



Schutz von Workloads auf Azure/AVS

NetApp Solutions

NetApp
April 26, 2024

Inhalt

- Schutz von Workloads auf Azure/AVS 1
 - Disaster Recovery mit ANF und JetStream 1
 - Disaster Recovery mit CVO und AVS (Storage mit Anbindung an den Gast) 14
 - TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS) 41
 - Verwenden von Veeam Replizierung und Azure NetApp Files-Datastore für die Disaster Recovery zu Azure VMware-Lösung 56

Schutz von Workloads auf Azure/AVS

Disaster Recovery mit ANF und JetStream

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz der Workloads vor Standortausfällen und Datenbeschädigungen (z. B. Ransomware). Mithilfe des VMware VAAI Frameworks können VMware On-Premises-Workloads auf Azure Blob Storage und für die Recovery repliziert werden, was zu minimalen oder fast keinem Datenverlust und nahezu keinem RTO führt.

Jetstream DR kann verwendet werden, um die Workloads, die von On-Premises-Systemen auf AVS repliziert wurden, nahtlos wiederherzustellen. Insbesondere können sie auf Azure NetApp Files übertragen werden. Sie ermöglicht eine kostengünstige Disaster Recovery, da minimale Ressourcen am DR-Standort und kostengünstiger Cloud Storage genutzt werden. Jetstream DR automatisiert die Recovery auf ANF-Datstores über Azure Blob Storage. Jetstream DR stellt unabhängige VMs oder Gruppen zugehöriger VMs in der Infrastruktur des Recovery-Standorts entsprechend der Netzwerkzuordnung wieder her und sorgt für zeitpunktgenaue Recovery zur Sicherung von Ransomware.

Dieses Dokument vermittelt ein Verständnis der JetStream DR-Prinzipien des Betriebs und seiner Hauptkomponenten.

Übersicht über die Lösungsimplementierung

1. Installation der JetStream DR-Software im lokalen Datacenter
 - a. Laden Sie das JetStream DR-Software-Bundle aus Azure Marketplace (ZIP) herunter, und implementieren Sie das JetStream DR MSA (OVA) im dafür vorgesehenen Cluster.
 - b. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket (JetStream VIB installieren).
 - c. Bereitstellen von Azure Blob (Azure Storage-Konto) in derselben Region wie das DR-AVS-Cluster
 - d. Implementierung von DRVA-Appliances und Zuweisung von Protokoll-Volumes (VMDK aus vorhandenem Datastore oder gemeinsam genutztem iSCSI-Storage)
 - e. Erstellen Sie geschützte Domänen (Gruppen zugehöriger VMs) und weisen Sie DRVAs und Azure Blob Storage/ANF zu.
 - f. Schutz starten.
2. Installieren Sie die JetStream DR-Software in der Private Cloud der Azure VMware Lösung.
 - a. Verwenden Sie den Befehl Ausführen, um JetStream DR zu installieren und zu konfigurieren.
 - b. Fügen Sie denselben Azure Blob-Container hinzu und entdecken Sie Domänen mithilfe der Option „Scan Domains“.
 - c. Bereitstellung der erforderlichen DRVA-Appliances
 - d. Verwenden von verfügbaren vSAN oder ANF-Datastores für Replizierungsprotokolle erstellen
 - e. Importieren Sie geschützte Domänen und konfigurieren Sie RocVA (Recovery VA), um einen ANF-Datenspeicher für VM-Platzierungen zu verwenden.
 - f. Wählen Sie die entsprechende Failover-Option aus, und beginnen Sie mit der kontinuierlichen Wiederherstellung nach RTO-Domänen von nahezu null oder VMs.
3. Bei einem Notfall wird ein Failover zu Azure NetApp Files-Datastores am zugewiesenen AVS-DR-Standort ausgelöst.
4. Rufen Sie den geschützten Standort nach der Wiederherstellung des geschützten Standorts auf. Bevor Sie beginnen, stellen Sie sicher, dass die Voraussetzungen wie in diesem angegeben erfüllt sind ["Verlinken"](#) Führen Sie außerdem das von JetStream Software zur Verfügung gestellte Bandwidth Testing Tool (BWT) aus, um die potenzielle Performance des Azure Blob Storage und dessen Replikationsbandbreite in Verbindung mit der JetStream DR-Software zu bewerten. Nachdem die Voraussetzungen, einschließlich Konnektivität, vorhanden sind, richten Sie JetStream DR für AVS von der ein und abonnieren Sie sie ["Azure Marketplace"](#). Nachdem das Software Bundle heruntergeladen wurde, fahren Sie mit dem oben beschriebenen Installationsvorgang fort.

Verwenden Sie beim Planen und Starten des Schutzes für eine große Anzahl von VMs (z. B. 100+) das Capacity Planning Tool (CPT) aus dem JetStream DR Automation Toolkit. Geben Sie eine Liste der VMs an, die zusammen mit ihren RTO- und Recovery-Gruppeneinstellungen geschützt werden sollen, und führen Sie dann das CPT aus.

CPT führt die folgenden Funktionen aus:

- Die Kombination von VMs in Sicherungsdomänen entsprechend ihrer RTO-Vorgaben.
- Die optimale Anzahl von DRVAs und deren Ressourcen festlegen.
- Schätzen der erforderlichen Replikationsbandbreite
- Ermittlung der Merkmale von Replikationsprotokollvolumes (Kapazität, Bandbreite usw.)

- Schätzung der erforderlichen Objekt-Storage-Kapazität und mehr



Die Anzahl und der Inhalt der Domänen hängen von den verschiedenen VM-Merkmalen ab, wie beispielsweise durchschnittlichen IOPS, Gesamtkapazität, Priorität (die Failover-Reihenfolge definiert), RTO und anderen.

Installation der JetStream DR im lokalen Datacenter

Die Jetstream DR-Software besteht aus drei Hauptkomponenten: Jetstream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) und Host-Komponenten (I/O-Filterpakete). MSA wird verwendet, um Hostkomponenten auf dem Computing-Cluster zu installieren und zu konfigurieren und anschließend JetStream DR-Software zu verwalten. Die folgende Liste enthält eine ausführliche Beschreibung des Installationsprozesses:

Installation von JetStream DR für On-Premises

1. Voraussetzungen prüfen.
2. Führen Sie das Capacity Planning Tool für Ressourcen- und Konfigurationsempfehlungen aus (optional, jedoch für Proof-of-Concept-Tests empfohlen).
3. Implementieren Sie JetStream DR MSA auf einem vSphere-Host im zugewiesenen Cluster.
4. Starten Sie das MSA-Produkt mit dem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server mit dem MSA, um die Installation durchzuführen, führen Sie die folgenden detaillierten Schritte aus:
6. Nachdem JetStream DR MSA implementiert und der vCenter Server registriert wurde, greifen Sie über den vSphere Web Client auf das JetStream DR Plug-in zu. Dazu können Sie im Datacenter > Configure > JetStream DR navigieren.



7. Wählen Sie über die JetStream DR-Schnittstelle den entsprechenden Cluster aus.



8. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket.

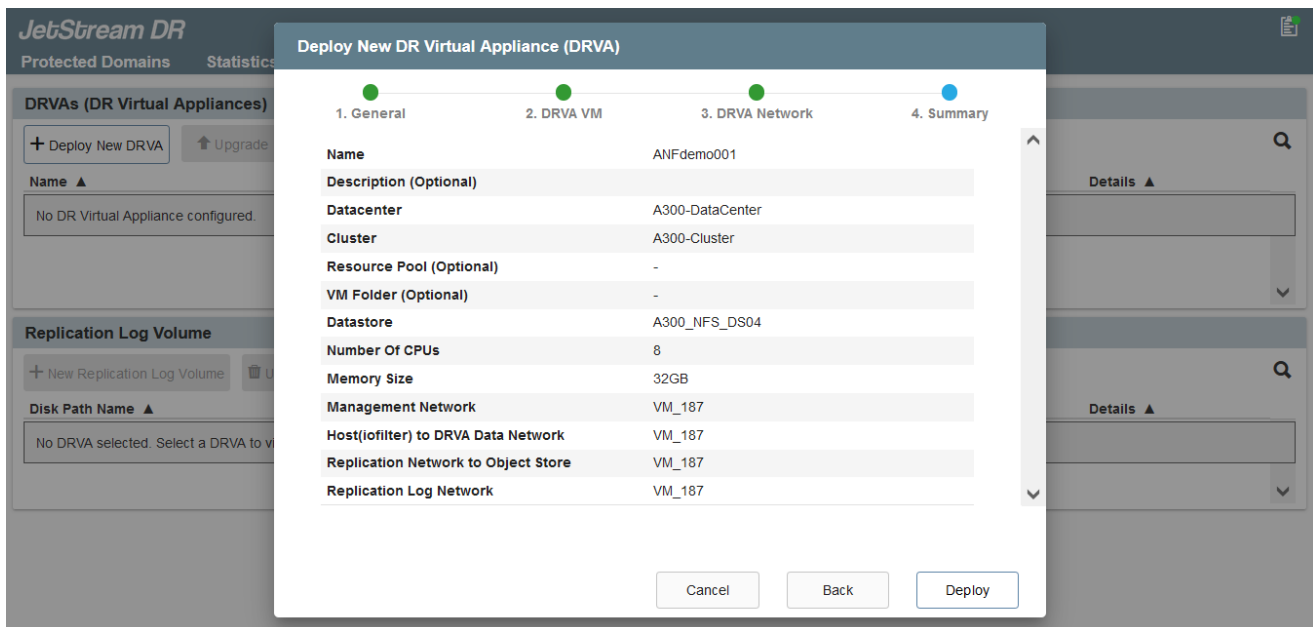


9. Fügen Sie Azure Blob Storage am Recovery-Standort hinzu.
10. Stellen Sie eine DR Virtual Appliance (DRVA) über die Registerkarte Appliances bereit.



DRVAs können automatisch durch CPT erstellt werden. Für POC-Tests wird jedoch empfohlen, den DR-Zyklus manuell zu konfigurieren und auszuführen (Schutz starten > Failover > Failback).

JetStream DRVA ist eine virtuelle Appliance, die wichtige Funktionen bei der Datenreplizierung unterstützt. Ein geschützter Cluster muss mindestens eine DRVA enthalten, und normalerweise ist pro Host ein DRVA konfiguriert. Jeder DRVA kann mehrere geschützte Domänen verwalten.



In diesem Beispiel wurden vier DRVA's für 80 virtuelle Maschinen erstellt.

1. Erstellen Sie Protokoll-Volumes für jedes DRVA unter Verwendung von VMDK aus den verfügbaren Datastores oder unabhängigen, gemeinsam genutzten iSCSI-Speicherpools.

- Erstellen Sie auf der Registerkarte geschützte Domänen die erforderliche Anzahl geschützter Domänen mithilfe von Informationen über die Azure Blob Storage-Site, die DRVA-Instanz und das Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von VMs innerhalb des Clusters, die gemeinsam geschützt werden, und weist eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zu.

- Wählen Sie VMs aus, die Sie sichern möchten, und starten Sie den VM-Schutz der geschützten Domäne. Dies beginnt mit der Datenreplizierung zum zugewiesenen Blob-Store.



Vergewissern Sie sich, dass derselbe Sicherungsmodus für alle VMs in einer geschützten Domäne verwendet wird.



Write Back(VMDK)-Modus kann eine höhere Performance bieten.

VM Name	# of Disks...	Protection Mode
1		
<input checked="" type="checkbox"/> AuctionAppA1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionAppB1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionDB1	2	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionLB1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionMSQ1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionNoSQL1	2	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionWebA1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> AuctionWebB1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> Client1	1	Write-Back(VMDK)
<input checked="" type="checkbox"/> DB1	2	Write-Back(VMDK)

Vergewissern Sie sich, dass die Protokoll-Volumes für die Replizierung auf hochperformanten Storage

platziert sind.



Failover Run Books können so konfiguriert werden, dass sie die VMs (namens Recovery Group) gruppieren, die Boot-Reihenfolge festlegen und die CPU-/Speichereinstellungen sowie die IP-Konfigurationen ändern.

Installieren Sie JetStream DR für AVS mit dem Befehl Run in einer Private Cloud der Azure VMware Lösung

Eine Best Practice für einen Recovery-Standort (AVS) ist die Erstellung eines Pilotlichtclusters mit drei Knoten im Voraus. Dadurch kann die Infrastruktur am Recovery-Standort vorkonfiguriert werden, einschließlich der folgenden Elemente:

- Netzwerkzielsegmente, Firewalls, Services wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF Volumes als Datastores und mehrJetStream DR unterstützt RTO-Modus von nahezu null für geschäftskritische Domänen. In diesen Domänen sollte der Ziel-Storage vorinstalliert sein. ANF ist in diesem Fall ein empfohlener Speichertyp.



Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster entsprechend den Anforderungen vor Ort konfiguriert werden.

Je nach SLA- und RTO-Anforderungen kann für einen kontinuierlichen Failover oder einen normalen (Standard-) Failover-Modus verwendet werden. Für eine RTO von nahezu null sollte am Recovery-Standort eine kontinuierliche Rehydrierung gestartet werden.

So installieren Sie JetStream DR für AVS in einer Private Cloud

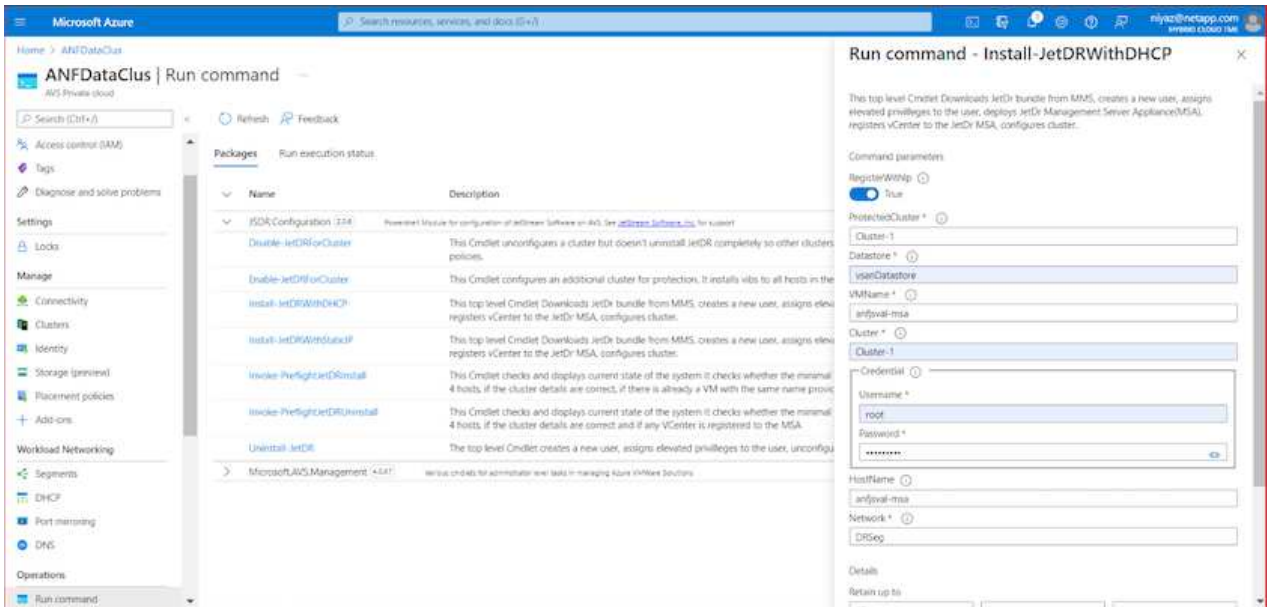
So installieren Sie JetStream DR für AVS auf einer privaten Cloud der Azure VMware-Lösung:

1. Wählen Sie im Azure-Portal die Azure VMware-Lösung aus, wählen Sie die Private Cloud aus und wählen Sie Ausführen Command > Packages > JSDR.Configuration.



Der CloudAdmin-Standardbenutzer in Azure VMware verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Lösung ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Befehls Azure VMware Solution Run für JetStream DR.

Der folgende Screenshot zeigt die Installation mithilfe einer DHCP-basierten IP-Adresse.



2. Nachdem die JetStream DR für AVS-Installation abgeschlossen ist, aktualisieren Sie den Browser. Um auf die JetStream DR-UI zuzugreifen, wechseln Sie zum SDDC Datacenter > Configure > JetStream DR.

JetStream DR

Protected Domains Statistics Storage Sites Appliances **Configurations** Task Log

Site Details [Alarm Settings](#)

vCenter Server Hostname 172.30.156.2

Management Appliance Hostname anfsval-msa

Software Version 4.0.2.450

Subscription ID - [Configure](#)

Tenant ID / Application ID - [Configure](#)

Application Secret - [Configure](#)

<input type="checkbox"/>	Cluster Name ▲	Datacenter Name ▲	Status ▲	Software Version ▲	Host Details ▲
<input type="checkbox"/>	Cluster-1	SDDC-Datacenter	Ok	4.0.2.132	Details

- Fügen Sie über die JetStream DR-Schnittstelle das Azure Blob Storage-Konto hinzu, das zum Schutz des lokalen Clusters als Storage-Standort verwendet wurde, und führen Sie die Option Scan Domains aus.

JetStream DR

Protected Domains

Available Protected Domain(s) For Import

Protected Domain ...	Description	Recoverable V...	VMs ...	Import
ANFPD000	Protected Domain Tile0	20	20	Import
ANFPD001	-	20	20	Import
ANFPD002	Protected Domain 02	20	20	Import
ANFPD003	Protected Domain Tile 03	20	20	Import

[Close](#)

- Nachdem die geschützten Domains importiert wurden, sollten DRVA-Appliances bereitgestellt werden. In diesem Beispiel wird mithilfe der JetStream DR-Benutzeroberfläche eine kontinuierliche Rehydrierung manuell vom Wiederherstellungsstandort gestartet.



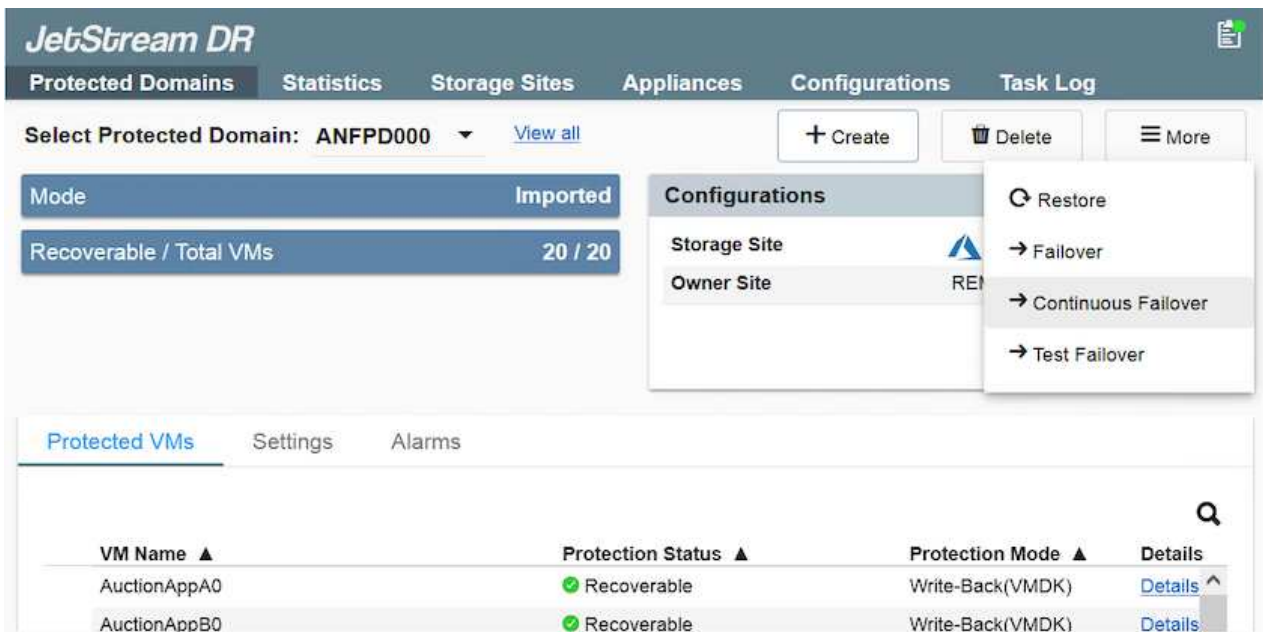
Diese Schritte können auch mithilfe von CPT erstellten Plänen automatisiert werden.

- Verwenden von verfügbaren vSAN oder ANF-Datstores für Replizierungsprotokolle erstellen
- Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery VA, um den ANF-Datenspeicher für VM-Platzierungen zu verwenden.



Stellen Sie sicher, dass DHCP für das ausgewählte Segment aktiviert ist und genügend IP-Adressen verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen sich wiederherstellen. Jede wiederherzustellende VM (einschließlich kontinuierlicher Rehydrierung) erfordert eine individuelle dynamische IP-Adresse. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

- Wählen Sie die entsprechende Failover-Option (Continuous Failover oder Failover) aus. In diesem Beispiel wird die kontinuierliche Rehydrierung (kontinuierliches Failover) ausgewählt.



Failover/Failback Wird Durchgeführt

So führen Sie ein Failover/Failback aus

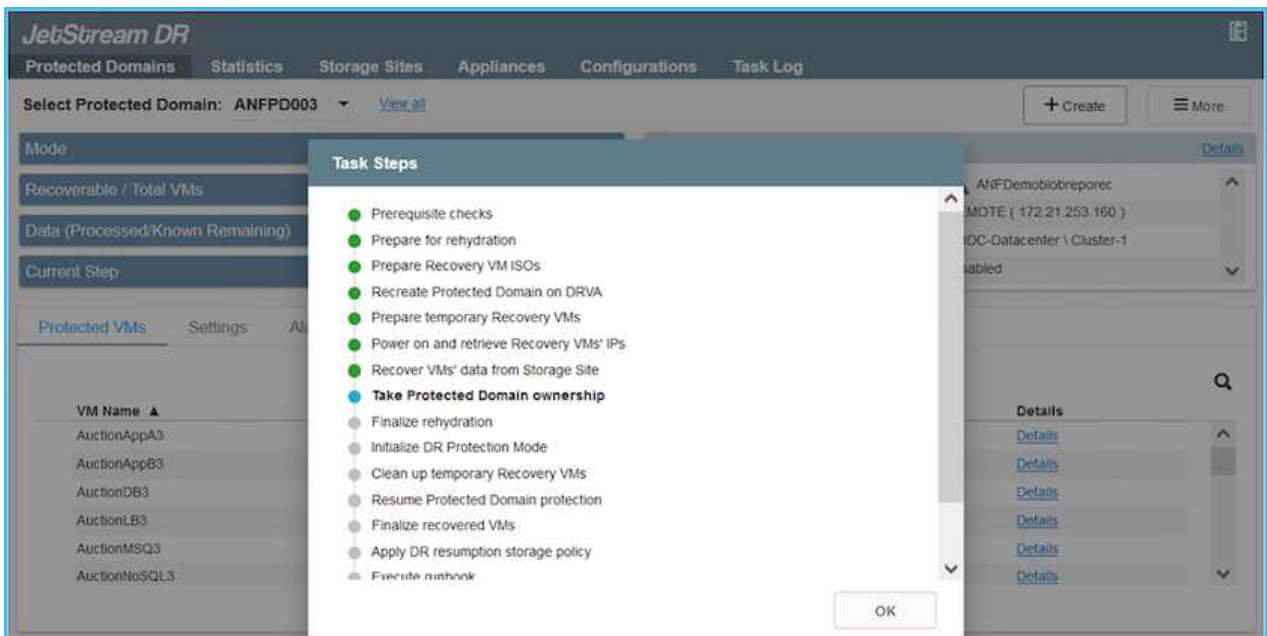
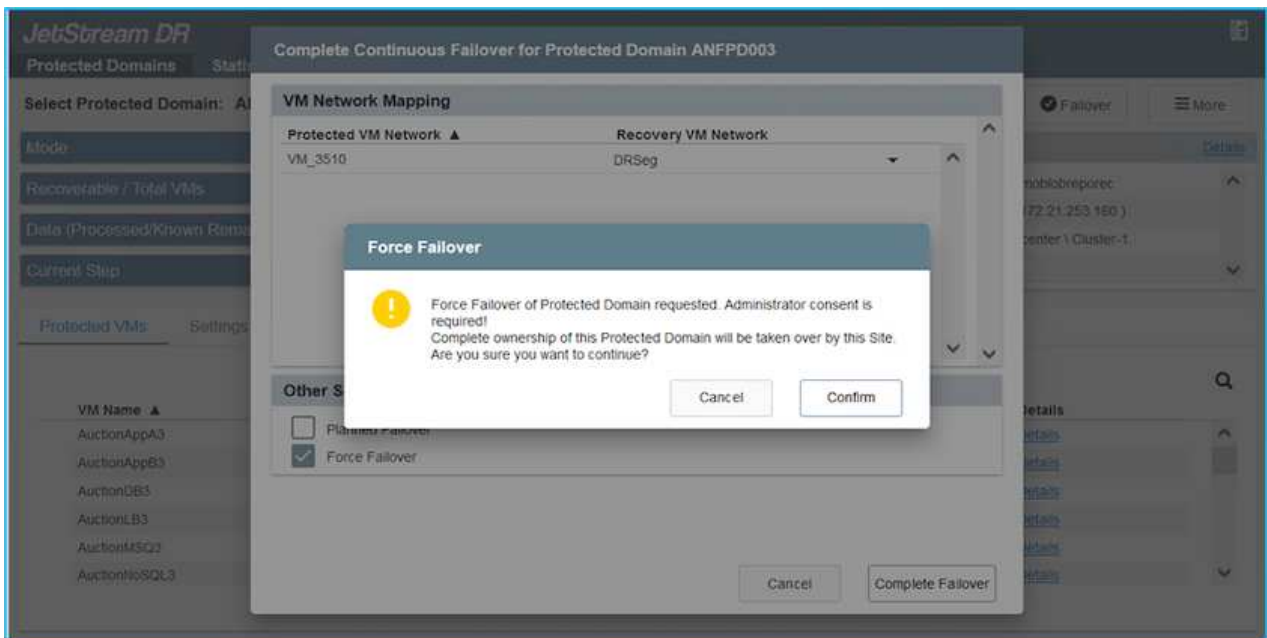
1. Nachdem im geschützten Cluster der lokalen Umgebung ein Ausfall auftritt (ein teilweiser oder vollständiger Ausfall), lösen Sie den Failover aus.



