Disaster Recovery mit ANF und JetStream

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions-cloud/vmware/vmw-azure-avs-dr-jetstream.html on August 18, 2025. Always check docs.netapp.com for the latest.

Inhalt

Disaster Recovery mit ANF und JetStream 1
Installieren Sie JetStream DR im lokalen Rechenzentrum 3
Installieren Sie JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud mit dem Befehl „Ausführen“. 7
Durchführen eines Failovers/Failbacks 10
Ransomware-Wiederherstellung 13

Disaster Recovery mit ANF und JetStream

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen. Mithilfe des VMware VAIO-Frameworks können lokale VMware-Workloads in den Azure Blob-Speicher repliziert und wiederhergestellt werden, wodurch ein minimaler oder nahezu kein Datenverlust und eine RTO von nahezu null möglich sind.

Mit JetStream DR können die vom lokalen Standort auf AVS und insbesondere auf Azure NetApp Files replizierten Workloads nahtlos wiederhergestellt werden. Es ermöglicht eine kostengünstige Notfallwiederherstellung durch die Nutzung minimaler Ressourcen am DR-Standort und kostengünstigen Cloud-Speicher. JetStream DR automatisiert die Wiederherstellung in ANF-Datenspeichern über Azure Blob Storage. JetStream DR stellt unabhängige VMs oder Gruppen verwandter VMs gemäß der Netzwerkzuordnung in der Infrastruktur des Wiederherstellungsstandorts wieder her und bietet eine zeitpunktbezogene Wiederherstellung zum Schutz vor Ransomware.

Dieses Dokument vermittelt ein Verständnis der Betriebsprinzipien und Hauptkomponenten von JetStream DR.

Übersicht über die Lösungsbereitstellung

1. Installieren Sie die JetStream DR-Software im lokalen Rechenzentrum.
   a. Laden Sie das JetStream DR-Softwarepaket vom Azure Marketplace (ZIP) herunter und stellen Sie das JetStream DR MSA (OVA) im vorgesehenen Cluster bereit.
   b. Konfigurieren Sie den Cluster mit dem E/A-Filterpaket (installieren Sie JetStream VIB).
   c. Stellen Sie Azure Blob (Azure Storage-Konto) in derselben Region wie der DR AVS-Cluster bereit.
   d. Stellen Sie DRVA-Geräte bereit und weisen Sie Replikationsprotokollvolumes zu (VMDK aus vorhandenem Datenspeicher oder gemeinsam genutztem iSCSI-Speicher).
   e. Erstellen Sie geschützte Domänen (Gruppen verwandter VMs) und weisen Sie DRVAs und Azure Blob Storage/ANF zu.
   f. Schutz starten.
2. Installieren Sie die JetStream DR-Software in der privaten Azure VMware Solution-Cloud.
   a. Verwenden Sie den Befehl „Ausführen“, um JetStream DR zu installieren und zu konfigurieren.
   b. Fügen Sie denselben Azure Blob-Container hinzu und ermitteln Sie Domänen mithilfe der Option „Domänen scannen“.
   c. Stellen Sie die erforderlichen DRVA-Geräte bereit.
   d. Erstellen Sie Replikationsprotokollvolumes mithilfe verfügbarer vSAN- oder ANF-Datenspeicher.
   e. Importieren Sie geschützte Domänen und konfigurieren Sie RocVA (Recovery VA), um den ANF-Datenspeicher für VM-Platzierungen zu verwenden.
   f. Wählen Sie die entsprechende Failover-Option aus und starten Sie die kontinuierliche Rehydrierung für Domänen oder VMs mit nahezu null RTO.
3. Lösen Sie während eines Notfallereignisses ein Failover zu Azure NetApp Files Datenspeichern am angegebenen AVS DR-Standort aus.
4. Rufen Sie das Failback zur geschützten Site auf, nachdem die geschützte Site wiederhergestellt wurde. Stellen Sie vor dem Start sicher, dass die Voraussetzungen erfüllt sind, wie in diesem Abschnitt angegeben. "Link" und führen Sie außerdem das von JetStream Software bereitgestellte Bandwidth Testing Tool (BWT) aus, um die potenzielle Leistung des Azure Blob-Speichers und seine Replikationsbandbreite bei Verwendung mit der JetStream DR-Software zu bewerten. Nachdem die Voraussetzungen, einschließlich der Konnektivität, erfüllt sind, richten Sie JetStream DR für AVS ein und abonnieren Sie es über die "Azure Marketplace" . Nachdem das Softwarepaket 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. Stellen Sie eine Liste der zu schützenden VMs zusammen mit ihren RTO- und Wiederherstellungsgruppeneinstellungen bereit und führen Sie dann CPT aus.

CPT erfüllt die folgenden Funktionen:

- Kombinieren Sie VMs entsprechend ihrer RTO in Schutzdomänen.
- Festlegen der optimalen Anzahl von DRVAs und ihrer Ressourcen.
- Schätzung der erforderlichen Replikationsbandbreite.
- Identifizieren der Merkmale des Replikationsprotokollvolumens (Kapazität, Bandbreite usw.).

- Schätzen der erforderlichen Objektspeicherkapazität und mehr.

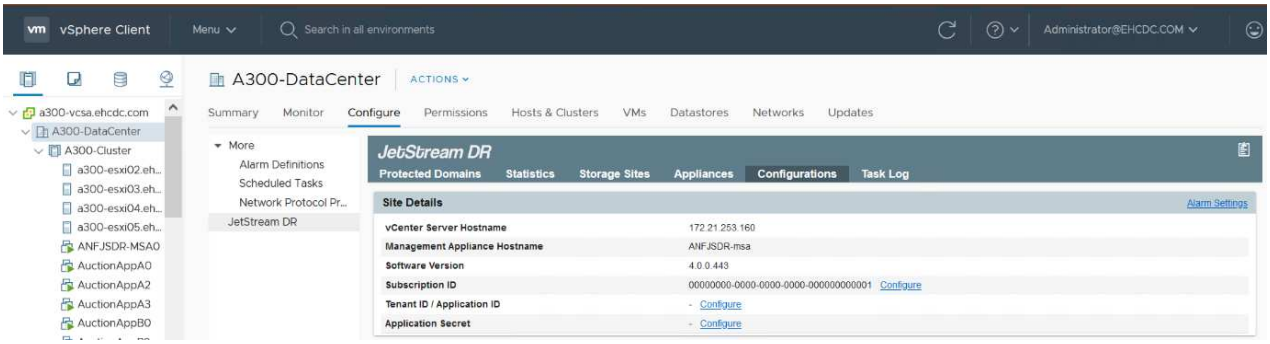
> Die Anzahl und der Inhalt der vorgeschriebenen Domänen hängen von verschiedenen VM-Eigenschaften ab, wie z. B. durchschnittlichen IOPS, Gesamtkapazität, Priorität (die die Failover-Reihenfolge definiert), RTO und anderen.

