januar 2021) sind in der folgenden Tabelle aufgeführt.

GPU-Modell	Microsoft Azure	Google Compute (GCP)	Amazon Web Services (AWS)	On-Premises (NetApp HCI)
NVIDIA M60	Ja.	Ja.	Ja.	Nein
NVIDIA T4	Nein	Ja.	Ja.	Ja.
NVIDIA P100	Nein	Ja.	Nein	Nein
NVIDIA P4	Nein	Ja.	Nein	Nein

Darüber hinaus sind auch gemeinsame Desktop-Sitzungen mit anderen Benutzern und dedizierte persönliche Desktops verfügbar. Virtual Desktops können über eine oder vier GPUs verfügen oder mit NetApp HCI TeilaufGPUs nutzen. Die NVIDIA T4 ist eine vielseitige GPU-Karte, die sich den Anforderungen eines breiten Spektrums an Benutzer-Workloads anpasst. Jede GPU-Karte auf dem NetApp HCI H615C verfügt über 16 GB Frame-Puffer-Speicher und drei Karten pro Server. Die Anzahl der Benutzer, die auf einem einzelnen H615C Server gehostet werden können, hängt von der Benutzer-Workload ab.

Benutzer/Server	Licht (4 GB)	Mittel (8 GB)	Schwer (16 GB)
H615C	12	6	3

Zur Ermittlung des Benutzertyps führen Sie das GPU-Profiler-Tool aus, während Benutzer mit Anwendungen arbeiten, die typische Aufgaben ausführen. Der GPU-Profiler erfasst die Speicheranforderungen, die Anzahl der Anzeigen und die Auflösung, die Benutzer benötigen. Sie können dann das vGPU-Profil auswählen, das Ihre Anforderungen erfüllt.

Virtuelle Desktops mit GPUs können eine Anzeigeauflösung von bis zu 8 KB unterstützen. Das Utility nView kann einen einzelnen Monitor in Regionen aufteilen und mit unterschiedlichen Datensätzen arbeiten.

ONTAP File Storage bietet folgende Vorteile:

- Ein Single Namespace kann bis zu 20 PB Storage mit 400 Milliarden Dateien anwachsen und dabei keinen großen administrativen Aufwand haben
- Ein Namespace, der sich mit einem globalen File Cache weltweit erstrecken kann
- Sichere Mandantenfähigkeit mit gemanagtem NetApp Storage
- Migration von kalten Daten zu Objektspeichern mit NetApp FabricPool
- Schnelle Dateistatistiken mit Dateisystemanalysen
- Storage-Cluster auf bis zu 24 Nodes skalieren, was Kapazität und Performance erhöht
- Storage-Platzbedarf lässt sich mithilfe von Kontingenten und garantierter Performance mit QoS-Limits kontrollieren

- Sicherung von Daten durch Verschlüsselung
- Erfüllen umfassender Anforderungen an Datensicherung und Compliance
- Flexible Business Continuity-Optionen

### Schlussfolgerung

Der NetApp Virtual Desktop Service bietet eine einfach zu nutzende Umgebung, in der virtuelle Desktop-Computer und Applikationen leicht zu belegen sind, und konzentriert sich auf geschäftliche Herausforderungen. Durch die Erweiterung von VDS auf die lokale ONTAP Umgebung können Unternehmen leistungsstarke NetApp Funktionen in einer VDS-Umgebung nutzen, darunter Rapid Clone, Inline-Deduplizierung, Data-Compaction, Thin Provisioning Und Komprimierung. Diese Funktionen senken die Storage-Kosten und verbessern die Performance mit All-Flash-Storage. Mit VMware vSphere Hypervisor, der die Server-Bereitstellung durch die Verwendung von Virtual Volumes und vSphere API für die Array-Integration auf ein Minimum reduziert Mithilfe der Hybrid Cloud wählen Kunden die richtige Umgebung für ihre anspruchsvollen Workloads und sparen Geld. Die Desktop-Session, bei der lokale Systeme ausgeführt wird, kann richtlinienbasiert auf Cloud-Ressourcen zugreifen.

### Weitere Informationen

Sehen Sie sich die folgenden Dokumente und/oder Websites an, um mehr über die in diesem Dokument beschriebenen Informationen zu erfahren:

- ["NetApp Cloud"](#)
- ["NetApp VDS Produktdokumentation"](#)
- ["Das lokale Netzwerk mit Azure verbinden Sie über VPN Gateway"](#)
- ["Azure-Portal"](#)
- ["Microsoft Windows Virtual Desktop"](#)
- ["Azure NetApp Files-Anmeldung"](#)

## VMware Horizon

### NVA-1132-DESIGN: VMware Endbenutzer-Computing mit NetApp HCI

Suresh ThopPay, NetApp

Das VMware Endbenutzer-Computing mit NetApp HCI ist eine validierte Best-Practice Datacenter-Architektur zur Implementierung virtueller Desktop Workloads im Enterprise-Maßstab. Dieses Dokument beschreibt das Architekturdesign und Best Practices für eine zuverlässige und risikofreie Implementierung der Lösung im Produktionsskala.

["NVA-1132-DESIGN: VMware Endbenutzer-Computing mit NetApp HCI"](#)

## **NVA-1129-DESIGN: VMware End-User Computing mit NetApp HCI und NVIDIA GPUs**

Suresh ThopPay, NetApp

Das VMware Endbenutzer-Computing mit NetApp HCI ist eine validierte Best-Practice Datacenter-Architektur zur Implementierung virtueller Desktop Workloads im Enterprise-Maßstab. Dieses Dokument beschreibt das Architekturdesign und Best Practices für eine zuverlässige und risikofreie Implementierung der Lösung im Produktionsskala.

["NVA-1129-DESIGN: VMware End-User Computing mit NetApp HCI und NVIDIA GPUs"](#)

## **NVA-1129-DEPLOY: VMware Endbenutzer-Computing mit NetApp HCI und NVIDIA-GPUs**

Suresh ThopPay, NetApp

VMware End-User Computing with NetApp HCI ist eine vorab validierte, Best Practice Datacenter-Architektur zur Implementierung virtueller Desktop Workloads auf Enterprise-Niveau. In diesem Dokument wird beschrieben, wie Sie die Lösung im Produktionsskala zuverlässig und risikofrei bereitstellen

["NVA-1129-DEPLOY: VMware Endbenutzer-Computing mit NetApp HCI und NVIDIA-GPUs"](#)

## **NetApp HCI for Virtual Desktop Infrastructure mit VMware Horizon 7 – stärken Sie Ihre Power-User mit 3D-Grafiken**

Suresh ThopPay, NetApp

TR-4792 enthält Anweisungen zur Verwendung des NetApp H615C Computing-Nodes für 3D-Grafik-Workloads in einer VMware Horizon-Umgebung mit NVIDIA-GPUs (Graphics Processing Units) und Virtualisierungssoftware. Er enthält außerdem die Ergebnisse der vorläufigen Tests von SPECviewperf 13 für den H615C.

["NetApp HCI for Virtual Desktop Infrastructure mit VMware Horizon 7 – stärken Sie Ihre Power-User mit 3D-Grafiken"](#)

## **FlexPod Lösungen für die Desktop-Virtualisierung**

Weitere Informationen zu FlexPod Virtualisierungslösungen finden Sie im ["FlexPod Designrichtlinien"](#)

## **NetApp All-Flash SAN-Array mit VMware vSphere 8**

Autor: Josh Powell – NetApp Solutions Engineering

### **Lösungsüberblick**

#### **Einführung**

Seit fast zwei Jahrzehnten hat sich die NetApp ONTAP Software als eine der führenden Storage-Lösungen für VMware vSphere Umgebungen etabliert und führt kontinuierlich innovative Funktionen ein, die das



Management vereinfachen und Kosten senken. NetApp ist führend in der Entwicklung von NAS und Unified Storage-Plattformen, die eine Vielzahl von Protokollen und Konnektivitätsunterstützung bieten. Neben diesem Marktsegment gibt es viele Kunden, die die Einfachheit und die Kostenvorteile von blockbasierten SAN-Storage-Plattformen bevorzugen, die sich nur um eine gute Arbeit bewerben möchten. Die All-Flash SAN-Arrays (ASA) von NetApp werden diesem Versprechen gerecht: Sie profitieren von einfacher Skalierbarkeit sowie von konsistenten Management- und Automatisierungsfunktionen für alle Applikationen und Cloud-Provider.

## Zweck dieses Dokuments

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

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

## Technologischer Überblick

Diese Lösung umfasst innovative Technologien von VMware und NetApp.

### VMware vSphere 8.0

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

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

### Neue Verbesserungen in vSphere 8.0

vSphere 8.0 bringt einige neue Verbesserungen mit sich, darunter:

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

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

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

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

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

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

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

## VMware Virtual Volumes (VVols)

VVols stellen eine revolutionäre neue Herangehensweise an das Storage-Management in vSphere Clustern dar, die ein vereinfachtes Management und eine granularere Kontrolle der Storage-Ressourcen bietet. In einem VVols Datastore ist jede virtuelle Festplatte ein vVol und wird zu einem nativen LUN-Objekt auf dem Storage-System. Die Integration des Storage-Systems mit vSphere erfolgt über den Provider **VMware API's for Storage Awareness (VASA)** und ermöglicht es dem Storage-System, die VM-Daten zu erkennen und entsprechend zu managen. Storage-Richtlinien, die im vCenter Client definiert werden, werden zur Zuweisung und Verwaltung von Speicherressourcen verwendet.

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

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

## NVMe over Fabric

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

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

---

## NetApp ONTAP

Seit fast zwei Jahrzehnten ist die NetApp ONTAP Software eine der führenden Storage-Lösungen für VMware vSphere Umgebungen und wird kontinuierlich mit innovativen Funktionen erweitert, die nicht nur zur Vereinfachung des Managements, sondern auch zu Kostensenkungen beitragen. Die Kombination von ONTAP und vSphere ermöglicht Kosteneinsparungen für Host-Hardware und VMware Software. Sichern Sie Ihre Daten außerdem zu niedrigeren Kosten durch eine konstant hohe Performance und profitieren Sie gleichzeitig von der nativen Storage-Effizienz.

### Basis-ONTAP-Funktionen

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

- **Storage-Effizienz** – ONTAP bietet Deduplizierung und Komprimierung im Hintergrund in Echtzeit, Zero-Block-Deduplizierung und Data-Compaction.
- **Volume- und LUN-Verschiebung** - ermöglicht unterbrechungsfreies Verschieben von Volumes und LUNs, die vSphere Datastores und VVols im ONTAP-Cluster unterstützen, um Performance und Kapazität auszubalancieren oder unterbrechungsfreie Wartung und Upgrades zu ermöglichen.
- **Relocation von Volume und LUN** - ONTAP ermöglicht die unterbrechungsfreie Verschiebung von Volumes und LUNs auf denen vSphere Datastores und VVols im ONTAP Cluster gehostet werden. Dadurch können Performance und Kapazität besser ausbalanciert und unterbrechungsfreie Upgrades ermöglicht werden.

- **Quality of Service** - QoS ist eine Funktion, die das Management der Performance auf einer einzelnen LUN, einem Volume oder einer Datei ermöglicht. Mit dieser Lösung kann eine aggressive VM begrenzt oder sichergestellt werden, dass eine kritische VM ausreichend Performance-Ressourcen erhält.
- **Verschlüsselung** - NetApp-Volume-Verschlüsselung und NetApp-Aggregat-Verschlüsselung. Diese Optionen bieten einen einfachen, softwarebasierten Ansatz zur Verschlüsselung von Daten im Ruhezustand und gewährleisten somit ihren Schutz.
- **Fabric Pool** - bei dieser Funktion werden Daten, auf die weniger häufig zugegriffen wird, in einen separaten Objektspeicher verlagert, wodurch wertvoller Flash-Speicher freigegeben wird. Auf Block-Ebene werden kältere Daten effizient erkannt und verschoben. So lassen sich Storage-Ressourcen optimieren und Kosten senken.
- **Automatisierung** – vereinfacht Storage- und Datenmanagementaufgaben durch den Einsatz von ONTAP REST-APIs zur Automatisierung und durch die Nutzung von Ansible-Modulen für ein nahtloses Konfigurationsmanagement von ONTAP-Systemen. Ansible-Module bieten eine praktische Lösung zum effizienten Management der Konfigurationen von ONTAP-Systemen. Durch die Kombination dieser leistungsstarken Tools werden die Workflows optimiert und das gesamte Management der Storage-Infrastruktur verbessert.