CPT kann verwendet werden, um den Failover-Plan zur Wiederherstellung der VMs von Azure Blob Storage auf dem AVS Cluster Recovery-Standort auszuführen.

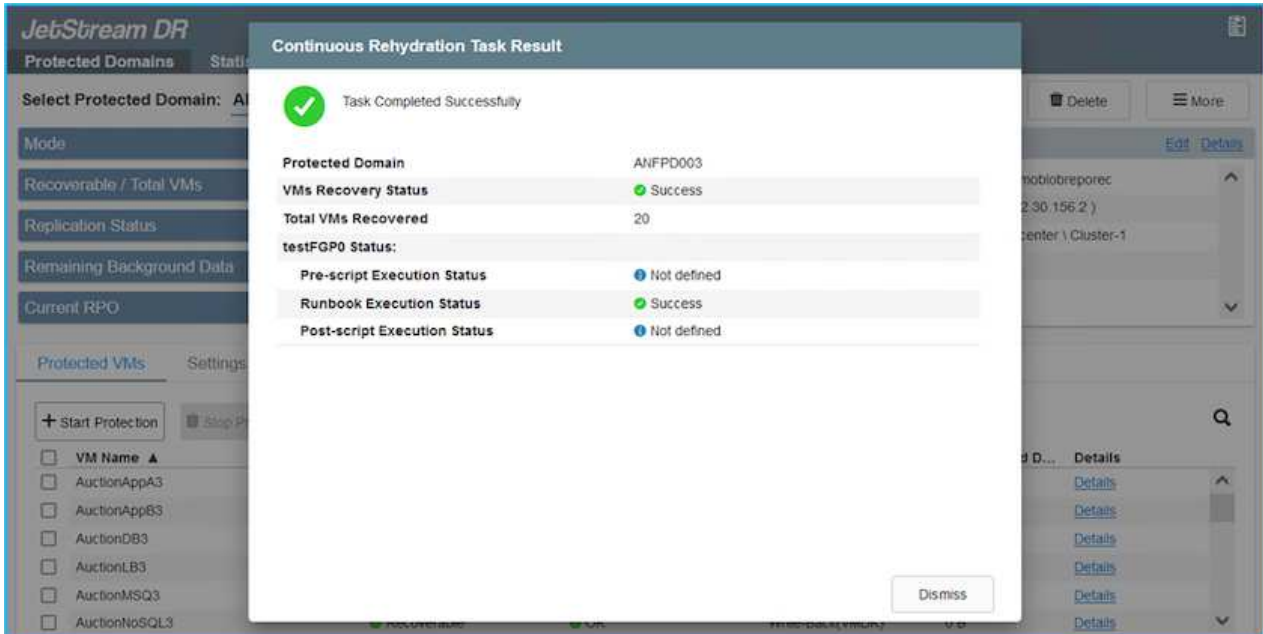


Nach dem Failover (zur kontinuierlichen oder standardmäßigen Wiederherstellung), wenn die geschützten VMs in AVS gestartet wurden, wird der Schutz automatisch fortgesetzt und JetStream DR repliziert ihre Daten weiterhin in den entsprechenden/Original-Containern im Azure Blob Storage.



In der Taskleiste wird der Status von Failover-Aktivitäten angezeigt.

2. Nach Abschluss der Aufgabe greifen Sie auf die wiederhergestellten VMs zu, und der Geschäftsbetrieb läuft normal weiter.



Wenn der primäre Standort wieder in Betrieb ist, kann ein Failback durchgeführt werden. Der VM-Schutz wird wieder aufgenommen und die Datenkonsistenz sollte überprüft werden.

3. Wiederherstellung der lokalen Umgebung Je nach Art des Notfalleinfalls sind möglicherweise die Wiederherstellung und/oder Überprüfung der Konfiguration des geschützten Clusters erforderlich. Falls erforderlich, muss die JetStream DR-Software möglicherweise erneut installiert werden.



Hinweis: Der `recovery_utility_prepare_failback` Das im Automation Toolkit zur Verfügung gestellte Skript kann verwendet werden, um die ursprüngliche geschützte Site von veralteten VMs, Domäneninformationen usw. zu reinigen.

4. Greifen Sie auf die wiederhergestellte On-Premises-Umgebung zu, rufen Sie die Jetstream DR UI auf und wählen Sie die entsprechende geschützte Domäne aus. Nachdem der geschützte Standort für Failback bereit ist, wählen Sie die Failback-Option in der UI aus.

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: **ANFPD003** [View all](#)

Mode Running in Failover

Active Site 172.30.156.2

Recoverable / Total VMs 20 / 20

Configurations

- Storage Site
- Owner Site

Protected VMs | Settings | Alarms

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
AuctionAppA3	Recoverable	Write-Back(VMDK)	Details
AuctionAppB3	Recoverable	Write-Back(VMDK)	Details
AuctionDB3	Recoverable	Write-Back(VMDK)	Details
AuctionLB3	Recoverable	Write-Back(VMDK)	Details
AuctionMSQ3	Recoverable	Write-Back(VMDK)	Details
AuctionNoSQL3	Recoverable	Write-Back(VMDK)	Details



Mit dem durch CPT generierten Failback-Plan kann außerdem die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher in die ursprüngliche VMware Umgebung initiiert werden.



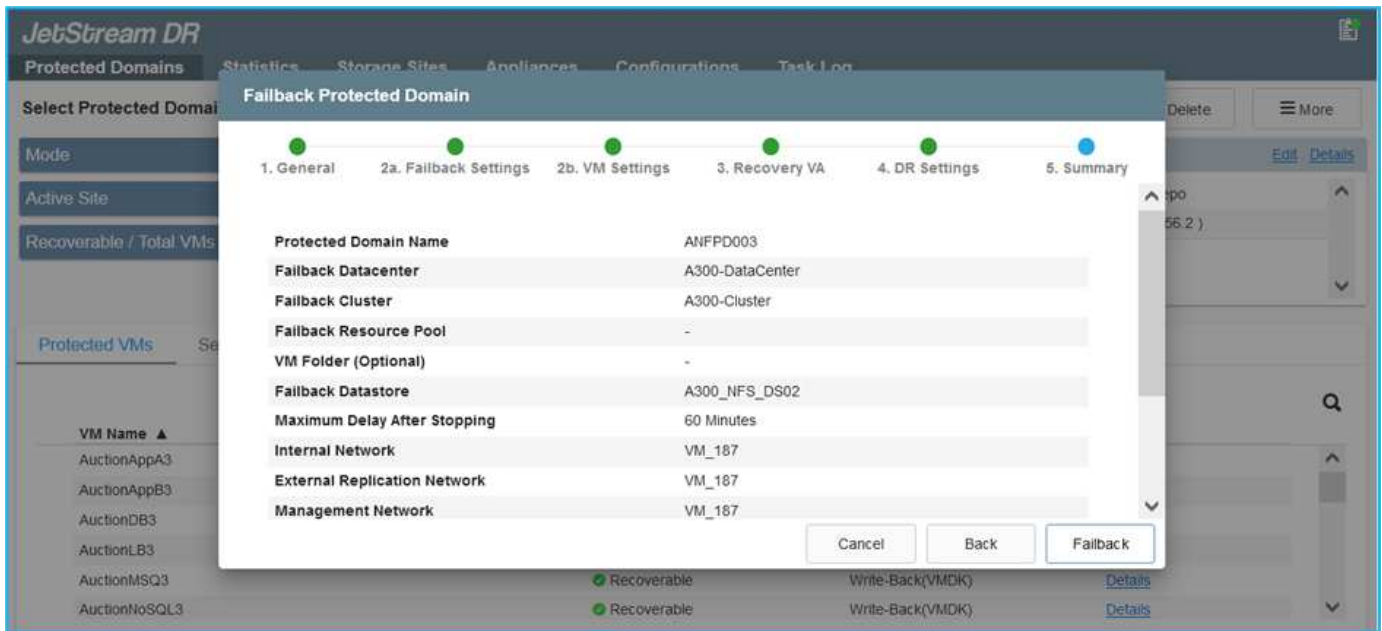
Geben Sie die maximale Verzögerung an, nachdem Sie die VMs am Recovery-Standort angehalten und am geschützten Standort neu gestartet haben. Diese Zeit umfasst das Abschließen der Replizierung nach dem Stoppen von Failover-VMs, die Zeit für die Bereinigung des Recovery-Standorts und die Zeit zur Wiederherstellung von VMs am geschützten Standort. Der von NetApp empfohlene Wert beträgt 10 Minuten.

Schließen Sie den Failback-Prozess ab, und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

Wiederherstellung Von Lösegeld-Waren

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Abteilungen schwierig sein, den sicheren Rückgabepunkt zu ermitteln und einmal festgestellt zu haben, wie sichergestellt werden kann, dass wiederhergestellte Workloads vor den erneuten Angriffen (vom Schlafen von Malware oder durch anfällige Anwendungen) geschützt sind.

Jetstream DR für AVS kann zusammen mit Azure NetApp Files Datastores diese Bedenken lösen, da Unternehmen eine Recovery von verfügbaren Zeitpunkten durchführen können, sodass Workloads bei Bedarf in einem funktionsfähigen, isolierten Netzwerk wiederhergestellt werden können. Durch Recovery können Applikationen funktionieren und miteinander kommunizieren, ohne dass sie dem Nord- Süd-Datenverkehr ausgesetzt werden. So erhalten Sicherheitsteams einen sicheren Ort, um forensische und andere notwendige Korrekturmaßnahmen durchzuführen.



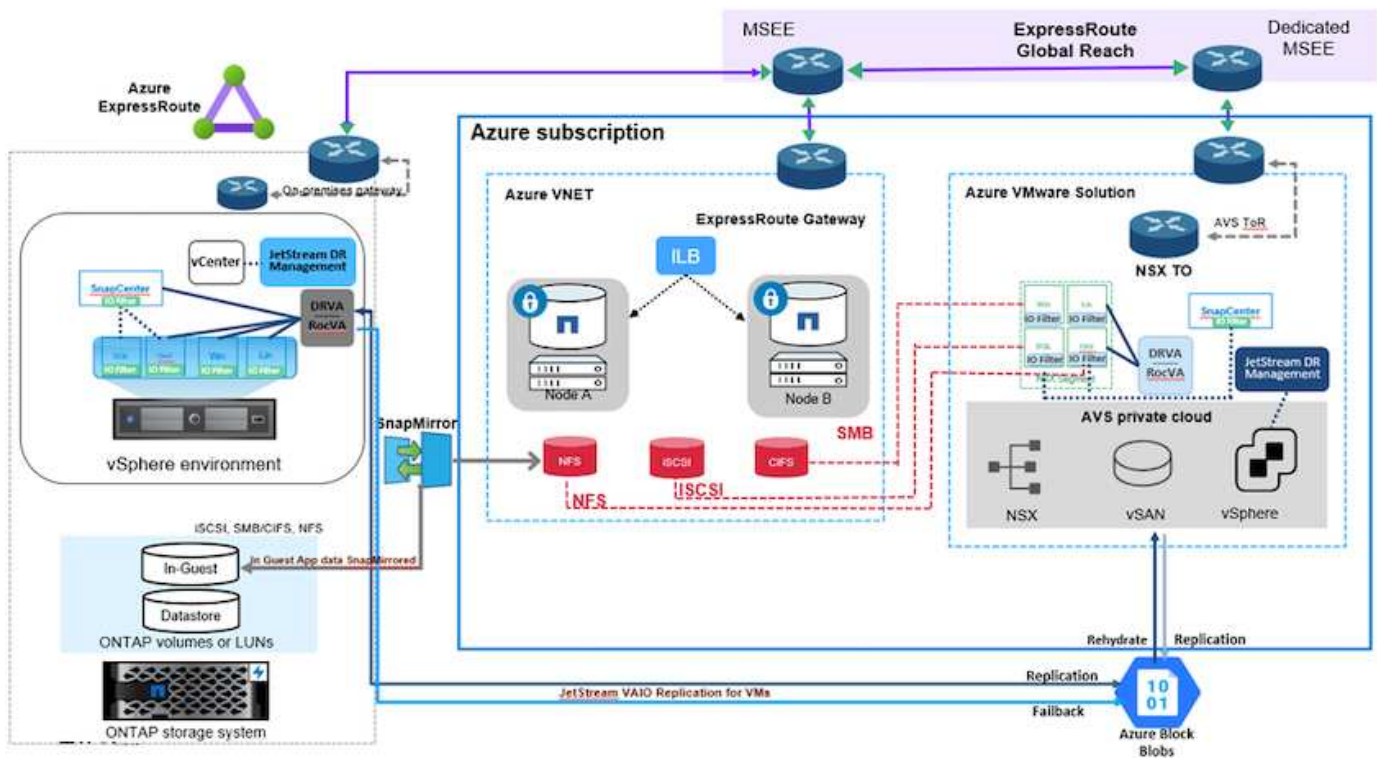
Disaster Recovery mit CVO und AVS (Storage mit Anbindung an den Gast)

Überblick

Autoren: Ravi BCB und Niyaz Mohamed, NetApp

Disaster Recovery in die Cloud ist eine stabile und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware. Mit NetApp SnapMirror können lokale VMware Workloads, die einen mit dem Gast verbundenen Storage verwenden, auf NetApp Cloud Volumes ONTAP in Azure repliziert werden. Dies bezieht sich auf Applikationsdaten, doch was ist mit den eigentlichen VMs selbst. Disaster Recovery sollte alle abhängigen Komponenten, einschließlich Virtual Machines, VMDKs, Applikationsdaten und mehr, abdecken. Zu diesem Zweck kann SnapMirror zusammen mit Jetstream verwendet werden, um Workloads, die von On-Premises zu Cloud Volumes ONTAP repliziert wurden, nahtlos wiederherzustellen und gleichzeitig vSAN Storage für VM-VMDKs zu verwenden.

Dieses Dokument bietet einen Schritt-für-Schritt-Ansatz zur Einrichtung und Durchführung von Disaster Recovery mit NetApp SnapMirror, JetStream und der Azure VMware Lösung (AVS).



Voraussetzungen

Dieses Dokument konzentriert sich auf den Gast-Storage für Applikationsdaten (auch als Gastsystem bekannt) und wir gehen davon aus, dass die On-Premises-Umgebung SnapCenter für applikationskonsistente Backups verwendet.



Dieses Dokument bezieht sich auf jede Backup- oder Recovery-Lösung eines Drittanbieters. Je nach der in der Umgebung verwendeten Lösung befolgen Sie Best Practices, um Backup-Richtlinien zu erstellen, die die SLAs des Unternehmens erfüllen.

Für die Konnektivität zwischen der On-Premises-Umgebung und dem virtuellen Azure-Netzwerk nutzen Sie die globale Express Route oder ein virtuelles WAN mit einem VPN-Gateway. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.



Es gibt mehrere Optionen, um On-Premises-Datacenter mit Azure zu verbinden, sodass wir nicht einen bestimmten Workflow in diesem Dokument beschreiben können. Die entsprechende On-Premises-zu-Azure-Konnektivitätsmethode finden Sie in der Azure-Dokumentation.

Implementieren der DR-Lösung

Übersicht Zur Lösungsimplementierung

1. Stellen Sie sicher, dass die Applikationsdaten mit SnapCenter zusammen mit den erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie mithilfe von Cloud Manager Cloud Volumes ONTAP mit der richtigen Instanzgröße innerhalb des entsprechenden Abonnements und des virtuellen Netzwerks bereit.
 - a. Konfiguration von SnapMirror für die entsprechenden Applikations-Volumes

- b. Aktualisieren Sie die Backup-Richtlinien in SnapCenter, um SnapMirror Updates nach den geplanten Aufgaben auszulösen.
3. Installieren Sie die JetStream DR-Software im lokalen Datacenter, und beginnen Sie mit dem Schutz für Virtual Machines.
4. Installieren Sie die JetStream DR-Software in der Private Cloud der Azure VMware Lösung.
5. Bei einem Notfall können Sie die SnapMirror Beziehung mithilfe von Cloud Manager unterbrechen und das Failover von Virtual Machines zu Azure NetApp Files oder zu vSAN Datastores im vorgesehenen AVS-DR-Standort auslösen.
 - a. Schließen Sie die ISCSI-LUNs und NFS-Mounts für die Applikations-VMs wieder an.
6. Rufen Sie Failback auf den geschützten Standort auf, indem Sie SnapMirror nach der Wiederherstellung des primären Standorts erneut resynchronisieren.

Einzelheiten Zur Bereitstellung

Konfiguration von CVO auf Azure und Replizierung von Volumes zu CVO

Als ersten Schritt müssen Sie Cloud Volumes ONTAP auf Azure konfigurieren ("[Verlinken](#)") Und replizieren Sie die gewünschten Volumes zu Cloud Volumes ONTAP mit den gewünschten Frequenzen und Snapshot-Aufbewahrung.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	17 seconds	idle	snapmirrored	May 6, 2022, 11:43:18 AM 105.06 KiB	...
	gcsdrsqldid_sc46_copy ANFCVODRDemo	gcsdrsqldid_sc46 ntaphci-a300e9u25	7 seconds	idle	snapmirrored	May 6, 2022, 11:42:20 AM 7.22 MiB	...
	gcsdrsqllg_sc46 ntaphci-a300e9u25	gcsdrsqllg_sc46_copy ANFCVODRDemo	16 seconds	idle	snapmirrored	May 6, 2022, 11:43:52 AM 130.69 KiB	...

Konfigurieren Sie AVS-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Implementierung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der Azure VMware Lösung und die Dauer des SDDC im Service. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann mit nur drei Hosts eingerichtet sein und bis hin zu einem Cluster mit mehreren Hosts in einer umfassenden Implementierung.

Die Entscheidung für die Implementierung eines AVS-Clusters hängt in erster Linie von den RPO/RTO-Anforderungen ab. Mit der Azure VMware Lösung kann das SDDC bereits rechtzeitig zur Verfügung gestellt werden, um entweder für das Testen oder für ein tatsächliches Notfallereignis zu sorgen. Ein durch die Just-in-time-Implementierung implementierter SDDC spart ESXi Hostkosten, wenn Sie keine Katastrophe mehr haben. Diese Form der Implementierung wirkt sich jedoch auf das RTO um einige Stunden aus, während das SDDC bereitgestellt wird.

Am häufigsten implementiert wird die SDDC-Option in einem Pilot-Light-Modus, der immer aktiviert ist. Diese Option bietet einen kleinen Platzbedarf von drei Hosts, die immer verfügbar sind. Außerdem werden Recovery-Vorgänge durch eine Basis für Simulationsaktivitäten und Compliance-Prüfungen beschleunigt, sodass das Risiko einer operativen Abweichungen zwischen dem Produktions- und dem DR-Standort vermieden wird. Der Pilot-Light-Cluster kann bei Bedarf schnell auf das gewünschte Niveau skaliert werden, um tatsächliche DR-Ereignisse zu bewältigen.

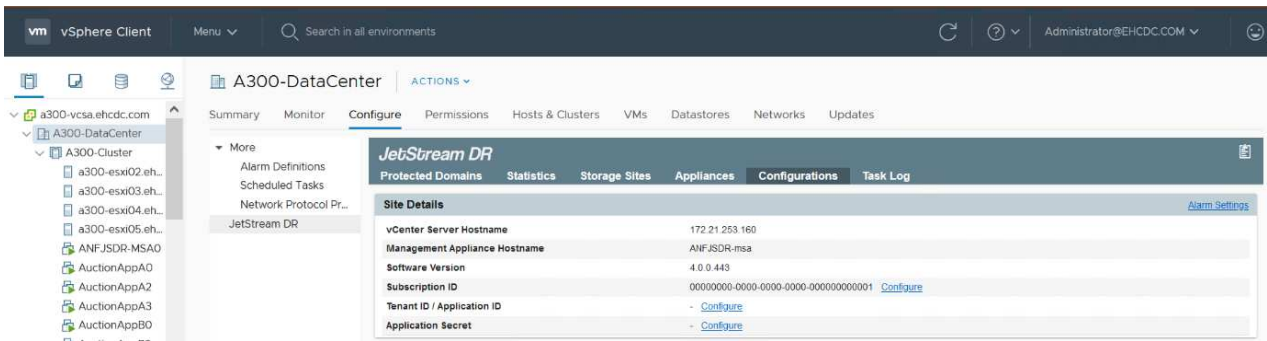
Informationen zur Konfiguration des AVS SDDC (ob On-Demand oder im Pilot-Light-Modus) finden Sie unter ["Implementieren und Konfigurieren der Virtualisierungs Umgebung auf Azure"](#). Überprüfen Sie als Voraussetzung, ob die Gast-VMs auf den AVS-Hosts nach dem Einrichten der Konnektivität Daten von Cloud Volumes ONTAP nutzen können.

Nach der ordnungsgemäßen Konfiguration von Cloud Volumes ONTAP und AVS beginnen Sie mit der Konfiguration des Jetstream zur Automatisierung der Wiederherstellung lokaler Workloads auf AVS (VMs mit Applikations-VMDKs und VMs mit in-Guest-Storage) mithilfe des VAIO Mechanismus und durch Nutzung von SnapMirror für Applikations-Volumes-Kopien auf Cloud Volumes ONTAP.

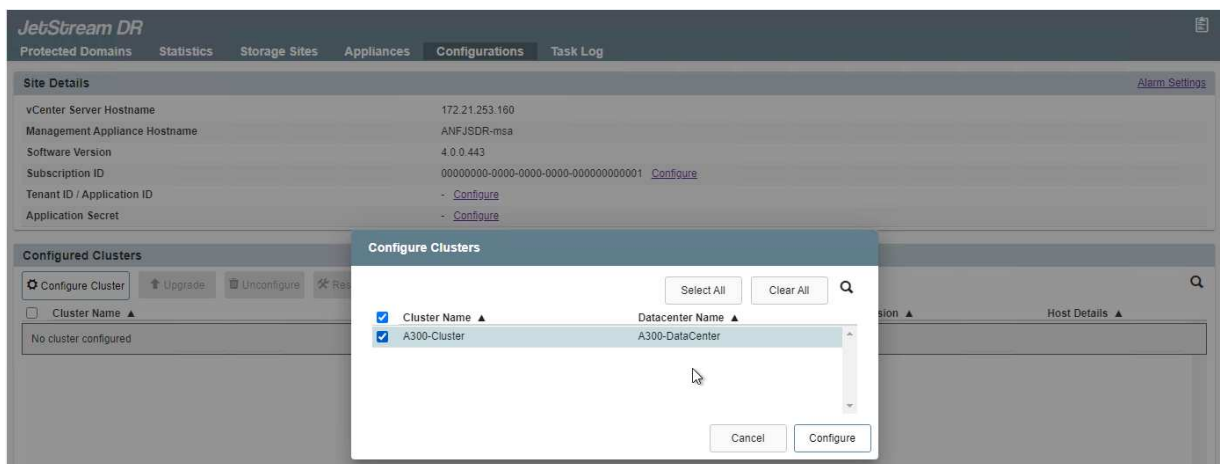
Installieren Sie JetStream DR im lokalen Datacenter

Die Jetstream DR-Software besteht aus drei Hauptkomponenten: Der JetStream DR Management Server Virtual Appliance (MSA), der DR Virtual Appliance (DRVA) und den Host-Komponenten (I/O-Filterpakete). Mit dem MSA-System werden Hostkomponenten auf dem Compute-Cluster installiert und konfiguriert und JetStream DR-Software verwaltet. Die Installation erfolgt wie folgt:

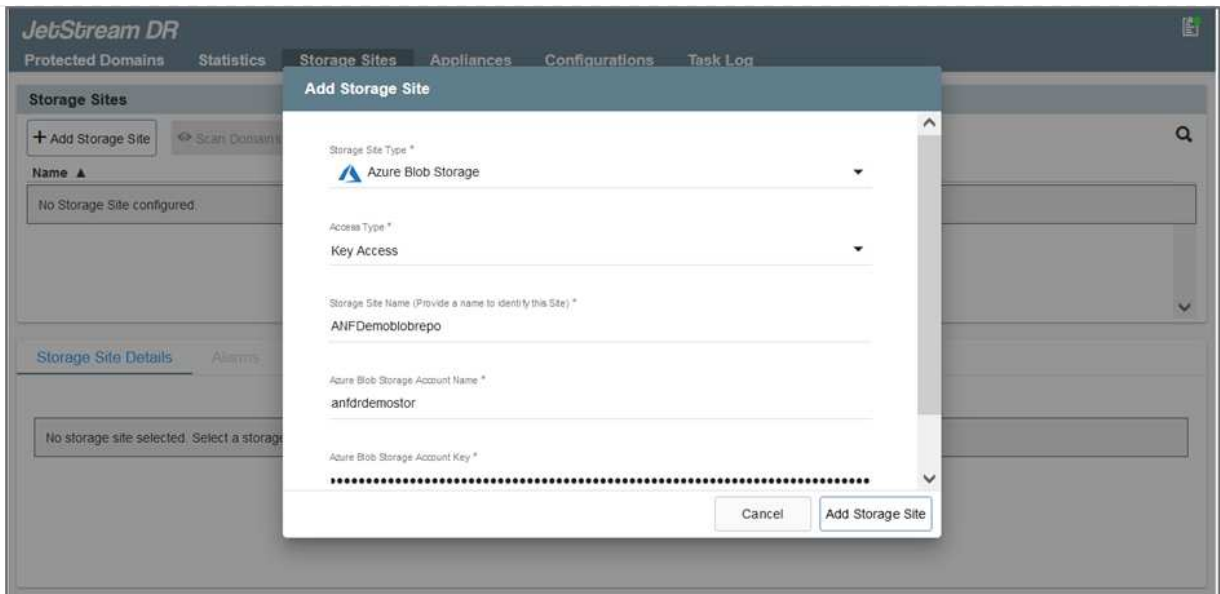
1. Voraussetzungen prüfen.
2. Nutzen Sie das Kapazitätsplanungs-Tool für Ressourcen- und Konfigurationsempfehlungen.
3. Implementieren Sie JetStream DR MSA auf jedem vSphere-Host im zugewiesenen Cluster.
4. Starten Sie das MSA-Produkt mit dem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server mit dem MSA.
6. Nachdem JetStream DR MSA implementiert und der vCenter Server registriert wurde, navigieren Sie zum JetStream DR Plug-in mit dem vSphere Web Client. Dazu können Sie im Datacenter > Configure > JetStream DR navigieren.



7. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
 - a. Konfigurieren Sie das Cluster mit dem I/O-Filterpaket.



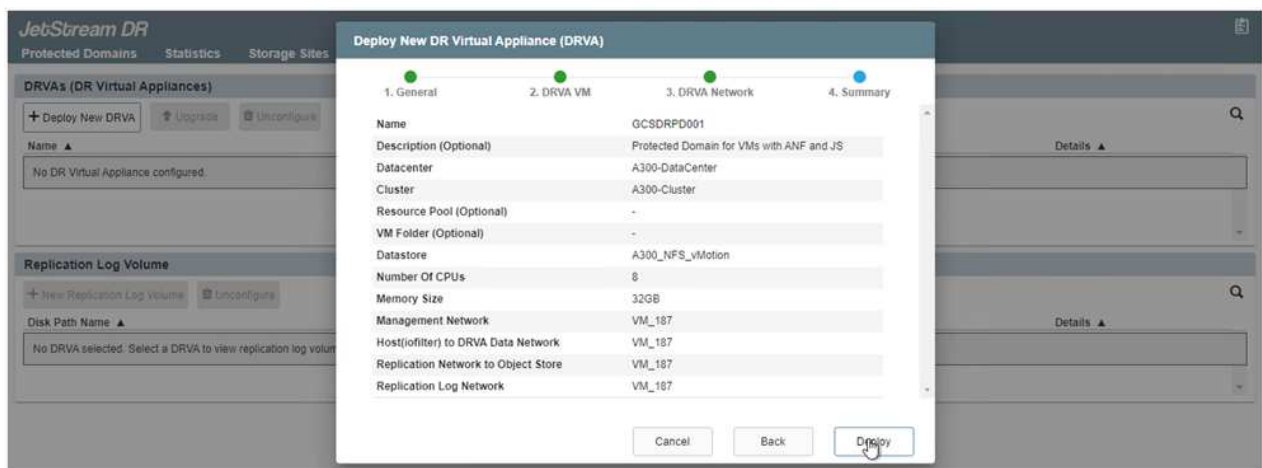
- b. Fügen Sie den Azure Blob-Storage am Recovery-Standort hinzu.



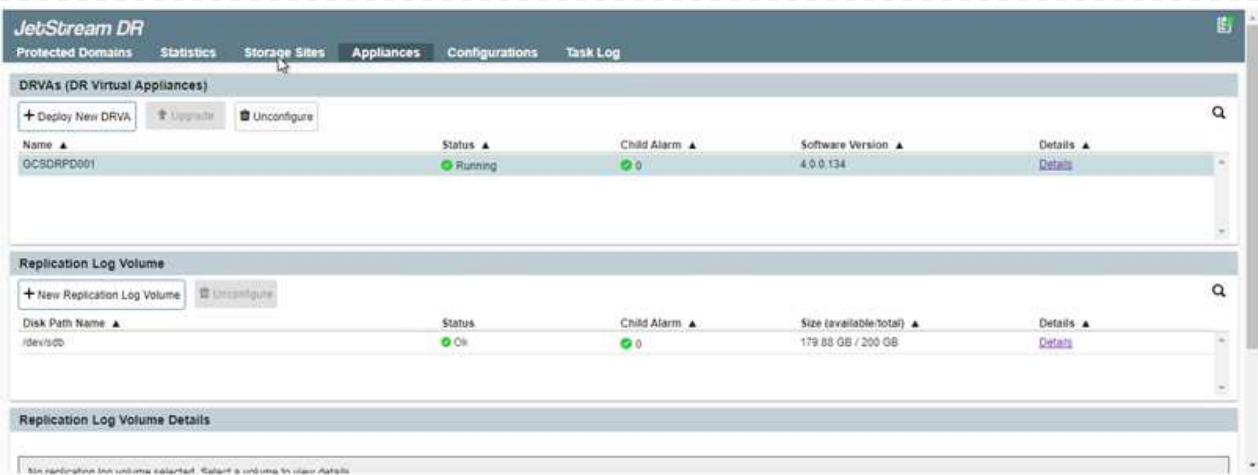
8. Stellen Sie die erforderliche Anzahl an DR Virtual Appliances (DRVAs) über die Registerkarte Appliances bereit.



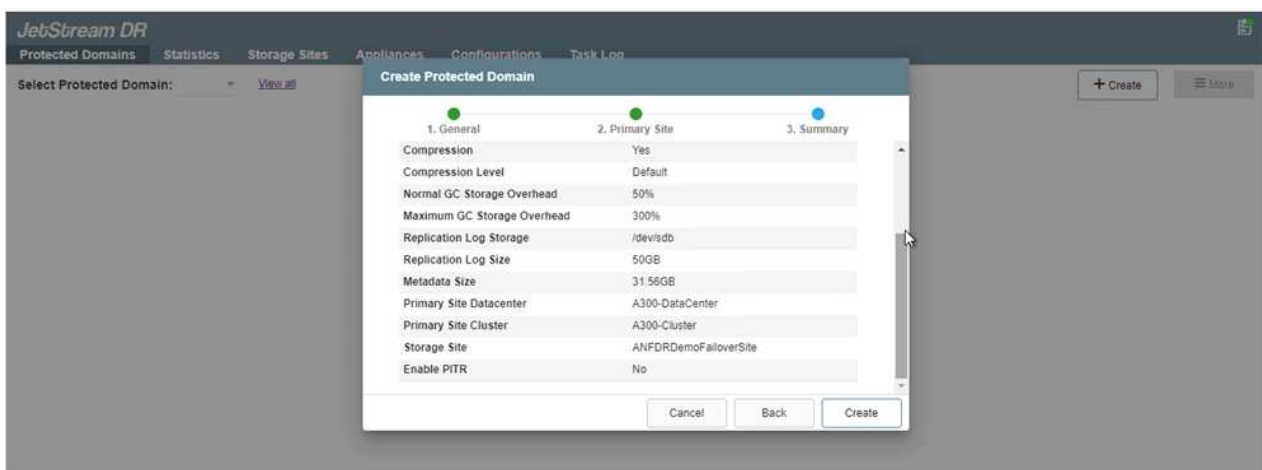
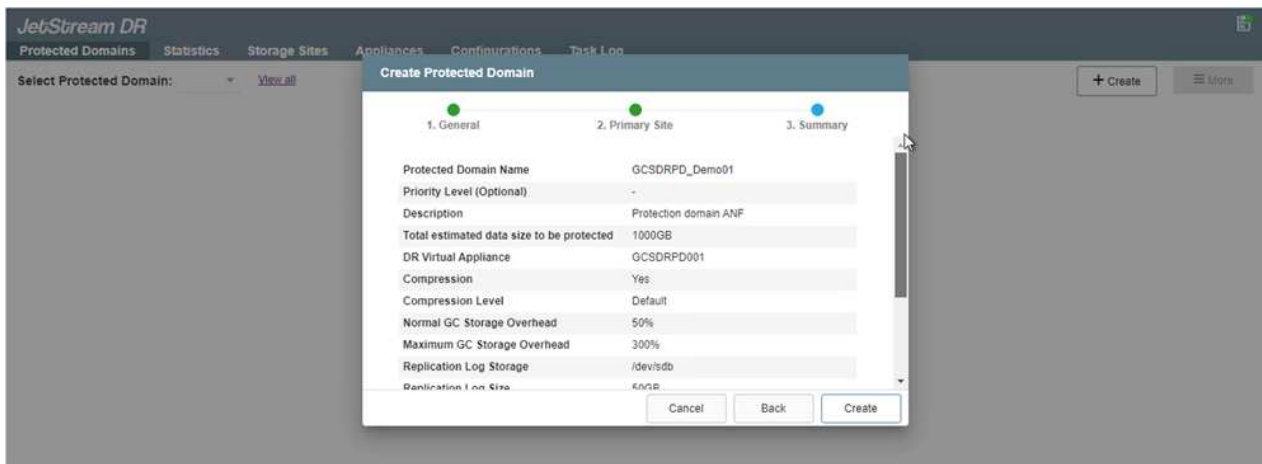
Verwenden Sie das Kapazitätsplanungs-Tool, um die Anzahl der benötigten DRVAs zu ermitteln.



9. Erstellen Sie Protokoll-Volumes für jedes DRVA unter Verwendung der VMDK aus den verfügbaren Datenspeichern oder dem unabhängigen gemeinsamen iSCSI-Speicherpool.



10. Erstellen Sie auf der Registerkarte geschützte Domänen die erforderliche Anzahl geschützter Domänen mithilfe von Informationen über die Azure Blob Storage-Site, die DRVA-Instanz und das Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder einen Satz von Applikations-VMs innerhalb des Clusters, die gemeinsam gesichert werden und einer Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen ist.



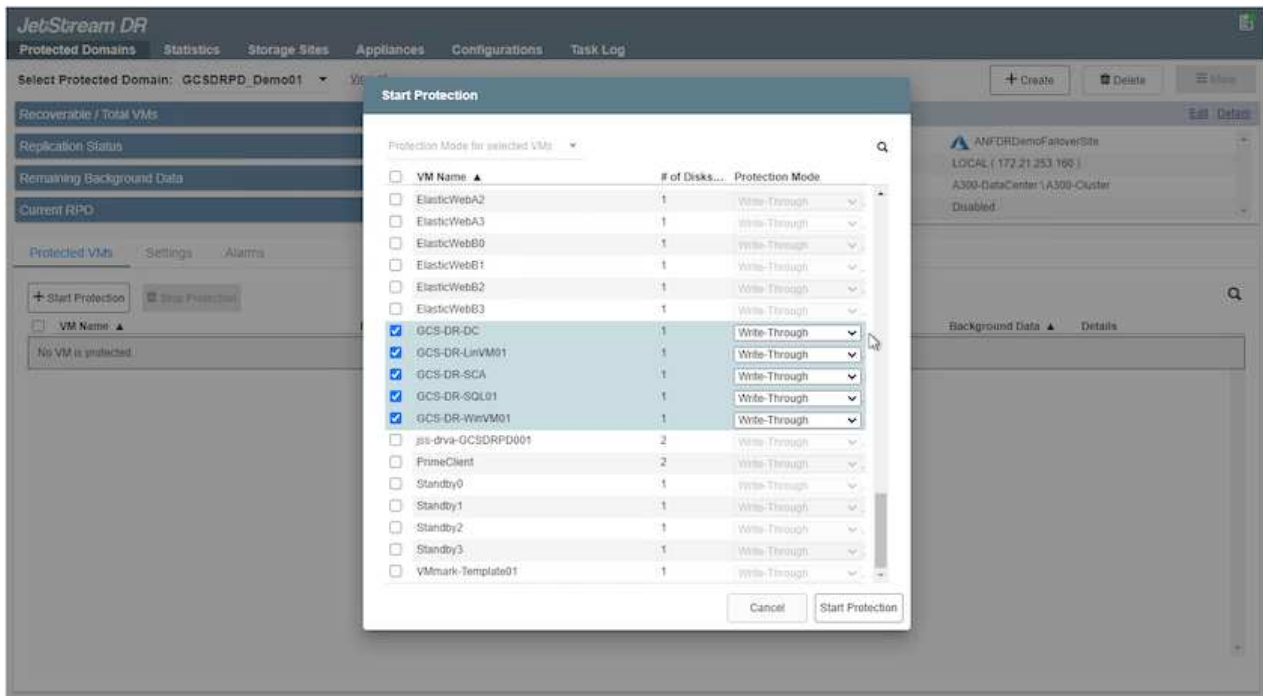
11. Wählen Sie die zu sichernden VMs aus und gruppieren Sie die VMs je nach Abhängigkeit in Applikationsgruppen. Anhand von Applikationsdefinitionen können Gruppen von VMs zu logischen Gruppen gruppiert werden, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen enthalten, die nach der Recovery ausgeführt werden können.



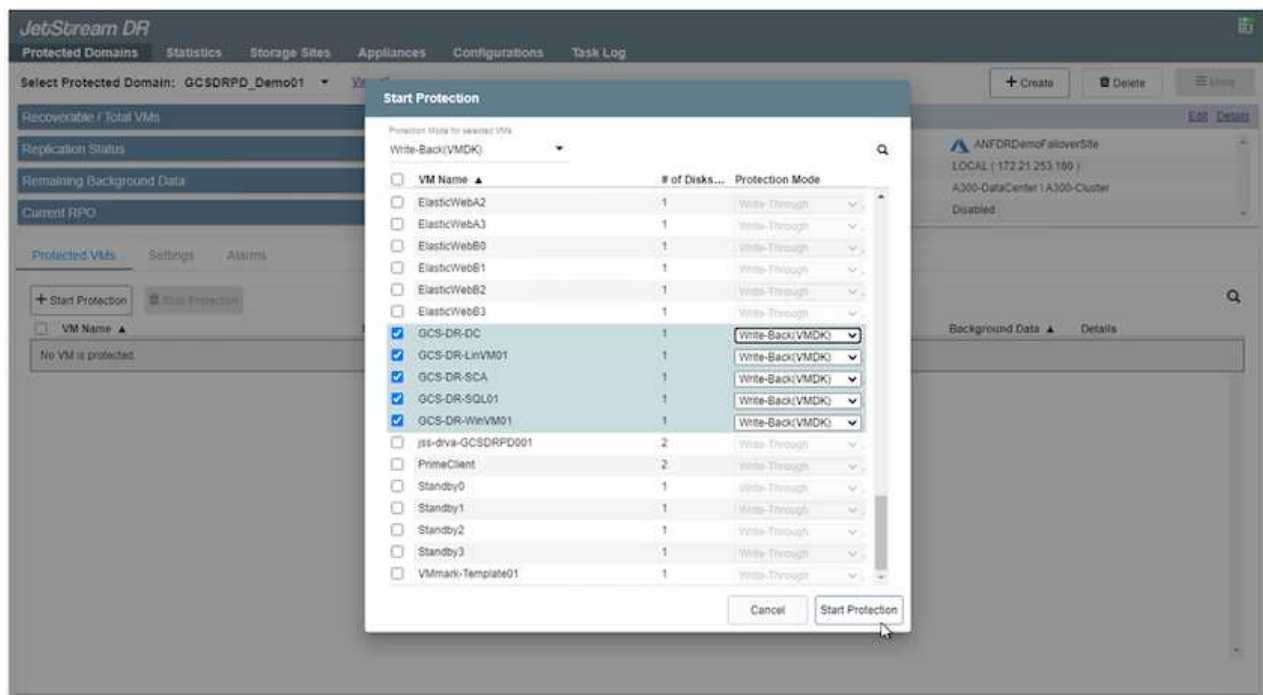
Vergewissern Sie sich, dass derselbe Sicherungsmodus für alle VMs in einer geschützten Domäne verwendet wird.



Write Back(VMDK)-Modus bietet eine höhere Performance.



12. Stellen Sie sicher, dass Replizierungs-Protokoll-Volumes auf hochperformanten Storage platziert werden.



13. Klicken Sie nach dem Abschluss auf Schutz für die geschützte Domäne starten. Damit wird die Datenreplizierung für die ausgewählten VMs auf den zugewiesenen Blob-Speicher gestartet.

JetStream DR
Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Recoverable / Total VMs: 0 / 5
Replication Status: OK
Remaining Background Data: 0 B
Current RPO: -

Configurations

- Storage Site: ANFDRD
- Owner Site: LOCAL (172.2
- Datacenter \ Cluster: A300-DataCen
- Point-in-time Recovery: Disabled

Running Tasks

- Start Protection (GCS-DR-SCA) 50%
- Start Protection (GCS-DR-Win...) 50%
- Start Protection (GCS-DR-Lin...) 50%
- Start Protection (GCS-DR-DC) 50%
- Start Protection (GCS-DR-SQ...) 50%
- Configure VMDK Re... Completed

Protected VMs Settings Alarms

+ Start Protection Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-LinVM01	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-SCA	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-SQL01	Initializing	-	Write-Back(VMDK)	-	Details
GCS-DR-WinVM01	Initializing	-	Write-Back(VMDK)	-	Details

14. Nach Abschluss der Replizierung wird der Sicherungsstatus der VM als wiederherstellbar markiert.

JetStream DR
Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Recoverable / Total VMs: 5 / 5
Replication Status: OK
Remaining Background Data: 0 B
Current RPO: 0s

Configurations

- Storage Site: ANFDRDdemoFailoverSite
- Owner Site: LOCAL (172.21.253.160)
- Datacenter \ Cluster: A300-DataCenter \ A300-Cluster
- Point-in-time Recovery: Disabled

Protected VMs Settings Alarms

+ Start Protection Stop Protection

VM Name	Protection Status	Replication Status	Protection Mode	Background Data	Details
GCS-DR-DC	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-LinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-SCA	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-SQL01	Recoverable	OK	Write-Back(VMDK)	0 B	Details
GCS-DR-WinVM01	Recoverable	OK	Write-Back(VMDK)	0 B	Details



Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (so genannte Recovery-Gruppe), die Boot-Reihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

15. Klicken Sie auf Einstellungen und dann auf den Link Runbook Configure, um die Runbook-Gruppe zu konfigurieren.

JetStream DR
Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Recoverable / Total VMs: 5 / 5
Replication Status: OK
Remaining Background Data: 0 B
Current RPO: 0s

Configurations

- Storage Site: ANFDRDdemoFailoverSite
- Owner Site: LOCAL (172.21.253.160)
- Datacenter \ Cluster: A300-DataCenter \ A300-Cluster
- Point-in-time Recovery: Disabled

Protected VMs Settings Alarms

Failover Runbook Not Configured [Configure](#)

Test Failover Runbook Not Configured [Configure](#)

Fallback Runbook Not Configured [Configure](#)

Memory Setting Not Configured [Configure](#)

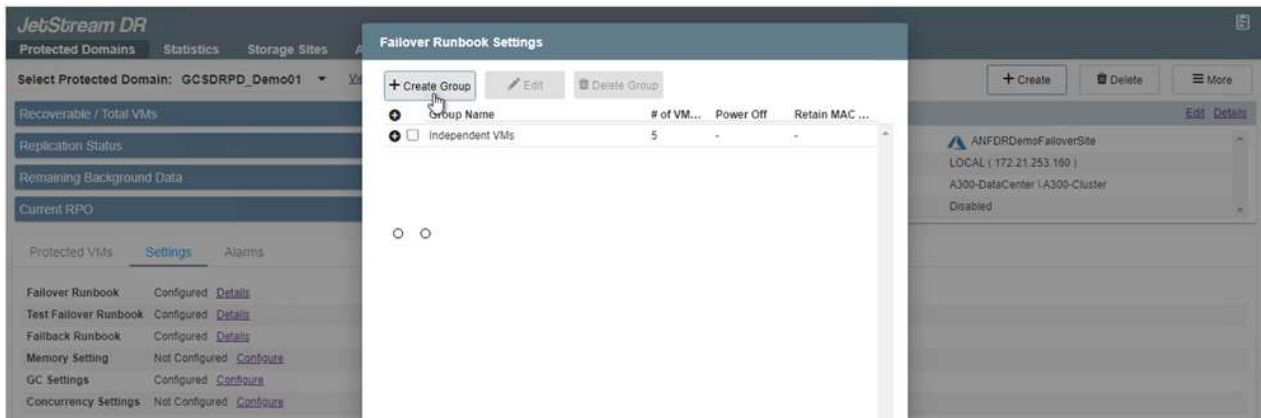
GC Settings Configured [Configure](#)

Concurrency Settings Not Configured [Configure](#)

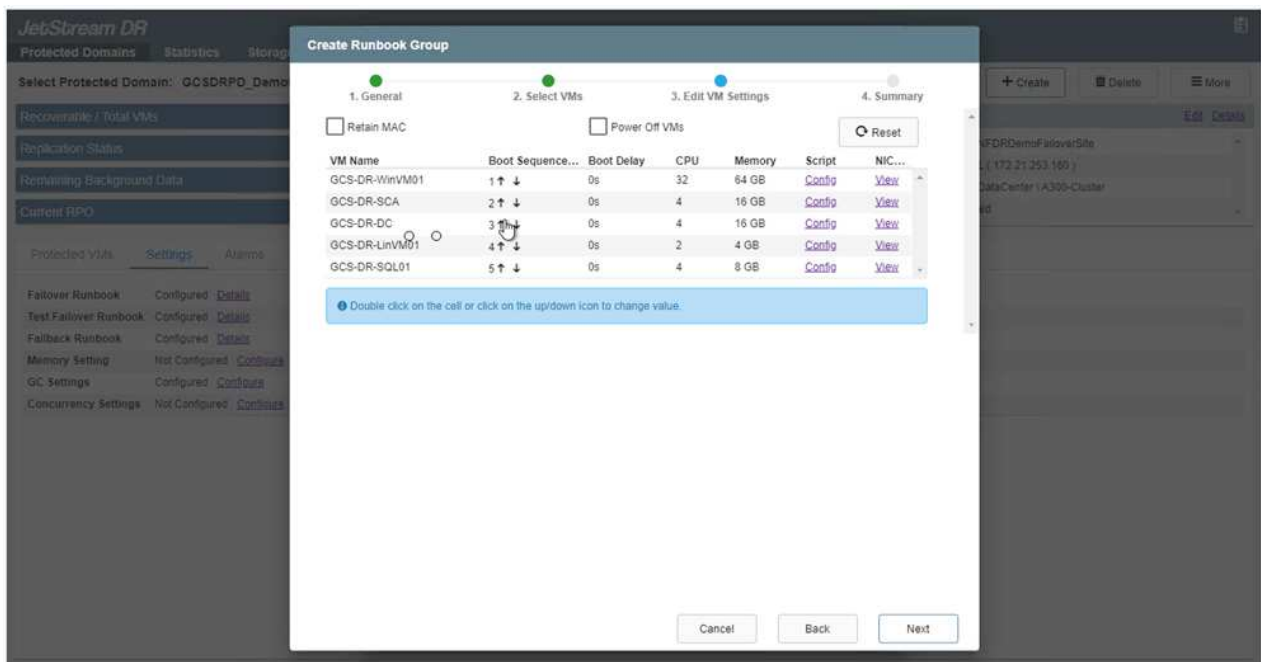
16. Klicken Sie auf die Schaltfläche Gruppe erstellen, um mit der Erstellung einer neuen Runbook-Gruppe zu beginnen.