Installieren Sie JetStream DR im lokalen Rechenzentrum

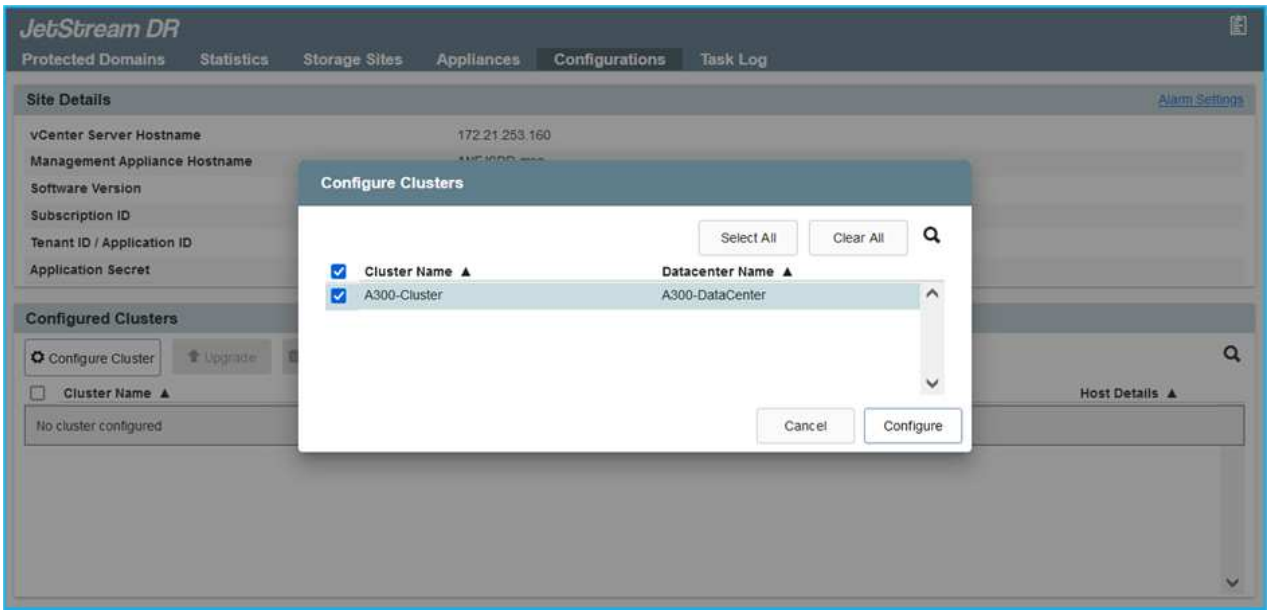
Die JetStream DR-Software besteht aus drei Hauptkomponenten: JetStream DR Management Server Virtual Appliance (MSA), DR Virtual Appliance (DRVA) und Hostkomponenten (E/A-Filterpakete). MSA wird verwendet, um Hostkomponenten auf dem Computercluster zu installieren und zu konfigurieren und anschließend die JetStream DR-Software zu verwalten. Die folgende Liste bietet eine allgemeine Beschreibung des Installationsvorgangs:

So installieren Sie JetStream DR vor Ort

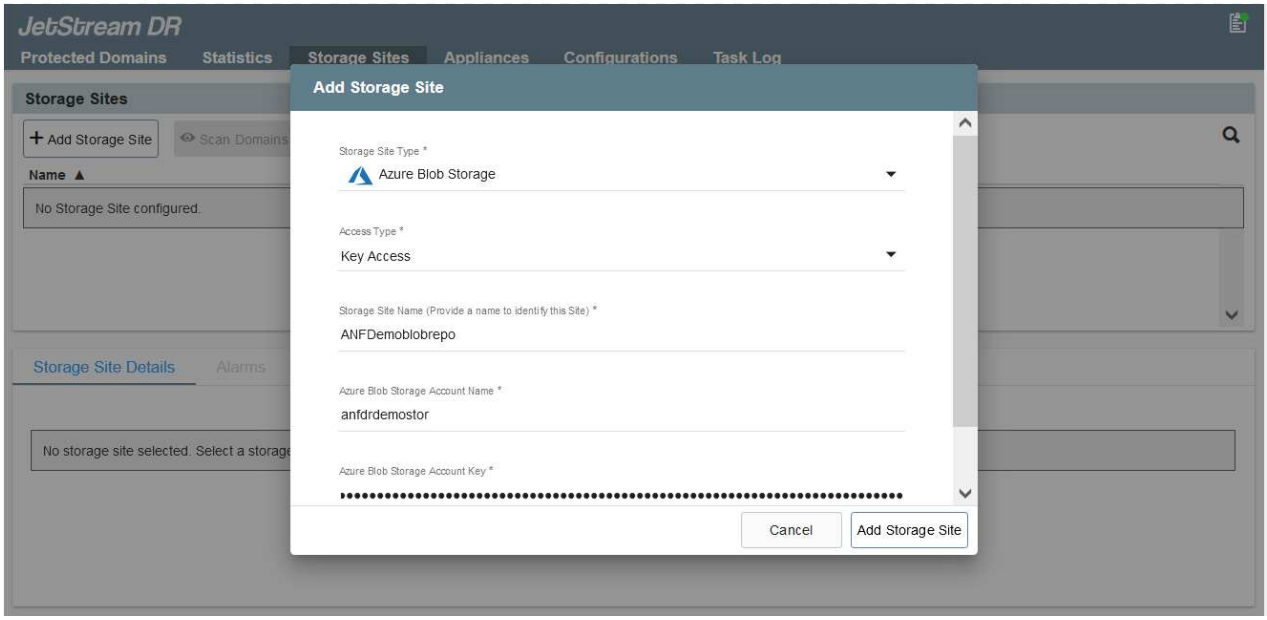
1. Voraussetzungen prüfen.
2. Führen Sie das Kapazitätsplanungstool aus, um Empfehlungen zu Ressourcen und Konfigurationen zu erhalten (optional, aber für Proof-of-Concept-Tests empfohlen).
3. Stellen Sie den JetStream DR MSA auf einem vSphere-Host im vorgesehenen Cluster bereit.
4. Starten Sie das MSA mit seinem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server beim MSA. Führen Sie zur Durchführung der Installation die folgenden detaillierten Schritte aus:
6. Nachdem JetStream DR MSA bereitgestellt und der vCenter Server registriert wurde, greifen Sie über den vSphere Web Client auf das JetStream DR-Plug-In zu. Dies kann durch Navigieren zu Rechenzentrum > Konfigurieren > JetStream DR erfolgen.