### ONTAP Funktionen für die Disaster Recovery

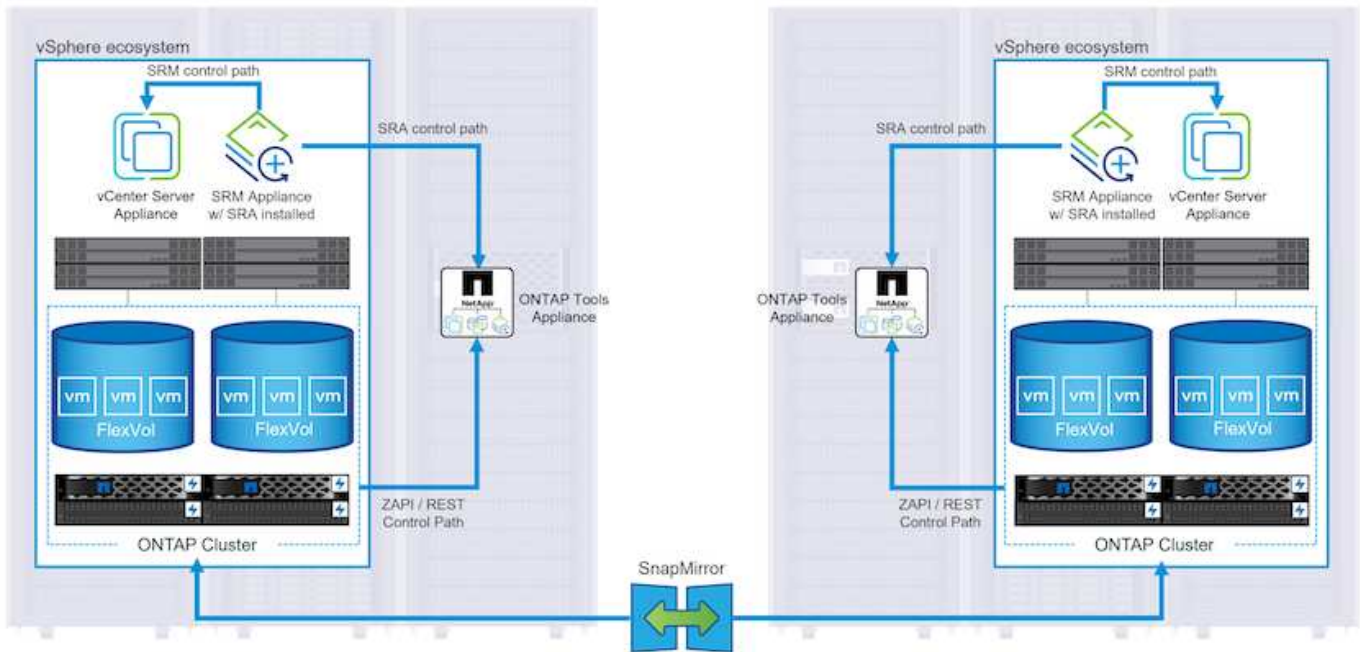
NetApp ONTAP bietet robuste Disaster Recovery-Lösungen für VMware Umgebungen. Diese Lösungen nutzen die SnapMirror Replizierungstechnologien zwischen primären und sekundären Storage-Systemen, um bei Ausfällen Failover und schnelle Recoverys zu ermöglichen.

#### Storage Replication Adapter:

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

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

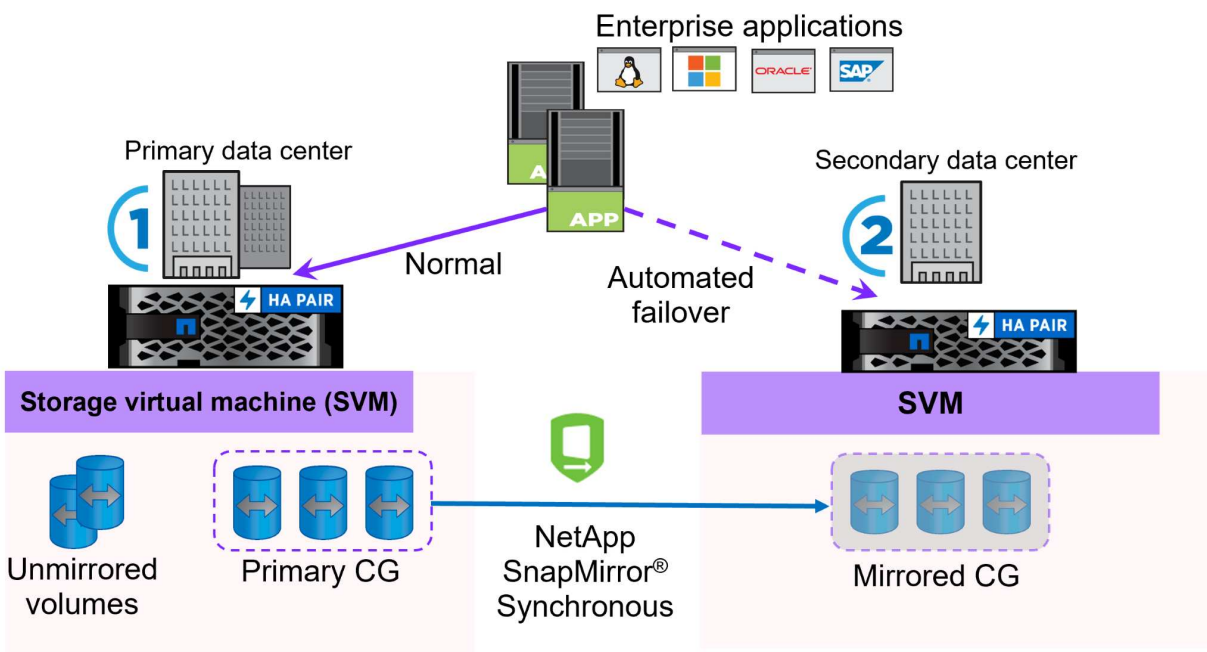
NetApp SRA wird im Rahmen der ONTAP-Tools für VMware vSphere installiert.



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

### SnapMirror Business Continuity:

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



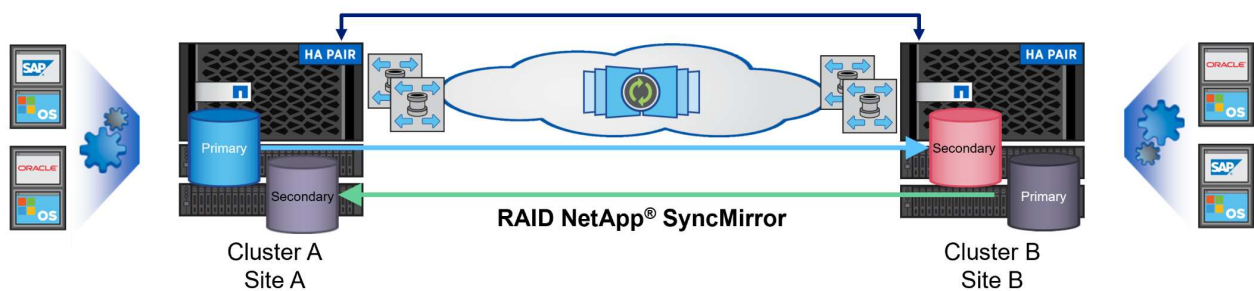
Weitere Informationen finden Sie unter SnapMirror "[Business Continuity im Überblick](#)".

### NetApp MetroCluster:

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

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

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



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

### ONTAP One Lizenzmodell

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

Die Lizenzierung von ONTAP One umfasst alle folgenden Funktionen:

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

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

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

**SnapRestore** – ermöglicht schnelle Wiederherstellung von Daten aus Snapshots.

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

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

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

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

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

---

## NetApp All-Flash-SAN-Array

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

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

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



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



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

### Funktionen von NetApp ASA

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

**Performance** – das All-Flash-SAN-Array nutzt SSD-Laufwerke (Solid-State Drives) mit einer End-to-End-



NVMe-Architektur, um eine blitzschnelle Performance bereitzustellen, die Latenz erheblich zu reduzieren und die Reaktionszeiten von Applikationen zu verbessern. Sie bietet konsistent hohe IOPS bei niedriger Latenz und ist somit für latenzkritische Workloads wie Datenbanken, Virtualisierung und Analysen geeignet.

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

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

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

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

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

#### **Unterstützte Protokolle**

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

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

Designanleitungen zu iSCSI-Konfigurationen finden Sie unter .

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

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

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

Netzwerke.

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

### **Aktiv/aktiv-Technologie**

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

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

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

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

### **Storage-Garantien**

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

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

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

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

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

---

### **NetApp Plug-ins für VMware vSphere**

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

#### **ONTAP Tools für VMware vSphere**

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

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

ONTAP-Tools enthält die folgenden Komponenten:



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

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

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

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

### **SnapCenter Plug-in für VMware vSphere**

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

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

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

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

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

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

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

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

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

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

## NetApp Cloud Insights

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

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

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

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

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

## NetApp All-Flash SAN-Array mit VMware vSphere 8

Autor: Josh Powell – NetApp Solutions Engineering

### Managen von Blockspeicher mit ONTAP-Tools für VMware vSphere

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

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

ONTAP-Tools enthält die folgenden Komponenten:

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

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

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

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

## Übersicht Zur Lösungsimplementierung

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

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

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

Diese Lösung deckt die folgenden grundlegenden Schritte ab:

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

### Voraussetzungen

Folgende Komponenten wurden in dieser Lösung verwendet:

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

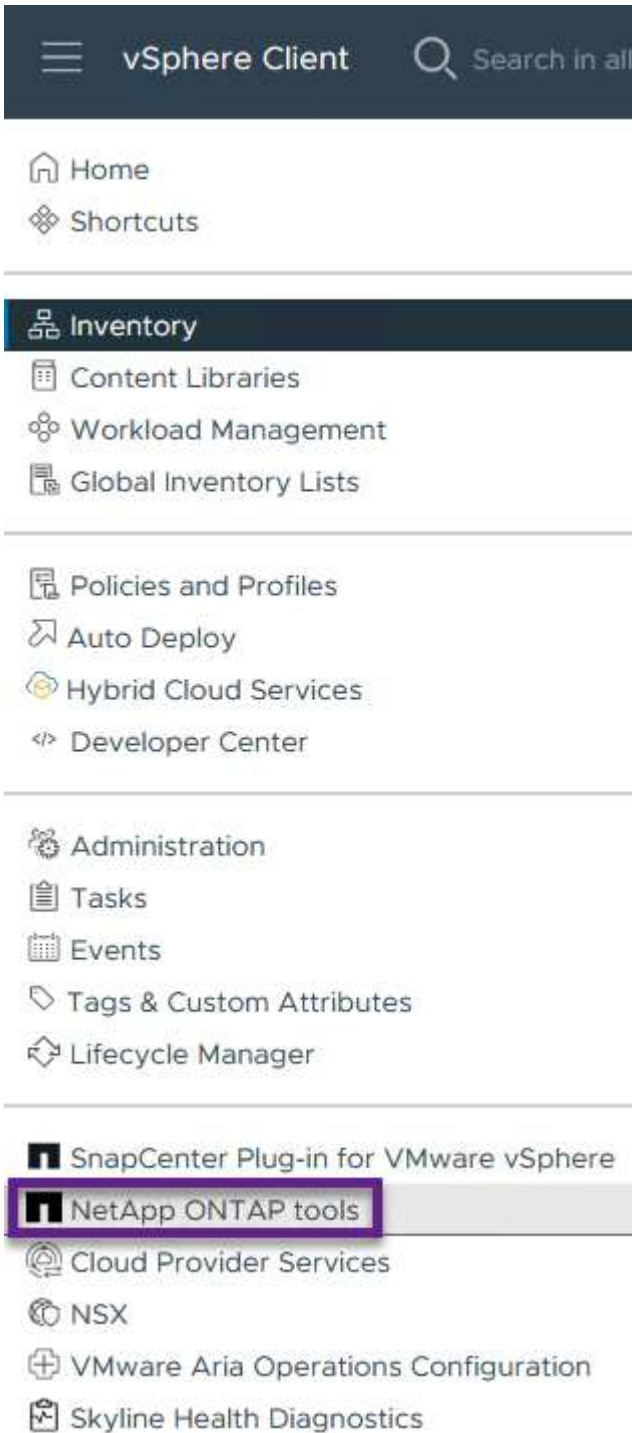
### Lösungsimplementierung

#### Erstellen Sie einen VVols-Datastore in ONTAP Tools

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

**Fügen Sie ONTAP Tools ein Storage-System hinzu.**

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



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



NetApp ONTAP tools INSTANCE 10.61.181.154:8443 ▾

Overview

## Storage Systems

Storage Systems

ADD

REDISCOVER ALL

Storage capability profile

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

## Add Storage System



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

vCenter server

10.61.181.205 ▾

Name or IP address:

10.192.102.103

Username:

admin

Password:

●●●●●●●●

Port:

443

Advanced options ^

ONTAP Cluster Certificate:



Automatically fetch



Manually upload

CANCEL

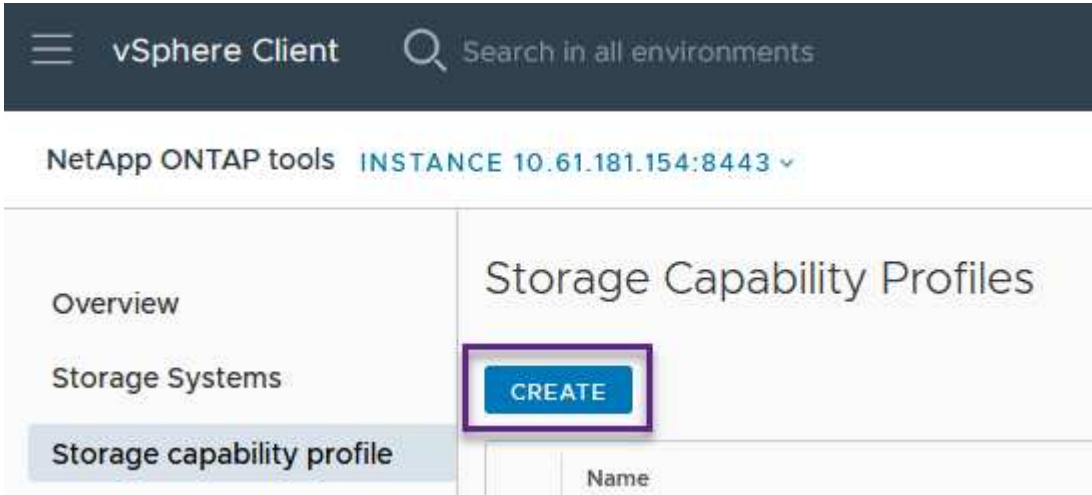
ADD

## Erstellen Sie in ONTAP-Tools ein Storage-Funktionsprofil

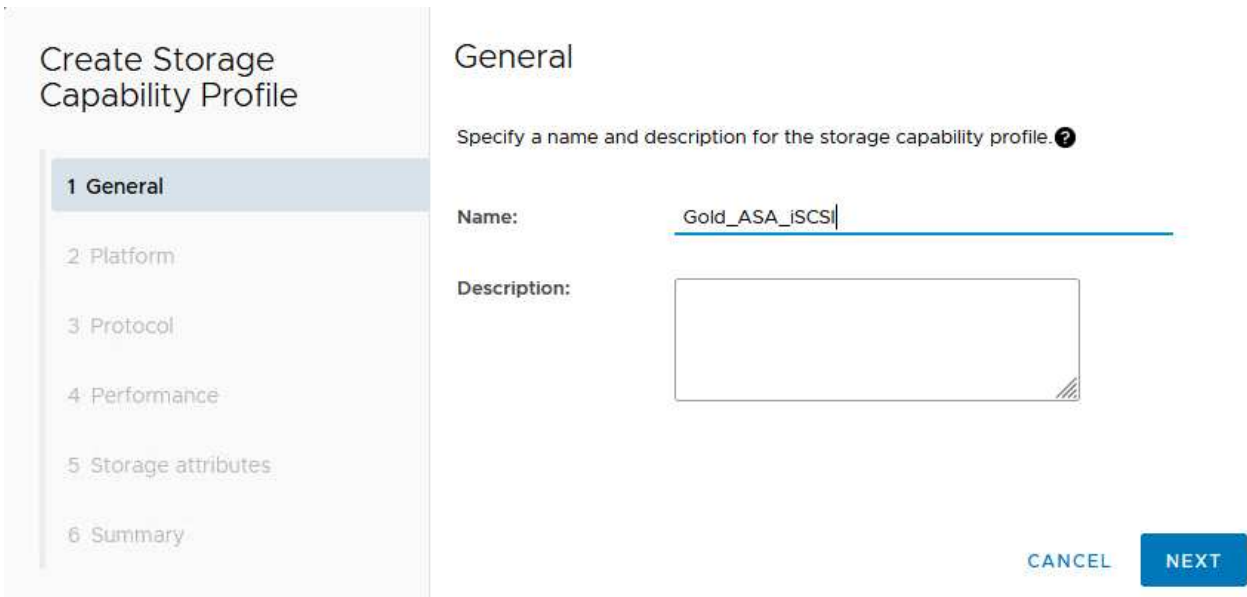
Storage-Funktionsprofile beschreiben die Funktionen eines Storage-Arrays oder Storage-Systems. Sie umfassen Definitionen zur Servicequalität und werden zur Auswahl von Storage-Systemen verwendet, die die im Profil definierten Parameter erfüllen.

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

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



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

The screenshot shows the 'Create Storage Capability Profile' wizard in the 'General' step. The left sidebar lists the steps: '1 General', '2 Platform', '3 Protocol', '4 Performance', '5 Storage attributes', and '6 Summary'. The main area is titled 'General' and contains the instruction 'Specify a name and description for the storage capability profile.' Below this, 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', with 'NEXT' being highlighted in blue.

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

## Create Storage Capability Profile

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

### Platform

Platform: Performance

Asymmetric:

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

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

### Protocol

Protocol: Any

- Any
- FCP
- iSCSI
- NVMe/FC

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Performance

None ⓘ

QoS policy group ⓘ

Min IOPS:

\_\_\_\_\_

Max IOPS:

6000

Unlimited

CANCEL

BACK

NEXT

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

## Create Storage Capability Profile

1 General

2 Platform

3 Protocol

4 Performance

5 Storage attributes

6 Summary

## Storage attributes

Deduplication:

Yes

Compression:

Yes

Space reserve:

Thin

Encryption:

No

Tiering policy (FabricPool):

None

CANCEL

BACK

NEXT

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



## Create Storage Capability Profile

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

## Summary

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

CANCEL

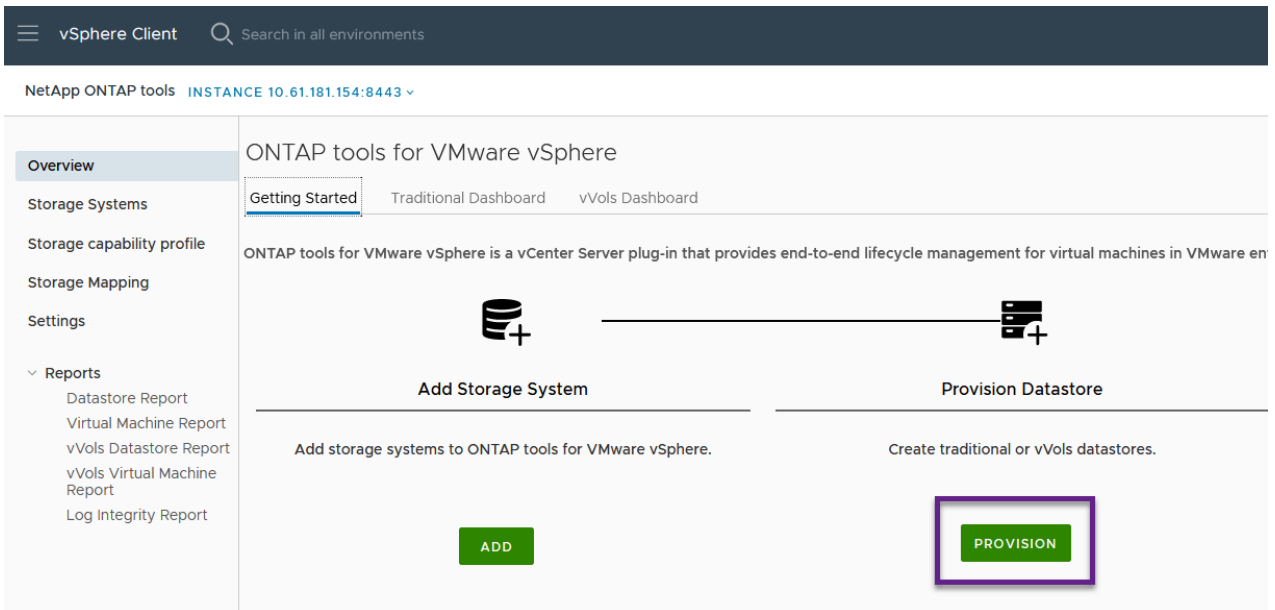
BACK

FINISH

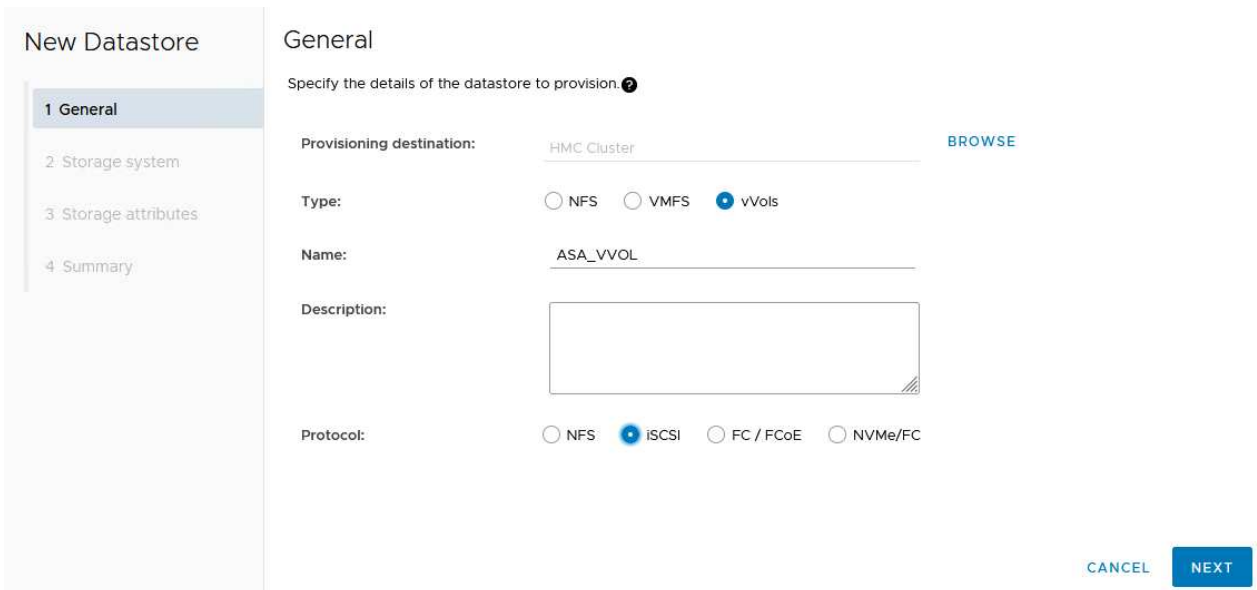
## Erstellen Sie einen VVols-Datstore in ONTAP Tools

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

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



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



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

## New Datastore

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

## Storage system

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

Storage capability profiles:

FAS\_Default  
FAS\_Max20  
**Custom profiles**  
Gold\_ASA\_JSCSI  
Gold\_ASA

Storage system:

HCG-NetApp-A400-E3U03 (10.192.102.103)

Storage VM:

svml

CANCEL

BACK

NEXT

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

## New Datastore

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

## Storage attributes

Specify the storage details for provisioning the datastore.