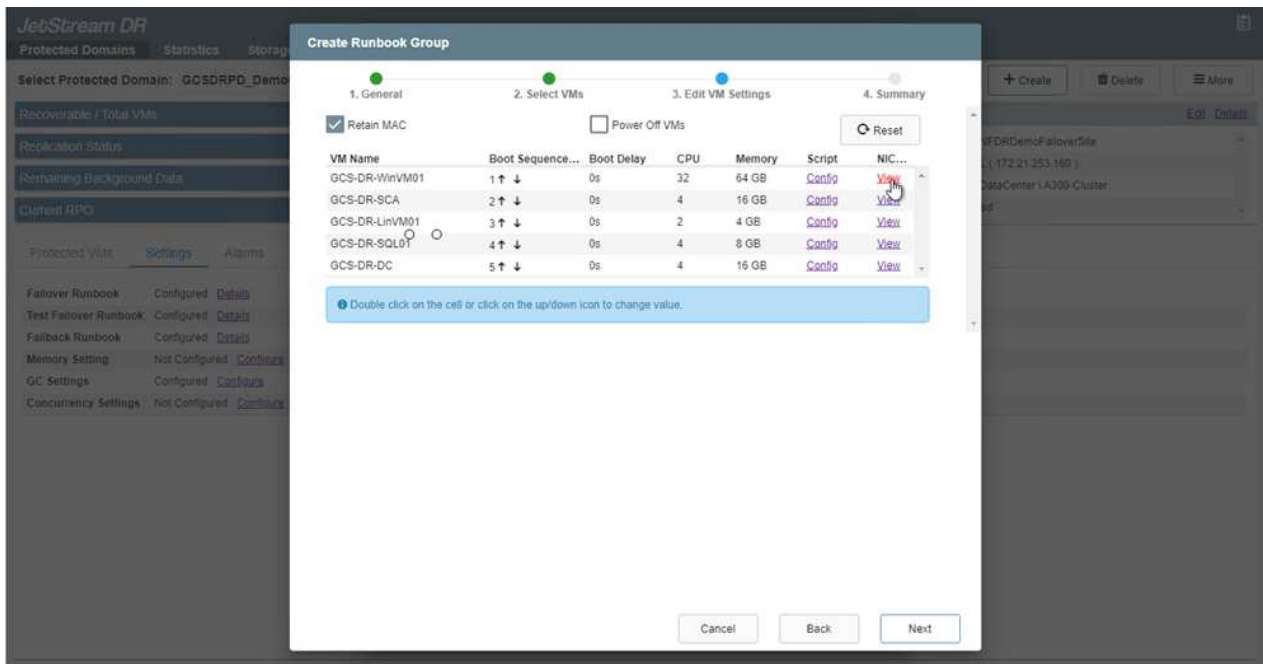
Falls erforderlich, wenden Sie im unteren Teil des Bildschirms benutzerdefinierte Pre-scripts und Post-scripts an, um automatisch vor und nach dem Betrieb der Runbook-Gruppe auszuführen. Stellen Sie sicher, dass die Runbook-Skripte auf dem Management-Server residieren.



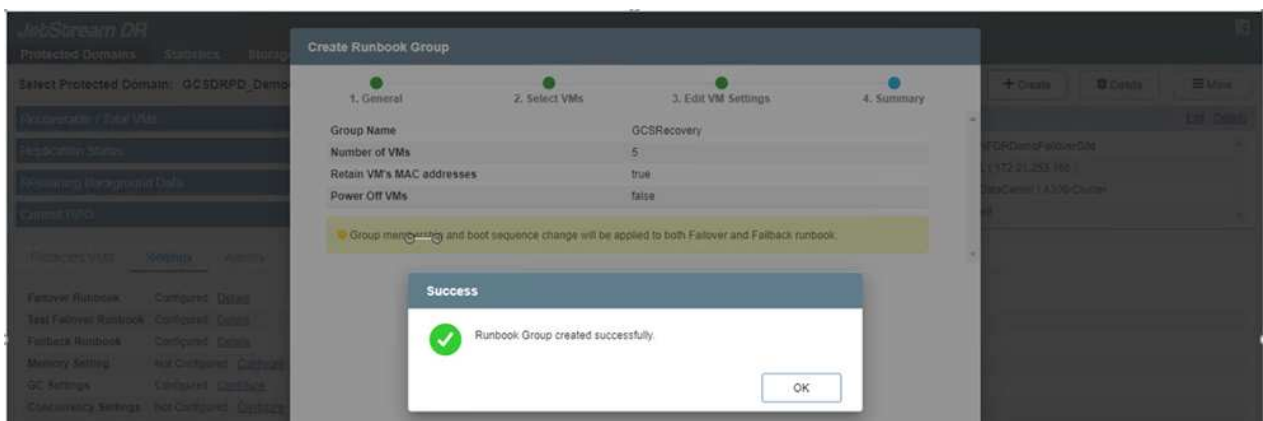
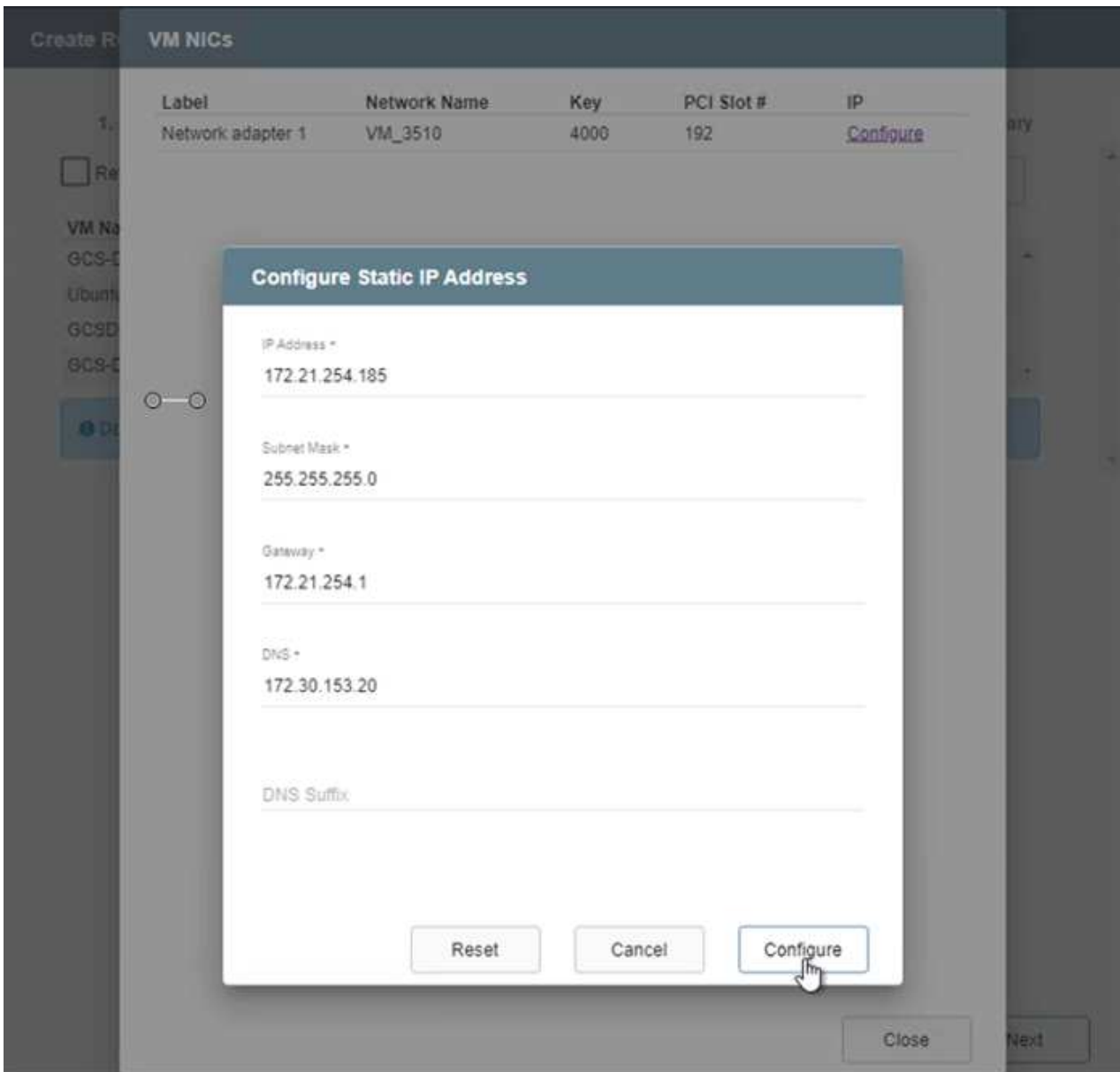
17. Bearbeiten Sie die VM-Einstellungen nach Bedarf. Geben Sie die Parameter für die Wiederherstellung der VMs an, einschließlich der Boot-Sequenz, der Boot-Verzögerung (angegeben in Sekunden), der Anzahl der CPUs und der zuzuzuzuzuzuzuzuzuzuzuzuzuweist. Ändern Sie die Boot-Sequenz der VMs, indem Sie auf die Pfeile nach oben oder unten klicken. Zur Aufbewahrung von MAC stehen auch Optionen zur Verfügung.



18. Statische IP-Adressen können manuell für die einzelnen VMs der Gruppe konfiguriert werden. Klicken Sie auf den Link „NIC-Ansicht“ einer VM, um die IP-Adresseinstellungen manuell zu konfigurieren.



19. Klicken Sie auf die Schaltfläche Konfigurieren, um die NIC-Einstellungen für die jeweiligen VMs zu speichern.



Der Status der Failover- und Failback-Runbooks wird nun als konfiguriert aufgeführt. Failover- und Failback-Runbook-Gruppen werden paarweise erstellt, wobei dieselbe erste Gruppe von VMs und Einstellungen verwendet wird. Bei Bedarf können die Einstellungen einer Runbook-Gruppe individuell angepasst werden, indem Sie auf den entsprechenden Link Details klicken und Änderungen vornehmen.

Installieren Sie JetStream DR für AVS in der Private Cloud

Eine Best Practice für einen Recovery-Standort (AVS) ist die Erstellung eines Pilotlichtclusters mit drei Knoten im Voraus. Dadurch kann die Infrastruktur am Recovery-Standort vorkonfiguriert werden, einschließlich:

- Netzwerkzielsegmente, Firewalls, Services wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF-Volumes als Datastores und mehr

Jetstream DR unterstützt einen RTO-Modus von nahezu null für geschäftskritische Domänen. In diesen Domänen sollte der Ziel-Storage vorinstalliert sein. ANF ist in diesem Fall ein empfohlener Speichertyp.



Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster entsprechend den Anforderungen vor Ort konfiguriert werden.



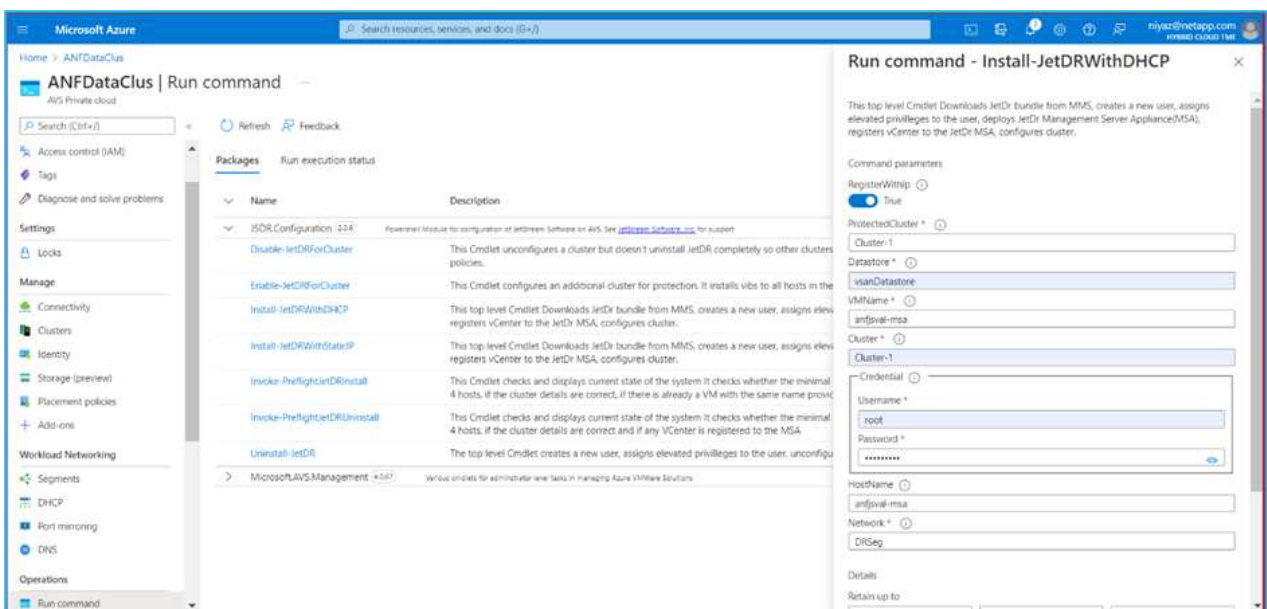
Je nach SLA- und RTO-Anforderungen können Sie einen kontinuierlichen Failover oder einen normalen (Standard-) Failover-Modus verwenden. Bei einer RTO von nahezu null sollten Sie am Recovery-Standort mit der kontinuierlichen Rehydrierung beginnen.

1. Verwenden Sie den Befehl Ausführen, um JetStream DR für AVS auf einer privaten Cloud der Azure VMware-Lösung zu installieren. Wählen Sie im Azure-Portal zur Azure VMware-Lösung die Private Cloud aus und wählen Sie Ausführen Command > Packages > JSDR.Configuration.



Der CloudAdmin-Standardbenutzer der Azure VMware-Lösung verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Lösung ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Befehls Azure VMware Solution Run für JetStream DR.

Der folgende Screenshot zeigt die Installation mithilfe einer DHCP-basierten IP-Adresse.



2. Nachdem die JetStream DR für AVS-Installation abgeschlossen ist, aktualisieren Sie den Browser.

Um auf die JetStream DR-UI zuzugreifen, wechseln Sie zum SDDC Datacenter > Configure > JetStream DR.

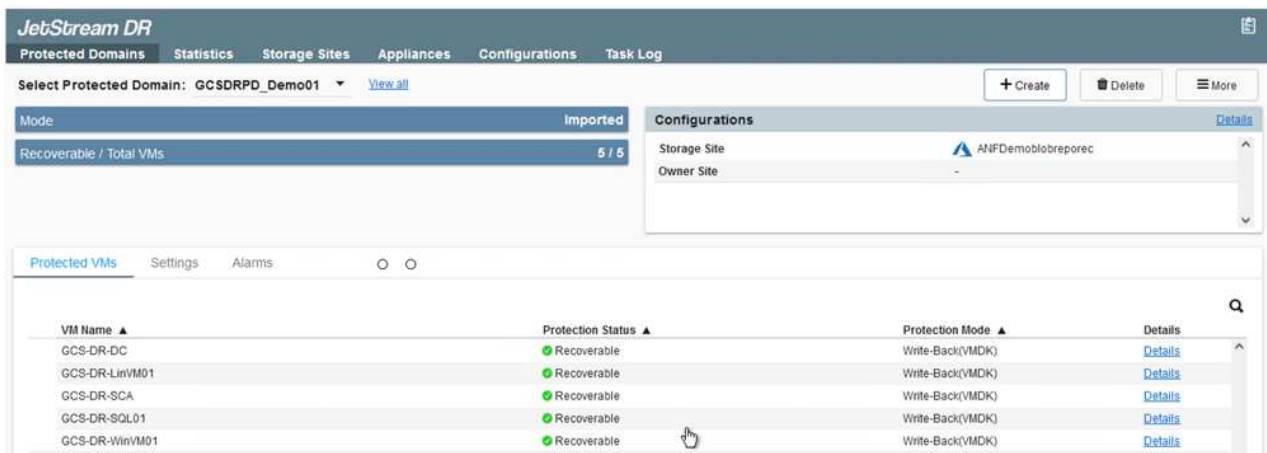


3. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:

- Fügen Sie das Azure Blob Storage-Konto hinzu, das zur Sicherung des lokalen Clusters als Storage-Standort verwendet wurde, und starten Sie dann die Option Scan Domains.
- Wählen Sie im angezeigten Popup-Dialogfeld die zu importierende geschützte Domäne aus, und klicken Sie anschließend auf den Link Importieren.



4. Die Domäne wird zur Wiederherstellung importiert. Gehen Sie auf die Registerkarte geschützte Domänen und überprüfen Sie, ob die vorgesehene Domäne ausgewählt wurde, oder wählen Sie die gewünschte aus dem Menü geschützte Domäne auswählen aus. Eine Liste der wiederherstellbaren VMs in der geschützten Domäne wird angezeigt.



5. Nachdem die geschützten Domains importiert wurden, sollten DRVA-Appliances bereitgestellt werden.



Diese Schritte können auch mithilfe von CPT- erstellten Plänen automatisiert werden.

6. Verwenden von verfügbaren vSAN oder ANF-Datstores für Replizierungsprotokolle erstellen
7. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery-VA, um einen ANF-Datenspeicher für VM-Platzierungen zu verwenden.

Step	Configuration
1. General	Protected Domain Name: ANFPD002, Datacenter: SDDC-Datacenter, Cluster: Cluster-1, Resource Pool (Optional): -, VM Folder (Optional): -, Datastore: ANFRecoDSU002, Internal Network: DRSeg, External Replication Network: DRSeg, Management Network: DRSeg, Storage Site: ANFDemoblobreporec, DR Virtual Appliance: ANFRecDRVA003
2a. Failover Settings	
2b. VM Settings	
3. Recovery VA	
4. DR Settings	
5. Summary	



Stellen Sie sicher, dass DHCP für das ausgewählte Segment aktiviert ist und genügend IP-Adressen verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen sich wiederherstellen. Jede wiederherzuernde VM (einschließlich kontinuierlicher Rehydrierung) erfordert eine individuelle dynamische IP-Adresse. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

8. Wählen Sie die entsprechende Failover-Option (Continuous Failover oder Failover) aus. In diesem Beispiel wird die kontinuierliche Rehydrierung (kontinuierliches Failover) ausgewählt.



Obwohl sich der kontinuierliche Failover- und Failover-Modus bei der Konfiguration unterscheiden, werden beide Failover-Modi mit den gleichen Schritten konfiguriert. Failover-Schritte werden als Reaktion auf ein Notfall konfiguriert und durchgeführt. Ein kontinuierlicher Failover kann jederzeit konfiguriert werden und dann im Hintergrund während des normalen Systembetriebs ausgeführt werden. Nach einem Zwischenfall wird der fortlaufende Failover abgeschlossen, sodass die Eigentümerschaft der geschützten VMs direkt auf den Recovery-Standort übertragen wird (RTO von nahezu null).

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCDRDP_Demo01 [View all](#)

Mode: Imported Recoverable / Total VMs: 5 / 5

Configurations

Storage Site: ANFDemoblobrepor
Owner Site: REMOTE (172.21.253.11)

+ Create | Delete | More

Restore
→ Failover
→ Continuous Failover
→ Test Failover

Protected VMs | Settings | Alarms

VM Name ▲	Protection Status ▲	Protection Mode ▲	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	Details
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	Details

Der kontinuierliche Failover-Prozess beginnt und der Fortschritt kann über die UI überwacht werden. Durch Klicken auf das blaue Symbol im Abschnitt „Aktueller Schritt“ wird ein Popup-Fenster angezeigt, in dem Details zum aktuellen Schritt des Failover-Prozesses angezeigt werden.

Failover und Failback

1. Nach einem Ausfall im geschützten Cluster der lokalen Umgebung (teilweiser oder kompletter Ausfall) können Sie das Failover für VMs auslösen. Dazu verwenden Sie Jetstream, nachdem die SnapMirror Beziehung für die jeweiligen Applikations-Volumes unterbrochen wurde.

The screenshot displays the Jetstream Replication interface. At the top, a summary bar shows: 3 Volume Relationships, 4.78 GiB Replicated Capacity, 0 Currently Transferring, 3 Healthy, and 0 Failed. Below this, a table titled '3 Volume Relationships' lists the following data:

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	snapmirrored	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqhld_sc46 ntaphci-a300e9u25	gcsdrsqhld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	snapmirrored	
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	snapmirrored	

A context menu is open for the first row, showing options: Information, Break, Reverse Resync, Edit Schedule, Edit Max Transfer Rate, Update, and Delete. The 'Break' option is highlighted.

Below the table, a 'Break Relationship' dialog box is displayed with the text: 'Are you sure that you want to break the relationship between "gcsdrsqldb_sc46" and "gcsdrsqldb_sc46_copy"?'. It has 'Break' and 'Cancel' buttons. The 'Break' button is being clicked.



Dieser Schritt kann zur Erleichterung des Recovery-Prozesses einfach automatisiert werden.

2. Greifen Sie auf die Jetstream UI auf dem AVS SDDC (Zielseite) zu und lösen Sie die Failover-Option aus, um den Failover abzuschließen. Die Taskleiste zeigt den Fortschritt für Failover-Aktivitäten an.

Im Dialogfeld, das beim Abschluss des Failover angezeigt wird, kann die Failover-Aufgabe als geplant oder als erzwungen angegeben werden.

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: **GCSDRPD_Demo01** [View all](#)

Mode: Continuous Rehydration in Progress

Recoverable / Total VMs: 4 / 4

Data (Processed/Known Remaining): 329.01 GB / 6.19 GB

Current Step: Recover VMs' data from Storage Site

Configurations

Storage Site	ANFDemo01breporec
Owner Site	REMOTE (172.21.253.160)
Datacenter \ Cluster	SDDC-Datacenter \ Cluster-1
Point-in-time Recovery	Disabled

Protected VMs | Settings | Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	Details
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	Details

Complete Continuous Failover for Protected Domain

VM Network Mapping

Protected VM Network	Recovery VM Network
VM_3510	DRStretchSeg

Other Settings


☐ Planned Failover
☒ Force Failover

Some VM's guest credential are required because of network configuration: [Configure](#)

[Cancel](#)
[Complete Failover](#)

Erzwungenes Failover geht davon aus, dass auf den primären Standort nicht mehr zugegriffen werden kann und die Eigentümerschaft der geschützten Domäne direkt vom Recovery-Standort übernommen werden muss.

Force Failover


Force Failover of Protected Domain requested. Administrator consent is required!
 Complete ownership of this Protected Domain will be taken over by this Site.
 Are you sure you want to continue?

[Cancel](#)
[Confirm](#)

Complete Continuous Failover for Protected Domain

VM Network Mapping

Protected VM Network ▲	Recovery VM Network
VM_3510	DRStretchSeg

○ ○

Other Settings

☐ Planned Failover

☒ Force Failover

Some VM's guest credential are required because of network configuration: [Configure](#)

[Cancel](#) [Complete Failover](#)

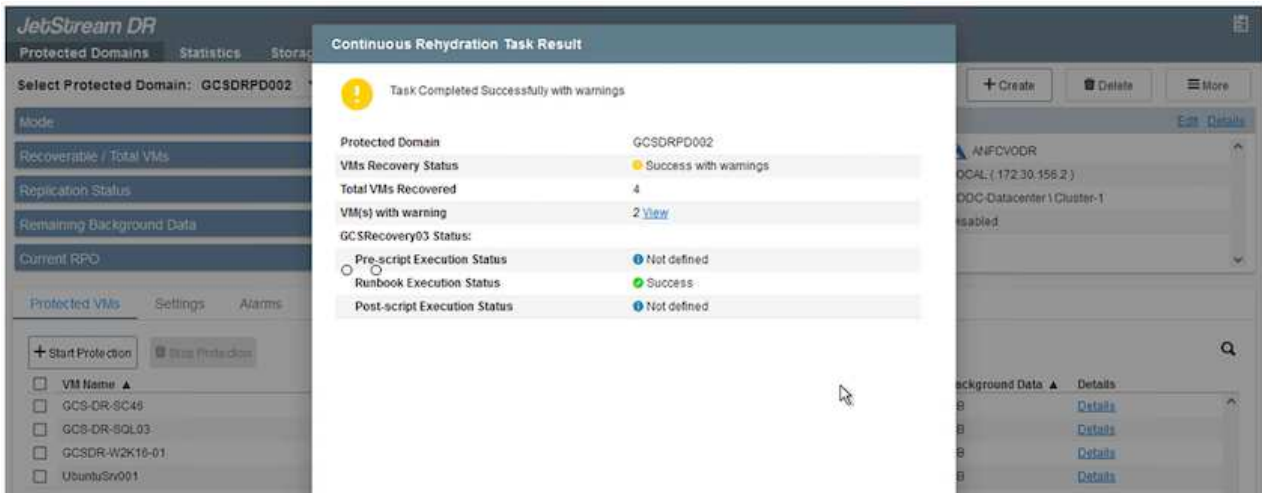
3. Nachdem der kontinuierliche Failover abgeschlossen ist, wird eine Meldung angezeigt, die den Abschluss der Aufgabe bestätigt. Nach Abschluss der Aufgabe greifen Sie auf die wiederhergestellten VMs zu, um ISCSI- oder NFS-Sitzungen zu konfigurieren.



Der Failover-Modus wird in Failover ausgeführt, und der Status der VM ist wiederherstellbar. Alle VMs der geschützten Domäne werden jetzt am Recovery-Standort in dem von den Failover-Runbook-Einstellungen angegebenen Zustand ausgeführt.



