Disaster Recovery mit CVO und AVS (Gastspeicher)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

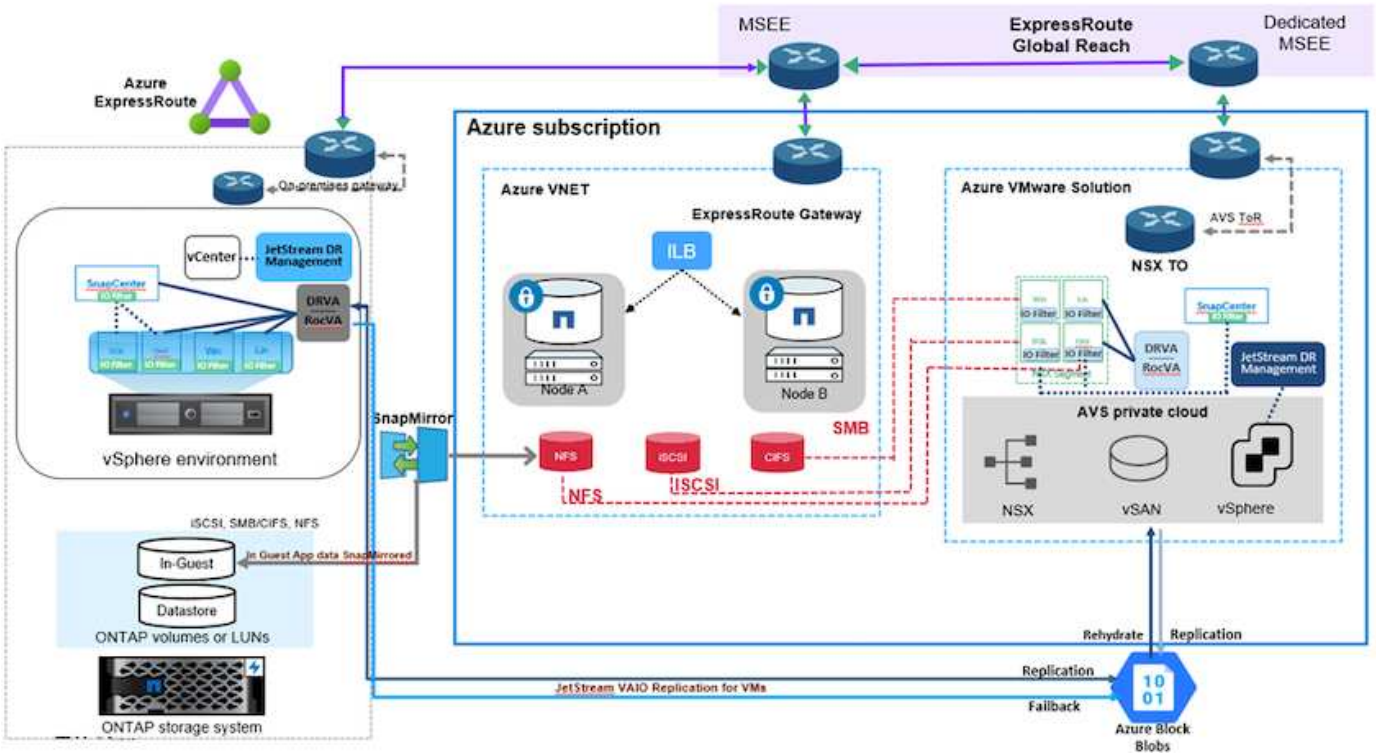
Inhalt

Disaster Recovery mit CVO und AVS (Gastspeicher)

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, Workloads vor Site-Ausfällen und Datenbeschädigungen wie Ransomware zu schützen. Mit NetApp SnapMirror können lokale VMware-Workloads, die über den Gast verbundenen Speicher verwenden, auf NetApp Cloud Volumes ONTAP repliziert werden, das in Azure ausgeführt wird.

Überblick

```
 This covers application data; however, what about the actual VMs
themselves. Disaster recovery should cover all dependent components,
including virtual machines, VMDKs, application data, and more. To
accomplish this, SnapMirror along with Jetstream can be used to seamlessly
recover workloads replicated from on-premises to Cloud Volumes ONTAP while
using vSAN storage for VM VMDKs.
Dieses Dokument bietet eine schrittweise Anleitung zum Einrichten und
Durchführen einer Notfallwiederherstellung unter Verwendung von NetApp
SnapMirror, JetStream und der Azure VMware Solution (AVS).
```



Annahmen

Dieses Dokument konzentriert sich auf die In-Guest-Speicherung für Anwendungsdaten (auch als Gastverbindung bezeichnet) und wir gehen davon aus, dass die lokale Umgebung SnapCenter für anwendungskonsistente Sicherungen verwendet.

> Dieses Dokument gilt für alle Sicherungs- oder Wiederherstellungslösungen von Drittanbietern. Befolgen Sie je nach der in der Umgebung verwendeten Lösung Best Practices, um Sicherungsrichtlinien zu erstellen, die den SLAs des Unternehmens entsprechen.

Verwenden Sie für die Konnektivität zwischen der lokalen Umgebung und dem virtuellen Azure-Netzwerk die Express Route Global Reach oder ein virtuelles WAN mit einem VPN-Gateway. Segmente sollten basierend auf dem lokalen VLAN-Design erstellt werden.

> Es gibt mehrere Optionen zum Verbinden lokaler Rechenzentren mit Azure, weshalb wir in diesem Dokument keinen bestimmten Workflow beschreiben können. Informationen zur geeigneten Methode zur Konnektivität zwischen lokalen Standorten und Azure finden Sie in der Azure-Dokumentation.

Bereitstellen der DR-Lösung

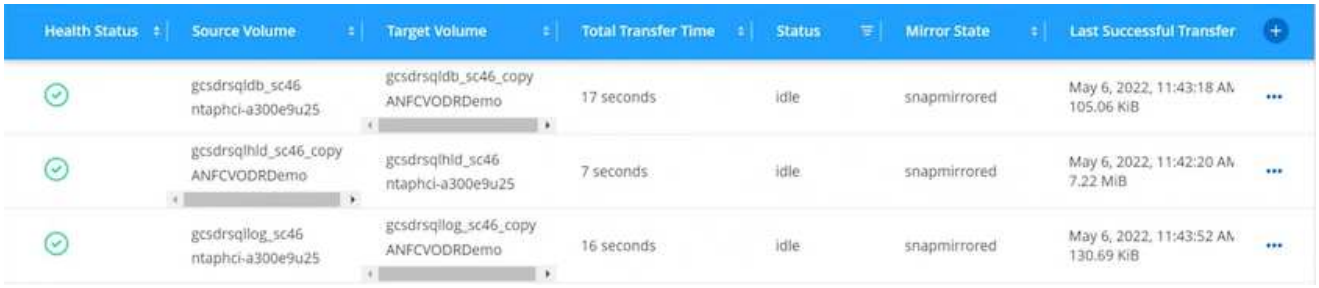
Übersicht über die Lösungsbereitstellung

1. Stellen Sie sicher, dass Anwendungsdaten mit SnapCenter unter Einhaltung der erforderlichen RPO-Anforderungen gesichert werden.
2. Stellen Sie Cloud Volumes ONTAP mit der richtigen Instanzgröße bereit, indem Sie den Cloud Manager innerhalb des entsprechenden Abonnements und virtuellen Netzwerks verwenden.
   a. Konfigurieren Sie SnapMirror für die relevanten Anwendungsvolumes.
   b. Aktualisieren Sie die Sicherungsrichtlinien in SnapCenter , um SnapMirror -Updates nach den geplanten Jobs auszulösen.
3. Installieren Sie die JetStream DR-Software im lokalen Rechenzentrum und starten Sie den Schutz für virtuelle Maschinen.
4. Installieren Sie die JetStream DR-Software in der privaten Azure VMware Solution-Cloud.
5. Unterbrechen Sie während eines Katastrophenfalls die SnapMirror Beziehung mithilfe von Cloud Manager und lösen Sie ein Failover virtueller Maschinen zu Azure NetApp Files oder zu vSAN-Datenspeichern am angegebenen AVS DR-Standort aus.
   a. Verbinden Sie die ISCSI-LUNs und NFS-Mounts für die Anwendungs-VMs erneut.
6. Rufen Sie ein Failback zur geschützten Site auf, indem Sie SnapMirror nach der Wiederherstellung der primären Site rückwärts neu synchronisieren.

Bereitstellungsdetails

Konfigurieren Sie CVO auf Azure und replizieren Sie Volumes nach CVO

Der erste Schritt besteht darin, Cloud Volumes ONTAP auf Azure zu konfigurieren ("Link") und replizieren Sie die gewünschten Volumes mit den gewünschten Frequenzen und Snapshot-Aufbewahrungen auf Cloud Volumes ONTAP .



Konfigurieren Sie AVS-Hosts und CVO-Datenzugriff

Zwei wichtige Faktoren, die bei der Bereitstellung des SDDC berücksichtigt werden müssen, sind die Größe des SDDC-Clusters in der Azure VMware-Lösung und die Dauer des Betriebs des SDDC. Diese beiden wichtigen Überlegungen für eine Disaster-Recovery-Lösung tragen zur Senkung der Gesamtbetriebskosten bei. Das SDDC kann aus nur drei Hosts bestehen, bei einer vollständigen Bereitstellung kann es aber auch ein Cluster mit mehreren Hosts sein.