Volumes:  Create new volumes  Select volumes

Create new volumes

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

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

ADD

CANCEL

BACK

NEXT

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

### New Datastore

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

### Summary

**General**

vCenter server: 10.61.181.205

Provisioning destination: HMC Cluster

Datastore name: ASA\_VVOL

Datastore type: vVols

Protocol: iSCSI

Storage capability profile: Gold\_ASA

**Storage system details**

Storage system: HCG-NetApp-A400-E3U03

SVM: svm1

**Storage attributes**

New FlexVol Name	New FlexVol Size	Aggregate	Storage Capability Profile

CANCEL
BACK
FINISH

## Erstellen Sie eine VM-Storage-Richtlinie im vSphere Client

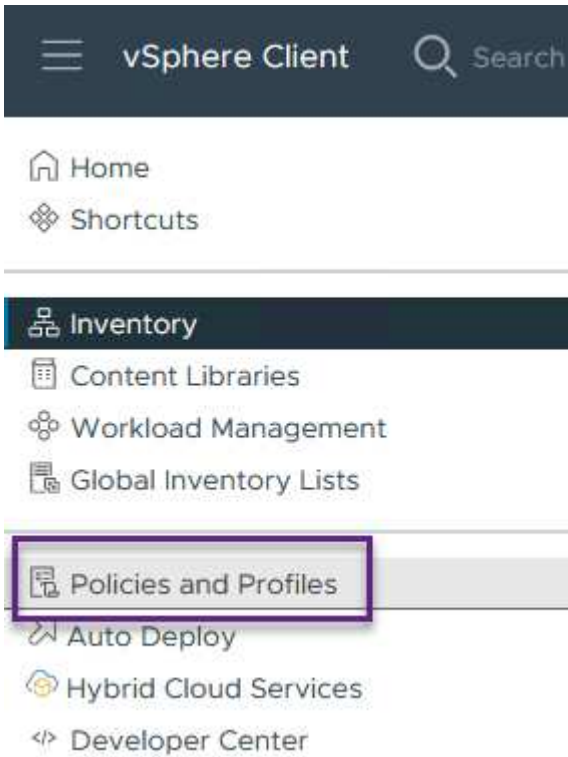
Eine VM Storage-Richtlinie ist eine Reihe von Regeln und Anforderungen, die festlegen, wie Daten für Virtual Machines (VM) gespeichert und gemanagt werden sollen. Er gibt die gewünschten Storage-Merkmale wie Performance, Verfügbarkeit und Datenservices für eine bestimmte VM an.

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

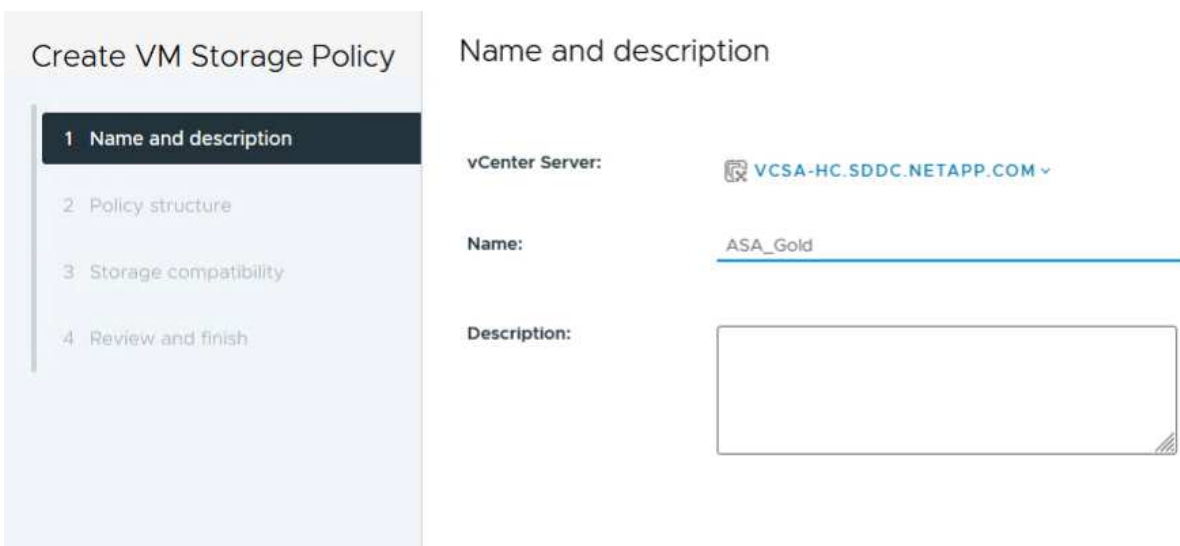
## Erstellen einer VM-Storage-Richtlinie

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

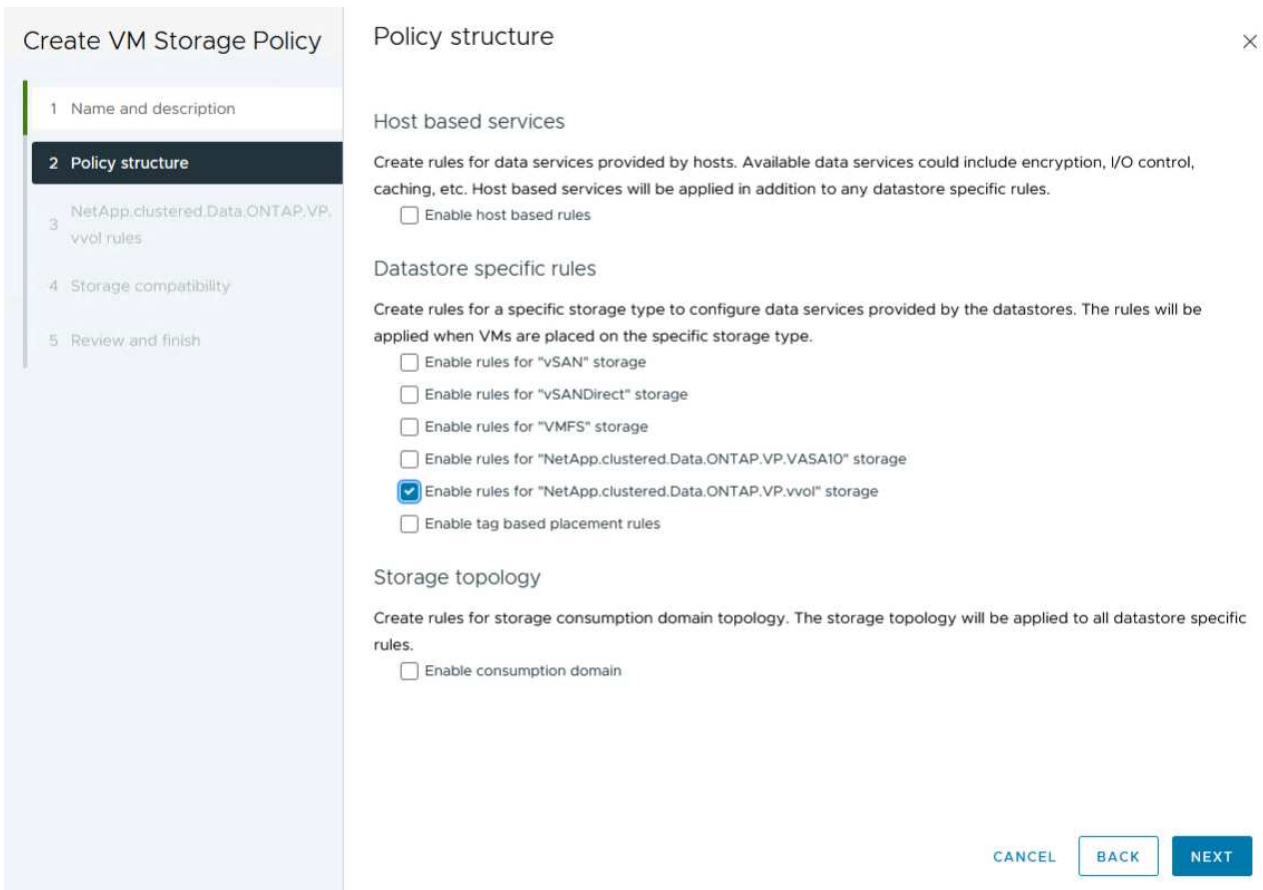
1. Wählen Sie im vSphere Clients Hauptmenü **Policies und Profile**.



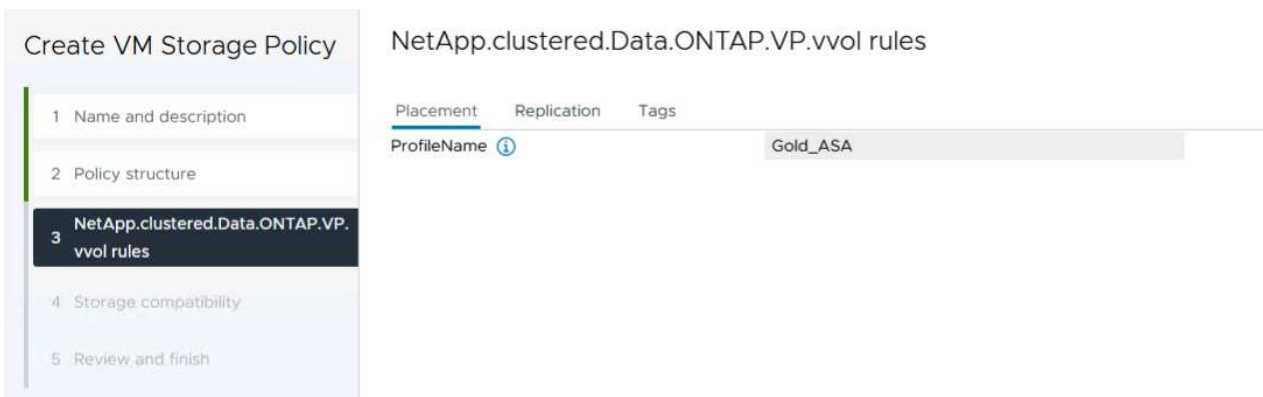
2. Geben Sie im Assistenten **Create VM Storage Policy** zunächst einen Namen und eine Beschreibung für die Richtlinie ein und klicken Sie auf **Weiter**, um fortzufahren.

The image shows the 'Create VM Storage Policy' wizard. On the left, there is a vertical list of steps: '1 Name and description', '2 Policy structure', '3 Storage compatibility', and '4 Review and finish'. The first step is highlighted. On the right, under the heading 'Name and description', there are three fields: 'vCenter Server' with a dropdown menu showing 'VCSA-HC.SDDC.NETAPP.COM', 'Name' with a text input field containing 'ASA\_Gold', and 'Description' with a large empty text area.

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



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



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

## Erstellen Sie eine VM-Storage-Richtlinie im vSphere Client

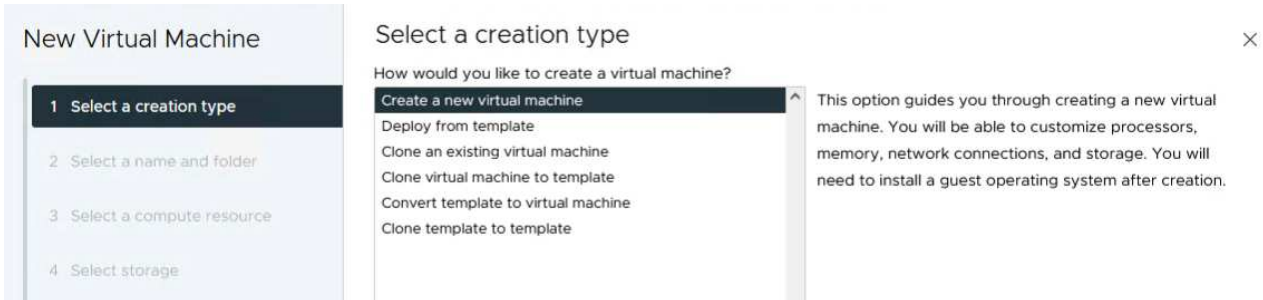
Eine VM Storage-Richtlinie ist eine Reihe von Regeln und Anforderungen, die festlegen, wie Daten für Virtual Machines (VM) gespeichert und gemanagt werden sollen. Er gibt die gewünschten Storage-Merkmale wie Performance, Verfügbarkeit und Datenservices für eine bestimmte VM an.

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

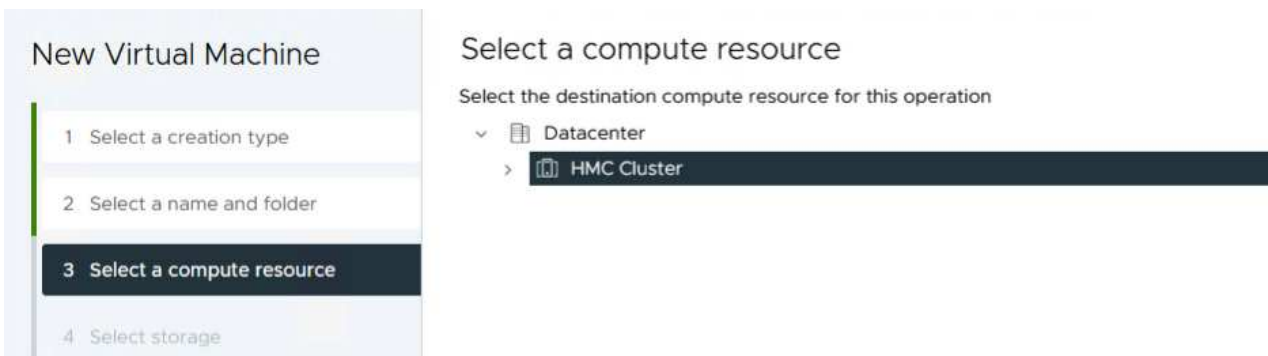
## Erstellen Sie eine virtuelle Maschine auf einem vVol-Datastore

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

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



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



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



## New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage**
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

## Select storage

Select the storage for the configuration and disk files

Encrypt this virtual machine [?](#)

VM Storage Policy ASA\_Gold ▾

Disable Storage DRS for this virtual machine

	Name	Storage Compatibility	Capacity	Provisioned	Free	
<input checked="" type="radio"/>	ASA_VVOLS_1	Compatible	1.95 TB	9 MB	1.95 TB	V
<input type="radio"/>	ASA400_ISCSI01	Incompatible	2 TB	185.32 GB	1.9 TB	V
<input type="radio"/>	DemoDS	Incompatible	800 GB	6.99 GB	793.01 GB	N
<input type="radio"/>	destination	Incompatible	250 GB	32.66 MB	249.97 GB	N
<input type="radio"/>	DRaaSTest	Incompatible	1 TB	133.27 GB	956.83 GB	N
<input type="radio"/>	esxi-hc-01 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-02 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V
<input type="radio"/>	esxi-hc-03 local	Incompatible	349.25 GB	1.41 GB	347.84 GB	V

Manage Columns      Items per page 10 ▾      1 - 10 of 15 items      < < < 1 / 2 > >

Compatibility

Validating...