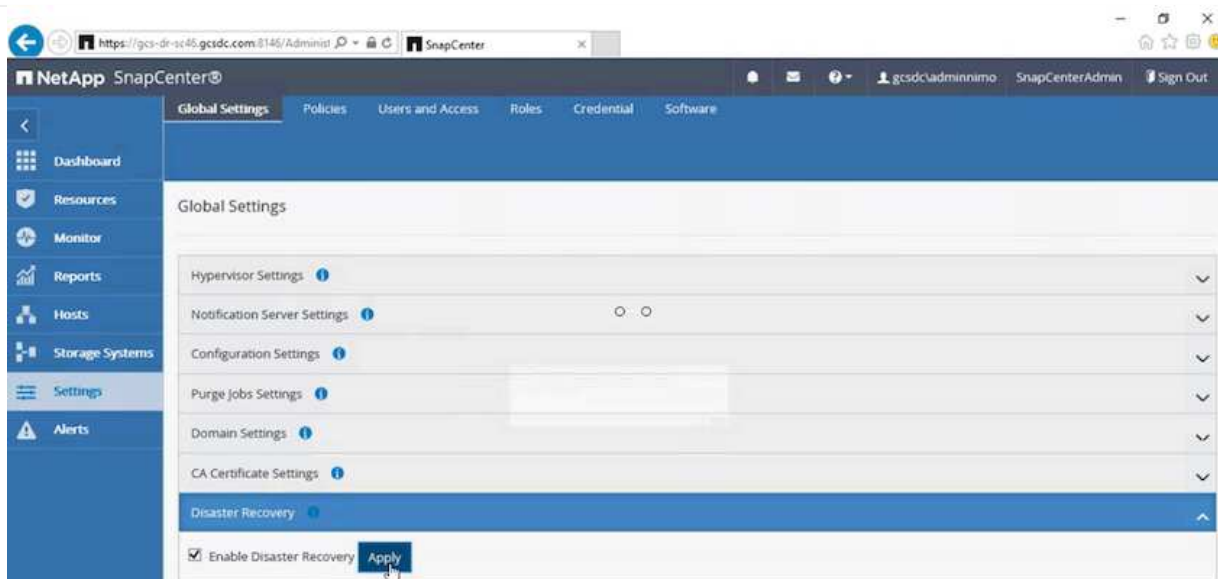
Um die Failover-Konfiguration und die Infrastruktur zu überprüfen, kann JetStream DR im Testmodus (Option Test Failover) betrieben werden, um die Wiederherstellung von Virtual Machines und deren Daten vom Objektspeicher in einer Test-Recovery-Umgebung zu beobachten. Wenn ein Failover-Verfahren im Testmodus ausgeführt wird, ähnelt sein Vorgang einem tatsächlichen Failover-Prozess.



4. Sobald die Virtual Machines wiederhergestellt sind, wird Disaster Recovery für Storage auf dem Gast-Storage eingesetzt. Um diesen Prozess zu demonstrieren, wird SQL-Server in diesem Beispiel verwendet.
5. Melden Sie sich bei der wiederhergestellten SnapCenter-VM auf dem AVS SDDC an und aktivieren Sie den DR-Modus.
 - a. Greifen Sie über Browsern auf die SnapCenter-Benutzeroberfläche zu.



- b. Navigieren Sie auf der Seite Einstellungen zu Einstellungen > Globale Einstellungen > Disaster Recovery.
- c. Wählen Sie Disaster Recovery Aktivieren.
- d. Klicken Sie Auf Anwenden.

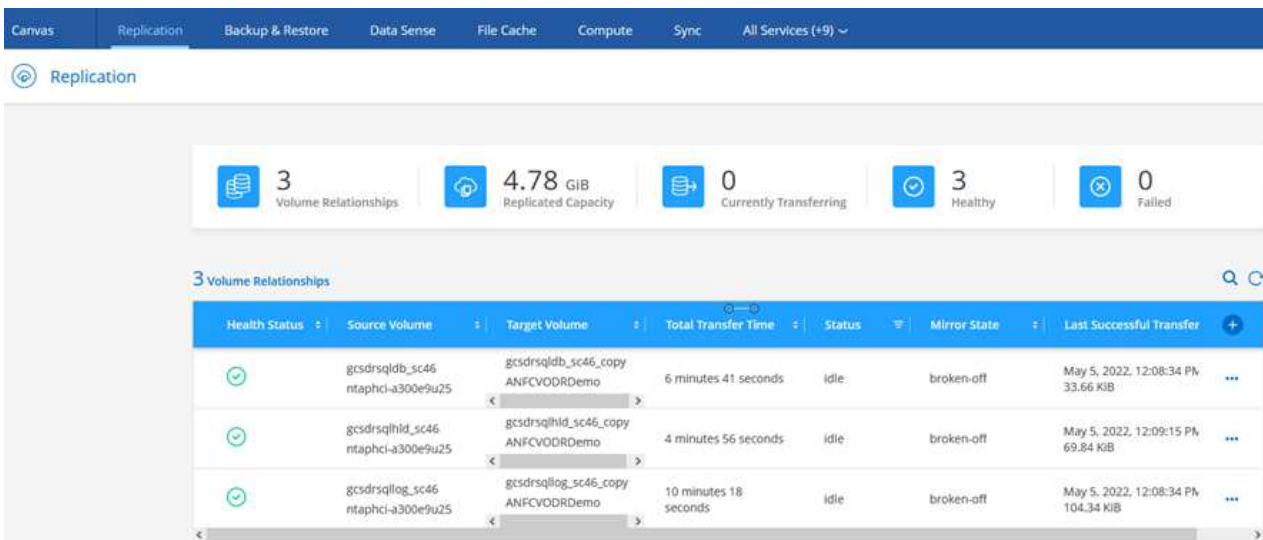


e. Überprüfen Sie, ob der DR-Job aktiviert ist, indem Sie auf Überwachen > Jobs klicken.

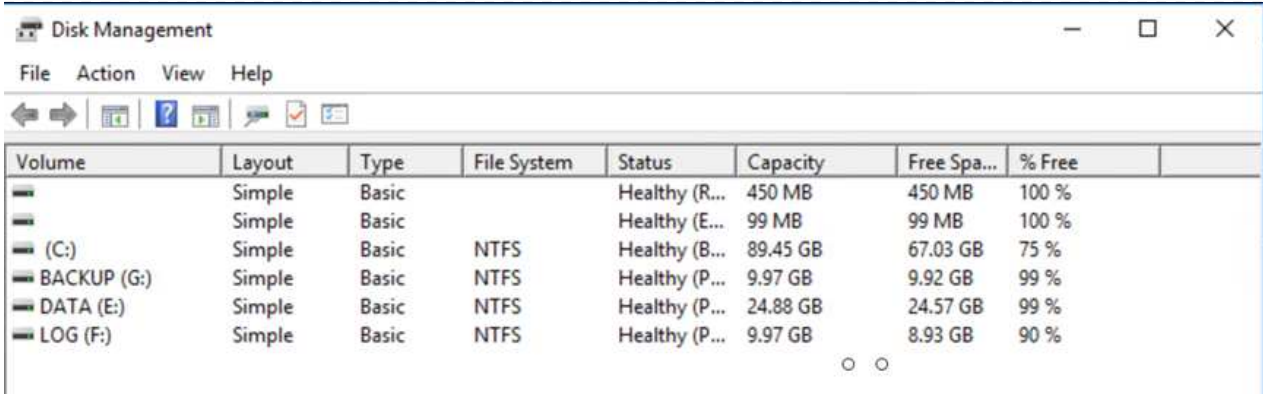


Für das Storage Disaster Recovery sollte NetApp SnapCenter 4.6 oder höher verwendet werden. Frühere Versionen sollten applikationskonsistente Snapshots (replizierte mit SnapMirror) verwenden und ein manuelles Recovery ausführen, falls frühere Backups am Disaster Recovery-Standort wiederhergestellt werden müssen.

6. Stellen Sie sicher, dass die SnapMirror Beziehung beschädigt ist.



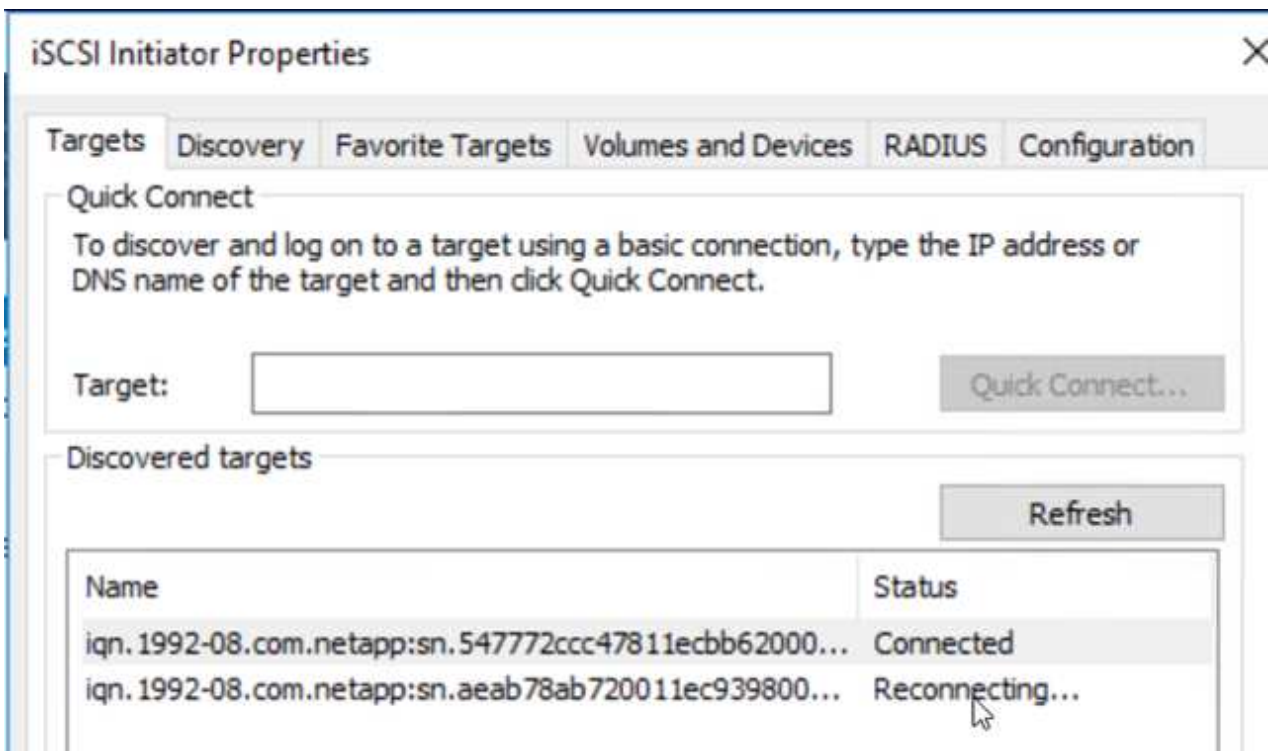
7. Verbinden Sie die LUN aus Cloud Volumes ONTAP mit der wiederhergestellten SQL Gast-VM mit gleichen Laufwerksbuchstaben.



Disk Management window showing disk layout and status. The table below represents the data shown in the window.

Volume	Layout	Type	File System	Status	Capacity	Free Space	% Free
Simple	Simple	Basic		Healthy (R...)	450 MB	450 MB	100 %
Simple	Simple	Basic		Healthy (E...)	99 MB	99 MB	100 %
(C:)	Simple	Basic	NTFS	Healthy (B...)	89.45 GB	67.03 GB	75 %
BACKUP (G:)	Simple	Basic	NTFS	Healthy (P...)	9.97 GB	9.92 GB	99 %
DATA (E:)	Simple	Basic	NTFS	Healthy (P...)	24.88 GB	24.57 GB	99 %
LOG (F:)	Simple	Basic	NTFS	Healthy (P...)	9.97 GB	8.93 GB	90 %

8. Öffnen Sie den iSCSI-Initiator, löschen Sie die vorherige getrennte Sitzung und fügen Sie das neue Ziel zusammen mit Multipath für die replizierten Cloud Volumes ONTAP Volumes hinzu.



iSCSI Initiator Properties dialog box. The 'Targets' tab is selected. The 'Quick Connect' section is visible. The 'Discovered targets' section shows a list of targets with their names and status.

Quick Connect
To discover and log on to a target using a basic connection, type the IP address or DNS name of the target and then click Quick Connect.

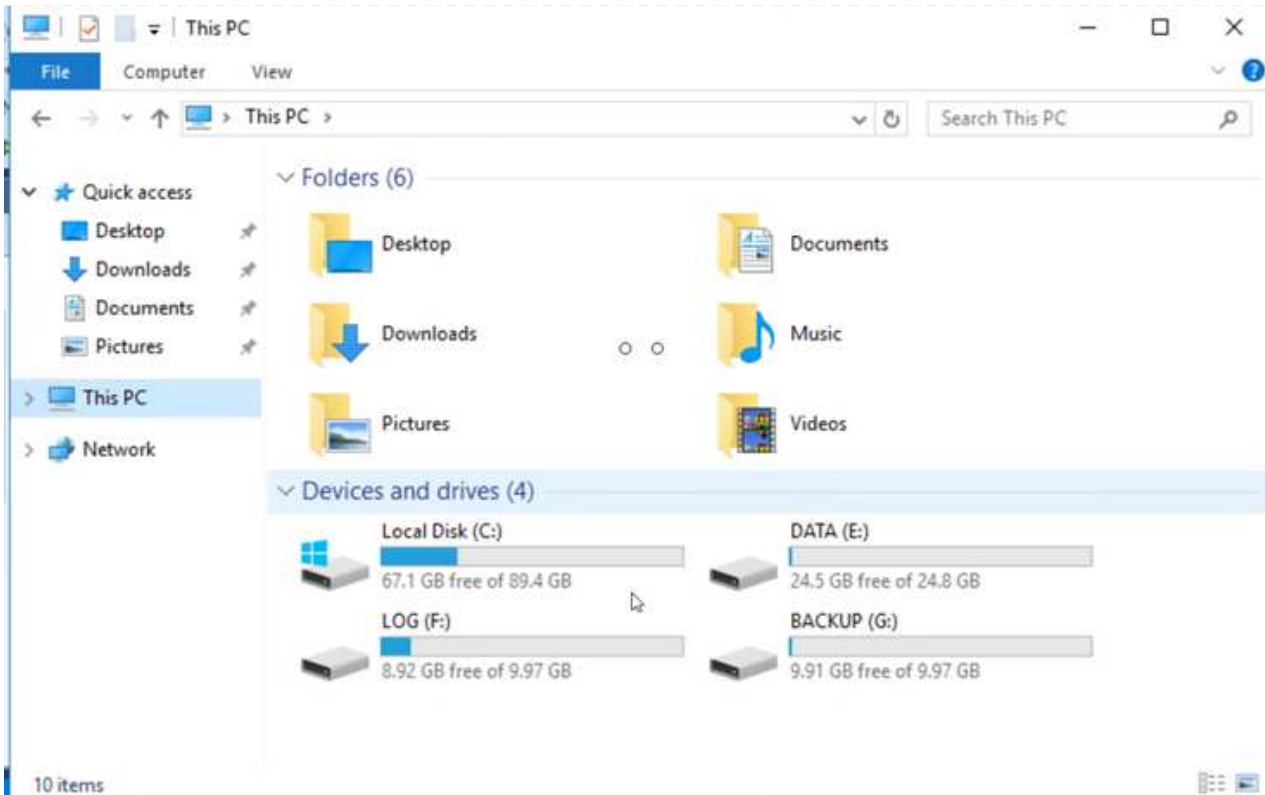
Target: Quick Connect...

Discovered targets

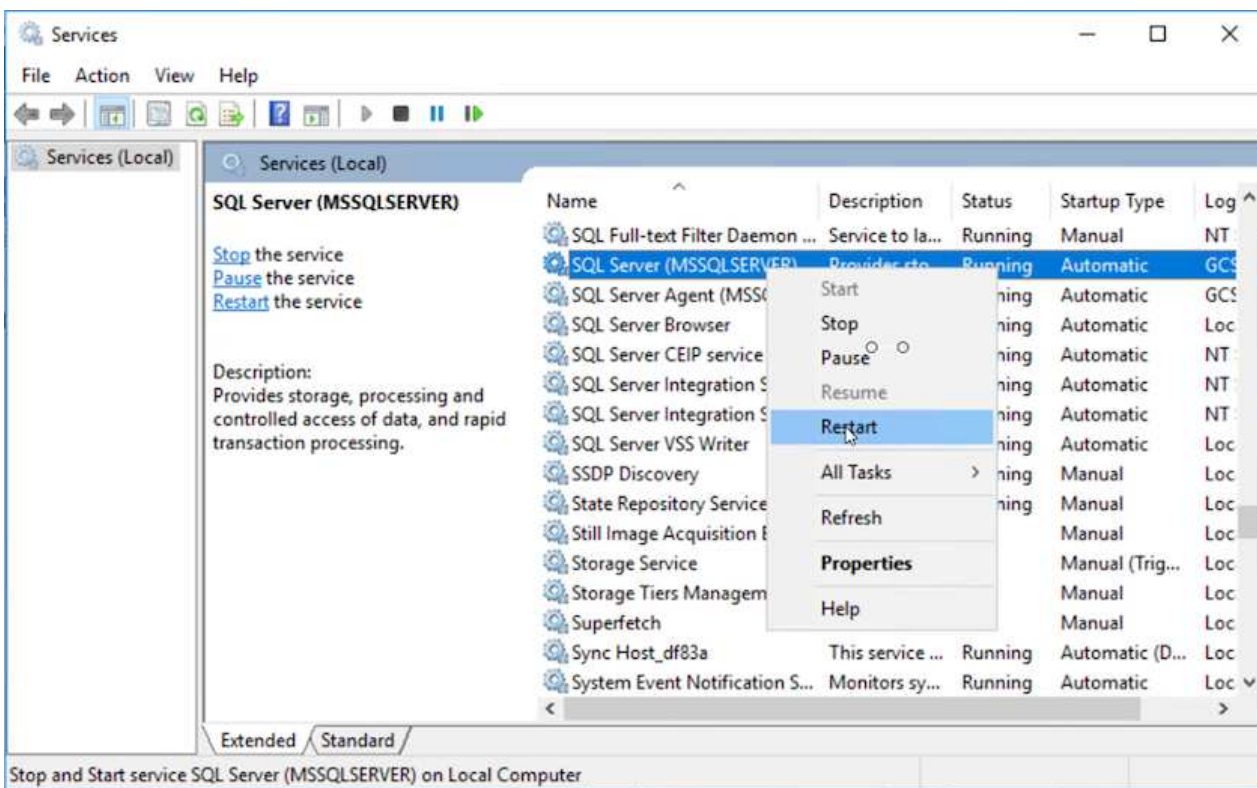
Refresh

Name	Status
iqn.1992-08.com.netapp:sn.547772ccc47811ecbb62000...	Connected
iqn.1992-08.com.netapp:sn.aeab78ab720011ec939800...	Reconnecting...

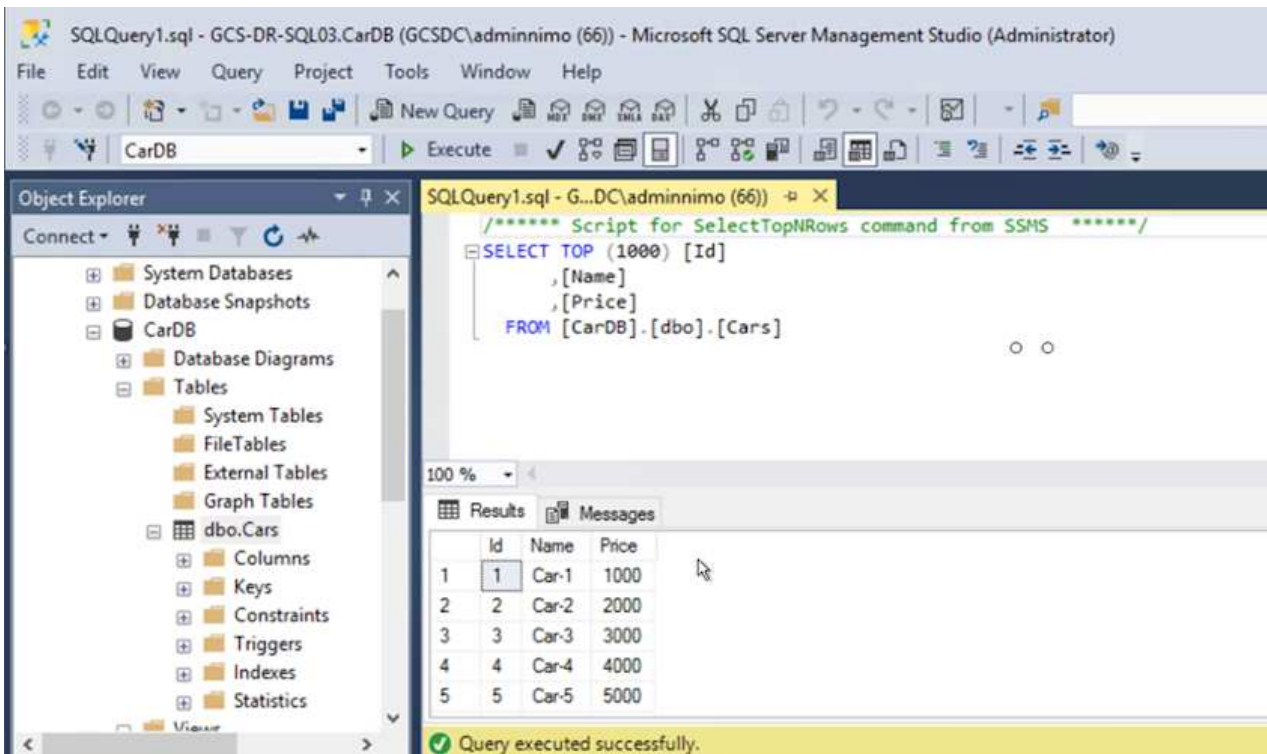
9. Stellen Sie sicher, dass alle Laufwerke mit denselben Laufwerksbuchstaben verbunden sind, die vor DR verwendet wurden.



10. Starten Sie den MSSQL-Serverdienst neu.



11. Stellen Sie sicher, dass die SQL-Ressourcen wieder online sind.



Hängen Sie im Fall von NFS die Volumes mit dem Mount-Befehl an, und aktualisieren Sie die `/etc/fstab` Einträge.

An diesem Punkt können Betriebsabläufe ausgeführt werden und der Geschäftsbetrieb normal weiterläuft.



Am NSX-T-Ende kann ein separates, dediziertes Tier-1 Gateway zur Simulation von Failover-Szenarien erstellt werden. So ist sichergestellt, dass alle Workloads miteinander kommunizieren können, dass jedoch kein Traffic in die bzw. aus der Umgebung geleitet werden kann. So können alle Triage-, Containment- oder Härteaufgaben ohne das Risiko einer Kreuzkontamination durchgeführt werden. Dieser Vorgang ist außerhalb des Anwendungsbereichs dieses Dokuments, kann aber problemlos zur Simulation der Isolation durchgeführt werden.

Wenn der primäre Standort wieder in Betrieb ist, können Sie ein Failback durchführen. Die VM-Sicherung wird durch Jetstream fortgesetzt, und die SnapMirror Beziehung muss umgekehrt werden.

1. Wiederherstellung der lokalen Umgebung Je nach Art des Notfalleinfalls sind möglicherweise die Wiederherstellung und/oder Überprüfung der Konfiguration des geschützten Clusters erforderlich. Falls erforderlich, muss die JetStream DR-Software möglicherweise erneut installiert werden.
2. Greifen Sie auf die wiederhergestellte On-Premises-Umgebung zu, rufen Sie die Jetstream DR UI auf und wählen Sie die entsprechende geschützte Domäne aus. Nachdem der geschützte Standort für Failback bereit ist, wählen Sie die Failback-Option in der UI aus.



Mit dem CPT-generierten Failback-Plan kann außerdem die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher in die ursprüngliche VMware Umgebung initiiert werden.

JetStream DR

Protected Domains | Statistics | Storage Sites | Appliances | Configurations | Task Log

Select Protected Domain: GCSDRPD_Demo01 [View all](#)

Mode: Running in Failover

Active Site: 172.30.156.2

Recoverable / Total VMs: 4 / 4

Configurations

Storage Site: ANFCVODR

Owner Site: REMOTE (172.30.156.2)

Actions: + Create, Delete, More

Dropdown menu: Restore, Resume Continuous Rehydration, Failback

Protected VMs | Settings | Alarms

VM Name	Protection Status	Protection Mode	Details
GCS-DR-DC	Recoverable	Write-Back(VMDK)	Details
GCS-DR-LinVM01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SCA	Recoverable	Write-Back(VMDK)	Details
GCS-DR-SQL01	Recoverable	Write-Back(VMDK)	Details
GCS-DR-WinVM01	Recoverable	Write-Back(VMDK)	Details



Geben Sie die maximale Verzögerung an, nachdem Sie die VMs am Recovery-Standort angehalten und am geschützten Standort neu gestartet haben. Die zum Abschluss dieses Prozesses erforderliche Zeit umfasst das Abschließen der Replizierung nach dem Stoppen von Failover-VMs, die zum Reinigen des Recovery-Standorts benötigte Zeit und die Zeit zur Wiederherstellung von VMs am geschützten Standort. NetApp empfiehlt 10 Minuten.