7. Wählen Sie in der JetStream DR-Schnittstelle den entsprechenden Cluster aus.



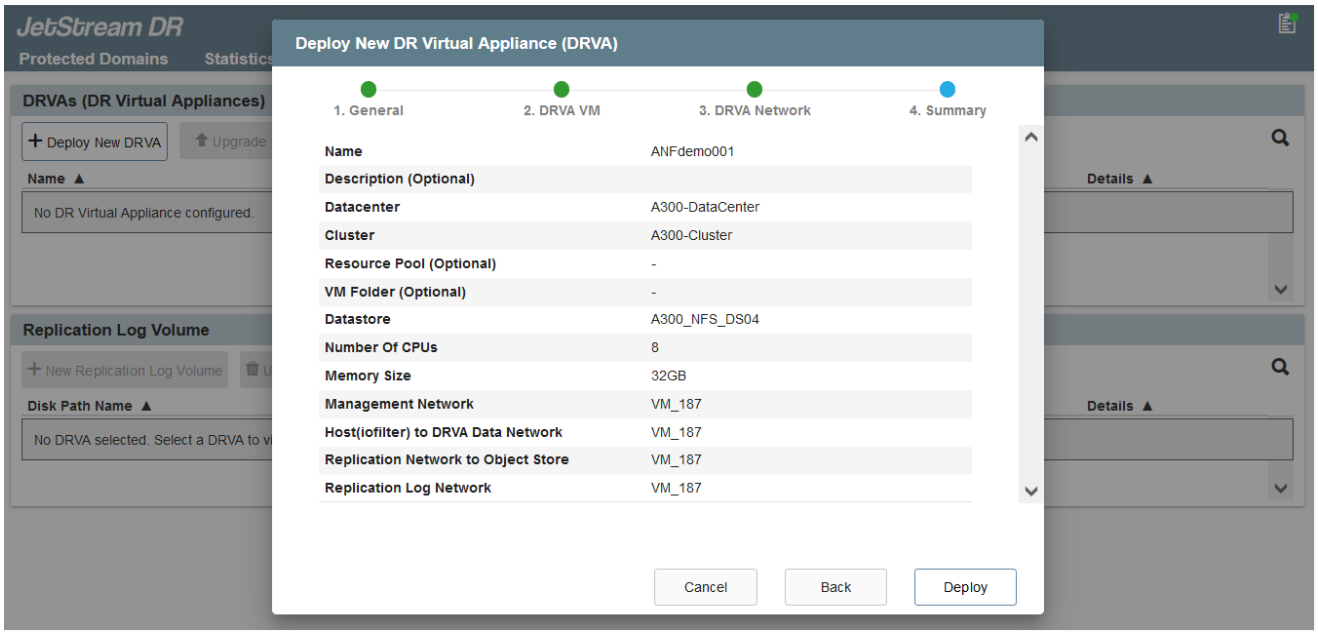
8. Konfigurieren Sie den Cluster mit dem E/A-Filterpaket.



9. Fügen Sie Azure Blob Storage am Wiederherstellungsstandort hinzu.
10. Stellen Sie eine DR Virtual Appliance (DRVA) über die Registerkarte „Appliances“ bereit.

> DRVAs können automatisch von CPT erstellt werden, für POC-Tests empfehlen wir jedoch, den DR-Zyklus manuell zu konfigurieren und auszuführen (Schutz starten > Failover > Failback).

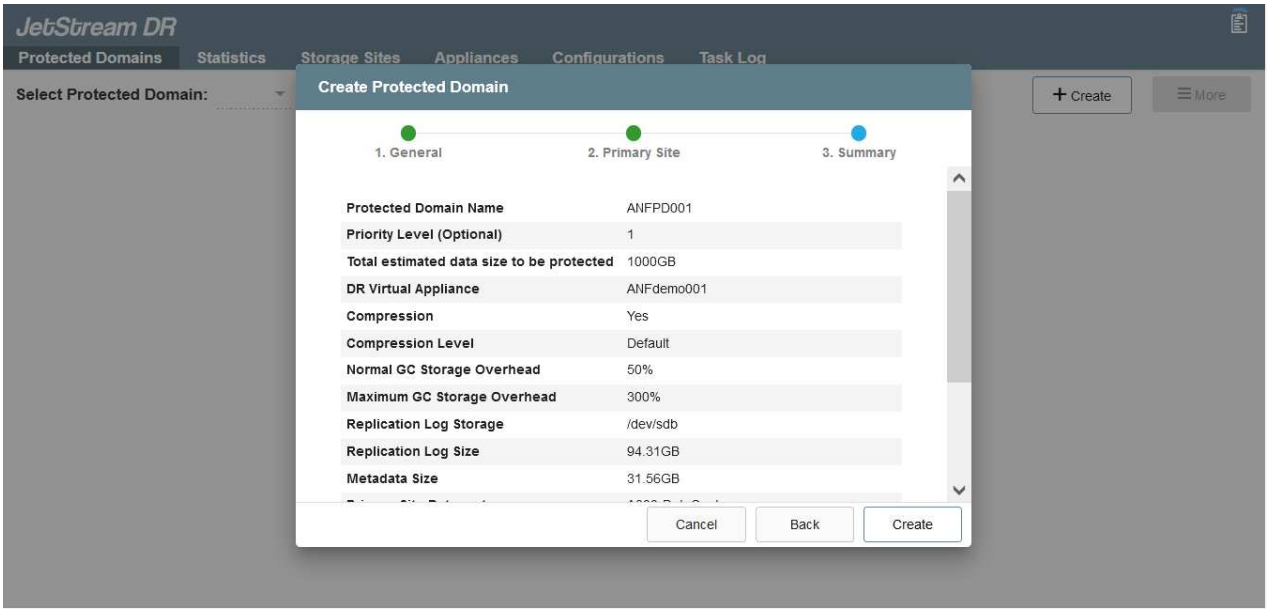
JetStream DRVA ist eine virtuelle Appliance, die wichtige Funktionen im Datenreplikationsprozess unterstützt. Ein geschützter Cluster muss mindestens einen DRVA enthalten und normalerweise wird pro Host ein DRVA konfiguriert. Jeder DRVA kann mehrere geschützte Domänen verwalten.



In diesem Beispiel wurden vier DRVAs für 80 virtuelle Maschinen erstellt.

1. Erstellen Sie Replikationsprotokollvolumes für jeden DRVA mithilfe von VMDK aus den verfügbaren Datenspeichern oder unabhängigen gemeinsam genutzten iSCSI-Speicherpools.