Die Entscheidung zur Bereitstellung eines AVS-Clusters basiert in erster Linie auf den RPO/RTO-Anforderungen. Mit der Azure VMware-Lösung kann das SDDC rechtzeitig bereitgestellt werden, um es entweder auf Tests oder einen tatsächlichen Katastrophenfall vorzubereiten. Ein Just-in-Time bereitgestelltes SDDC spart ESXi-Hostkosten, wenn Sie nicht mit einer Katastrophe zu kämpfen haben. Diese Art der Bereitstellung beeinträchtigt die RTO jedoch um einige Stunden, während SDDC bereitgestellt wird.

Die am häufigsten eingesetzte Option besteht darin, SDDC im ständig eingeschalteten Pilotlichtmodus laufen zu lassen. Diese Option bietet einen kleinen Platzbedarf von drei Hosts, die immer verfügbar sind. Darüber hinaus beschleunigt sie die Wiederherstellungsvorgänge, indem sie eine laufende Basislinie für Simulationsaktivitäten und Konformitätsprüfungen bereitstellt und so das Risiko einer Betriebsabweichung zwischen den Produktions- und DR-Standorten vermeidet. Der Pilotlicht-Cluster kann bei Bedarf schnell auf das gewünschte Niveau hochskaliert werden, um ein tatsächliches DR-Ereignis zu bewältigen.

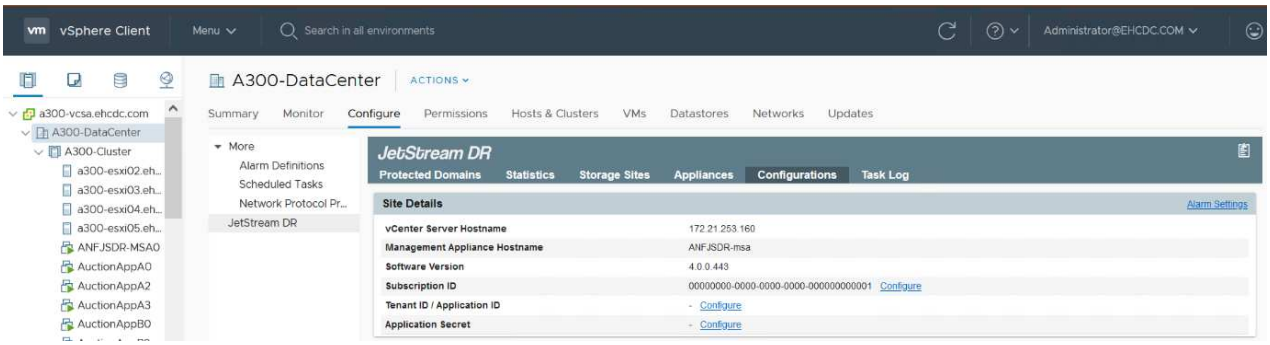
Informationen zum Konfigurieren von AVS SDDC (sei es auf Abruf oder im Pilotlichtmodus) finden Sie unter"Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf Azure" . Stellen Sie als Voraussetzung sicher, dass die auf den AVS-Hosts befindlichen Gast-VMs nach dem Herstellen der Verbindung Daten von Cloud Volumes ONTAP nutzen können.

Nachdem Cloud Volumes ONTAP und AVS ordnungsgemäß konfiguriert wurden, beginnen Sie mit der Konfiguration von Jetstream, um die Wiederherstellung lokaler Workloads auf AVS (VMs mit Anwendungs-VMDKs und VMs mit In-Guest-Speicher) zu automatisieren. Verwenden Sie dazu den VAIO-Mechanismus und nutzen Sie SnapMirror für Anwendungs-Volume-Kopien auf Cloud Volumes ONTAP.

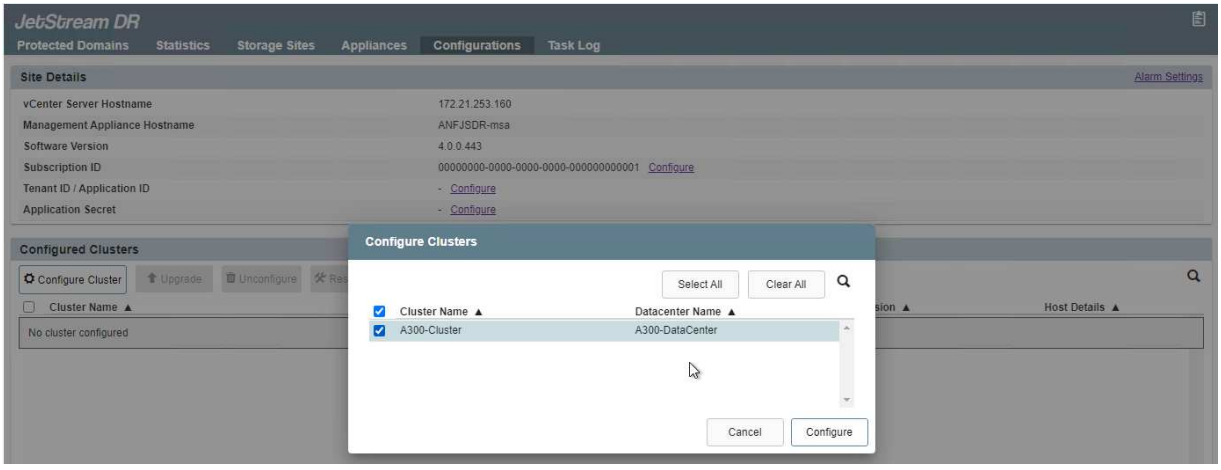
Installieren Sie JetStream DR im lokalen Rechenzentrum

Die JetStream DR-Software besteht aus drei Hauptkomponenten: der JetStream DR Management Server Virtual Appliance (MSA), der DR Virtual Appliance (DRVA) und Hostkomponenten (E/A-Filterpakete). Das MSA wird verwendet, um Hostkomponenten auf dem Computercluster zu installieren und zu konfigurieren und anschließend die JetStream DR-Software zu verwalten. Der Installationsvorgang läuft wie folgt ab:

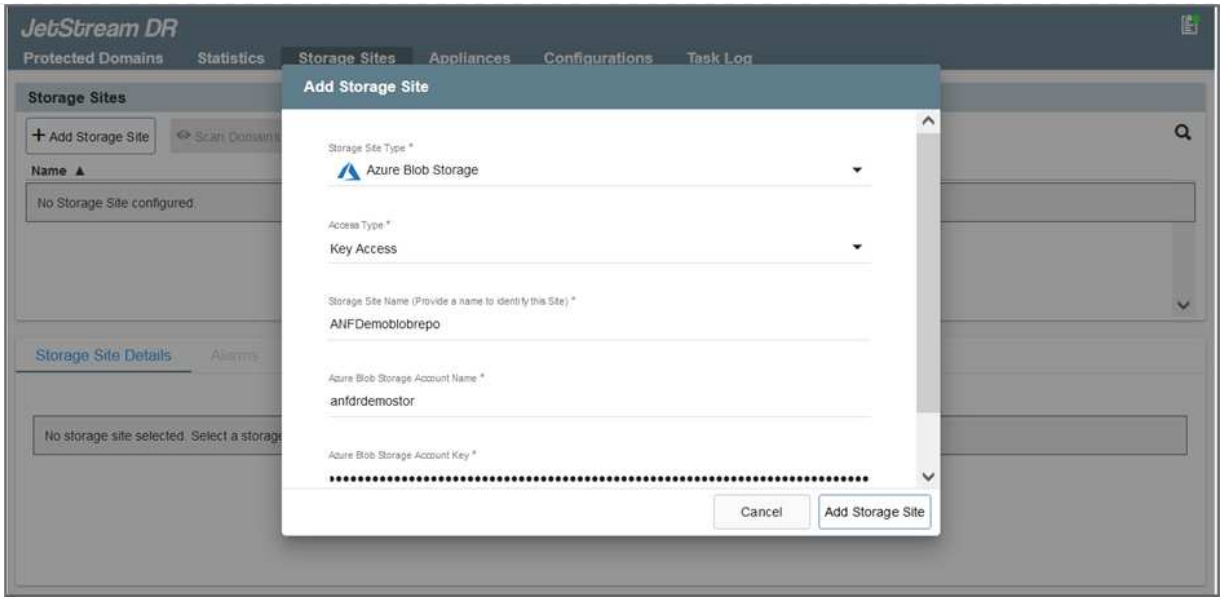
1. Prüfen Sie die Voraussetzungen.
2. Führen Sie das Kapazitätsplanungstool aus, um Empfehlungen zu Ressourcen und Konfigurationen zu erhalten.
3. Stellen Sie den JetStream DR MSA auf jedem vSphere-Host im vorgesehenen Cluster bereit.
4. Starten Sie das MSA mit seinem DNS-Namen in einem Browser.
5. Registrieren Sie den vCenter-Server beim MSA.
6. Nachdem JetStream DR MSA bereitgestellt und der vCenter Server registriert wurde, navigieren Sie mit dem vSphere Web Client zum JetStream DR-Plug-In. Dies kann durch Navigieren zu Rechenzentrum > Konfigurieren > JetStream DR erfolgen.



7. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
   a. Konfigurieren Sie den Cluster mit dem E/A-Filterpaket.