CANCEL

BACK

NEXT

5. Wählen Sie auf der Seite **Kompatibilität auswählen** die vSphere-Version(en) aus, mit der die VM kompatibel ist.
6. Wählen Sie die Gast-OS-Familie und -Version für die neue VM aus und klicken Sie auf **Weiter**.
7. Füllen Sie die Seite **Hardware anpassen** aus. Beachten Sie, dass für jede Festplatte (VMDK-Datei) eine separate VM-Storage-Richtlinie ausgewählt werden kann.

### New Virtual Machine

- 1 Select a creation type
- 2 Select a name and folder
- 3 Select a compute resource
- 4 Select storage
- 5 Select compatibility
- 6 Select a guest OS
- 7 Customize hardware
- 8 Ready to complete

### Customize hardware

Configure the virtual machine hardware

Virtual Hardware   VM Options   Advanced Parameters

ADD NEW DEVICE ▾

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

**Maximum Size** 1.95 TB

**VM storage policy** ASA\_Gold ▼

**Location** Store with the virtual machine ▼

**Disk Provisioning** Thin Provision ▼

**Sharing** Unspecified ▼

**Disk Mode** Dependent ▼

**Virtual Device Node** New SCSI controller ▼ SCSI(0:0) New Hard disk ▼

> New SCSI controller LSI Logic SAS

> New Network VM Network  Connected

CANCEL
BACK
NEXT

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

## NetApp All-Flash SAN-Array mit VMware vSphere 8

Autor: Josh Powell – NetApp Solutions Engineering

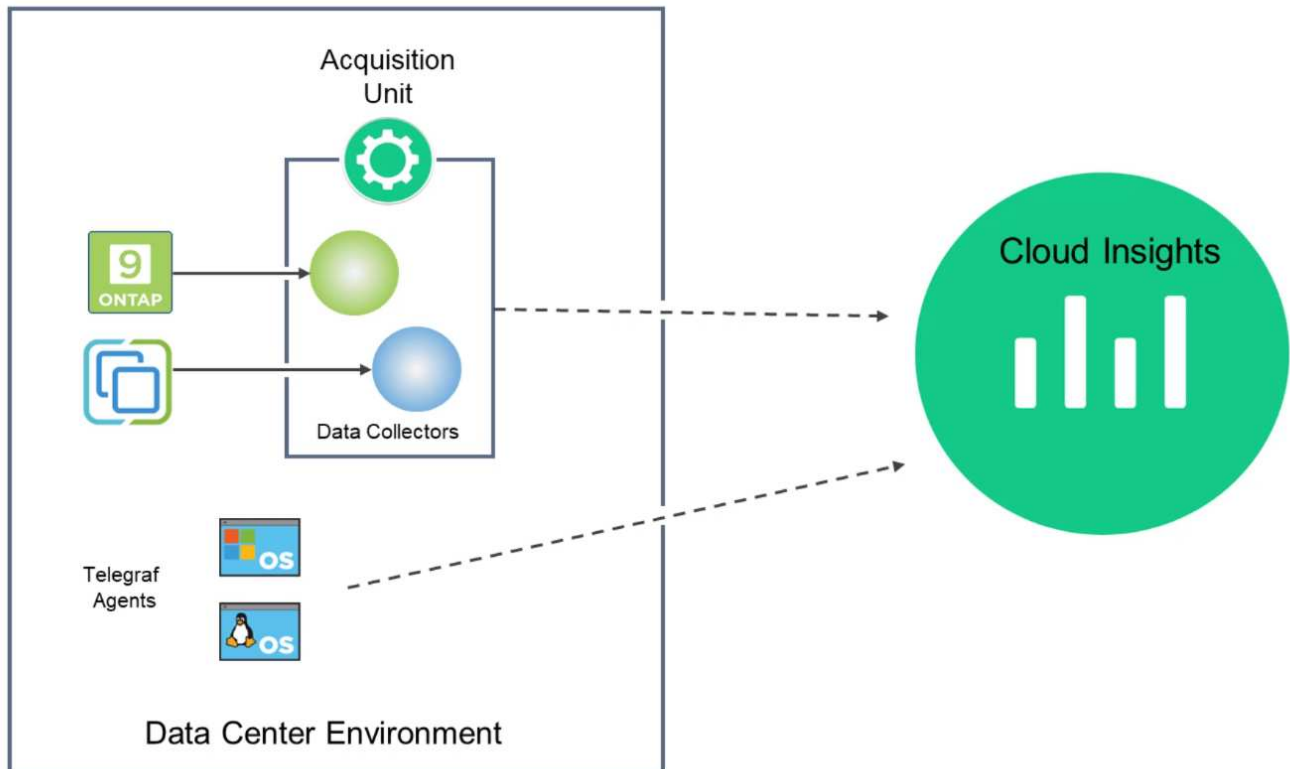
### Überwachen Sie Ihre lokalen Storage-Systeme mit NetApp Cloud Insights

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

NetApp Cloud Insights wird über die Acquisition Unit-Software ausgeführt, die mit Datensammlern für Assets wie VMware vSphere und NetApp ONTAP Storage-Systemen eingerichtet wird. Diese Sammler sammeln Daten und übermitteln sie an Cloud Insights. Die Plattform verwendet dann eine Vielzahl von Dashboards, Widgets und metrischen Abfragen, um die Daten in aufschlussreichen Analysen zu organisieren, die Benutzer

interpretieren können.

Architekturdiagramm von Cloud Insights:



### Übersicht Zur Lösungsimplementierung

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

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

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

### Voraussetzungen

Diese Lösung nutzt die folgenden Komponenten:

1. NetApp All-Flash SAN-Array A400 mit ONTAP 9.13
2. VMware vSphere 8.0-Cluster
3. NetApp Cloud Insights Konto.

4. NetApp Cloud Insights Acquisition Unit-Software auf einer lokalen VM mit Netzwerkverbindung zu Ressourcen zur Datenerfassung.

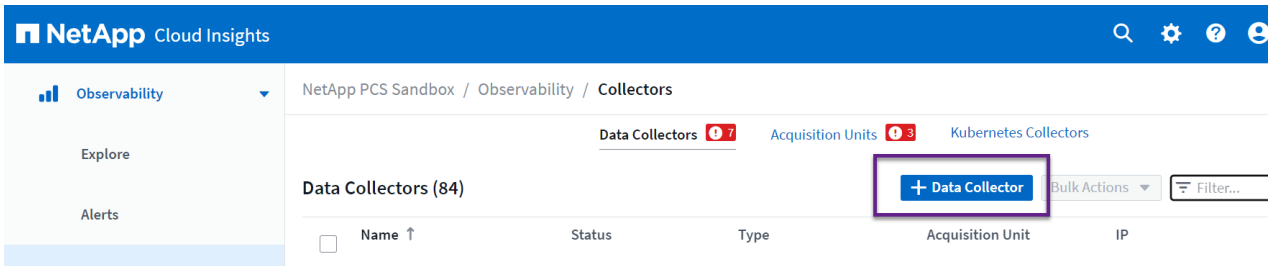
### **Lösungsimplementierung**

#### **Konfigurieren Sie Datensammler**

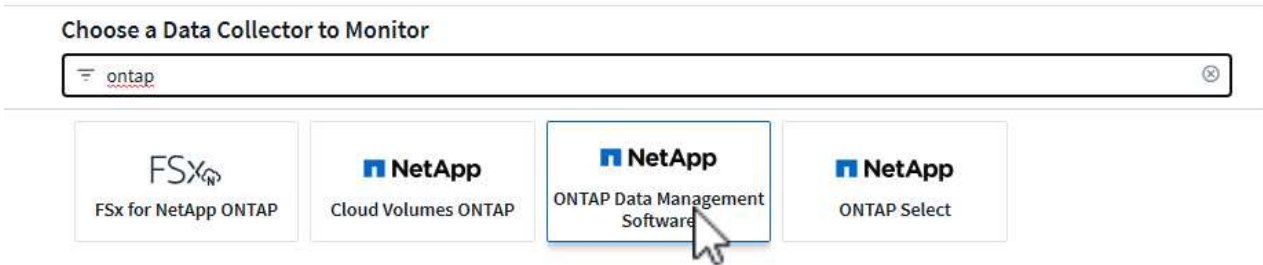
So konfigurieren Sie Data Collectors für VMware vSphere- und ONTAP-Speichersysteme:

## Fügen Sie einen Data Collector für ein ONTAP-Speichersystem hinzu

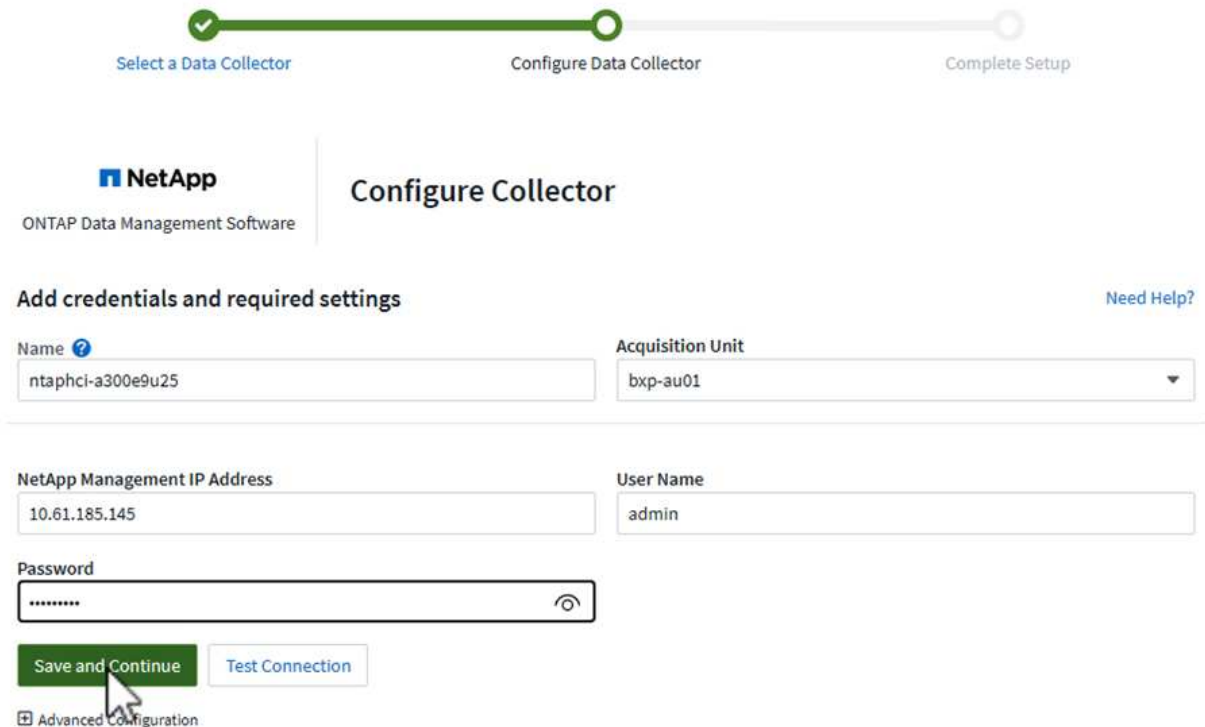
1. Sobald Sie sich bei Cloud Insights angemeldet haben, navigieren Sie zu **Observability > Collectors > Data Collectors**, und drücken Sie die Taste, um einen neuen Data Collector zu installieren.