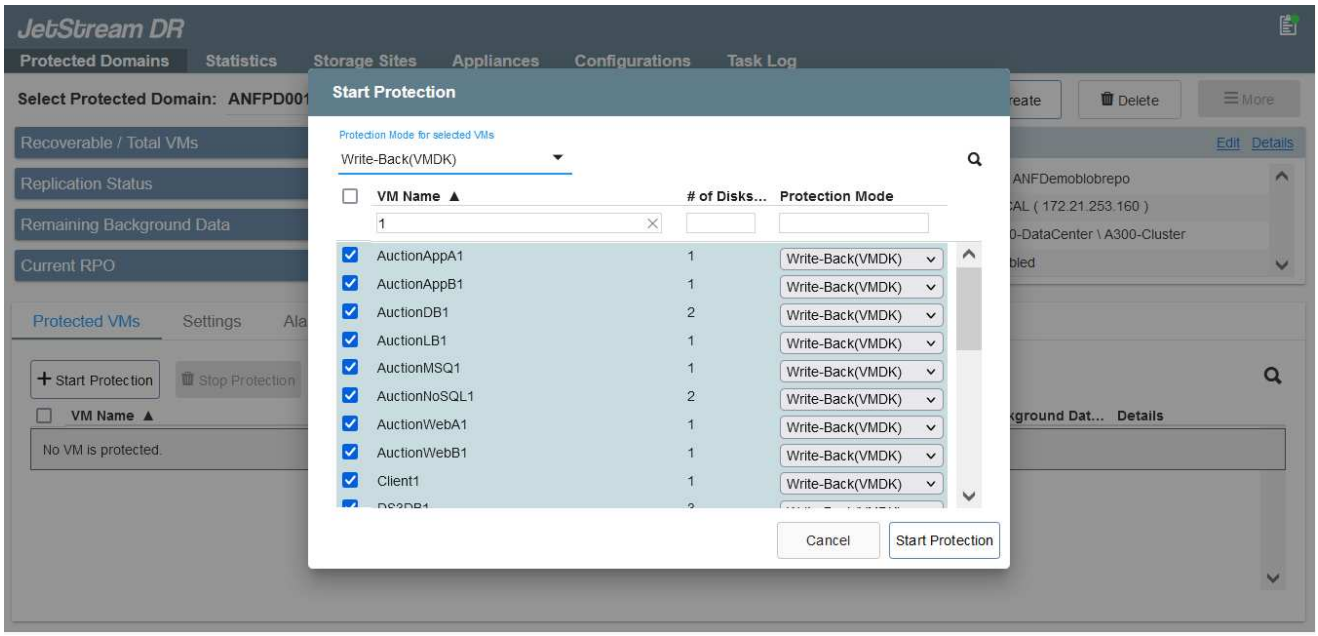
2. Erstellen Sie auf der Registerkarte „Geschützte Domänen“ die erforderliche Anzahl geschützter Domänen mithilfe von Informationen zur Azure Blob Storage-Site, der DRVA-Instanz und dem Replikationsprotokoll. Eine geschützte Domäne definiert eine bestimmte VM oder eine Gruppe von VMs innerhalb des Clusters, die gemeinsam geschützt werden und denen eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen wird.



3. Wählen Sie die VMs aus, die Sie schützen möchten, und starten Sie den VM-Schutz der geschützten Domäne. Dadurch wird die Datenreplikation in den angegebenen Blob Store gestartet.

> Stellen Sie sicher, dass für alle VMs in einer geschützten Domäne derselbe Schutzmodus verwendet wird.

> Der Write-Back-Modus (VMDK) kann eine höhere Leistung bieten.



Stellen Sie sicher, dass Replikationsprotokollvolumes auf Hochleistungsspeichern abgelegt werden.

Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (sogenannte Wiederherstellungsgruppen), die Startreihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

Installieren Sie JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud mit dem Befehl „Ausführen“

Eine bewährte Methode für eine Wiederherstellungssite (AVS) besteht darin, im Voraus einen Pilot-Light-Cluster mit drei Knoten zu erstellen. Dadurch kann die Infrastruktur des Wiederherstellungsstandorts vorkonfiguriert werden, einschließlich der folgenden Elemente:

- Zielnetzwerksegmente, Firewalls, Dienste wie DHCP und DNS usw.
- Installation von JetStream DR für AVS
- Konfiguration von ANF-Volumes als Datenspeicher und mehr. JetStream DR unterstützt den RTO-Modus nahezu Null für unternehmenskritische Domänen. Für diese Domänen sollte der Zielspeicher vorinstalliert sein. In diesem Fall ist ANF ein empfohlener Speichertyp.

Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster so konfiguriert werden, dass sie den lokalen Anforderungen entspricht.

Abhängig von den SLA- und RTO-Anforderungen kann ein kontinuierliches Failover oder ein regulärer (Standard-)Failover-Modus verwendet werden. Um eine RTO von nahezu Null zu erreichen, sollte am Wiederherstellungsort mit der kontinuierlichen Rehydration begonnen werden.

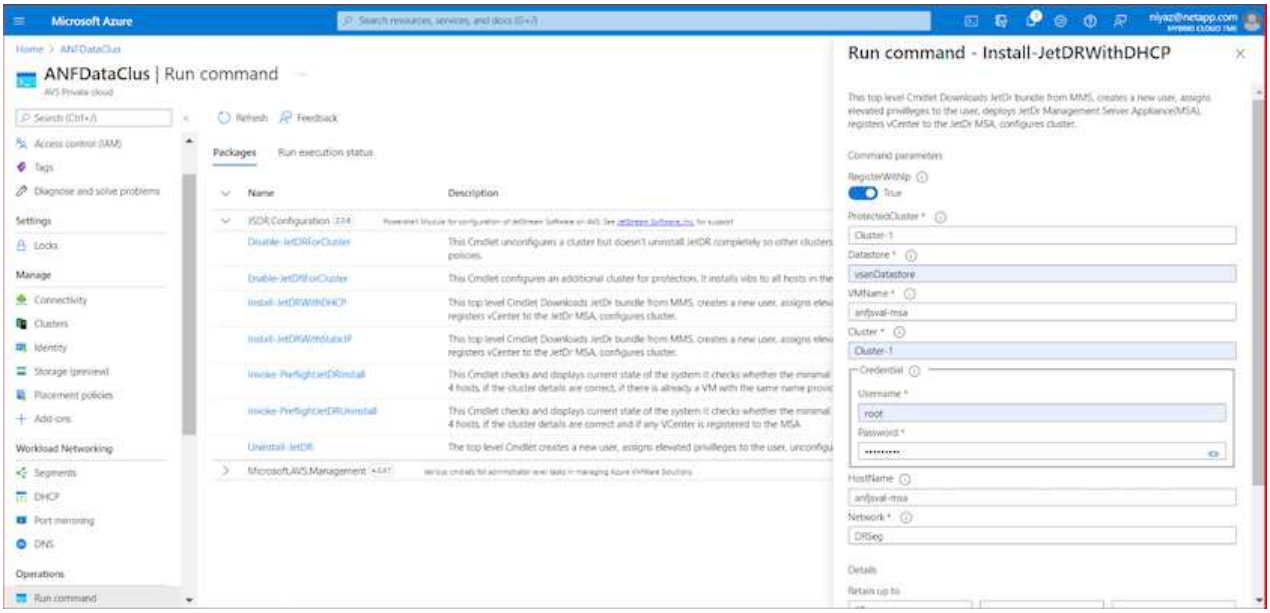
So installieren Sie JetStream DR für AVS in einer privaten Cloud

Führen Sie die folgenden Schritte aus, um JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud zu installieren:

1. Gehen Sie im Azure-Portal zur Azure VMware-Lösung, wählen Sie die private Cloud aus und wählen Sie „Befehl ausführen“ > „Pakete“ > „JSDR.Configuration“.