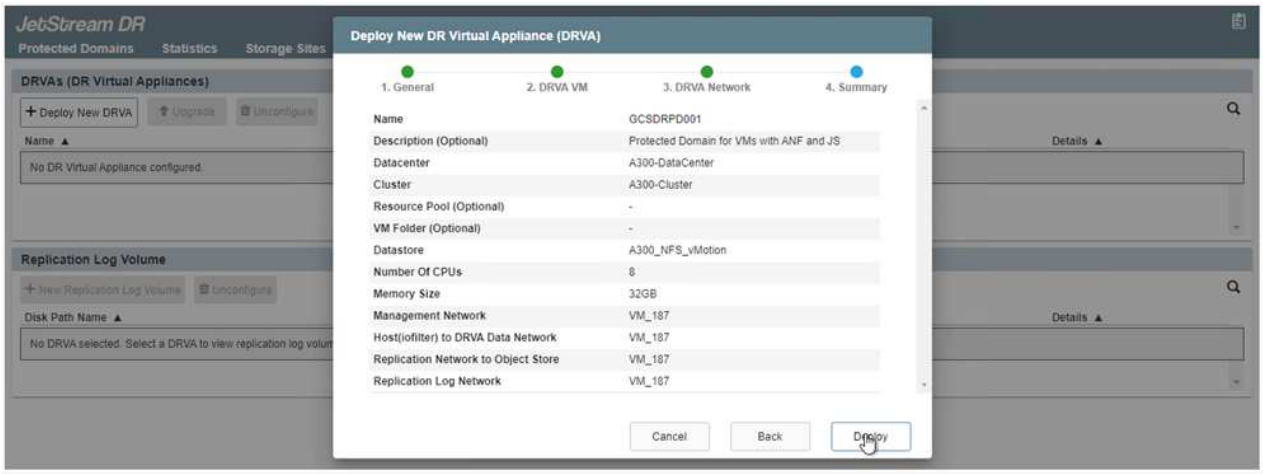


   b. Fügen Sie den Azure Blob-Speicher am Wiederherstellungsstandort hinzu.

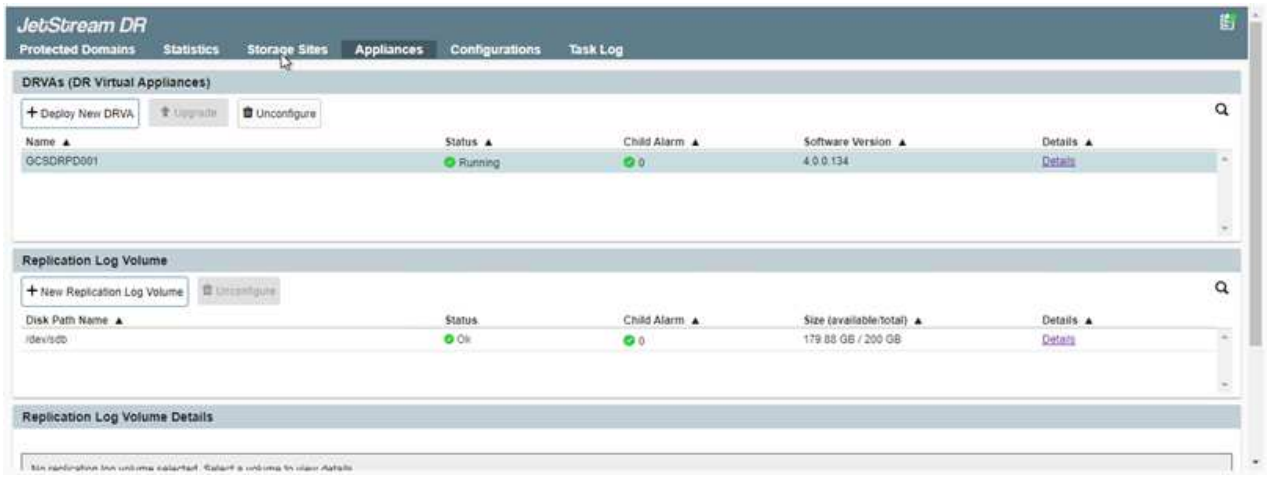


8. Stellen Sie die erforderliche Anzahl von DR Virtual Appliances (DRVAs) über die Registerkarte „Appliances“ bereit.

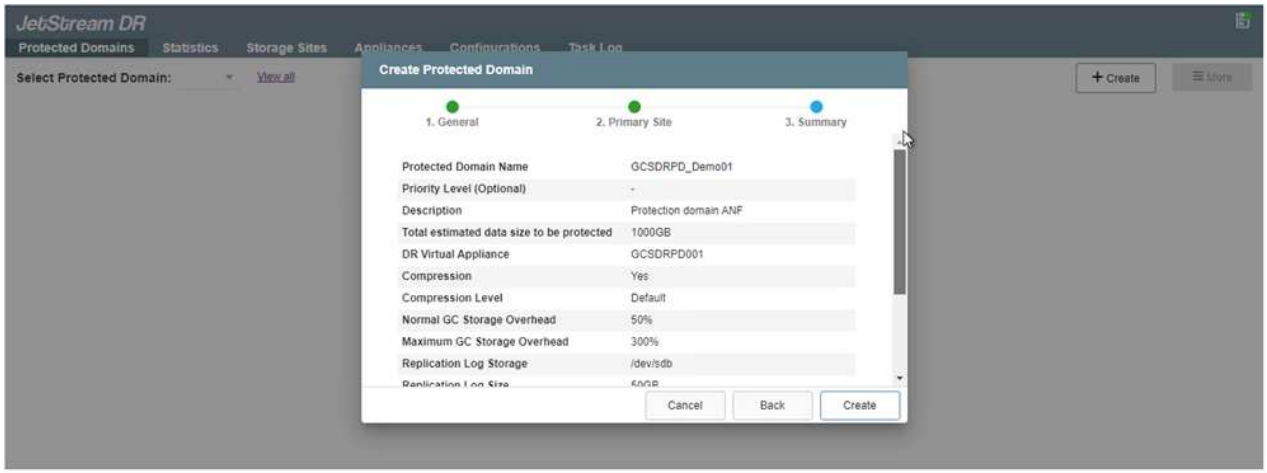
> Verwenden Sie das Kapazitätsplanungstool, um die Anzahl der erforderlichen DRVAs zu schätzen.

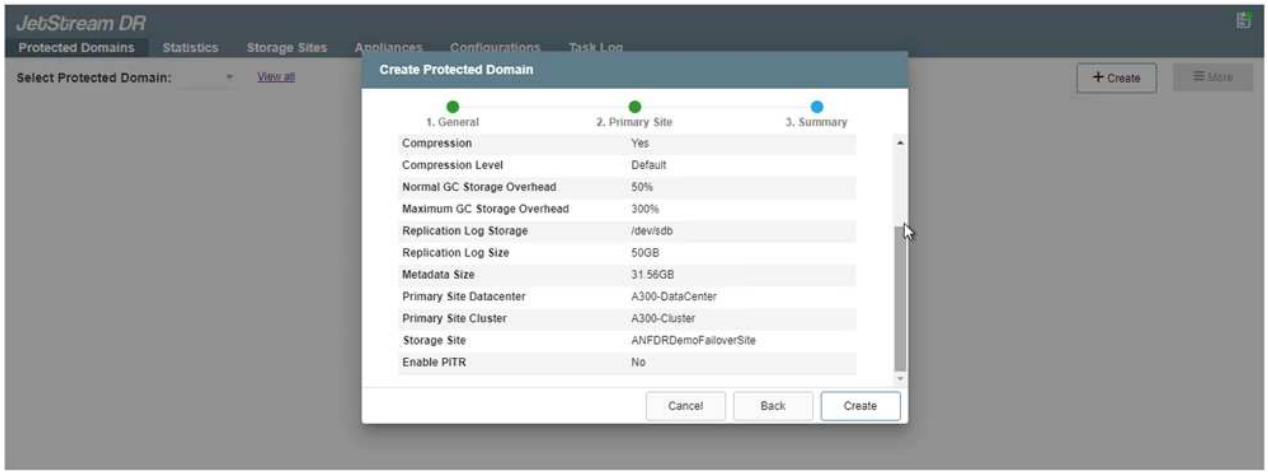


9. Erstellen Sie Replikationsprotokollvolumes für jeden DRVA mithilfe des VMDK aus den verfügbaren Datenspeichern oder dem unabhängigen gemeinsam genutzten iSCSI-Speicherpool.



10. 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 einen Satz von Anwendungs-VMs innerhalb des Clusters, die gemeinsam geschützt werden und denen eine Prioritätsreihenfolge für Failover-/Failback-Vorgänge zugewiesen wird.