Failback Protected Domain

1. General | 2a. Failback Settings | 2b. VM Settings | 3. Recovery VA | 4. DR Settings | 5. Summary

Failback Datacenter: A300-DataCenter

Failback Cluster: A300-Cluster

Failback Resource Pool: -

VM Folder (Optional): -

Failback Datastore: A300_NFS_vMotion

Maximum Delay After Stopping: 10 Minutes

Internal Network: VM_187

External Replication Network: VM_187

Management Network: VM_187

Storage Site: ANFCVODR

DR Virtual Appliance: GCSDRVA002

Replication Log Storage: /dev/sdb

Buttons: Cancel, Back, Failback

- Schließen Sie den Failback-Prozess ab, und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

JetStream DR

Protected Domains | Statistics | Storage S...

Select Protected Domain: **GCSDRPD002**

Recoverable / Total VMs

Replication Status

Remaining Background Data

Current RPO

Protected VMs | Settings | Alarms

Failback Task Result

Task Completed Successfully

Protected Domain: GCSDRPD002

VMs Recovery Status: Success

Total VMs Recovered: 4

GCSDRecovery03 Status:

Pre-script Execution Status: Not defined

Runbook Execution Status: Success

Post-script Execution Status: Not defined

4. Nachdem die VMs wiederhergestellt wurden, trennen Sie den sekundären Storage vom Host und stellen eine Verbindung zum primären Storage her.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	6 minutes 41 seconds	idle	broken-off	May 5, 2022, 12:08:34 PM 33.66 KiB
✓	gcsdrsqld_hld_sc46 ntaphci-a300e9u25	gcsdrsqld_hld_sc46_copy ANFCVODRDemo	4 minutes 56 seconds	idle	broken-off	
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	10 minutes 18 seconds	idle	broken-off	

Information

Resync

Reverse Resync

Edit Schedule

Edit Max Transfer Rate

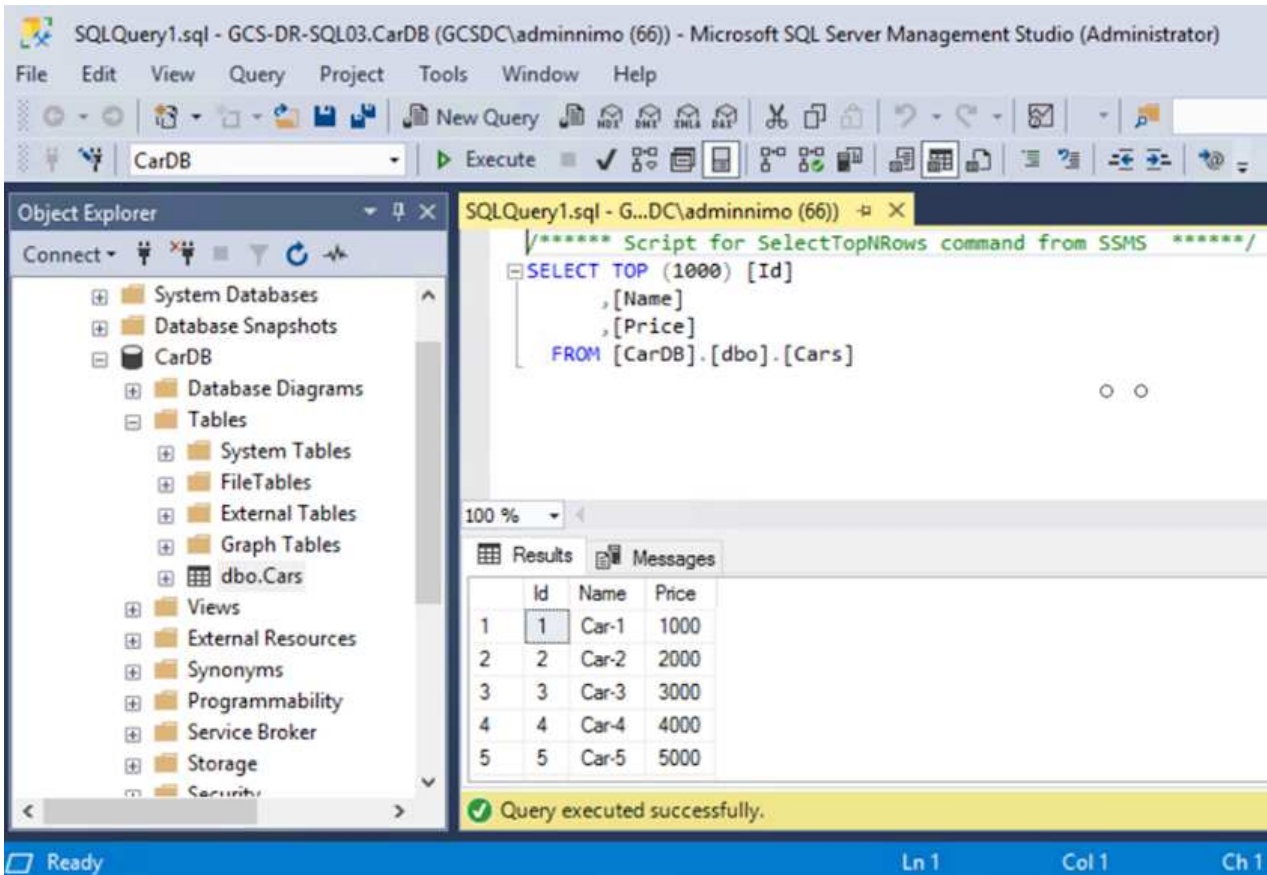
Delete

3 Volume Relationships | 6.54 GiB Replicated Capacity | 0 Currently Transferring | 3 Healthy | 0 Failed

3 Volume Relationships

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	gcsdrsqldb_sc46 ntaphci-a300e9u25	gcsdrsqldb_sc46_copy ANFCVODRDemo	19 seconds	idle	snapmirrored	May 6, 2022, 11:03:00 AM 5.73 MiB
✓	gcsdrsqld_hld_sc46 ANFCVODRDemo	gcsdrsqld_hld_sc46 ntaphci-a300e9u25	1 minute 46 seconds	idle	snapmirrored	May 6, 2022, 11:01:39 AM 800.76 MiB
✓	gcsdrsqlog_sc46 ntaphci-a300e9u25	gcsdrsqlog_sc46_copy ANFCVODRDemo	51 seconds	idle	snapmirrored	May 6, 2022, 11:03:15 AM 785.8 MiB

5. Starten Sie den MSSQL-Serverdienst neu.
6. Vergewissern Sie sich, dass die SQL-Ressourcen wieder online sind.



Für ein Failback auf den primären Storage sollten Sie sicherstellen, dass die Beziehungsrichtung vor dem Failover unverändert bleibt, indem Sie einen umgekehrten Resynchronisierungsvorgang durchführen.



Um die Rollen des primären und sekundären Storage nach der umgekehrten Resynchronisierung beizubehalten, führen Sie den umgekehrten Resync-Vorgang erneut aus.

Dieser Prozess gilt für andere Applikationen wie Oracle, ähnliche Datenbankumgebungen und andere Applikationen, die mit Gast-vernetztem Storage verwenden.

Testen Sie wie immer die Schritte zur Wiederherstellung der kritischen Workloads, bevor Sie sie in die Produktionsumgebung portieren.

Vorteile dieser Lösung

- Nutzt die effiziente und ausfallsichere Replizierung von SnapMirror
- Wiederherstellung zu beliebigen verfügbaren Zeitpunkten mit ONTAP Snapshot Aufbewahrung
- Eine vollständige Automatisierung steht für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs zur Verfügung – von den Schritten für Storage, Computing, Netzwerk und Applikationen.
- SnapCenter nutzt Klonmechanismen, die das replizierte Volume nicht ändern.
 - So wird das Risiko einer Beschädigung von Daten von Volumes und Snapshots vermieden.

- Keine Replizierungsunterbrechungen während der DR-Test-Workflows
- Nutzung der DR-Daten für Workflows über DR hinaus, wie Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Korrekturtests
- CPU- und RAM-Optimierung können die Cloud-Kosten senken, indem Recovery auf kleinere Computing-Cluster ermöglicht wird.

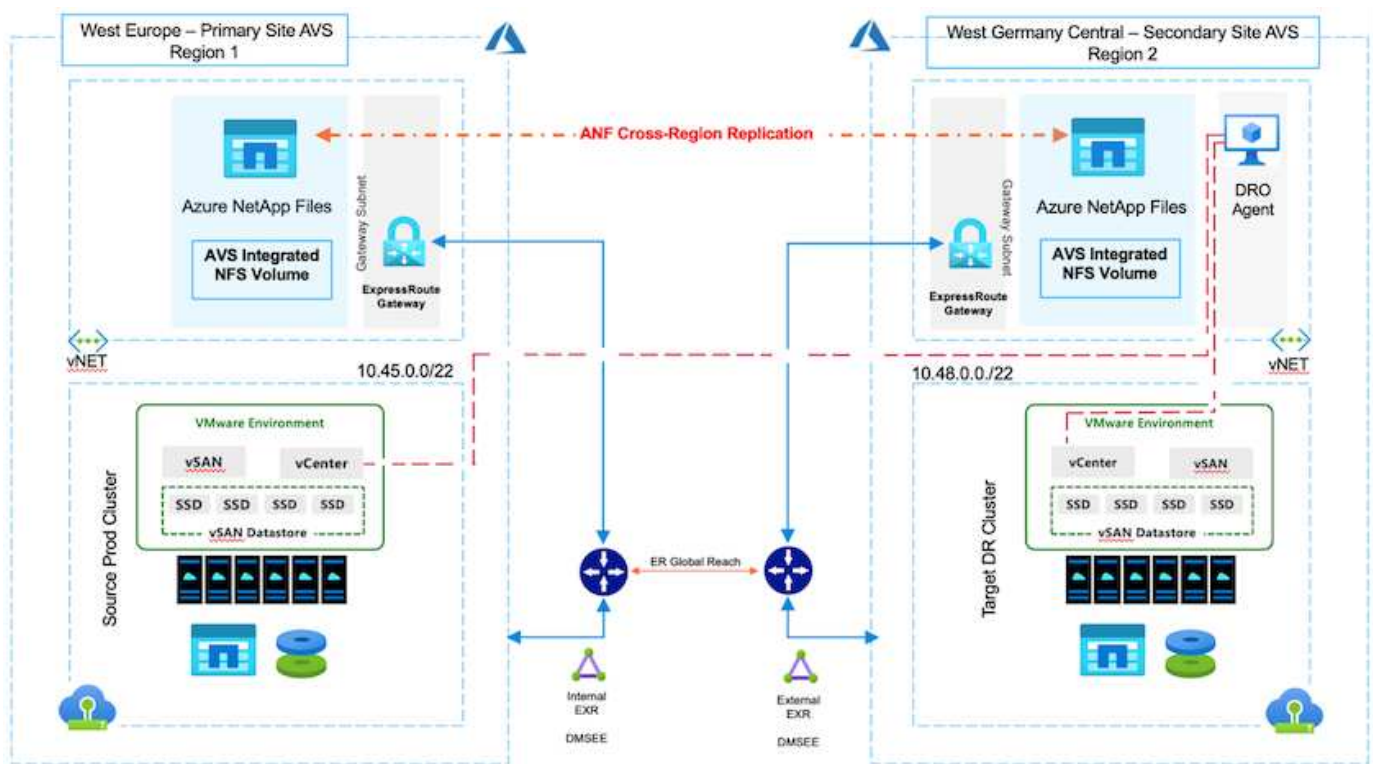
TR-4955: Disaster Recovery with Azure NetApp Files (ANF) and Azure VMware Solution (AVS)

Autor(en): Niyaz Mohamed, NetApp Solutions Engineering

Überblick

Disaster Recovery mit Replizierung auf Blockebene zwischen Regionen in der Cloud ist eine ausfallsichere und kostengünstige Möglichkeit, um Workloads vor Standortausfällen und Datenbeschädigung (z. B. Ransomware) zu schützen. Mit der regionsübergreifenden Volume-Replizierung über Azure NetApp Files (ANF) können VMware-Workloads, die auf einem AVS-Standort (Azure VMware Solution) mit Azure NetApp Files Volumes als NFS-Datstore auf dem primären AVS-Standort ausgeführt werden, auf einen designierten sekundären AVS-Standort in der Zielwiederherstellungsregion repliziert werden.

Disaster Recovery Orchestrator (DRO) (eine skriptbasierte Lösung mit einer Benutzeroberfläche) kann verwendet werden, um Workloads, die von einem AVS-SDDC zum anderen repliziert werden, nahtlos wiederherzustellen. DRO automatisiert die Recovery, indem Replikations-Peering gebrochen und das Ziel-Volume dann als Datstore gemountet wird. Dies geschieht durch VM-Registrierung in AVS, um Netzwerkzuordnungen direkt auf NSX-T (in allen AVS Private Clouds enthalten) zu ermöglichen.



Voraussetzungen und allgemeine Empfehlungen

- Vergewissern Sie sich, dass Sie die regionsübergreifende Replikation aktiviert haben, indem Sie Replikations-Peering erstellen. Siehe "[Volume-Replizierung für Azure NetApp Files erstellen](#)".
- Sie müssen ExpressRoute Global Reach zwischen den Private Clouds der Quell- und Ziellösung von Azure VMware konfigurieren.
- Sie müssen über einen Dienstprinzipal verfügen, der auf Ressourcen zugreifen kann.
- Die folgende Topologie wird unterstützt: Primärer AVS-Standort zum sekundären AVS-Standort.
- Konfigurieren Sie die "[Replizierung](#)" Planen Sie für jedes Volume entsprechend den Geschäftsanforderungen und der Datenänderungsrate ein.



Kaskadierung und Fan-in- und Fan-out-Topologien werden nicht unterstützt.

Erste Schritte

Implementieren Sie die Azure-VMware-Lösung

Der "[Azure VMware Lösung](#)" (AVS) ist ein Hybrid-Cloud-Service mit voll funktionsfähigen VMware SDDCs in einer Microsoft Azure Public Cloud. AVS ist eine Lösung eines Erstanbieters, die vollständig von Microsoft verwaltet und unterstützt wird und von VMware überprüft wurde, die eine Azure-Infrastruktur nutzt. Daher erhalten Kunden VMware ESXi für die Compute-Virtualisierung, vSAN für hyperkonvergenten Storage und NSX für Netzwerk und Sicherheit. Gleichzeitig profitieren sie von der globalen Präsenz und den erstklassigen Datacenter-Einrichtungen von Microsoft Azure sowie der Nähe zum umfassenden Ecosystem nativer Azure-Services und -Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Performance bei minimaler Netzwerklatenz.

Gehen Sie wie folgt vor, um eine AVS Private Cloud auf Azure zu konfigurieren "[Verlinken](#)" Zu NetApp-Dokumentation und in diesem "[Verlinken](#)" Für Microsoft-Dokumentation. Für DR-Zwecke kann eine Pilotumgebung mit minimaler Konfiguration verwendet werden. Dieses Setup enthält nur Kernkomponenten zur Unterstützung kritischer Applikationen. Es kann horizontal skalierbar sein und weitere Hosts aufbauen, um den Großteil der Auslastung bei einem Failover zu übernehmen.



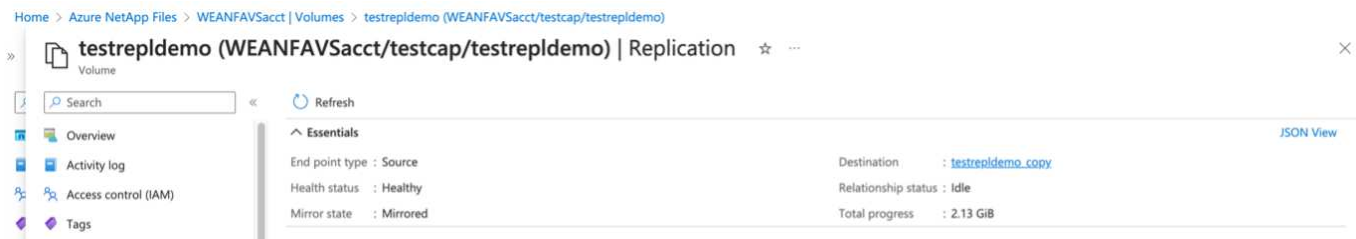
In der ersten Version unterstützt DRO einen vorhandenen AVS SDDC-Cluster. Die Erstellung eines On-Demand SDDC wird in einer kommenden Version verfügbar sein.

Bereitstellung und Konfiguration von Azure NetApp Files

"[Azure NetApp Dateien](#)" Der hochperformante gemessene File-Storage-Service der Enterprise-Klasse. Befolgen Sie die hier beschriebenen Schritte "[Verlinken](#)" Die Bereitstellung und Konfiguration von Azure NetApp Files als NFS-Datastore zur Optimierung von AVS Private-Cloud-Implementierungen.

Volume-Replizierung für Datastore-Volumes mit Azure NetApp Files erstellen

Der erste Schritt besteht darin, regionsübergreifende Replikation für die gewünschten Datastore Volumes vom primären AVS-Standort zum sekundären AVS-Standort mit den entsprechenden Frequenzen und Aufbewahrungen einzurichten.



Befolgen Sie die hier beschriebenen Schritte ["Verlinken"](#) Zur Einrichtung einer regionsübergreifenden Replikation durch Erstellen von Replikations-Peering. Das Service-Level für den Zielkapazitätspool kann mit dem des Quell-Kapazitäts-Pools übereinstimmen. Für diesen speziellen Anwendungsfall können Sie jedoch das Standard-Service-Level und dann auswählen ["Ändern Sie den Service-Level"](#) Im Falle einer echten Katastrophe oder DR-Simulationen.



Eine regionsübergreifende Replikationsbeziehung ist Voraussetzung und muss zuvor erstellt werden.

DRO-Installation

Um mit DRO zu beginnen, verwenden Sie das Ubuntu-Betriebssystem auf der zugewiesenen virtuellen Azure-Maschine und stellen Sie sicher, dass Sie die Voraussetzungen erfüllen. Installieren Sie dann das Paket.

Voraussetzungen:

- Dienstprinzipal, das auf Ressourcen zugreifen kann.
- Stellen Sie sicher, dass entsprechende Konnektivität mit den SDDC Quell- und Ziel-Instanzen und den Azure NetApp Files Instanzen besteht.
- DNS-Auflösung sollte vorhanden sein, wenn Sie DNS-Namen verwenden. Verwenden Sie andernfalls die IP-Adressen für vCenter.

OS-Anforderungen:

- Ubuntu Focal 20.04 (LTS) die folgenden Pakete müssen auf der zugewiesenen virtuellen Agent-Maschine installiert werden:
- Docker
- Docker – Komposition
- JqChange `docker.sock` Zu dieser neuen Berechtigung: `sudo chmod 666 /var/run/docker.sock`.



Der `deploy.sh` Skript führt alle erforderlichen Voraussetzungen aus.

Dies sind die Schritte:

1. Laden Sie das Installationspaket auf der angegebenen virtuellen Maschine herunter:

```
git clone https://github.com/NetApp/DRO-Azure.git
```



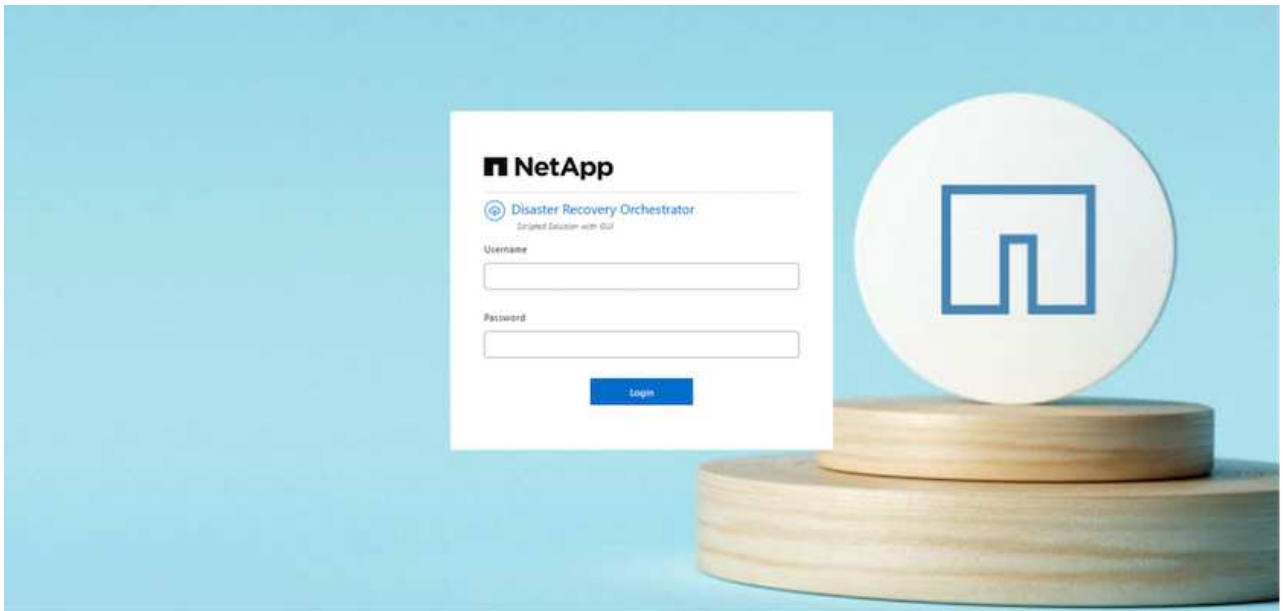
Der Agent muss in der sekundären AVS-Standortregion oder in der primären AVS-Standortregion in einer separaten AZ als dem SDDC installiert werden.

2. Entpacken Sie das Paket, führen Sie das Bereitstellungsskript aus, und geben Sie die Host-IP ein (z. B. 10.10.10.10).

```
tar xvf draas_package.tar
Navigate to the directory and run the deploy script as below:
sudo sh deploy.sh
```

3. Greifen Sie mit den folgenden Anmeldedaten auf die UI zu:

- **Benutzername:** admin
- **Kennwort:** admin



DRO-Konfiguration

Nachdem Azure NetApp Files und AVS ordnungsgemäß konfiguriert wurden, können Sie mit der Konfiguration von DRO beginnen, um die Wiederherstellung von Workloads vom primären AVS-Standort zum sekundären AVS-Standort zu automatisieren. NetApp empfiehlt, den DRO-Agent am sekundären AVS-Standort bereitzustellen und die ExpressRoute Gateway-Verbindung zu konfigurieren, damit der DRO-Agent über das Netzwerk mit den entsprechenden AVS- und Azure NetApp Files-Komponenten kommunizieren kann.

Der erste Schritt besteht darin, Anmeldeinformationen hinzuzufügen. FÜR DIE Erkennung von Azure NetApp Files und der Azure VMware-Lösung ist DIE DRO-Berechtigung erforderlich. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Azure Active Directory (AD)-Anwendung erstellen und einrichten und die Azure-Anmeldeinformationen erhalten, die DRO benötigt. Sie müssen den Service-Prinzipal an Ihr Azure-Abonnement binden und ihm eine benutzerdefinierte Rolle zuweisen, die über die entsprechenden erforderlichen Berechtigungen verfügt. Wenn Sie Quell- und Zielumgebungen hinzufügen, werden Sie aufgefordert, die Anmeldeinformationen auszuwählen, die dem Dienstprinzipal zugeordnet sind. Sie müssen diese Anmeldeinformationen zu DRO hinzufügen, bevor Sie auf Neuen Standort hinzufügen klicken können.