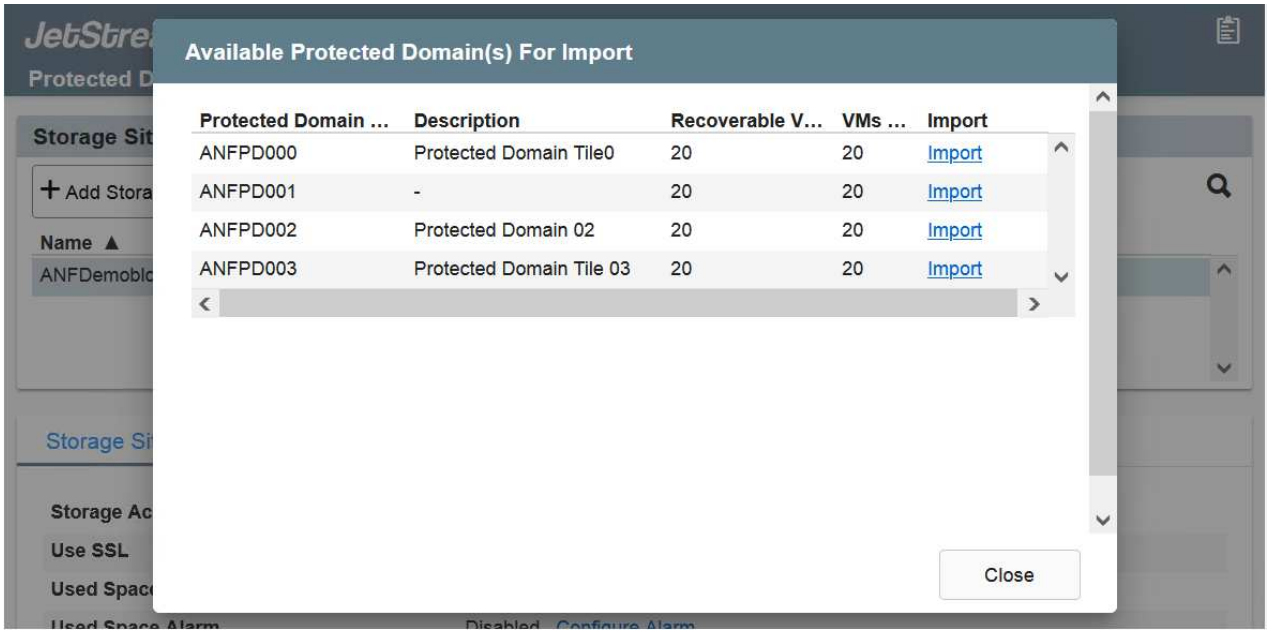
   > Der Standardbenutzer CloudAdmin in Azure VMware Solution verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Azure VMware Solution ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Azure VMware Solution-Befehls „Ausführen“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

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



2. Aktualisieren Sie den Browser, nachdem die Installation von JetStream DR für AVS abgeschlossen ist. Um auf die JetStream DR-Benutzeroberfläche zuzugreifen, gehen Sie zu SDDC Datacenter > Konfigurieren > JetStream DR.

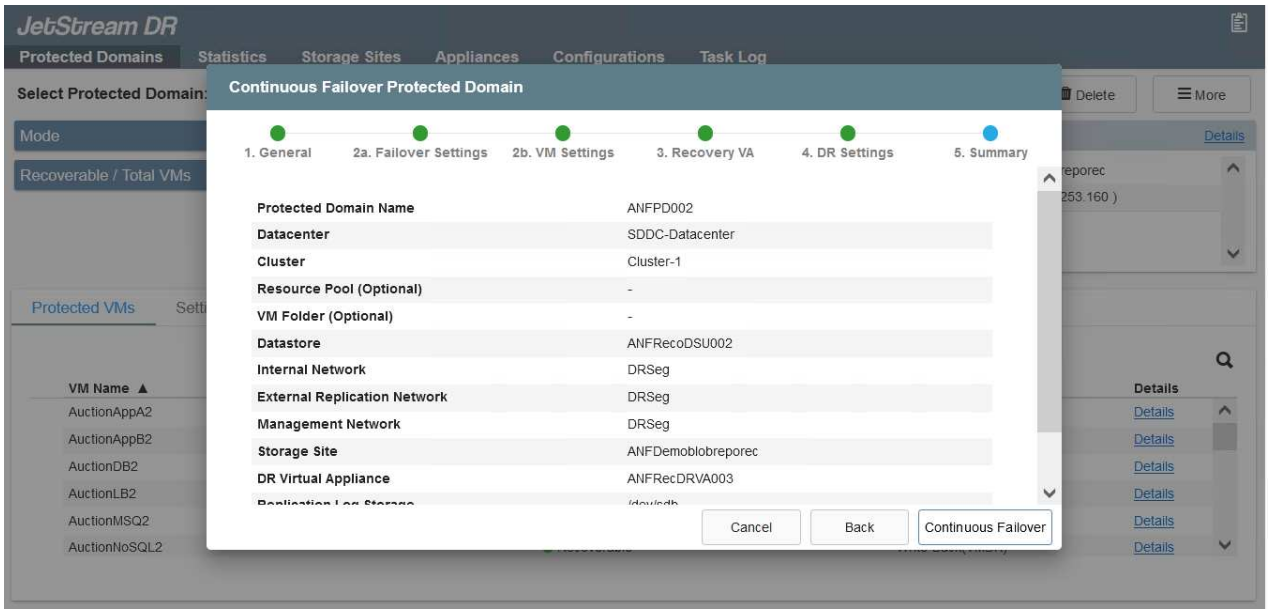
3. Fügen Sie über die JetStream DR-Schnittstelle das Azure Blob Storage-Konto hinzu, das zum Schutz des lokalen Clusters als Speicherort verwendet wurde, und führen Sie dann die Option „Domänen scannen“ aus.



4. Nachdem die geschützten Domänen importiert wurden, stellen Sie DRVA-Geräte bereit. In diesem Beispiel wird die kontinuierliche Rehydrierung manuell vom Wiederherstellungsstandort aus mithilfe der JetStream DR-Benutzeroberfläche gestartet.