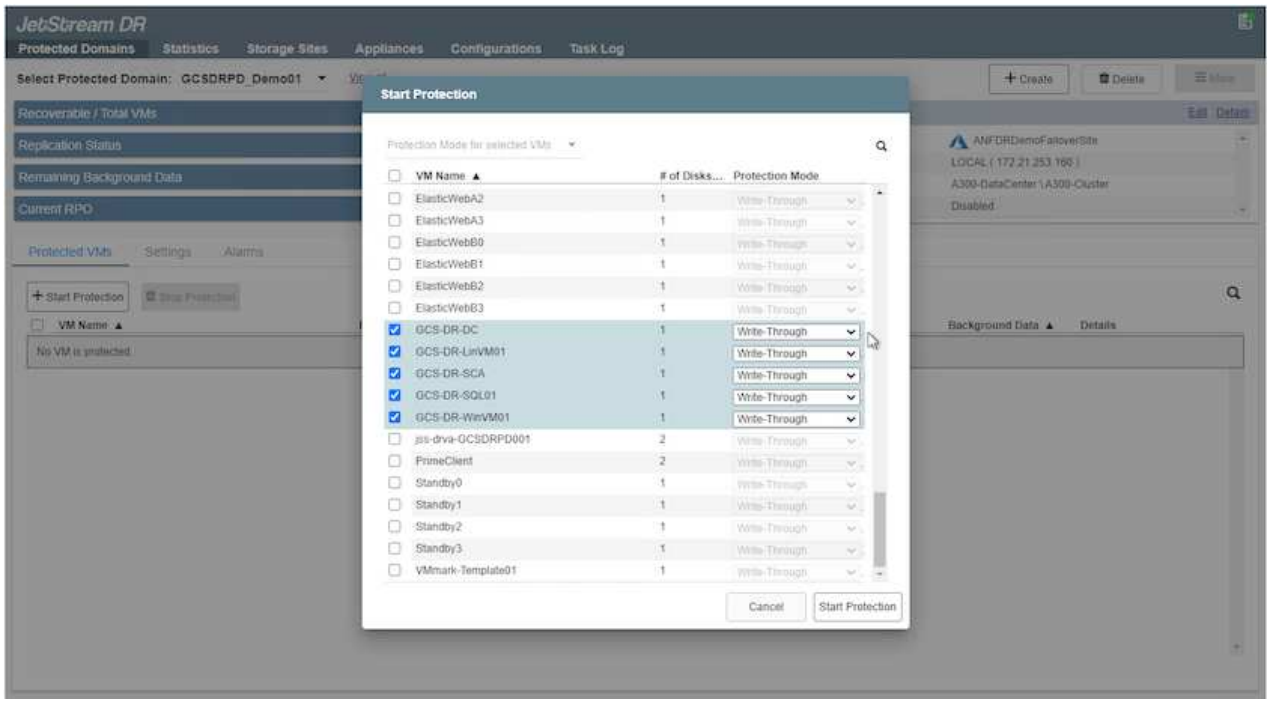




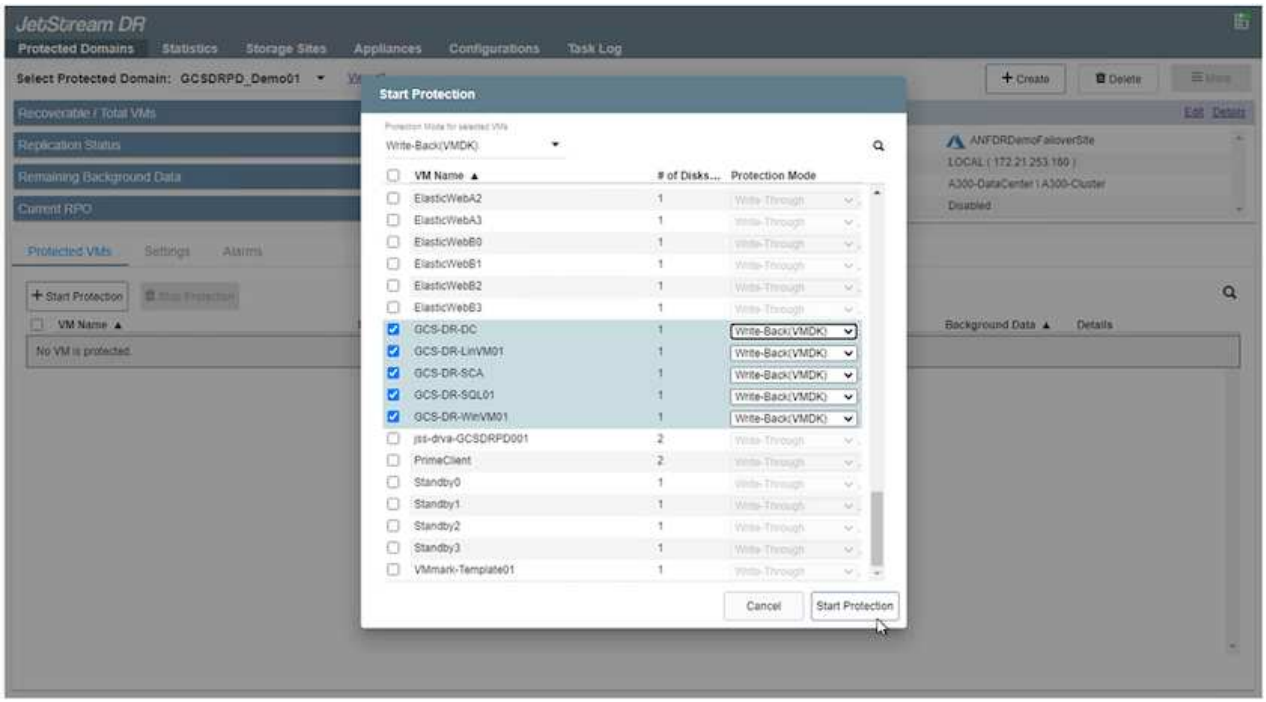
11. Wählen Sie die zu schützenden VMs aus und gruppieren Sie die VMs basierend auf der Abhängigkeit in Anwendungsgruppen. Mithilfe von Anwendungsdefinitionen können Sie VM-Sätze in logische Gruppen gruppieren, die deren Startreihenfolge, Startverzögerungen und optionale Anwendungsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

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

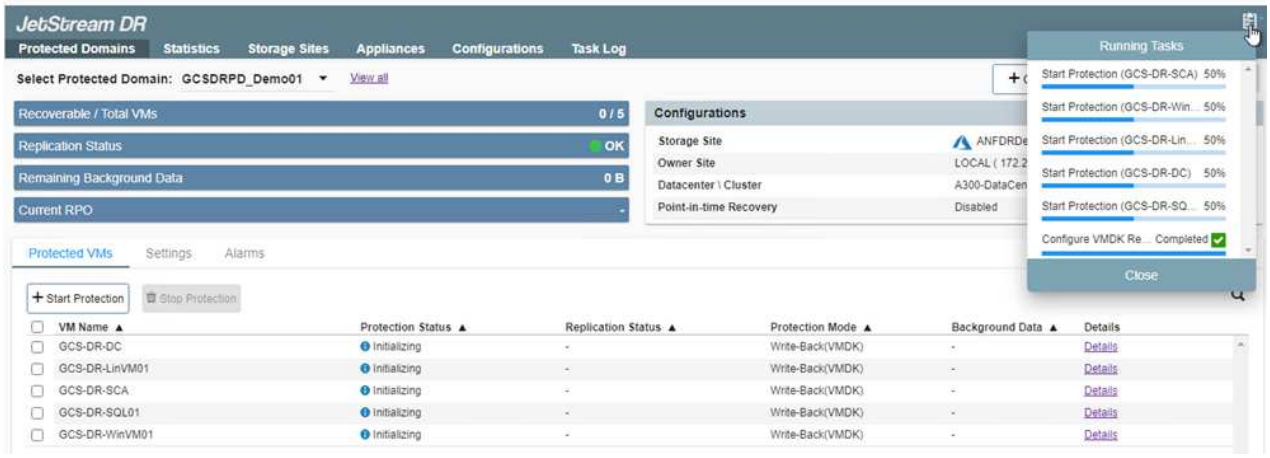
Der Write-Back-Modus (VMDK) bietet eine höhere Leistung.



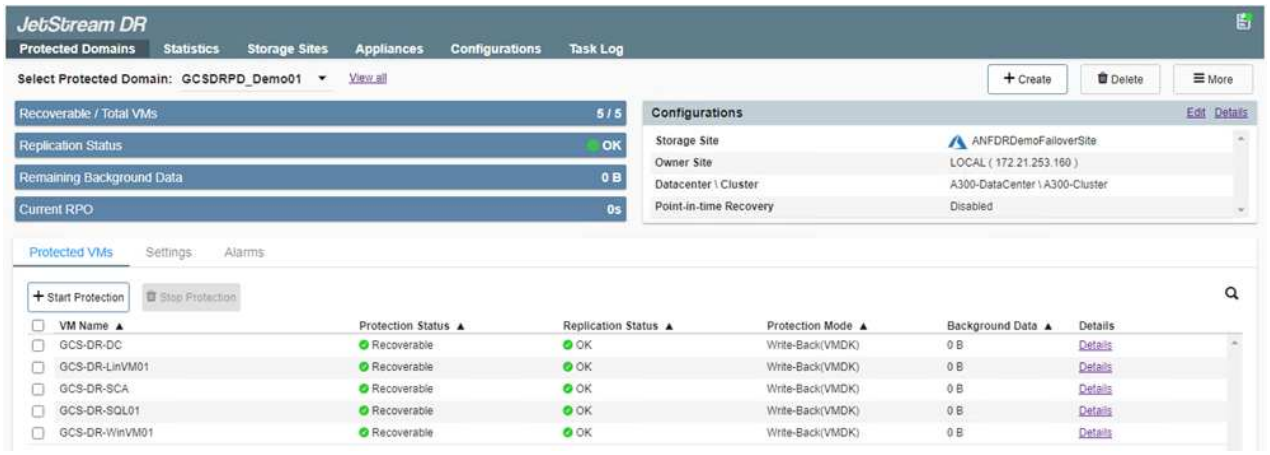
12. Stellen Sie sicher, dass Replikationsprotokollvolumes auf Hochleistungsspeichern abgelegt werden.



13. Wenn Sie fertig sind, klicken Sie auf „Schutz starten“ für die geschützte Domäne. Dadurch wird die Datenreplikation für die ausgewählten VMs in den angegebenen Blob-Speicher gestartet.