Um diesen Vorgang auszuführen, führen Sie die folgenden Schritte aus:

1. Öffnen Sie DRO in einem unterstützten Browser und verwenden Sie den Standardbenutzernamen und das Standardpasswort (/admin/admin). Das Passwort kann nach der ersten Anmeldung mit der Option Passwort ändern zurückgesetzt werden.
2. Klicken Sie oben rechts auf der DRO-Konsole auf das Symbol **Einstellungen** und wählen Sie **Anmeldeinformationen** aus.
3. Klicken Sie auf Neue Anmeldedaten hinzufügen, und befolgen Sie die Schritte im Assistenten.
4. Geben Sie zum Definieren der Anmeldeinformationen Informationen über den Azure Active Directory-Dienstprinzipal ein, der die erforderlichen Berechtigungen gewährt:
 - Name der Anmeldeinformationen
 - Mandanten-ID
 - Client-ID
 - Kundengeheimnis
 - Abonnement-ID

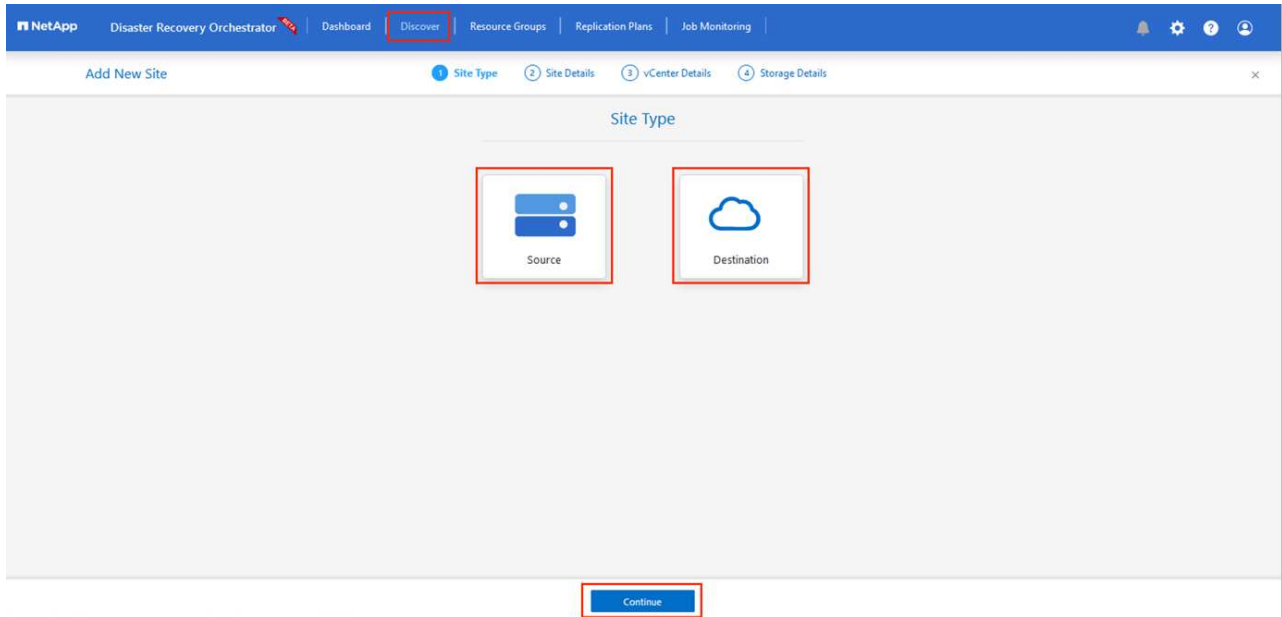
Sie sollten diese Informationen bei der Erstellung der AD-Anwendung erfasst haben.

5. Bestätigen Sie die Details zu den neuen Anmeldeinformationen, und klicken Sie auf Credential hinzufügen.

Nachdem Sie die Anmeldedaten hinzugefügt haben, wird es Zeit, den primären und sekundären AVS-Standort (sowohl vCenter als auch das Azure NetApp Files-Speicherkonto) zu ermitteln und zu DRO hinzuzufügen. Gehen Sie wie folgt vor, um den Quell- und Zielstandort hinzuzufügen:

6. Gehen Sie auf die Registerkarte **Entdecken**.
7. Klicken Sie Auf **Neue Site Hinzufügen**.
8. Fügen Sie den folgenden primären AVS-Standort hinzu (in der Konsole als **Quelle** bezeichnet).
 - SDDC vCenter
 - Azure NetApp Files Storage Konto
9. Fügen Sie den folgenden sekundären AVS-Standort hinzu (in der Konsole als **Ziel** bezeichnet).

- SDDC vCenter
- Azure NetApp Files Storage Konto



10. Fügen Sie Standortdetails hinzu, indem Sie auf **Quelle** klicken und einen freundlichen Standortnamen eingeben und den Konnektor auswählen. Klicken Sie dann auf **Weiter**.



Das Hinzufügen einer Quellwebsite wird zu Demonstrationszwecken in diesem Dokument behandelt.

11. Aktualisieren Sie die vCenter-Details. Wählen Sie dazu die Anmeldedaten, die Azure-Region und die Ressourcengruppe aus der Dropdown-Liste für das primäre AVS-SDDC aus.
12. DRO listet alle verfügbaren SDDCs innerhalb der Region auf. Wählen Sie die entsprechende Private-Cloud-URL aus der Dropdown-Liste aus.
13. Geben Sie das ein `cloudadmin@vsphere.local` Benutzeranmeldeinformationen. Auf diese kann über das Azure-Portal zugegriffen werden. Befolgen Sie die hier beschriebenen Schritte "[Verlinken](#)". Klicken Sie anschließend auf **Weiter**.

14. Wählen Sie die Details zum Quell-Storage (ANF) aus, indem Sie die Azure Ressourcengruppe und das NetApp Konto auswählen.
15. Klicken Sie Auf **Site Erstellen**.

Site Name	Site Type	Location	vCenter	Storage	VM List	Discovery Status
DemoDest	Destination	Cloud	1	1		• https://10.75.0.2/ Success
DemoSRC	Source	Cloud	1	1	View VM List	• https://172.30.156.2/ Success

Nach dem Hinzufügen führt DRO eine automatische Erkennung durch und zeigt die VMs an, die entsprechende regionsübergreifende Replikate vom Quellstandort zum Zielstandort haben. DRO erkennt automatisch die Netzwerke und Segmente, die von den VMs verwendet werden, und füllt diese aus.

Back

VM List

Site: DemoSRC | vCenter: https://172.30.156.2/

7 Datastores

128 Virtual Machines

VM Protection: 2 Protected, 126 Unprotected

VM Name	VM Status	VM State	DataStore	CPU	Memory (MB)
HCLBench_2.5.1	Not Protected	Powered On	vsanDatastore	8	8192
hcl-fio-datastore-13984-0-1	Not Protected	Powered Off	HCLxtDS	32	65536
ICCAu005-WO-R1	Not Protected	Powered On	vsanDatastore	8	14336
ICCAu005-HE-R1	Not Protected	Powered On	vsanDatastore	8	3072
ICCAu005-OL-R1	Not Protected	Powered On	vsanDatastore	8	3072
HCL_Demo_05	Not Protected	Powered Off	Demo002	1	2048
hcl-nim-datastore-13984-0-1	Not Protected	Powered Off	HCLxtDS	24	49152

Im nächsten Schritt werden die erforderlichen VMs als Ressourcengruppen in ihre funktionalen Gruppen gruppiert.

Ressourcen-Gruppierungen

Nachdem die Plattformen hinzugefügt wurden, gruppieren Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen. MIT DRO-Ressourcengruppen können Sie eine Gruppe abhängiger VMs zu logischen Gruppen gruppieren, die ihre Boot-Aufträge, Boot-Verzögerungen und optionale Applikationsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

Um Ressourcengruppen zu erstellen, klicken Sie auf den Menüpunkt **Neue Ressourcengruppe erstellen**.

1. Greifen Sie auf **Resource Groups** zu und klicken Sie auf ***Neue Ressourcengruppe erstellen**.

1 Resource Group

1 Site

1 vCenter

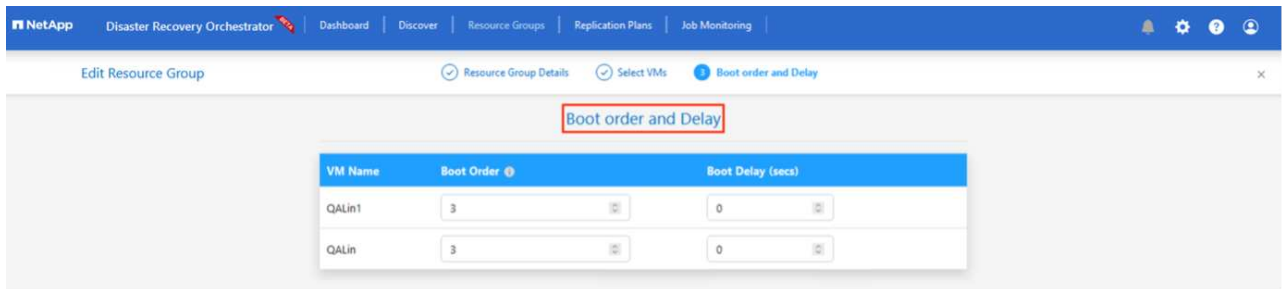
2 Virtual Machines

Resource Group Name	Site Name	Source vCenter	VM List
DemoRG	DemoSRC	https://172.30.156.2/	

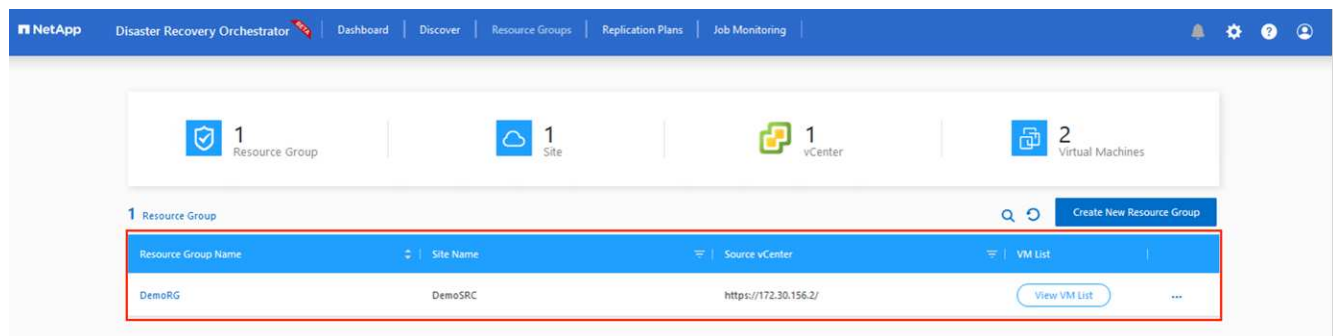
Create New Resource Group

2. Wählen Sie unter Neue Ressourcengruppe den Quellstandort aus dem Dropdown-Menü aus und klicken Sie auf **Erstellen**.
3. Geben Sie die Details der Ressourcengruppe ein und klicken Sie auf **Weiter**.
4. Wählen Sie über die Suchoption die entsprechenden VMs aus.
5. Wählen Sie für alle ausgewählten VMs die Optionen **Boot Order** und **Boot Delay** (s) aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede virtuelle Maschine auswählen und die Priorität für sie festlegen. Der Standardwert für alle virtuellen Maschinen ist 3. Folgende Optionen stehen zur Verfügung:

- Die erste virtuelle Maschine, die eingeschaltet wird
- Standard
- Die letzte virtuelle Maschine, die eingeschaltet werden muss



6. Klicken Sie Auf **Ressourcengruppe Erstellen**.

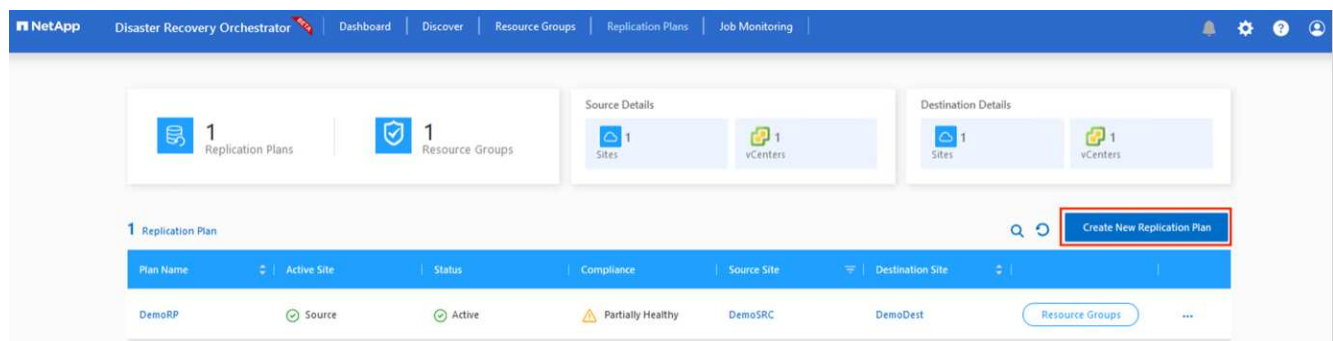


Replizierungspläne

Die Wiederherstellung von Applikationen im K-Fall ist unverzichtbar. Wählen Sie in der Dropdown-Liste die Quell- und Ziel-vCenter-Plattformen aus und wählen Sie die Ressourcengruppen aus, die in diesen Plan aufgenommen werden sollen. Außerdem berücksichtigen Sie die Gruppierung der wiederherzustellenden und hochzusteuenden Applikationen (z. B. Domain Controller, Tier-1, Tier-2 usw.). Pläne werden oft auch Blaupausen genannt. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte Replikationsplan und klicken Sie auf **Neuer Replikationsplan**.

Gehen Sie wie folgt vor, um mit der Erstellung eines Replikationsplans zu beginnen:

1. Navigieren Sie zu **Replikationspläne** und klicken Sie auf **Neuen Replikationsplan erstellen**.



2. Geben Sie im **New Replication Plan** einen Namen für den Plan ein und fügen Sie Wiederherstellungszuordnungen hinzu, indem Sie den Quellstandort, das zugehörige vCenter, den Zielstandort und das zugehörige vCenter auswählen.

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name: DemoRP

Recovery Mapping

Source Site: DemoSRC | Destination Site: DemoDest

Source vCenter: https://172.30.156.2/ | Destination vCenter: https://10.75.0.2/

Cluster Mapping

Source Site Resource: Cluster-1 | Destination Site Resource: Cluster-1 | Add

Source Resource	Destination Resource
No Mappings added!	

Continue

- Nachdem die Wiederherstellungszuordnung abgeschlossen ist, wählen Sie die Option **Cluster Mapping** aus.

NetApp Disaster Recovery Orchestrator | Dashboard | Discover | Resource Groups | Replication Plans | Job Monitoring

Create New Replication Plan | 1 Replication Plan and Site Details | 2 Select Resource Groups | 3 Set Execution Order | 4 Set VM Details

Replication Plan Details

Plan Name: DemoRP

Recovery Mapping

Source Site: DemoSRC | Destination Site: DemoDest

Source vCenter: https://172.30.156.2/ | Destination vCenter: https://10.75.0.2/

Cluster Mapping

No more Source/Destination cluster resources available for mapping

Source Resource	Destination Resource
Cluster-1	Cluster-1 Delete

Continue

- Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
- Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
- Stellen Sie anschließend die Netzwerkzuordnung auf das entsprechende Segment ein. Die Segmente sollten bereits auf dem sekundären AVS-Cluster bereitgestellt werden. Um die VMs diesen zuzuordnen, wählen Sie das entsprechende Segment aus.
- Aufgrund der Auswahl der VMs werden automatisch Datastore-Zuordnungen ausgewählt.



Die regionsübergreifende Replikation (CRR) befindet sich auf Volume-Ebene. Daher werden alle VMs auf dem jeweiligen Volume auf das CRR-Ziel repliziert. Stellen Sie sicher, dass alle VMs ausgewählt werden, die Teil des Datenspeichers sind, da nur virtuelle Maschinen verarbeitet werden, die Teil des Replikationsplans sind.

Resource Group Name	Execution Order
DemoRG	3

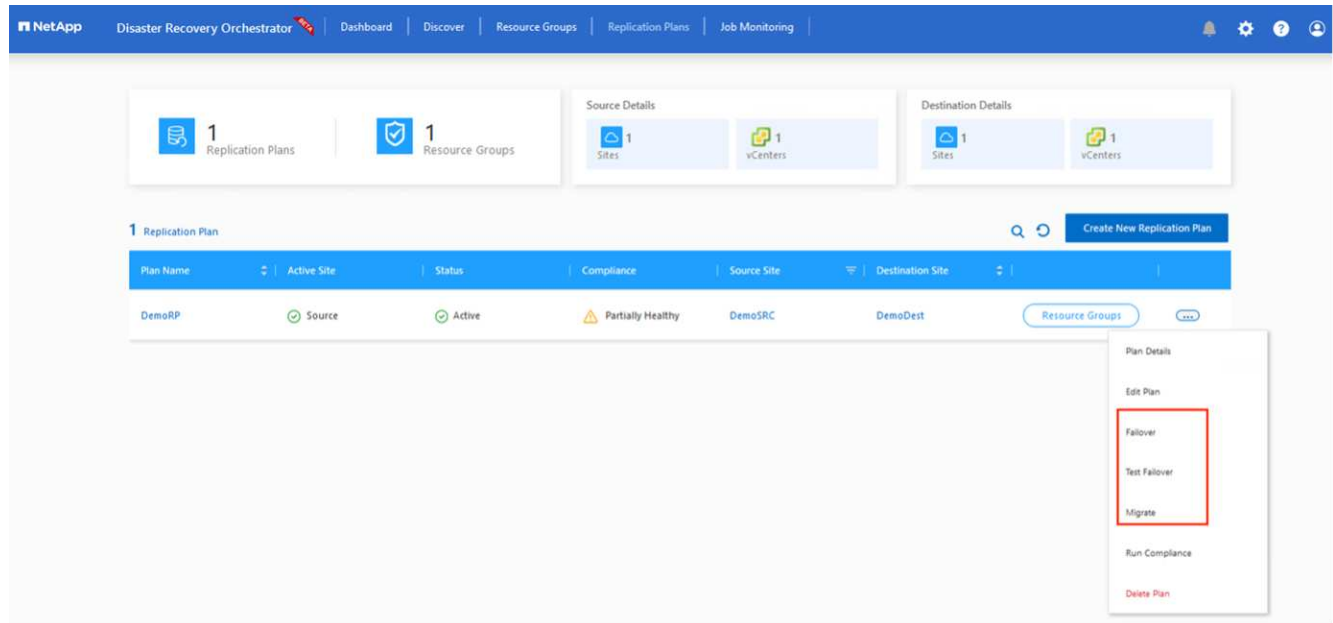
Source Resource	Destination Resource
SepSeg	SegDR

Source DataStore	Destination Volume
TestSrc01	gwc_ntap_acct/gwc_DRO_cp/testsrc01.copy

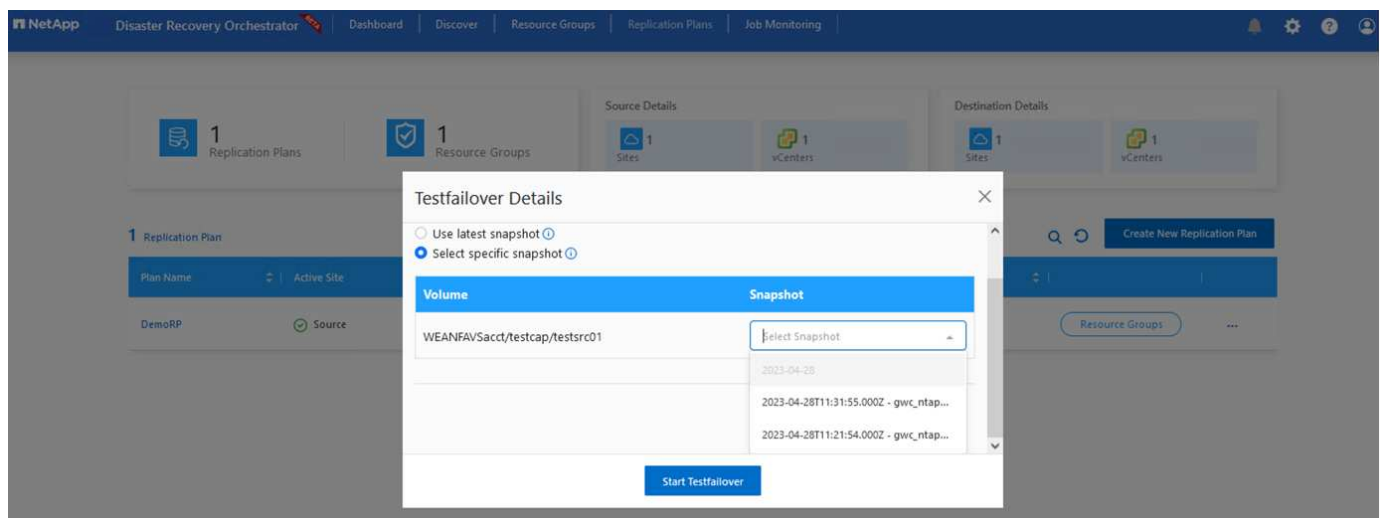
8. Unter VM-Details können Sie optional die Größe der CPU- und RAM-Parameter der VMs ändern. Das ist vor allem hilfreich, wenn Sie große Umgebungen auf kleinere Ziel-Cluster wiederherstellen oder DR-Tests durchführen, ohne eine 1:1-physische VMware-Infrastruktur bereitstellen zu müssen. Ändern Sie außerdem die Startreihenfolge und die Startverzögerung (s) für alle ausgewählten VMs in den Ressourcengruppen. Es gibt eine zusätzliche Option, um die Startreihenfolge zu ändern, wenn Änderungen an den Änderungen erforderlich sind, die Sie bei der Auswahl des Ressource- Gruppe- Startauftrags ausgewählt haben. Standardmäßig wird die während der Auswahl der Ressourcengruppe ausgewählte Startreihenfolge verwendet. Änderungen können jedoch in dieser Phase vorgenommen werden.

VM Name	No. of CPUs	Memory (MB)	NIC/IP	Boot Order
QALin1	1	1024	Dynamic	3
QALin	4	1024	Dynamic	3

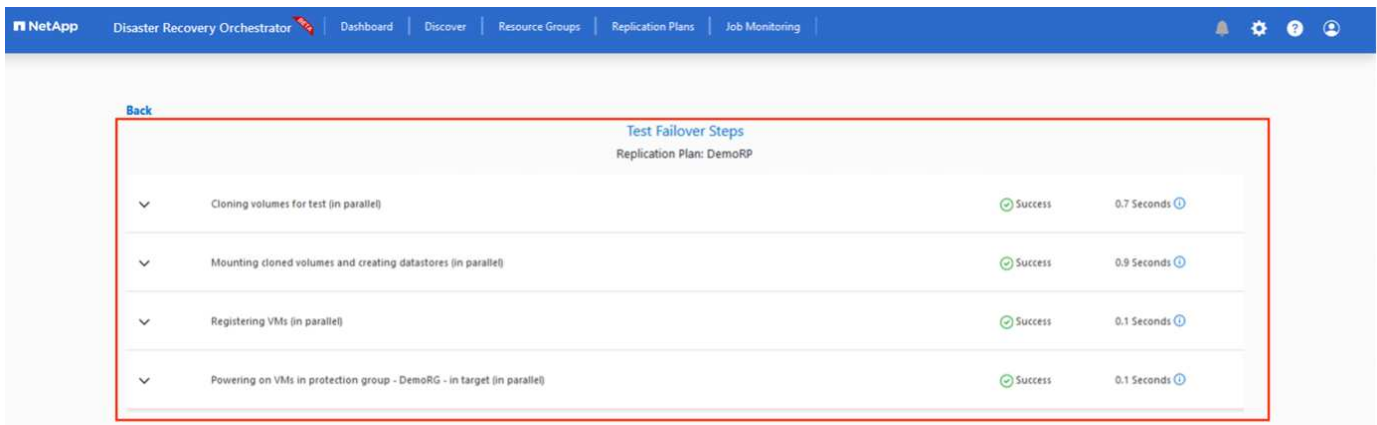
9. Klicken Sie auf **Create Replication Plan**. Nachdem der Replikationsplan erstellt wurde, können Sie die Failover-, Test-Failover- oder Migrationsoptionen je nach Ihren Anforderungen ausführen.



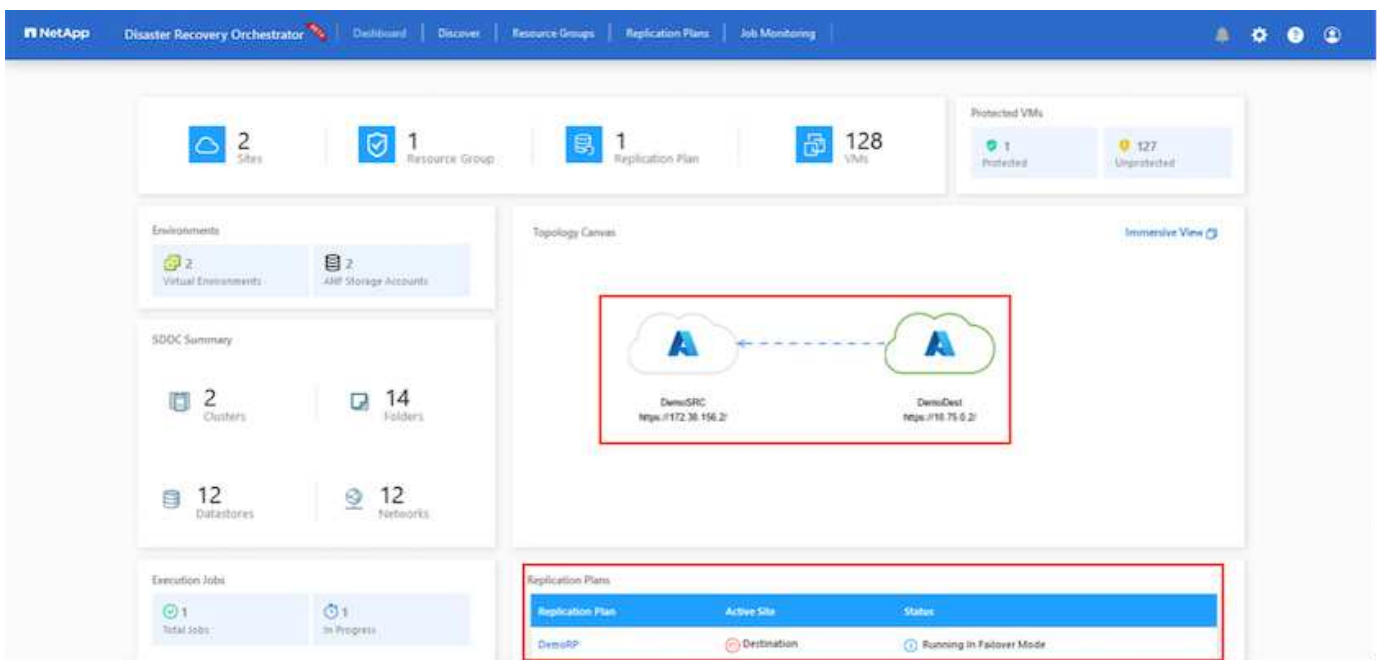
Während der Failover- und Test-Failover-Optionen wird der aktuellste Snapshot verwendet, oder ein bestimmter Snapshot kann aus einem Point-in-Time-Snapshot ausgewählt werden. Die Point-in-Time-Option kann sehr vorteilhaft sein, wenn Sie vor einem Korruptionsereignis wie Ransomware stehen, wo die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Zeitpunkte an.