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

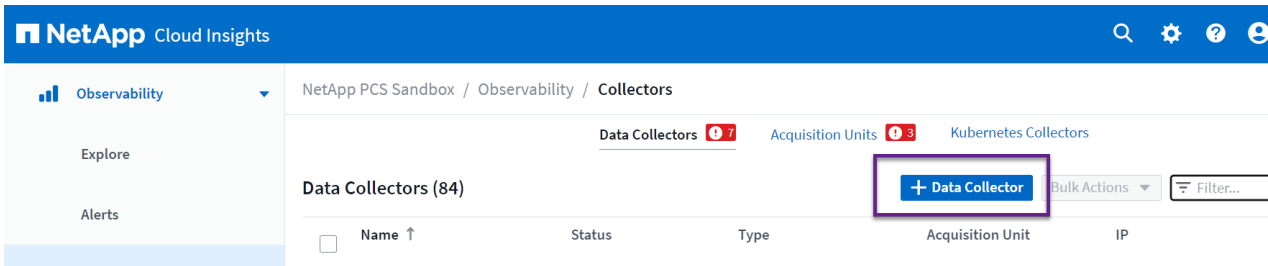


3. Geben Sie auf der Seite **Collector konfigurieren** einen Namen für den Collector ein, geben Sie die richtige **Acquisition Unit** an und geben Sie die Anmeldeinformationen für das ONTAP-Speichersystem an. Klicken Sie unten auf der Seite auf **Speichern und fortfahren** und dann auf **Setup abschließen**,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

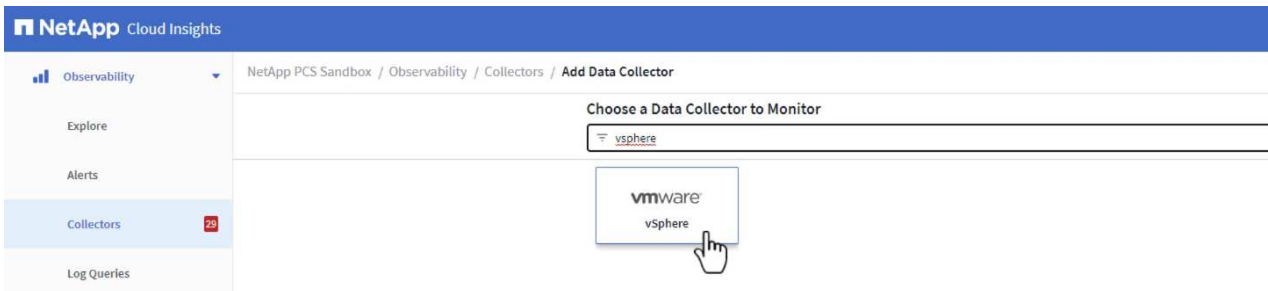


## Fügen Sie einen Data Collector für einen VMware vSphere-Cluster hinzu

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



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



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



## Configure Collector

### Add credentials and required settings [Need Help?](#)

Name <a href="#">?</a> VCSA7	Acquisition Unit bxp-au01
---------------------------------	------------------------------

Virtual Center IP Address 10.61.181.210	User Name administrator@vsphere.local
--	--

Password *****
-------------------

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

#### Advanced Configuration

#### Collecting:

- Inventory
- VM Performance

Inventory Poll Interval (min) 20	Communication Port 443
-------------------------------------	---------------------------

Filter VMs by ESX_HOST	Choose 'Exclude' or 'Include' to Specify a List Exclude
---------------------------	--

Filter Device List (Comma Separated Values For Filtering By ESX_HOST, CLUSTER, and DATACENTER Only)	Performance Poll Interval (sec) 300
---	--

Collect basic performance metrics only

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

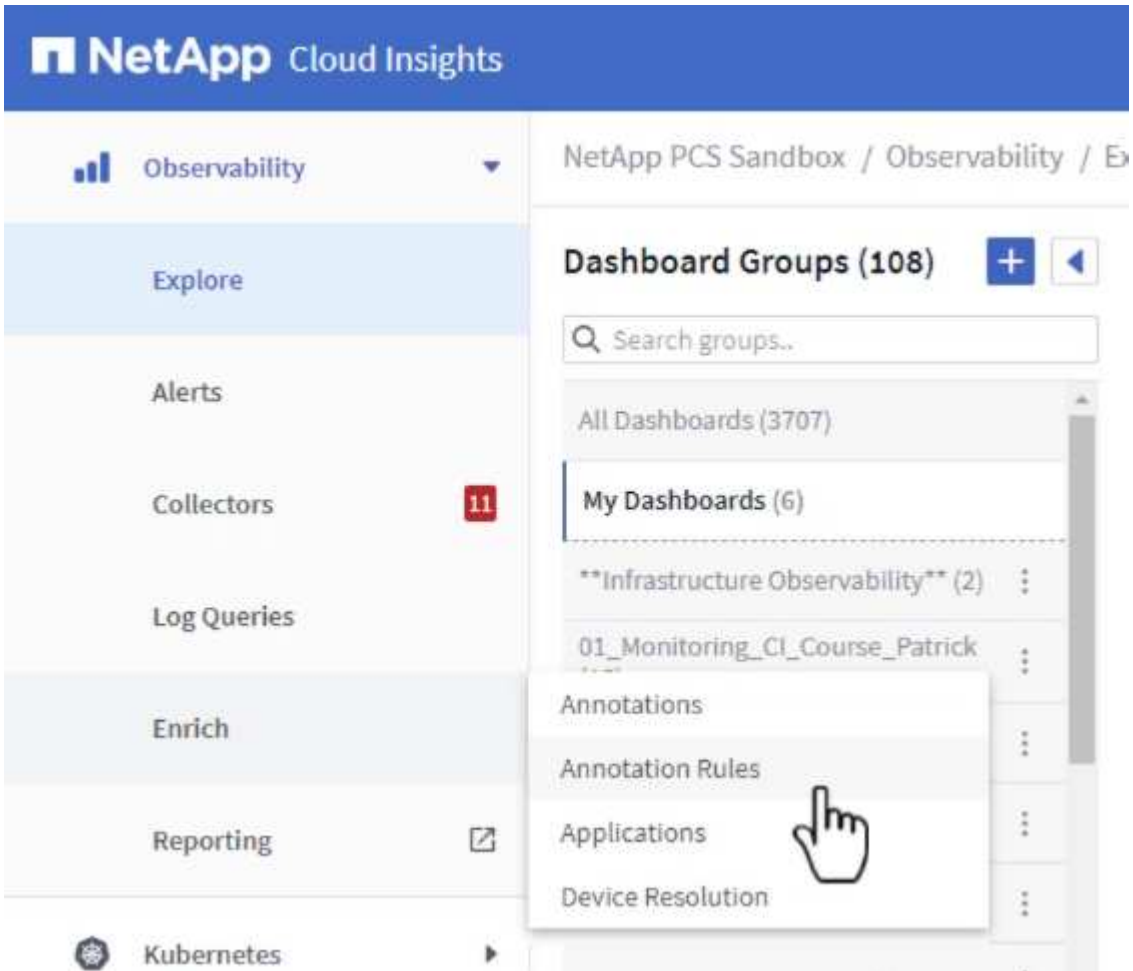
## Anmerkungen zu Assets hinzufügen

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

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

## Verwenden Sie Anmerksungsregeln, um Assets zu kennzeichnen

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



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



**Add Rule**
✕

**Name**

**Query**

**Annotation**

**Value**

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

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

Rules running... **Run All Rules**

**Annotation rules (217)** + Rule Filter...

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

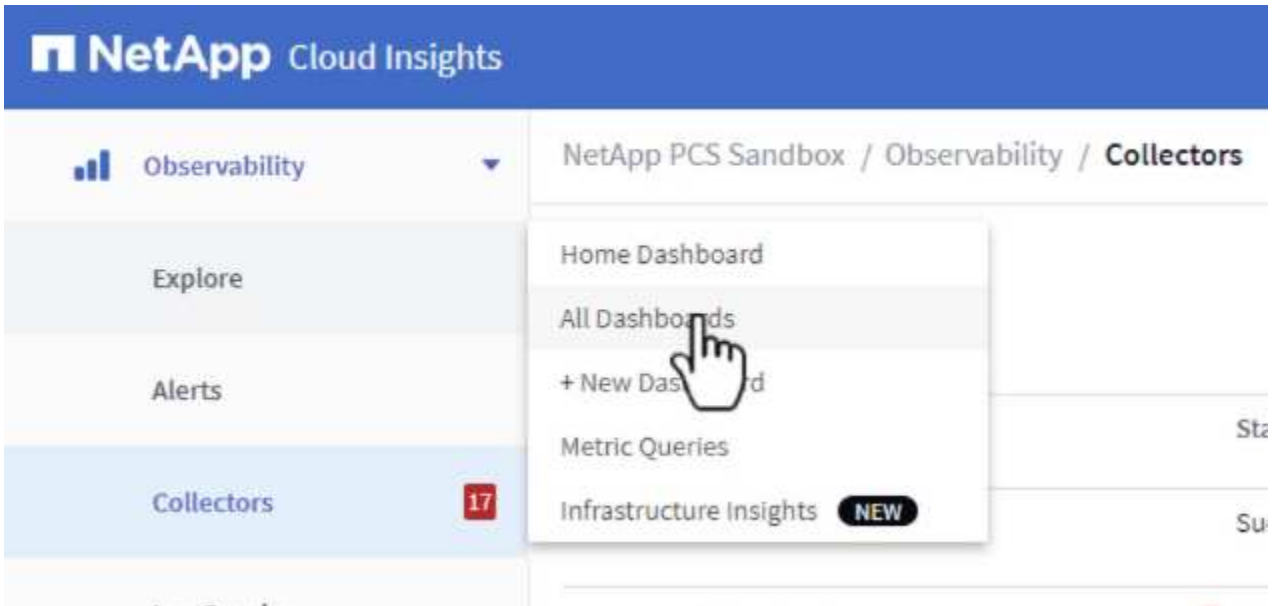
## Analysieren und Korrelieren von Ressourcen

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

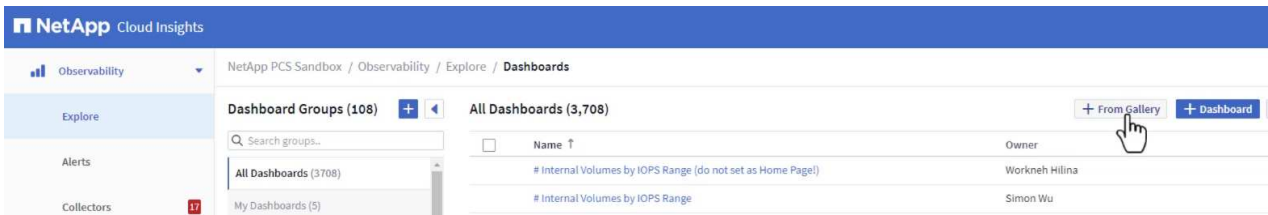
In diesen Abschnitten wird die Verwendung von Dashboards zur Korrelation von Assets erläutert.

## Korrelation von Assets aus einem Storage Performance Dashboard

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



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



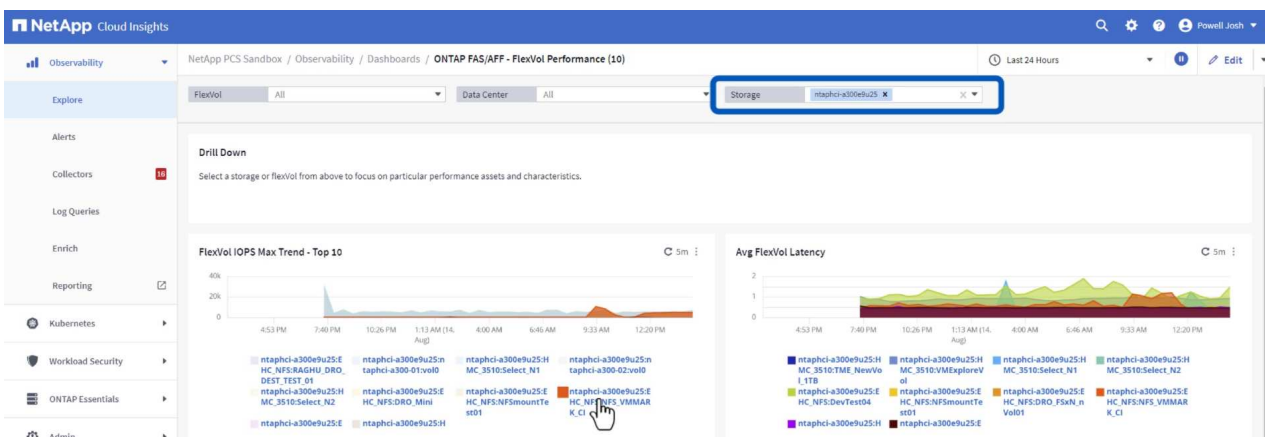
3. Wählen Sie aus der Liste ein Dashboard für die FlexVol-Performance aus und klicken Sie unten auf der Seite auf die Schaltfläche **Dashboards hinzufügen**.