14. Nach Abschluss der Replikation wird der VM-Schutzstatus als „Wiederherstellbar“ gekennzeichnet.

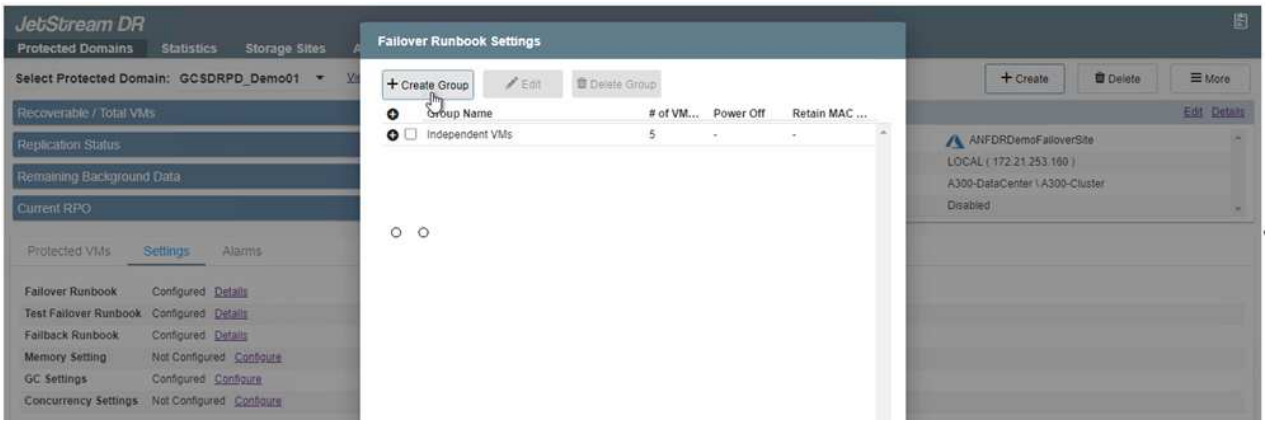


Failover-Runbooks können so konfiguriert werden, dass sie die VMs gruppieren (eine sogenannte Wiederherstellungsgruppe), die Startreihenfolge festlegen und die CPU-/Speichereinstellungen zusammen mit den IP-Konfigurationen ändern.

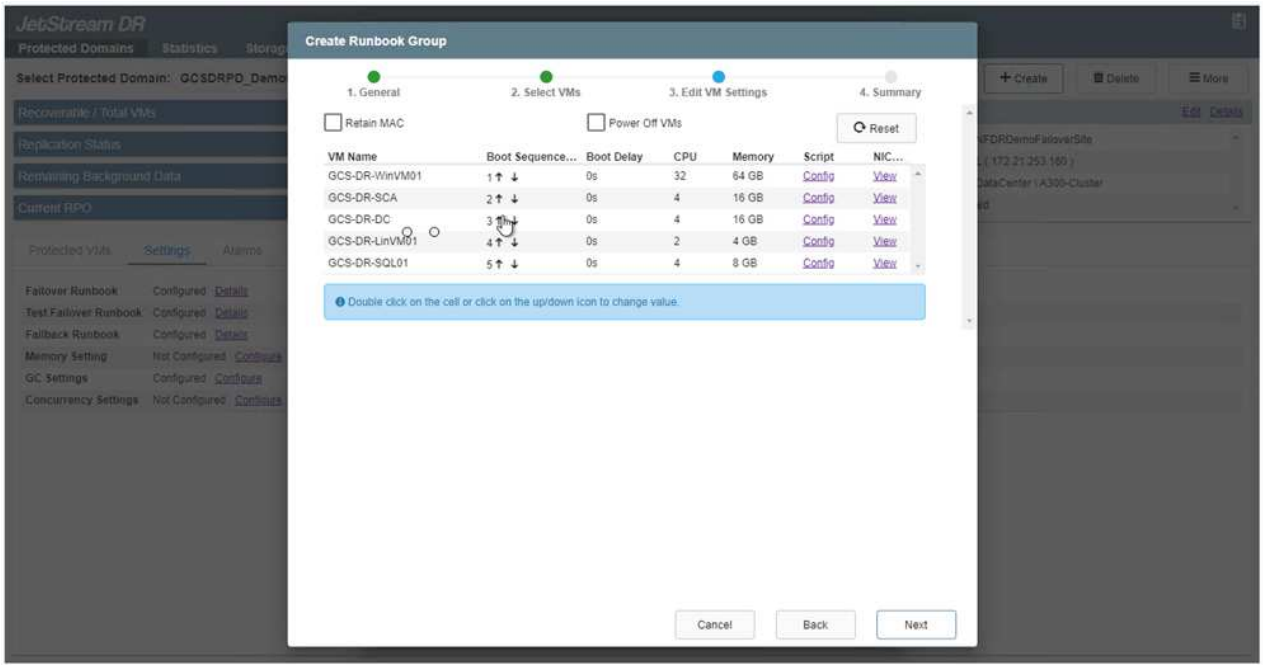
15. Klicken Sie auf „Einstellungen“ und dann auf den Link „Runbook konfigurieren“, um die Runbook-Gruppe zu konfigurieren.

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

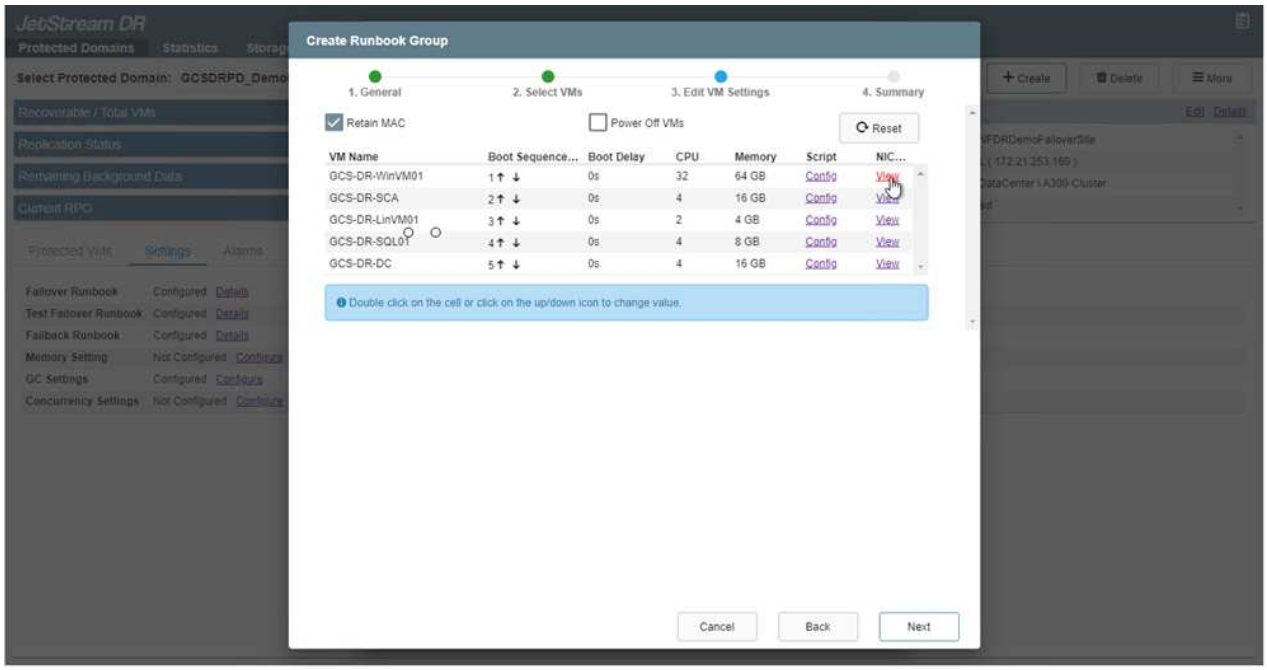
Wenden Sie bei Bedarf im unteren Teil des Bildschirms benutzerdefinierte Vor- und Nachskripte an, die vor und nach dem Betrieb der Runbook-Gruppe automatisch ausgeführt werden. Stellen Sie sicher, dass sich die Runbook-Skripte auf dem Verwaltungsserver befinden.