Um Failover oder Test Failover mit der im Replikationsplan angegebenen Konfiguration auszulösen, können Sie auf **Failover** oder **Test Failover** klicken. Sie können den Replikationsplan im Aufgabenmenü überwachen.



Nachdem der Failover ausgelöst wurde, können die wiederhergestellten Objekte im sekundären Standort AVS SDDC vCenter (VMs, Netzwerke und Datastores) erkannt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.



Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Im Falle eines Test-Failovers kann die Option zum Abreißen verwendet werden, um die Änderungen rückgängig zu machen und das neu erstellte Volume zu entfernen. Failbacks im Zusammenhang mit Failover sind ein zweistufiger Prozess. Wählen Sie den Replikationsplan aus und wählen Sie **Reverse Data Sync** aus.

The screenshot shows the NetApp Disaster Recovery Orchestrator interface. At the top, there's a navigation bar with 'Dashboard', 'Discover', 'Resource Groups', 'Replication Plans', and 'Job Monitoring'. Below this, there are summary cards for '1 Replication Plans' and '1 Resource Groups'. The main section displays a table for '1 Replication Plan' with columns: Plan Name, Active Site, Status, Compliance, Source Site, and Destination Site. The 'DemoRP' plan is highlighted, showing it is 'Running in Failover Mode' and 'Healthy'. A 'Resource Groups' button is visible, and a dropdown menu shows options like 'Plan Details', 'Reverse Data Sync', and 'Failback'.

Wenn dieser Schritt abgeschlossen ist, führen Sie ein Failback aus, um zum primären AVS-Standort zurückzukehren.

This screenshot shows the same interface as before, but the 'DemoRP' plan's status has changed to 'Active'. The 'Reverse Data Sync' option in the dropdown menu is now highlighted, indicating the next step in the process.

The screenshot displays a more detailed view of the system. It includes summary cards for '2 Sites', '1 Resource Group', '1 Replication Plan', and '128 VMs'. A 'Topology Canvas' shows a diagram with two nodes, 'DemoSRC' and 'DemoDest', connected by a bidirectional arrow. Below this, a table for 'Replication Plans' shows 'DemoRP' with 'Source' as the active site and 'Active' status. Other sections include 'Environments' (Virtual Environments, ATP Storage Accounts), 'SDDC Summary' (Clusters, Folders, Datastores, Networks), and 'Execution Jobs' (Total Jobs, In Progress).

Über das Azure-Portal können wir sehen, dass der Zustand der Replizierung für die entsprechenden Volumes unterbrochen wurde, die dem AVS SDDC am sekundären Standort als Lese-/Schreib-Volumes zugeordnet

wurden. Beim Test-Failover weist DRO nicht das Ziel- oder Replikatvolume zu. Stattdessen wird ein neues Volume des erforderlichen regionsübergreifenden Replikations-Snapshots erstellt und das Volume als Datenspeicher bereitgestellt, wodurch zusätzliche physische Kapazität aus dem Kapazitäts-Pool verbraucht wird und sichergestellt wird, dass das Quell-Volume nicht geändert wird. Bemerkenswert ist, dass Replizierungsjobs während DR-Tests oder Triage Workflows fortgesetzt werden können. Darüber hinaus stellt dieser Prozess sicher, dass die Wiederherstellung bereinigt werden kann, ohne dass das Risiko besteht, dass das Replikat zerstört wird, wenn Fehler auftreten oder beschädigte Daten wiederhergestellt werden.

Recovery durch Ransomware

Die Wiederherstellung von Ransomware kann eine gewaltige Aufgabe sein. Insbesondere KANN es für IT-Abteilungen schwierig sein, den sicheren Rückgabepunkt zu bestimmen und, sobald dies festgelegt ist, zu gewährleisten, dass wiederhergestellte Workloads vor den wiederholten Angriffen geschützt werden (zum Beispiel vor dem Einschlagen von Malware oder durch anfällige Anwendungen).

DRO löst diese Probleme, indem es Unternehmen ermöglicht, Wiederherstellungen von beliebigen Zeitpunkten aus durchzuführen. Die Workloads werden dann in funktionsfähigen, aber isolierten Netzwerken wiederhergestellt, sodass Applikationen zwar funktionieren und miteinander kommunizieren können, aber keinem Nord-/Süd-Datenverkehr ausgesetzt sind. Dieser Prozess bietet Sicherheitsteams einen sicheren Ort, um forensische Analysen durchzuführen und versteckte oder schlafende Malware zu identifizieren.

Schlussfolgerung

Die Disaster-Recovery-Lösung Azure NetApp Files und Azure VMware bietet folgende Vorteile:

- Effiziente und ausfallsichere regionsübergreifende Azure NetApp Files Replizierung
- Recovery zu einem beliebigen verfügbaren Point-in-Time mit Snapshot-Aufbewahrung.
- Automatisieren Sie alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden VMs aus den Validierungsschritten für Storage, Compute, Netzwerk und Applikationen.
- Workload Recovery nutzt den Prozess „Erstellung neuer Volumes aus den neuesten Snapshots“, der das replizierte Volume nicht manipuliert.
- Vermeiden Sie das Risiko der Datenbeschädigung auf den Volumes oder Snapshots.
- Keine Replizierungsunterbrechungen während DR-Test-Workflows
- Nutzen Sie DR-Daten und Cloud-Computing-Ressourcen für Workflows, die über DR hinausgehen, wie z. B. Entwicklungs-/Test, Sicherheitstests, Patch- und Upgrade-Tests oder Fehlerbehebungstests.
- Die CPU- und RAM-Optimierung kann dazu beitragen, Cloud-Kosten zu senken, indem eine Recovery auf kleinere Compute-Cluster ermöglicht wird.

Wo Sie weitere Informationen finden

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

- Volume-Replizierung für Azure NetApp Files erstellen

["https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering"](https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-create-peering)

- Regionsübergreifende Replizierung von Azure NetApp Files Volumes

["https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives"](https://learn.microsoft.com/en-us/azure/azure-netapp-files/cross-region-replication-introduction#service-level-objectives)

- "Azure VMware Lösung"

["https://learn.microsoft.com/en-us/azure/azure-vmware/introduction"](https://learn.microsoft.com/en-us/azure/azure-vmware/introduction)

- Implementieren und Konfigurieren der Virtualisierungsumgebung auf Azure

["https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html"](https://docs.netapp.com/us-en/netapp-solutions/ehc/azure-setup.html)

- Implementierung und Konfiguration der Azure-VMware-Lösung

<https://learn.microsoft.com/en-us/azure/azure-vmware/deploy-azure-vmware-solution?tabs=azure-portal>

Verwenden von Veeam Replizierung und Azure NetApp Files-Datstore für die Disaster Recovery zu Azure VMware-Lösung

Autor: Niyaz Mohamed - NetApp Solutions Engineering

Überblick

Azure NetApp Files Datastores (ANF) entkoppeln Storage von Computing und ermöglichen jedem Unternehmen die erforderliche Flexibilität, um Workloads in die Cloud zu verlagern. Sie bietet eine flexible, hochperformante Storage-Infrastruktur, die unabhängig von den Compute-Ressourcen skaliert werden kann. Azure NetApp Files Datastore vereinfacht und optimiert die Implementierung zusammen mit der Azure VMware Lösung (AVS) als Disaster-Recovery-Standort für lokale VMware Umgebungen.

Mit Volume-basierten Azure NetApp Files (ANF) NFS-Datstores können Daten mit jeder validierten Drittanbieterlösung, die VM-Replizierungsfunktionen bietet, aus On-Premises-Systemen repliziert werden. Durch das Hinzufügen von Azure NetApp Files-Datenspeichern kann eine kostenoptimierte Implementierung durchgeführt werden, anstatt eine SDDC-Lösung für Azure VMware mit einer enormen Anzahl an ESXi-Hosts für den Storage einzurichten. Dieser Ansatz wird als „Pilot Light Cluster“ bezeichnet. Ein Pilot-Light-Cluster ist eine minimale AVS-Hostkonfiguration (3 AVS-Knoten) zusammen mit der Kapazität des Azure NetApp Files-Datenspeichers.

Ziel ist es, eine kostengünstige Infrastruktur mit allen Kernkomponenten für ein Failover zu erhalten. Ein Pilot-Light-Cluster kann horizontal skalieren und im Falle eines Failovers weitere AVS-Hosts bereitstellen. Sobald der Failover abgeschlossen und der normale Betrieb wiederhergestellt ist, kann das Pilot Light-Cluster wieder auf den kostengünstigen Betriebsmodus zurückskaliert werden.

Zweck dieses Dokuments

In diesem Artikel wird beschrieben, wie Sie Azure NetApp Files mit Veeam Backup and Replication die Disaster Recovery für lokale VMware-VMs auf (AVS) mithilfe der Veeam VM-Replizierungssoftware einrichten.

Veeam Backup & Replication ist eine Backup- und Replizierungsapplikation für virtuelle Umgebungen. Wenn virtuelle Maschinen repliziert werden, wird Veeam Backup & Replication von auf AVS repliziert, erstellt die Software eine exakte Kopie der VMs im nativen VMware vSphere-Format auf dem Ziel-AVS SDDC-Cluster. Veeam Backup & Replication hält die Kopie mit der ursprünglichen VM synchron. Die Replizierung bietet die beste Recovery Time Objective (RTO), da am DR-Standort eine gemountete Kopie einer VM in einem startfähigen Zustand ist.

Dieser Replizierungsmechanismus sorgt dafür, dass die Workloads bei einem Notfall schnell in einem AVS

SDDC gestartet werden können. Die Veeam Backup & Replication Software optimiert darüber hinaus die Datenübertragung zur Replizierung über WAN und für langsame Verbindungen. Außerdem werden doppelte Datenblöcke, keine Datenblöcke, Swap-Dateien und „ausgeschlossene VM Gast-OS-Dateien“ herausgefiltert. Die Software komprimiert auch den Replikatverkehr. Um zu verhindern, dass Replikationsjobs die gesamte Netzwerkbandbreite verbrauchen, können WAN-Beschleuniger und Regeln zur Netzwerkdrosselung verwendet werden.

Der Replizierungsprozess in Veeam Backup & Replication ist auftragsgesteuert, d. h. die Replizierung wird durch Konfiguration von Replizierungsjobs durchgeführt. Bei einem Ausfall kann ein Failover zur Wiederherstellung der VMs durch einen Failover auf die Replikatkopie ausgelöst werden. Wenn ein Failover durchgeführt wird, übernimmt eine replizierte VM die Rolle der ursprünglichen VM. Ein Failover kann auf den neuesten Status eines Replikats oder auf einen der bekannten Wiederherstellungspunkte erfolgen. Dies ermöglicht bei Bedarf eine Wiederherstellung nach Ransomware-Angriffen oder isolierte Tests. Veeam Backup & Replication bietet mehrere Optionen für unterschiedliche Disaster-Recovery-Szenarien.

□

Lösungsimplementierung

Übergeordnete Schritte

1. Die Veeam Backup & Replication-Software wird in einer On-Premises-Umgebung mit entsprechender Netzwerkverbindung ausgeführt.
2. ["Implementieren der Azure-VMware-Lösung \(AVS\)"](#) Private Cloud und ["Verbinden Sie Azure NetApp Files-Datstores"](#) Auf Hosts der Azure-VMware-Lösung.

Für DR-Zwecke kann eine Pilot-Light-Umgebung mit minimaler Konfiguration verwendet werden. Bei einem Vorfall erfolgt ein Failover von VMs auf dieses Cluster, und es können weitere Nodes hinzugefügt werden).

3. Richten Sie den Replikationsjob ein, um VM-Replikate mit Veeam Backup and Replication zu erstellen.
4. Erstellen eines Failover-Plans und Durchführen eines Failover
5. Wechseln Sie zurück zu den Produktions-VMs, sobald der Notfall abgeschlossen und der primäre Standort eingerichtet ist.

Voraussetzungen für die Veeam VM Replication to AVS- und ANF-Datstores

1. Stellen Sie sicher, dass die Backup-VM von Veeam Backup & Replication sowohl mit den Quell- als auch den Ziel-AVS SDDC-Clustern verbunden ist.
2. Der Backup-Server muss in der Lage sein, Kurznamen aufzulösen und eine Verbindung zu Quell- und Ziel-vCenter herzustellen.
3. Der Ziel-Azure NetApp Files-Datstore muss über genügend freien Speicherplatz für die VMDKs replizierter VMs verfügen.

Weitere Informationen finden Sie unter „Überlegungen und Einschränkungen“ ["Hier"](#).

Einzelheiten Zur Bereitstellung

Schritt: Replizierung von VMs

Veeam Backup & Replication nutzt VMware vSphere Snapshot-Funktionen/während der Replizierung fordert Veeam Backup & Replication VMware vSphere zur Erstellung eines VM-Snapshots an. Der VM-Snapshot ist die Point-in-Time-Kopie einer VM, die virtuelle Laufwerke, den Systemstatus, die Konfiguration und Metadaten umfasst. Veeam Backup & Replication verwendet den Snapshot als Datenquelle für die Replizierung.

Gehen Sie wie folgt vor, um VMs zu replizieren:

1. Öffnen Sie die Veeam Backup & Replication Console.
2. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten Jobs, und wählen Sie Replikationsjob > Virtuelle Maschine aus.
3. Geben Sie einen Jobnamen an, und aktivieren Sie das entsprechende Kontrollkästchen für die erweiterte Steuerung. Klicken Sie Auf Weiter.
 - Aktivieren Sie das Kontrollkästchen Replikat-Seeding, wenn die Bandbreite zwischen On-Premises und Azure eingeschränkt ist.
 - *Aktivieren Sie das Kontrollkästchen Network Remapping (für AVS SDDC-Standorte mit unterschiedlichen Netzwerken), wenn Segmente auf der Azure VMware-Lösung SDDC nicht mit denen auf lokalen Netzwerken übereinstimmen.
 - Wenn sich das IP-Adressierungsschema am Produktionsstandort vor Ort vom Schema am Ziel-AVS-Standort unterscheidet, aktivieren Sie das Kontrollkästchen Replica RE-IP (für DR-Standorte mit unterschiedlichem IP-Adressierungsschema).

□

4. Wählen Sie im Schritt **Virtuelle Maschinen*** die VMs aus, die auf einen Azure NetApp Files-Datastore repliziert werden sollen, der mit einem Azure VMware-Lösung SDDC verbunden ist. Die Virtual Machines können auf vSAN platziert werden, um die verfügbare vSAN Datastore-Kapazität zu füllen. In einem Pilotcluster wird die nutzbare Kapazität eines 3-Knoten-Clusters begrenzt. Die restlichen Daten lassen sich problemlos auf Azure NetApp Files Datenspeichern platzieren, um die VMs wiederherzustellen und das Cluster zu erweitern, um die CPU-/mem-Anforderungen zu erfüllen. Klicken Sie auf **Hinzufügen**, wählen Sie dann im Fenster **Objekt hinzufügen** die erforderlichen VMs oder VM-Container aus und klicken Sie auf **Hinzufügen**. Klicken Sie Auf **Weiter**.

□

5. Wählen Sie anschließend das Ziel als Azure VMware Solution SDDC Cluster/Host und den entsprechenden Ressourcen-Pool, VM-Ordner und FSX for ONTAP Datastore für VM-Replikate aus. Klicken Sie anschließend auf **Weiter**.

□

6. Erstellen Sie im nächsten Schritt die Zuordnung zwischen dem virtuellen Quell- und Zielnetzwerk nach Bedarf.

□

7. Geben Sie im Schritt **Job-Einstellungen** das Backup-Repository an, in dem Metadaten für VM-Replikate, Aufbewahrungsrichtlinien usw. gespeichert werden.
8. Aktualisieren Sie die Proxy-Server **Source** und **Target** im Schritt **Data Transfer** und lassen Sie die Option **Automatic** (Standard) und halten Sie die Option **Direct** ausgewählt und klicken Sie auf **Next**.

9. Wählen Sie im Schritt **Gastverarbeitung** die Option **anwendungsorientierte Verarbeitung aktivieren** nach Bedarf aus. Klicken Sie Auf **Weiter**.



10. Wählen Sie den Replikationszeitplan aus, um den Replikationsjob regelmäßig auszuführen.



11. Überprüfen Sie im Schritt **Zusammenfassung** des Assistenten die Details des Replikationsjobs. Um den Job direkt nach dem Schließen des Assistenten zu starten, aktivieren Sie das Kontrollkästchen **Job ausführen, wenn ich auf Fertig stellen klicke**, andernfalls lassen Sie das Kontrollkästchen deaktiviert. Klicken Sie dann auf **Fertig stellen**, um den Assistenten zu schließen.



Sobald der Replikationsjob gestartet wurde, werden die VMs mit dem angegebenen Suffix auf dem Ziel-AVS SDDC-Cluster/Host aufgefüllt.



Weitere Informationen zur Veeam-Replizierung finden Sie unter "[Funktionsweise Der Replikation](#)"

Schritt 2: Erstellen eines Failover-Plans

Erstellen Sie nach Abschluss der ersten Replikation oder des Seeding den Failover-Plan. Mithilfe des Failover-Plans können Sie ein Failover für abhängige VMs einzeln oder als Gruppe automatisch durchführen. Der Failover-Plan ist das Modell für die Reihenfolge, in der die VMs verarbeitet werden, einschließlich der Boot-Verzögerungen. Der Failover-Plan trägt außerdem dazu bei, sicherzustellen, dass kritische abhängige VMs bereits laufen.

Um den Plan zu erstellen, navigieren Sie zum neuen Unterabschnitt **Replikate** und wählen Sie **Failover-Plan**. Wählen Sie die entsprechenden VMs aus. Veeam Backup & Replication sucht nach den nächstgelegenen Wiederherstellungspunkten zu diesem Zeitpunkt und verwendet diese, um VM-Replikate zu starten.



Der Failover-Plan kann nur hinzugefügt werden, wenn die erste Replikation abgeschlossen ist und sich die VM-Replikate im Bereitschaftszustand befinden.



Es können maximal 10 VMs gleichzeitig gestartet werden, wenn ein Failover-Plan ausgeführt wird



Während des Failover-Prozesses werden die Quell-VMs nicht ausgeschaltet

Um den **Failover Plan** zu erstellen, gehen Sie wie folgt vor:

1. In der Home-Ansicht. Klicken Sie mit der rechten Maustaste auf den Knoten Replikate, und wählen Sie Failover Plans > Failover Plan > VMware vSphere.



2. Geben Sie als nächstes einen Namen und eine Beschreibung für den Plan an. Pre- und Post-Failover-Skript können bei Bedarf hinzugefügt werden. Führen Sie beispielsweise ein Skript aus, um die VMs vor dem Starten der replizierten VMs herunterzufahren.



3. Fügen Sie die VMs zum Plan hinzu und ändern Sie die VM-Startreihenfolge und die Boot-Verzögerungen, um die Applikationsabhängigkeiten zu erfüllen.



Weitere Informationen zum Erstellen von Replikationsjobs finden Sie unter ["Erstellen Von Replikationsjobs"](#).

Schritt 3: Führen Sie den Failover-Plan aus

Bei einem Failover wird die Quell-VM am Produktionsstandort auf ihr Replikat am Disaster-Recovery-Standort umgeschaltet. Im Rahmen des Failover-Prozesses stellt Veeam Backup & Replication das VM-Replikat zum erforderlichen Wiederherstellungspunkt wieder her und verschiebt alle I/O-Aktivitäten von der Quell-VM auf das Replikat. Replikate können nicht nur im Notfall verwendet werden, sondern auch DR-Übungen simulieren. Während der Failover-Simulation bleibt die Quell-VM aktiv. Sobald alle erforderlichen Tests durchgeführt wurden, können Sie das Failover rückgängig machen und zum normalen Betrieb zurückkehren.



Stellen Sie sicher, dass die Netzwerksegmentierung vorhanden ist, um IP-Konflikte während des Failovers zu vermeiden.

Um den Failover-Plan zu starten, klicken Sie einfach auf die Registerkarte **Failover Plans** und klicken Sie mit der rechten Maustaste auf Ihren Failover-Plan. Wählen Sie ***Start**. Dabei wird ein Failover mit den neuesten Wiederherstellungspunkten der VM-Replikate durchgeführt. Um ein Failover zu bestimmten Wiederherstellungspunkten von VM-Replikaten durchzuführen, wählen Sie **Start to** aus.

□

□

Der Status des VM-Replikats ändert sich von „bereit“ zu „Failover“, und die VMs werden auf dem Ziel-Cluster/Host des SDDC der Azure VMware-Lösung (AVS) gestartet.

□

Sobald der Failover abgeschlossen ist, ändert sich der Status der VMs in „Failover“.

□



Veeam Backup & Replication hält alle Replikationsaktivitäten für die Quell-VM an, bis das Replikat in den Bereitschaftszustand zurückkehrt.

Ausführliche Informationen zu Failover-Plänen finden Sie unter "[Failover-Pläne](#)".

Schritt 4: Failback zum Produktionsstandort

Wenn der Failover-Plan ausgeführt wird, gilt er als Zwischenschritt und muss basierend auf den Anforderungen abgeschlossen werden. Folgende Optionen stehen zur Verfügung:

- **Failback zur Produktion** - Wechseln Sie zurück zur ursprünglichen VM und übertragen Sie alle Änderungen, die während des VM-Replikats auf die ursprüngliche VM ausgeführt wurden.



Wenn Sie ein Failback durchführen, werden die Änderungen nur übertragen, aber nicht veröffentlicht. Wählen Sie **commit Failback** (sobald die ursprüngliche VM wie erwartet funktioniert) oder Undo Failback, um zum VM-Replikat zurückzukehren, wenn die ursprüngliche VM nicht wie erwartet funktioniert.

- **Rückgängigmachen des Failover** - Wechseln Sie zurück zur ursprünglichen VM und verwerfen Sie alle Änderungen, die während der Ausführung am VM-Replikat vorgenommen wurden.
- **Permanent Failover** - Wechseln Sie dauerhaft von der ursprünglichen VM auf ein VM-Replikat und verwenden Sie dieses Replikat als ursprüngliche VM.

In dieser Demo wurde „Failback zur Produktion“ gewählt. Failback auf die ursprüngliche VM wurde während des Zielschritts des Assistenten ausgewählt und das Kontrollkästchen „VM nach der Wiederherstellung einschalten“ war aktiviert.

[]

[]

[]

[]

Failback-Commit ist eine der Möglichkeiten, den Failback-Vorgang abzuschließen. Wenn Failback durchgeführt wird, wird bestätigt, dass die an die zurückgeschickte VM (die Produktions-VM) gesendeten Änderungen wie erwartet funktionieren. Nach dem Commit-Vorgang setzt Veeam Backup & Replication die Replizierungsaktivitäten für die Produktions-VM fort.

Detaillierte Informationen zum Failback-Prozess finden Sie in der Veeam-Dokumentation für ["Failover und Failback für die Replikation"](#).

[]

Nach einem erfolgreichen Failback zur Produktion werden die VMs alle auf den ursprünglichen Produktionsstandort zurückgestellt.

[]

Schlussfolgerung

Mit der Datastore-Funktion von Azure NetApp Files können Veeam oder jedes beliebige validierte Drittanbieter-Tool eine kostengünstige DR-Lösung anbieten, indem Pilot-Light-Cluster eingesetzt werden, anstatt nur ein großes Cluster einzurichten, um VM-Replikate aufzunehmen. So wird ein maßgeschneiderter und individuell angepasster Disaster-Recovery-Plan effizient umgesetzt und vorhandene Backup-Produkte intern für DR wiederverwendet. So wird Cloud-basierte Disaster Recovery durch das Beenden von DR-Datacentern vor Ort möglich. Bei einem Ausfall kann ein Failover durch Klicken auf eine Schaltfläche oder bei

einem Ausfall automatisch durchgeführt werden.

Wenn Sie mehr über diesen Prozess erfahren möchten, folgen Sie bitte dem detaillierten Video zum Rundgang.

<https://netapp.hosted.panopto.com/Panopto/Pages/Embed.aspx?id=2855e0d5-97e7-430f-944a-b061015e9278>

Copyright-Informationen

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

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

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

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

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

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

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

Markeninformationen

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