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

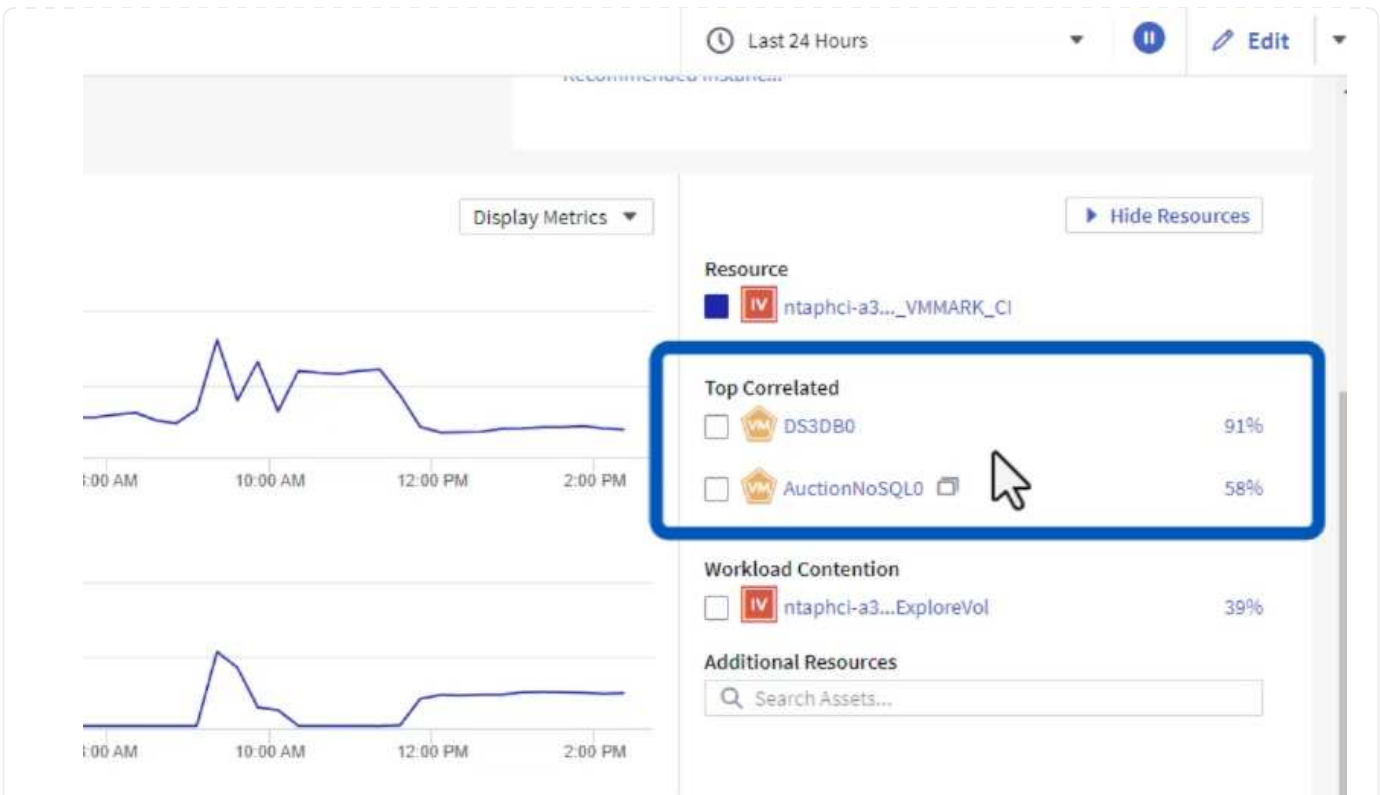
**+ Additional Dashboards (13)**  
These dashboards require additional data collectors to be installed. [Add More](#)

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

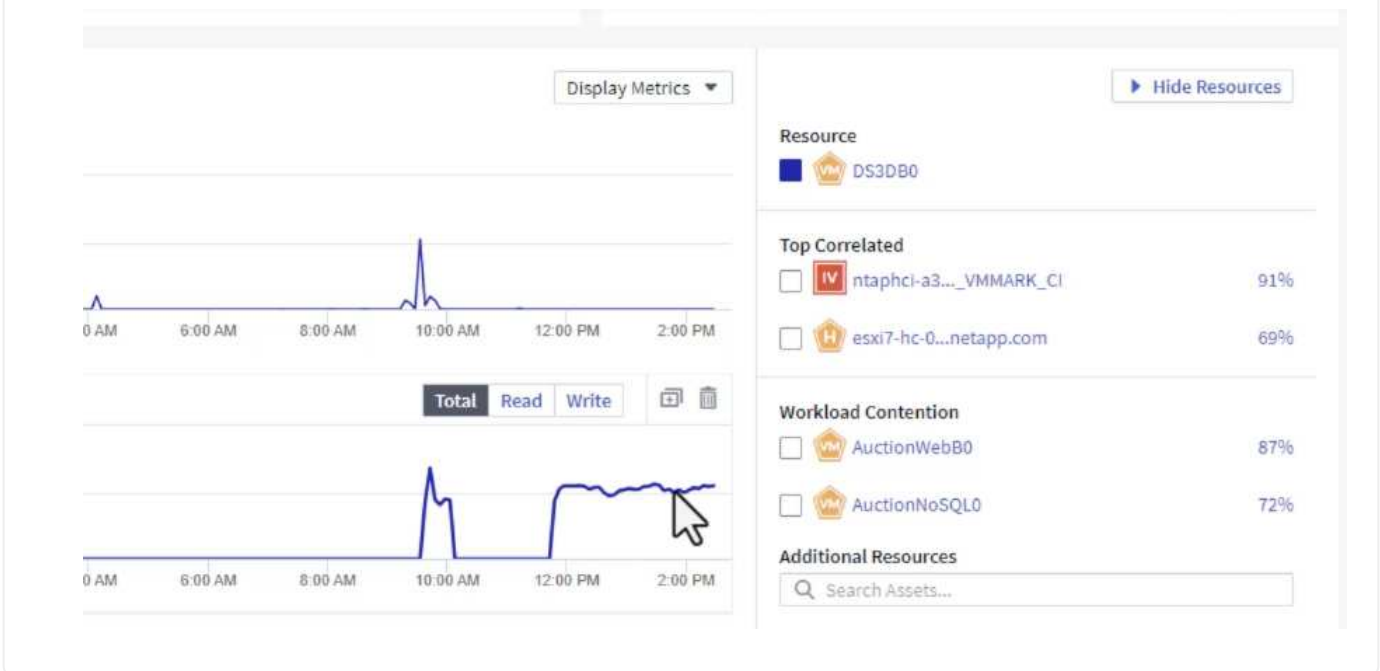
4. Öffnen Sie nach dem Import das Dashboard. Von hier aus können Sie verschiedene Widgets mit detaillierten Leistungsdaten sehen. Fügen Sie einen Filter hinzu, um ein einzelnes Storage-System anzuzeigen, und wählen Sie ein Storage-Volume aus, um detaillierte Informationen zu erhalten.



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



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



## Erkennen von „Noisy Neighbors“ mit Cloud Insights

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

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

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

NetApp PCS Sandbox / Observability / Explore / Dashboards

Dashboard Groups (108) + - Search groups..

All Dashboards (3709)

My Dashboards (6)

\*\*Infrastructure Observability\*\* (2)

01\_Monitoring\_CI\_Course\_Patrick (15)

02\_Monitoring\_CI\_Course\_Vish (5)

1\_Str Dashboards (8)

My Dashboards (6) + From Gallery + Dashboard

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

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

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

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

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

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

VM Count With Latency Concern

5m

50

VM's

Avg Latency (all VMs)

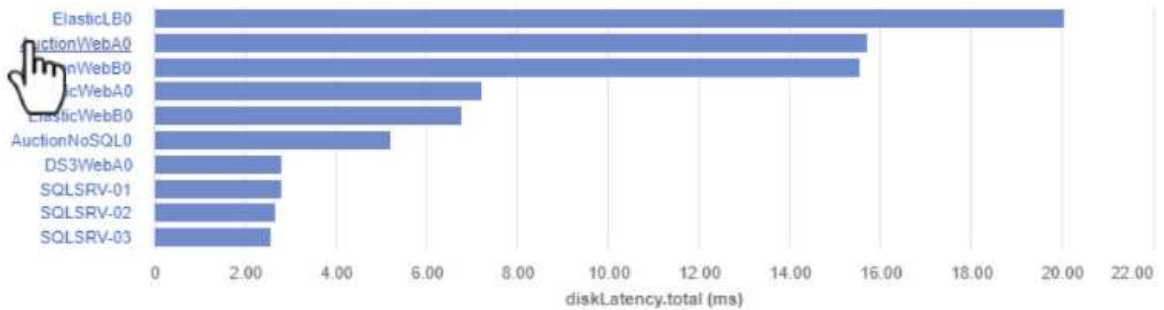
5m

1.55 ms

diskLatency.total

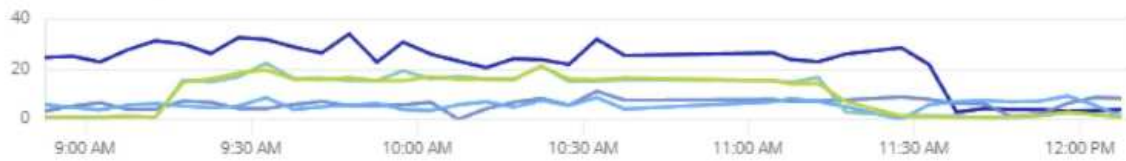
Avg VM Latency - Top 10

5m



Top 5 Avg VM Latency Trend

30s



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

Display Metrics

Hide Resources

Resource

- VM AuctionWebA0

Top Correlated

- esxi7-hc-0...netapp.com 91%
- ntaphci-a3...\_VMMARK\_CI 84%

Workload Contention

- AuctionNoSQL0 92%
- AuctionWebB0 57%

Additional Resources

Search Assets...