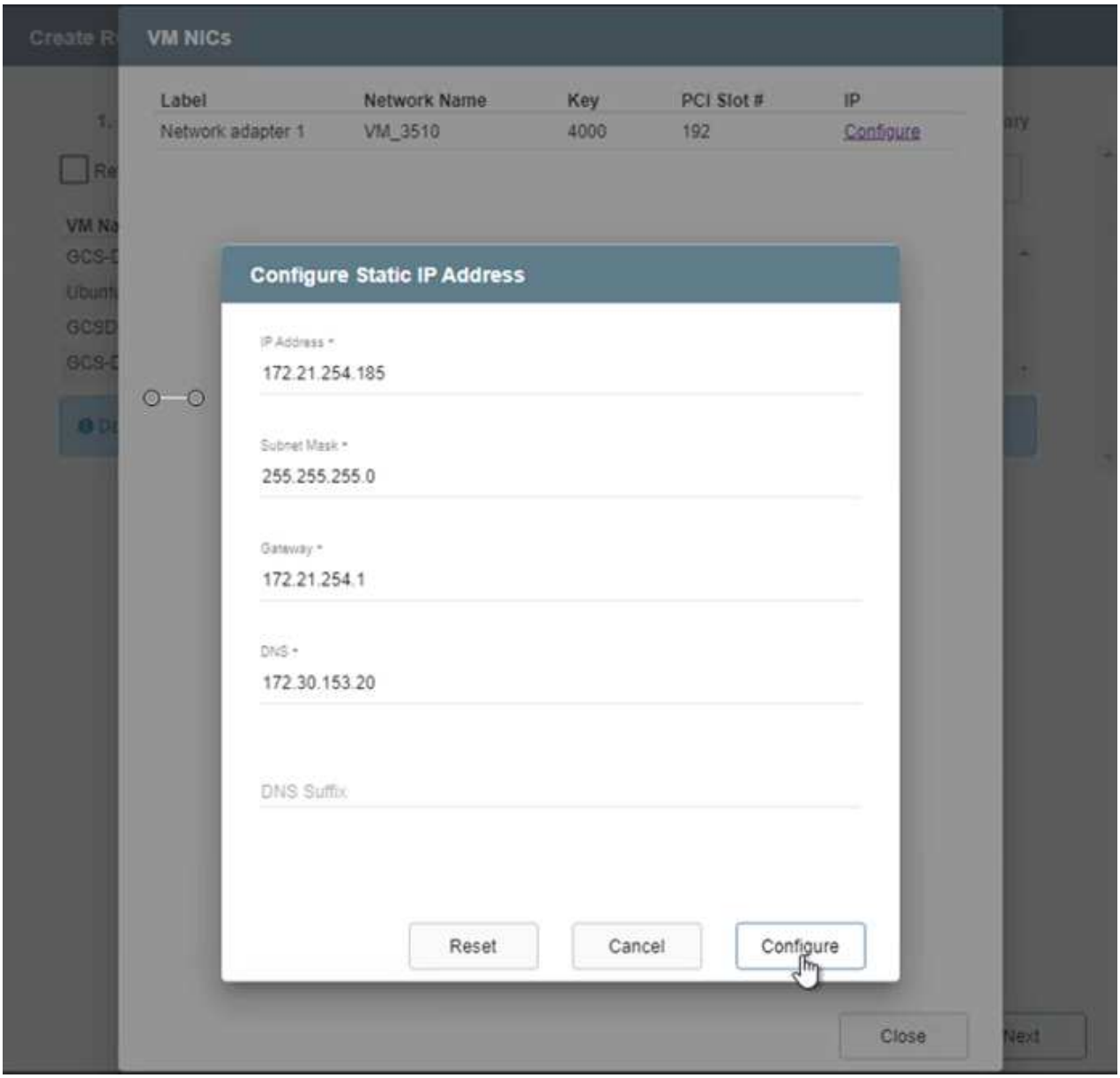
17. Bearbeiten Sie die VM-Einstellungen nach Bedarf. Geben Sie die Parameter für die Wiederherstellung der VMs an, einschließlich der Startreihenfolge, der Startverzögerung (angegeben in Sekunden), der Anzahl der CPUs und der Menge des zuzuweisenden Speichers. Ändern Sie die Startreihenfolge der VMs, indem Sie auf die Aufwärts- oder Abwärtspfeile klicken. Es werden auch Optionen zum Beibehalten des MAC bereitgestellt.

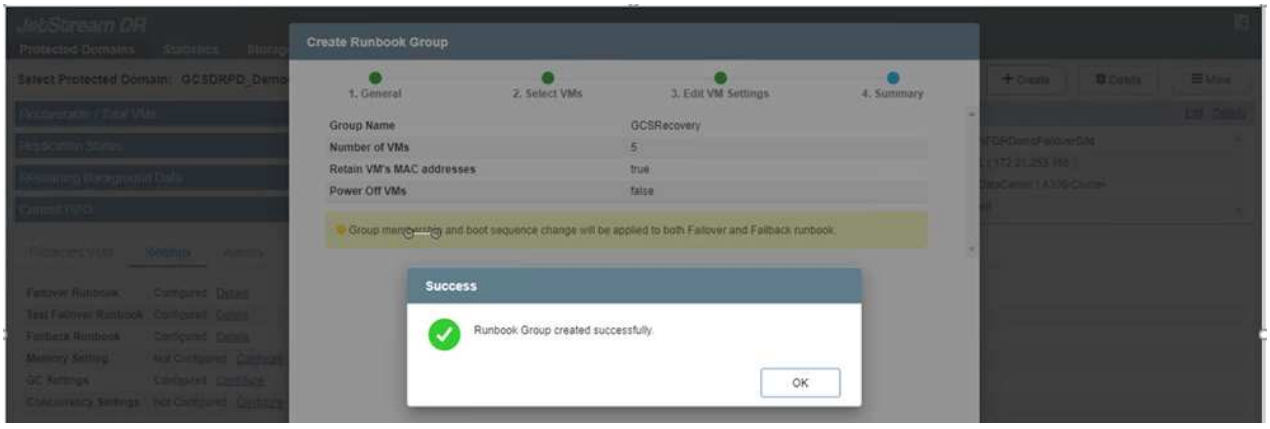


18. Für die einzelnen VMs der Gruppe können statische IP-Adressen manuell konfiguriert werden. Klicken Sie auf den Link „NIC-Ansicht“ einer VM, um ihre IP-Adresseinstellungen manuell zu konfigurieren.



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 jetzt als „Konfiguriert“ aufgeführt. Failover- und Failback-Runbookgruppen werden paarweise unter Verwendung derselben anfänglichen Gruppe von VMs und Einstellungen erstellt. Bei Bedarf können die Einstellungen jeder Runbook-Gruppe individuell angepasst werden, indem Sie auf den entsprechenden Link „Details“ klicken und Änderungen

vornehmen.

Installieren Sie JetStream DR für AVS in der privaten Cloud

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 Punkte:

- 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 einen RTO-Modus nahezu Null für unternehmenskritische Domänen. Für diese Domänen sollte der Zielspeicher vorinstalliert sein. In diesem Fall ist ANF ein empfohlener Speichertyp.

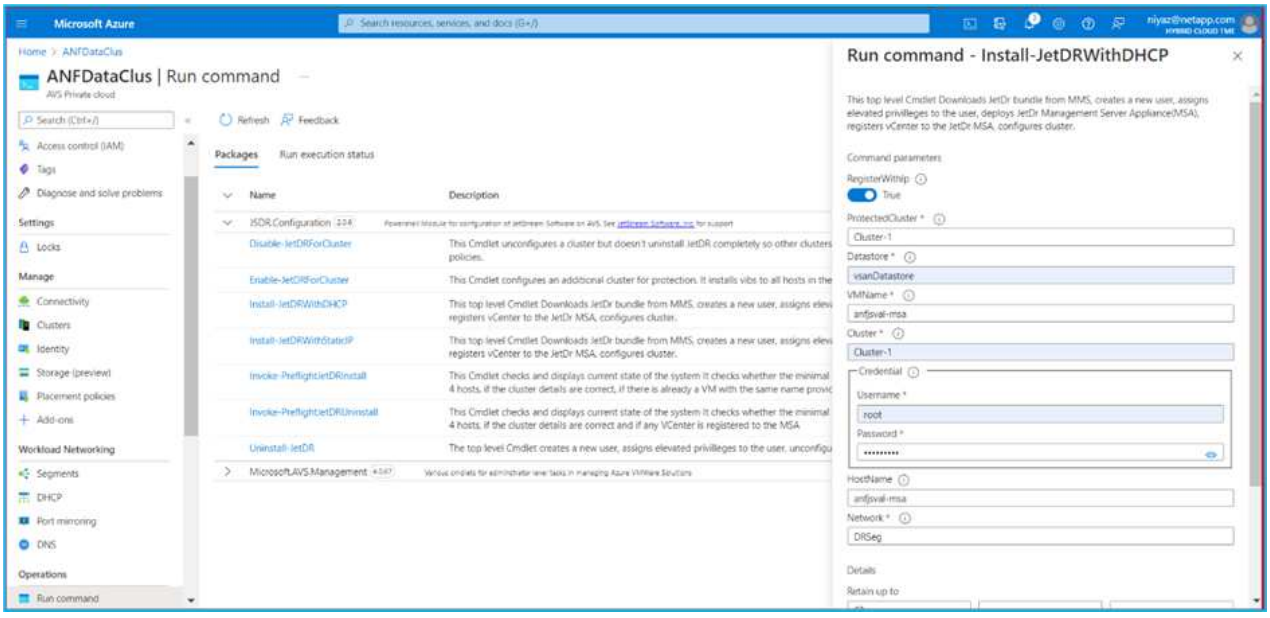
ⓘ Die Netzwerkkonfiguration einschließlich der Segmenterstellung sollte auf dem AVS-Cluster so konfiguriert werden, dass sie den lokalen Anforderungen entspricht.

ⓘ Abhängig von den SLA- und RTO-Anforderungen können Sie kontinuierliches Failover oder den regulären (Standard-)Failover-Modus verwenden. Um eine RTO von nahezu Null zu erreichen, sollten Sie am Wiederherstellungsort mit der kontinuierlichen Rehydrierung beginnen.

1. Um JetStream DR für AVS in einer privaten Azure VMware Solution-Cloud zu installieren, verwenden Sie den Befehl „Ausführen“. Gehen Sie im Azure-Portal zur Azure VMware-Lösung, wählen Sie die private Cloud aus und wählen Sie „Befehl ausführen“ > „Pakete“ > „JSDR.Configuration“.