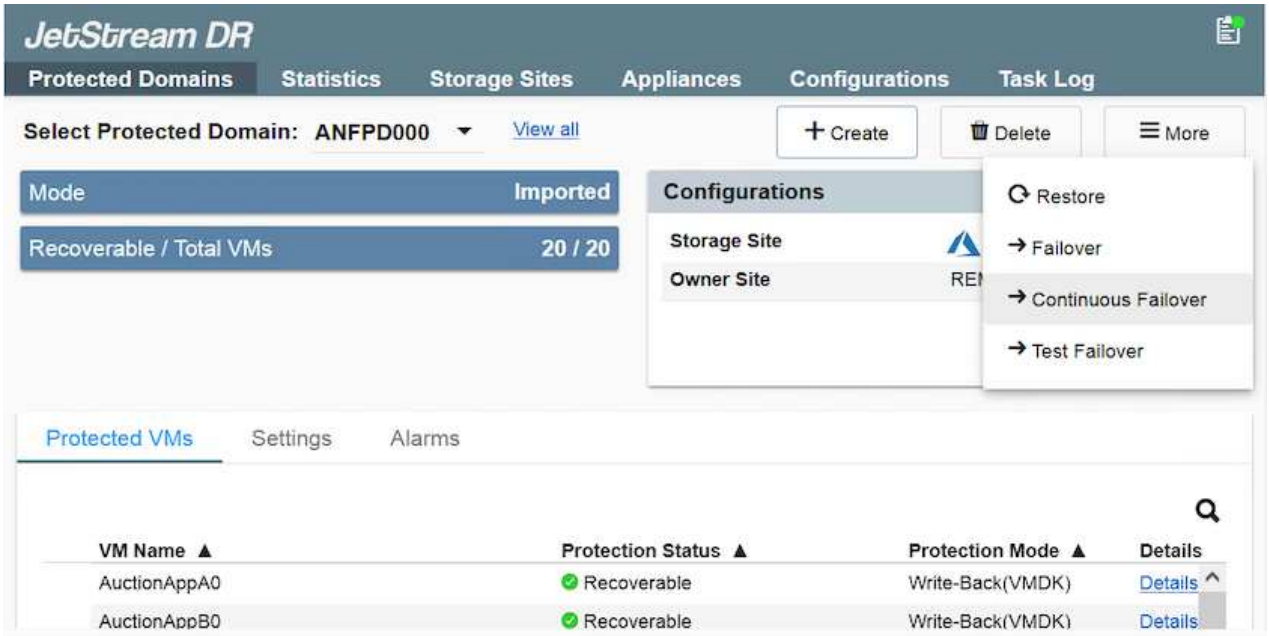
> Diese Schritte können auch mithilfe von CPT-erstellten Plänen automatisiert werden.

5. Erstellen Sie Replikationsprotokollvolumes mithilfe verfügbarer vSAN- oder ANF-Datenspeicher.
6. Importieren Sie die geschützten Domänen und konfigurieren Sie die Recovery VA so, dass der ANF-Datenspeicher für VM-Platzierungen verwendet wird.



Stellen Sie sicher, dass DHCP im ausgewählten Segment aktiviert ist und genügend IPs verfügbar sind. Dynamische IPs werden vorübergehend verwendet, während Domänen wiederhergestellt werden. Jede wiederherzustellende VM (einschließlich kontinuierlicher Rehydration) erfordert eine individuelle dynamische IP. Nach Abschluss der Wiederherstellung wird die IP freigegeben und kann wiederverwendet werden.

7. Wählen Sie die entsprechende Failover-Option (kontinuierliches Failover oder Failover). In diesem Beispiel wird die kontinuierliche Rehydration (kontinuierliches Failover) ausgewählt.



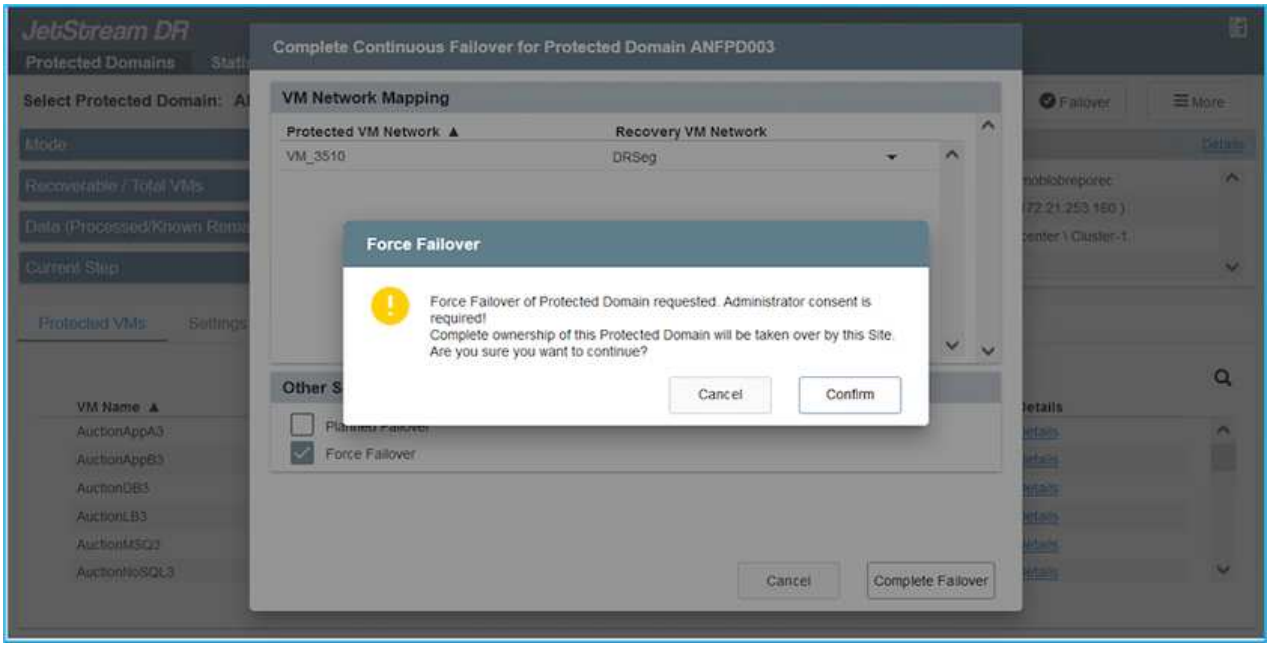
Durchführen eines Failovers/Failbacks

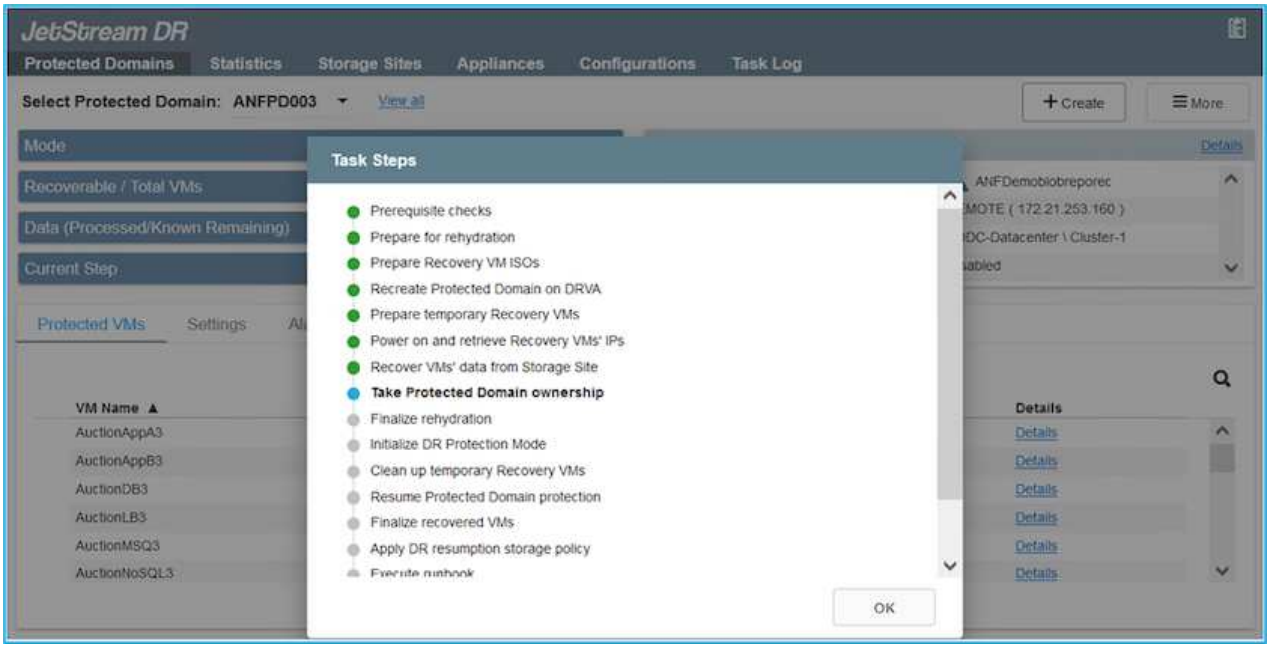
So führen Sie ein Failover/Failback durch