## **Übersicht über und zu wenig genutzte Ressourcen in Cloud Insights**

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

## Ermittlung von Möglichkeiten zur optimalen Dimensionierung von VMs

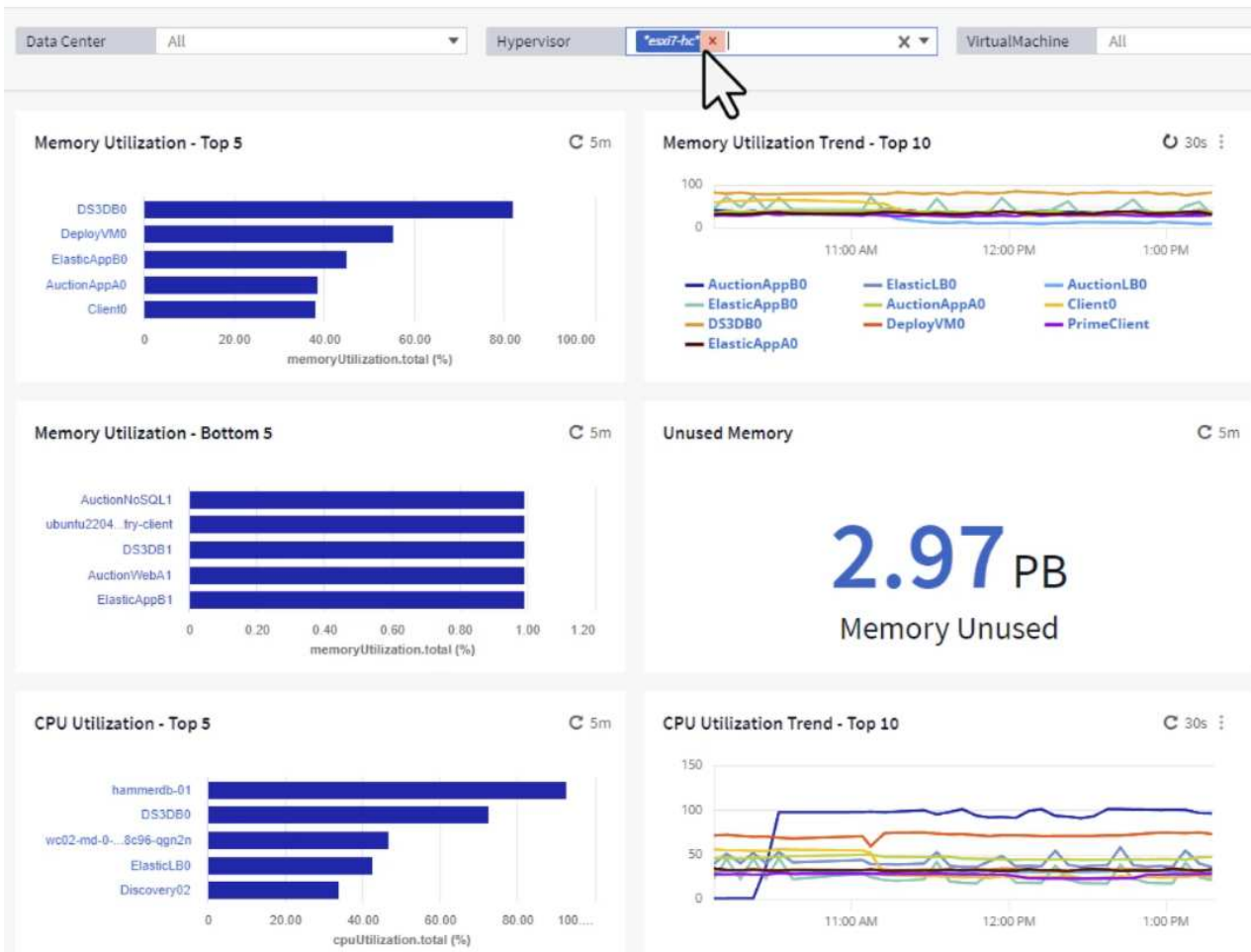
1. In diesem Beispiel greifen Sie auf ein Dashboard zu, das in der **Galerie** unter dem Namen **VMware Admin - wo gibt es Möglichkeiten, die richtige Größe zu haben?** verfügbar ist

### My Dashboards (6)

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

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





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

## Memory Usage

5m

121 items found

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

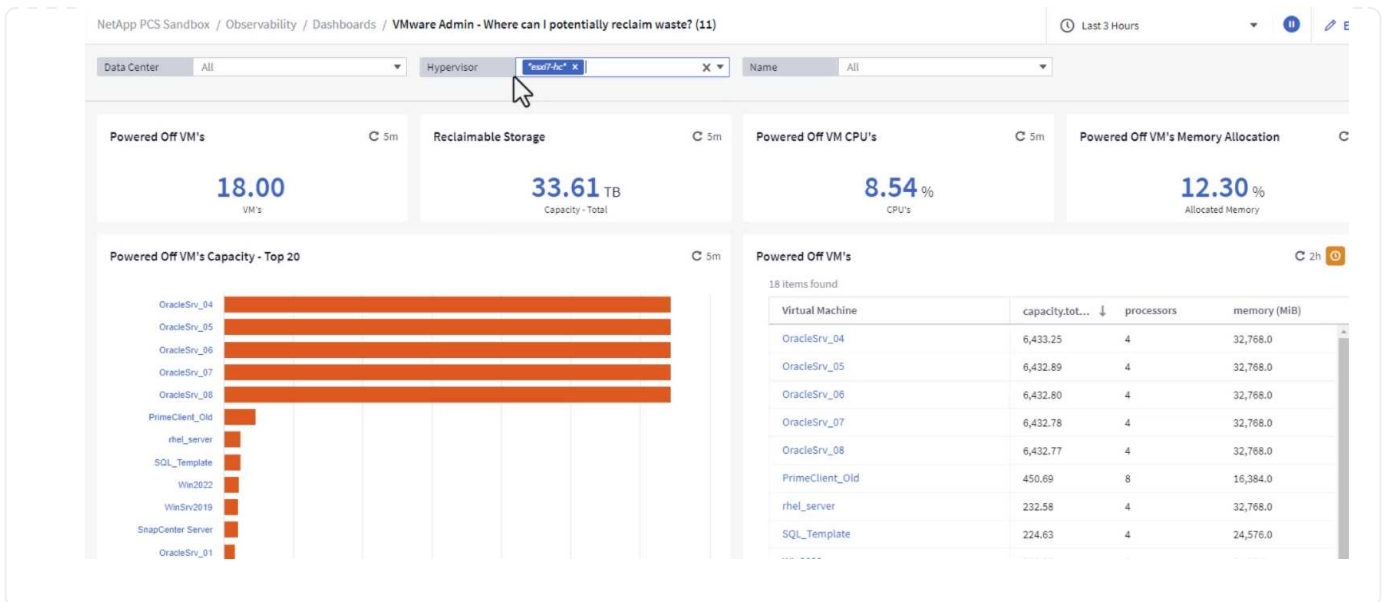
## CPU Utilization

5m

121 items found

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

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

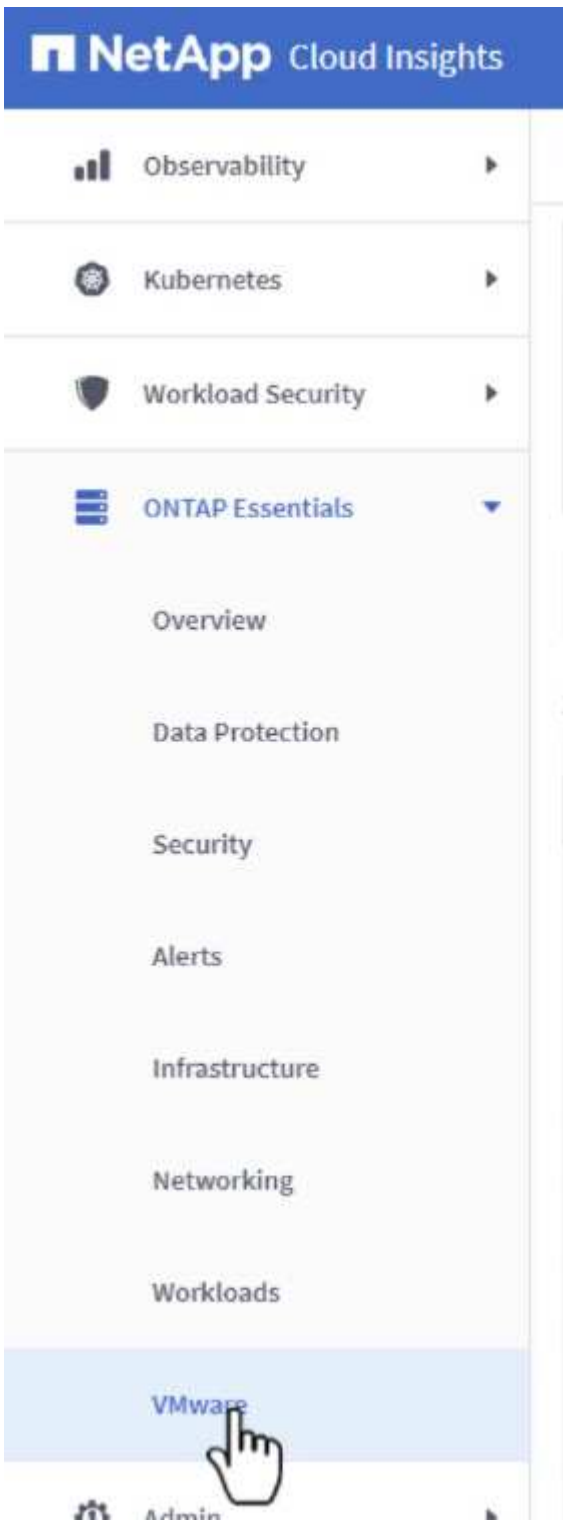


## Nutzen Sie Abfragen zum Isolieren und Sortieren von Kennzahlen

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

**Zeigen Sie eine detaillierte VMware-Abfrage unter ONTAP Essentials an**

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



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

VirtualMachine | All Virtual Machines

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

Filter by Metric: +

Group By: Virtual Machine

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

281 Items found

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

## Schlussfolgerung

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

## Weitere Informationen

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

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

# Demos und Tutorials

## Virtualisierungsvideos und -Demos

Sehen Sie sich die folgenden Videos und Demos an, in denen die spezifischen Funktionen von Hybrid Cloud-, Virtualisierungs- und Container-Lösungen vorgestellt werden.

### NetApp ONTAP Tools für VMware vSphere

[ONTAP Tools für VMware - Übersicht](#)

[Bereitstellung von VMware iSCSI-Datenspeichern mit ONTAP](#)

[Bereitstellung von VMware NFS-Datenspeichern mit ONTAP](#)

## SnapCenter Plug-in für VMware vSphere

Die NetApp SnapCenter Software ist eine unkomplizierte Enterprise-Plattform, die die Koordination und das Management der Datensicherung für alle Applikationen, Datenbanken und Filesysteme sicher gestaltet.

Das SnapCenter Plug-in für VMware vSphere ermöglicht Ihnen Backup-, Wiederherstellungs- und Anschlussvorgänge für VMs sowie Backup- und Mount-Vorgänge für Datastores, die bei SnapCenter direkt in VMware vCenter registriert sind.

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

[SnapCenter Plug-in für VMware vSphere – Voraussetzungen für eine Lösung](#)

[SnapCenter Plug-in für VMware vSphere – Implementierung](#)

[SnapCenter Plug-in für VMware vSphere – Backup-Workflow](#)

[SnapCenter Plug-in für VMware vSphere – Workflow wiederherstellen](#)

[SnapCenter - SQL Restore-Workflow](#)

## 3-2-1 Datensicherungslösungen

3-2-1-1 Datensicherungslösungen kombinieren primäre und sekundäre Backups vor Ort mithilfe von SnapMirror Technologie mit replizierten Kopien in Objekt-Storage mithilfe von BlueXP Backup und Recovery.

[3-2-1 Datensicherung für VMFS Datastores mit SnapCenter Plug-in für VMware vSphere und BlueXP Backup und Recovery für Virtual Machines](#)

## VMware Cloud auf AWS mit AWS FSX für NetApp ONTAP

[Windows Guest Connected Storage mit FSX ONTAP über iSCSI](#)

[Linux Guest Connected Storage with FSX ONTAP Using NFS](#)

[VMware Cloud auf AWS TCO-Einsparungen mit Amazon FSX für NetApp ONTAP](#)

[VMware Cloud auf AWS zusätzlicher Datastore mit Amazon FSX für NetApp ONTAP](#)

[VMware HCX Deployment and Configuration Setup für VMC](#)

[Demo für die Migration von vMotion mit VMware HCX für VMC und FSxN](#)

[Demonstration zur Cold-Migration mit VMware HCX für VMC und FSxN](#)

## **Azure VMware-Services auf Azure mit Azure NetApp Files (ANF)**

[Übersicht über die Azure VMware Lösung zusätzlichen Datastore mit Azure NetApp Files](#)

[Azure VMware Lösung für DR mit Cloud Volumes ONTAP, SnapCenter und JetStream](#)

[Demonstration zur Cold-Migration mit VMware HCX für AVS und ANF](#)

[VMotion-Demo mit VMware HCX für AVS und ANF](#)

[Massenmigration mit VMware HCX für AVS und ANF](#)

## **VMware Cloud Foundation mit NetApp ONTAP**

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

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

## NetApp mit VMware Tanzu

Mit VMware Tanzu können Kunden ihre Kubernetes-Umgebung über vSphere oder VMware Cloud Foundation implementieren, managen und managen. Mit diesem VMware Portfolio können Kunden alle relevanten Kubernetes Cluster über eine einzige Kontrollebene managen. Dazu wählen sie die für sie am besten geeignete VMware Tanzu Edition.

Weitere Informationen zu VMware Tanzu finden Sie im "[VMware Tanzu Overview](#)". Diese Überprüfung behandelt Anwendungsfälle, verfügbare Ergänzungen und mehr über VMware Tanzu.



### Verwendung von VVols mit NetApp und VMware Tanzu Basic, Teil 1



### Verwendung von VVols mit NetApp und VMware Tanzu Basic, Teil 2



### Verwendung von VVols mit NetApp und VMware Tanzu Basic, Teil 3



## NetApp Cloud Insights

NetApp Cloud Insights ist eine umfassende Monitoring- und Analyseplattform, die für Transparenz und Kontrolle der On-Premises- und Cloud-Infrastruktur konzipiert ist.

[NetApp Cloud Insights – Beobachtbarkeit für das moderne Datacenter](#)

## Copyright-Informationen

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

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

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, 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.