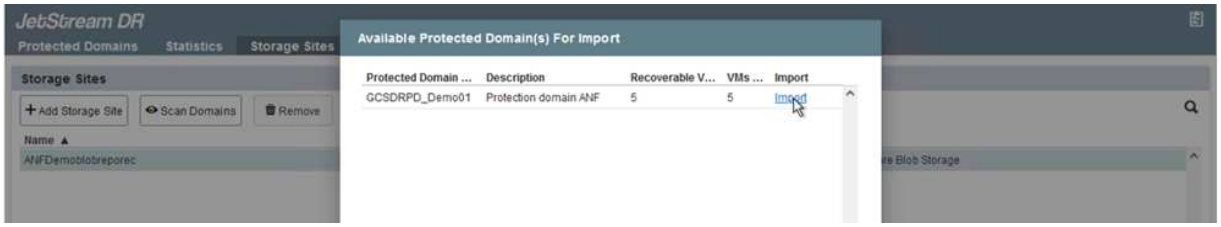
   ⓘ Der Standard-CloudAdmin-Benutzer der Azure VMware-Lösung verfügt nicht über ausreichende Berechtigungen, um JetStream DR für AVS zu installieren. Die Azure VMware Solution ermöglicht eine vereinfachte und automatisierte Installation von JetStream DR durch Aufrufen des Azure VMware Solution-Ausführungsbefehls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

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

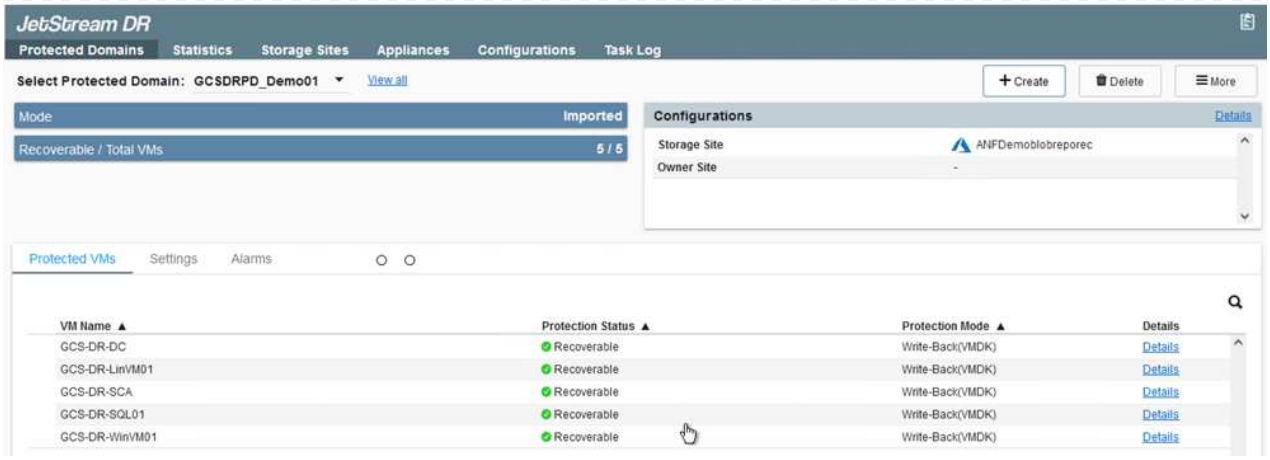


2. Aktualisieren Sie den Browser, nachdem die Installation von JetStream DR für AVS abgeschlossen ist. Um auf die JetStream DR-Benutzeroberfläche zuzugreifen, gehen Sie zu SDDC Datacenter > Konfigurieren > JetStream DR.

3. Führen Sie über die JetStream DR-Schnittstelle die folgenden Aufgaben aus:
   a. Fügen Sie das Azure Blob Storage-Konto, das zum Schutz des lokalen Clusters verwendet wurde, als Speicherstandort hinzu und führen Sie dann die Option „Domänen scannen“ aus.
   b. Wählen Sie im angezeigten Popup-Dialogfenster die zu importierende geschützte Domäne aus und klicken Sie dann auf den Link „Importieren“.



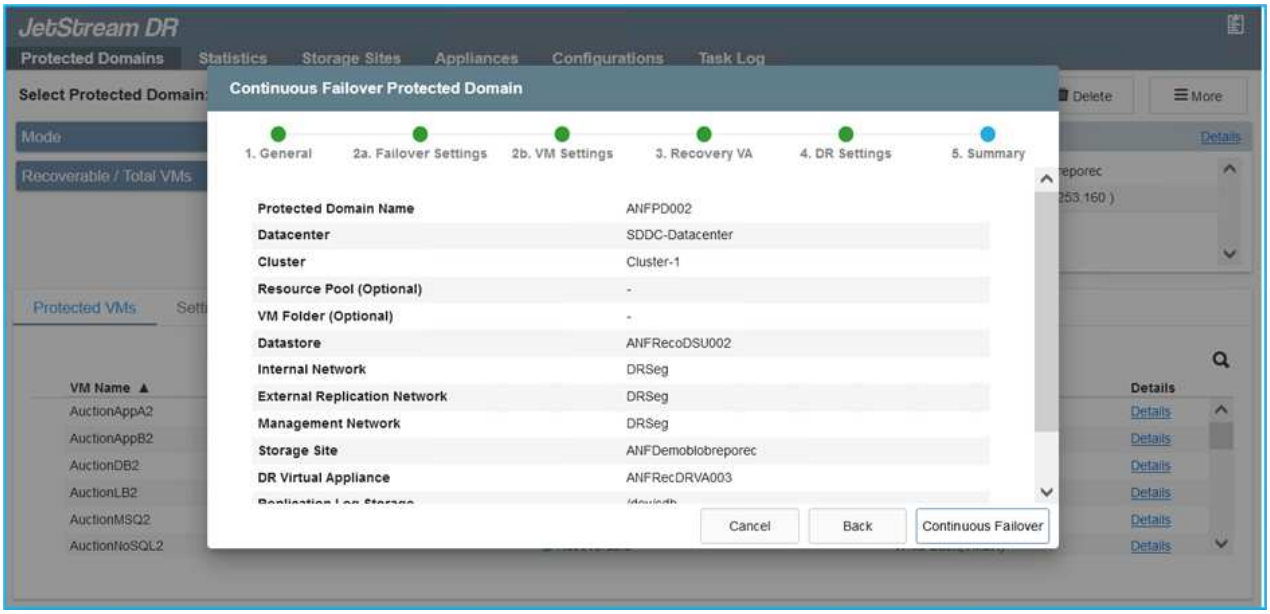
4. Die Domäne wird zur Wiederherstellung importiert. Gehen Sie zur Registerkarte „Geschützte Domänen“ und überprüfen Sie, ob die gewünschte Domäne ausgewählt wurde, oder wählen Sie die gewünschte Domäne aus dem Menü „Geschützte Domäne auswählen“ aus. Es wird eine Liste der wiederherstellbaren VMs in der geschützten Domäne angezeigt.



5. Nachdem die geschützten Domänen importiert wurden, stellen Sie DRVA-Geräte bereit.

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

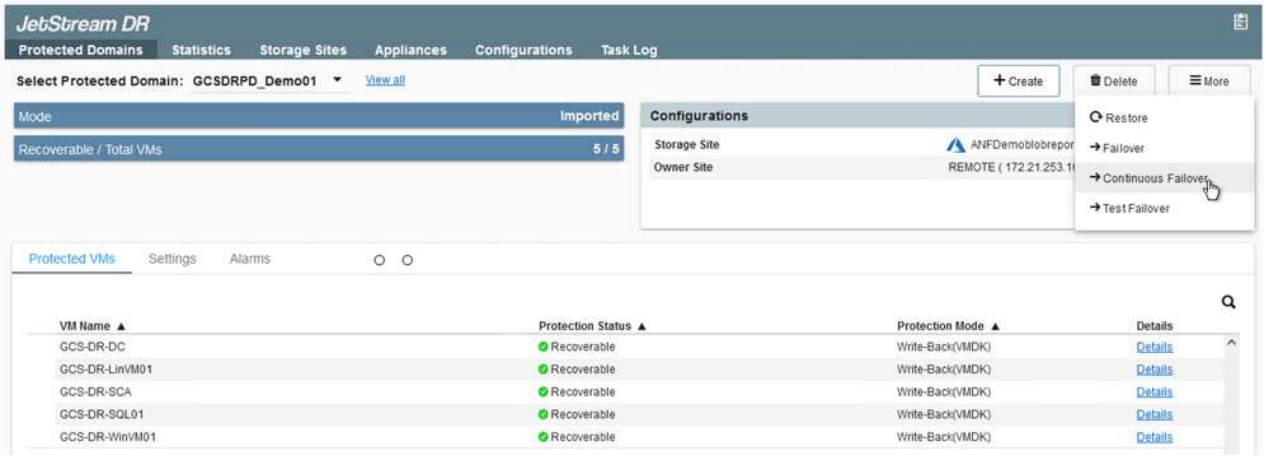
6. Erstellen Sie Replikationsprotokollvolumes mithilfe verfügbarer vSAN- oder ANF-Datenspeicher.
7. Importieren Sie die geschützten Domänen und konfigurieren Sie die Wiederherstellungs-VA so, dass ein ANF-Datenspeicher für VM-Platzierungen verwendet wird.



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.