1. Nachdem im geschützten Cluster der lokalen Umgebung ein Notfall (Teil- oder Vollausfall) aufgetreten ist, lösen Sie das Failover aus.

> CPT kann verwendet werden, um den Failoverplan auszuführen und die VMs aus Azure Blob Storage in der AVS-Cluster-Wiederherstellungssite wiederherzustellen.

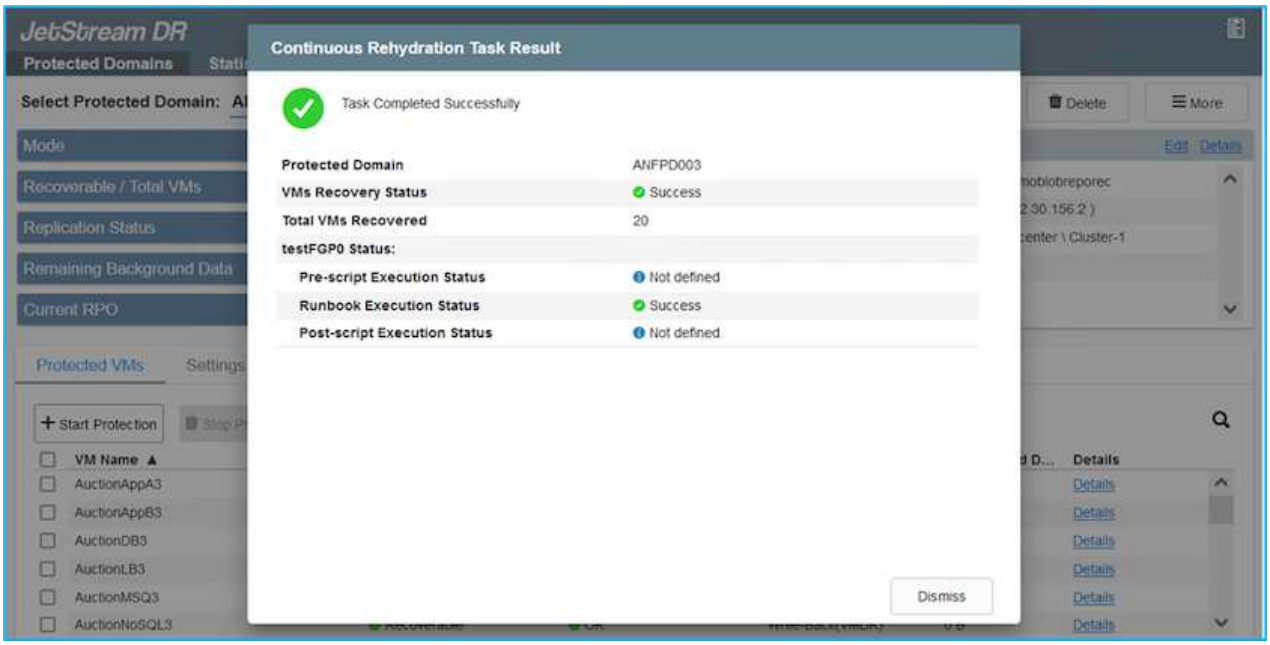
> Nach dem Failover (für kontinuierliche oder standardmäßige Rehydrierung), wenn die geschützten VMs in AVS gestartet wurden, wird der Schutz automatisch fortgesetzt und JetStream DR repliziert ihre Daten weiterhin in die entsprechenden/ursprünglichen Container in Azure Blob Storage.





Die Taskleiste zeigt den Fortschritt der Failover-Aktivitäten an.

2. Wenn die Aufgabe abgeschlossen ist, greifen Sie auf die wiederhergestellten VMs zu und das Geschäft wird wie gewohnt fortgesetzt.

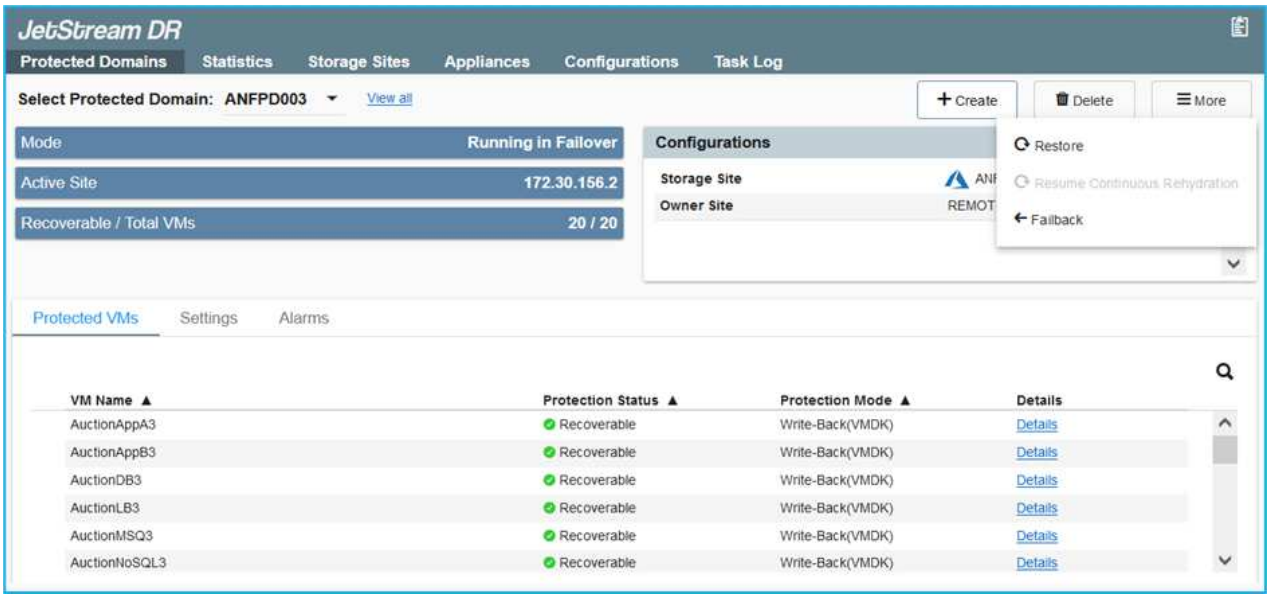


Nachdem die primäre Site wieder betriebsbereit ist, kann ein Failback durchgeführt werden. Der VM-Schutz wird fortgesetzt und die Datenkonsistenz sollte überprüft werden.

3. Stellen Sie die lokale Umgebung wieder her. Je nach Art des Katastrophenfalls kann es erforderlich sein, die Konfiguration des geschützten Clusters wiederherzustellen und/oder zu überprüfen. Gegebenenfalls muss die JetStream DR-Software neu installiert werden.

> Hinweis: Die `recovery_utility_prepare_failback` Das im Automation Toolkit bereitgestellte Skript kann verwendet werden, um die ursprünglich geschützte Site von veralteten VMs, Domäneninformationen usw. zu bereinigen.

4. Greifen Sie auf die wiederhergestellte lokale Umgebung zu, gehen Sie zur Jetstream DR-Benutzeroberfläche und wählen Sie die entsprechende geschützte Domäne aus. Nachdem die geschützte Site für das Failback bereit ist, wählen Sie die Failback-Option in der Benutzeroberfläche aus.



Der von CPT generierte Failback-Plan kann auch verwendet werden, um die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher zurück in die ursprüngliche VMware-Umgebung zu initiieren.

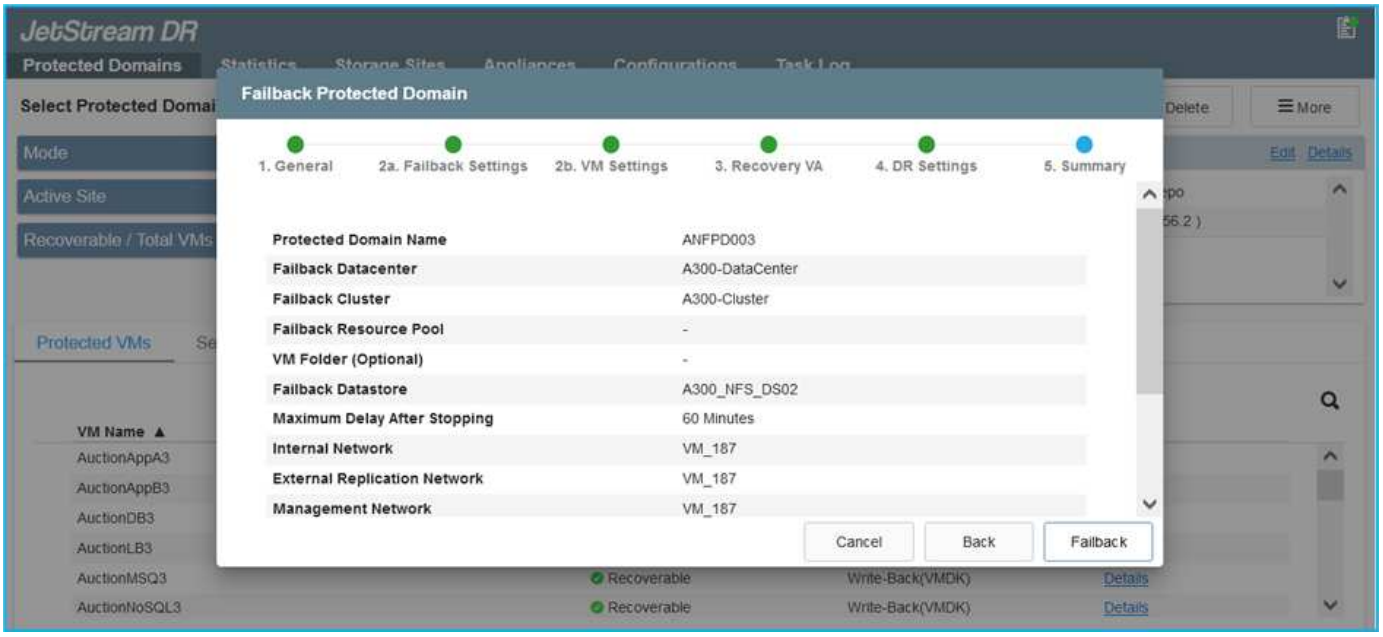
Geben Sie die maximale Verzögerung nach dem Anhalten von VMs am Wiederherstellungsstandort und dem Neustart am geschützten Standort an. Diese Zeit umfasst das Abschließen der Replikation nach dem Stoppen der Failover-VMs, die Zeit zum Bereinigen der Wiederherstellungssite und die Zeit zum Neuerstellen der VMs an der geschützten Site. 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.

Ransomware-Wiederherstellung

Die Wiederherstellung nach Ransomware kann eine gewaltige Aufgabe sein. Insbesondere kann es für IT-Organisationen schwierig sein, den sicheren Zeitpunkt der Rückkehr zu bestimmen und, nachdem dieser ermittelt wurde, sicherzustellen, dass wiederhergestellte Workloads vor erneuten Angriffen (durch schlafende Malware oder über anfällige Anwendungen) geschützt sind.

JetStream DR für AVS kann zusammen mit Azure NetApp Files -Datenspeichern diese Probleme lösen, indem es Unternehmen die Wiederherstellung von verfügbaren Zeitpunkten aus ermöglicht, sodass Workloads bei Bedarf in einem funktionsfähigen, isolierten Netzwerk wiederhergestellt werden. Durch die Wiederherstellung können Anwendungen weiterhin funktionieren und miteinander kommunizieren, ohne dass sie dem Nord-Süd-Verkehr ausgesetzt sind. Dadurch erhalten Sicherheitsteams einen sicheren Ort, um forensische Untersuchungen und andere notwendige Sanierungsmaßnahmen durchzuführen.


JetStream DR
Protected Domains
Statistics
Storage Sites
Appliances
Configurations
Task Log
Select Protected Domai
Delete
More
Mode
Active Site
Recoverable / Total VMs
Edit
Details
Protected VMs
VM Name
AuctionAppA3
AuctionAppB3
AuctionDB3
AuctionLB3
AuctionMSQ3
AuctionNoSQL3
Recoverable
Write-Back(VMDK)
Details
Failback Protected Domain
1. General
2a. Failback Settings
2b. VM Settings
3. Recovery VA
4. DR Settings
5. Summary
Protected Domain Name
ANFPD003
Failback Datacenter
A300-DataCenter
Failback Cluster
A300-Cluster
Failback Resource Pool
-
VM Folder (Optional)
-
Failback Datastore
A300_NFS_DS02
Maximum Delay After Stopping
60 Minutes
Internal Network
VM_187
External Replication Network
VM_187
Management Network
VM_187
Cancel
Back
Failback

Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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