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

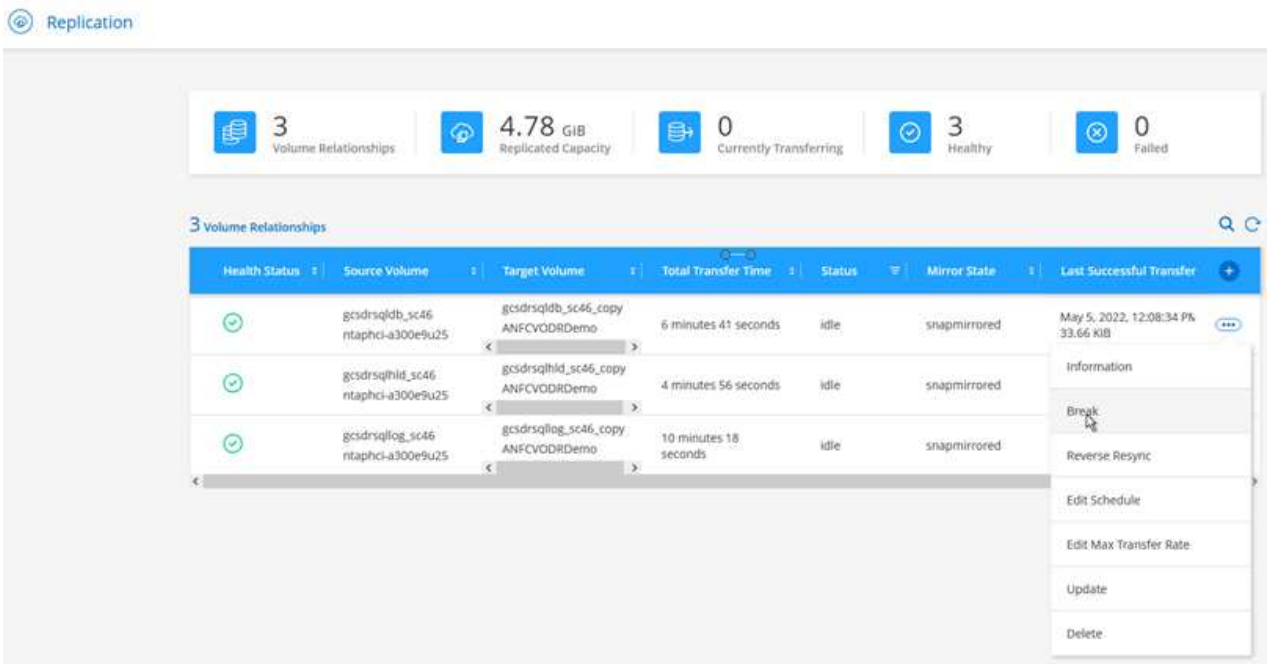
Obwohl sich die Modi „Continuous Failover“ und „Failover“ hinsichtlich des Zeitpunkts der Konfiguration unterscheiden, werden beide Failover-Modi mit denselben Schritten konfiguriert. Als Reaktion auf ein Katastrophenereignis werden Failover-Schritte konfiguriert und gemeinsam ausgeführt. Ein kontinuierliches Failover kann jederzeit konfiguriert und dann während des normalen Systembetriebs im Hintergrund ausgeführt werden. Nach dem Auftreten eines Katastrophenereignisses wird ein kontinuierliches Failover durchgeführt, um den Besitz der geschützten VMs sofort auf den Wiederherstellungsstandort zu übertragen (RTO nahe Null).

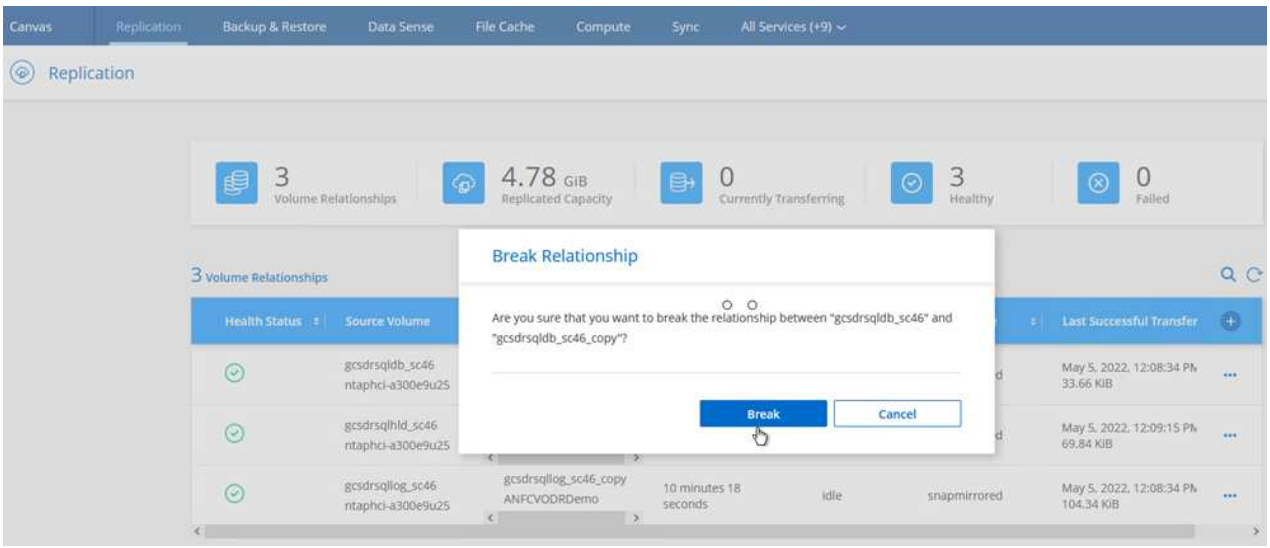


Der kontinuierliche Failover-Prozess beginnt und sein Fortschritt kann über die Benutzeroberfläche überwacht werden. Wenn Sie im Abschnitt „Aktueller Schritt“ auf das blaue Symbol klicken, wird ein Popup-Fenster mit Details zum aktuellen Schritt des Failover-Prozesses angezeigt.

Failover und Failback

1. Nach einem Desaster im geschützten Cluster der On-Premises-Umgebung (Teil- oder Komplettausfall) können Sie nach Aufhebung der SnapMirror -Beziehung für die jeweiligen Anwendungsvolumes das Failover für VMs mit Jetstream auslösen.

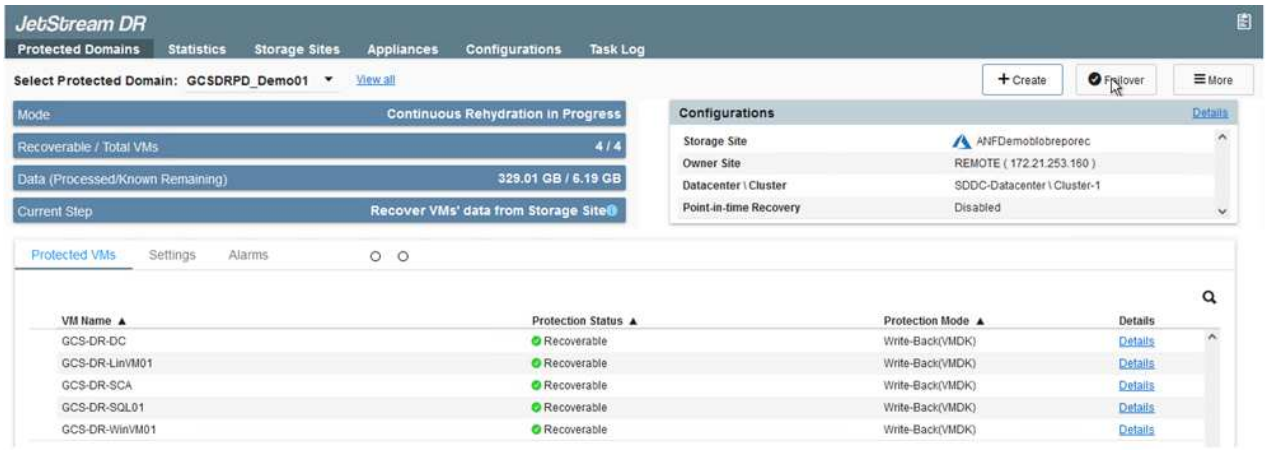


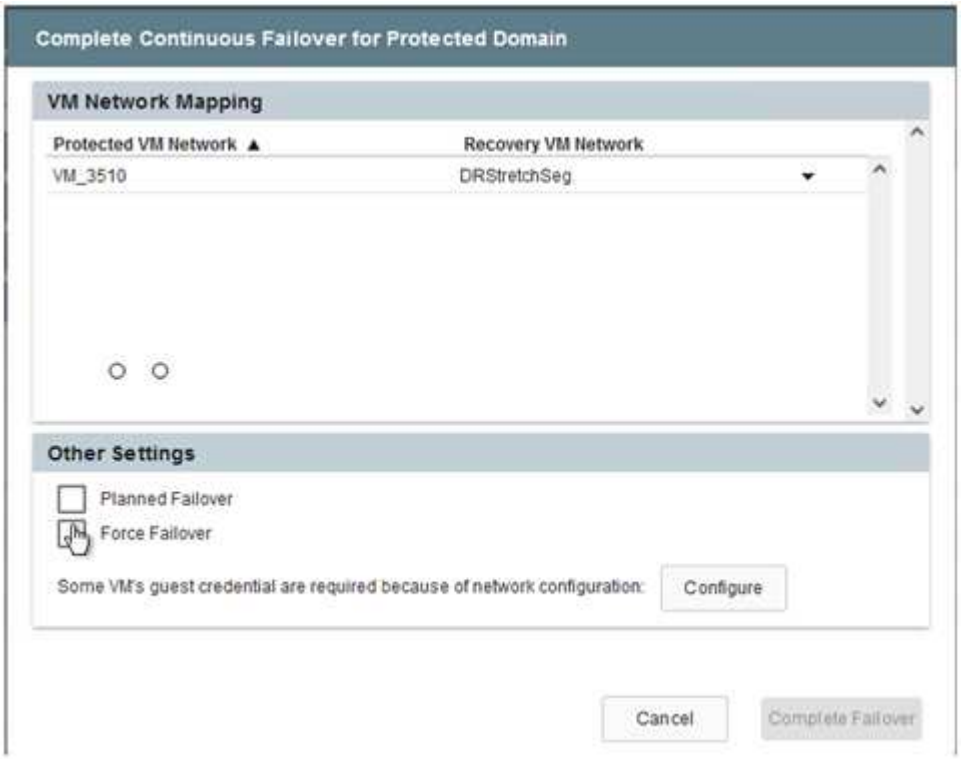


Dieser Schritt kann leicht automatisiert werden, um den Wiederherstellungsprozess zu erleichtern.

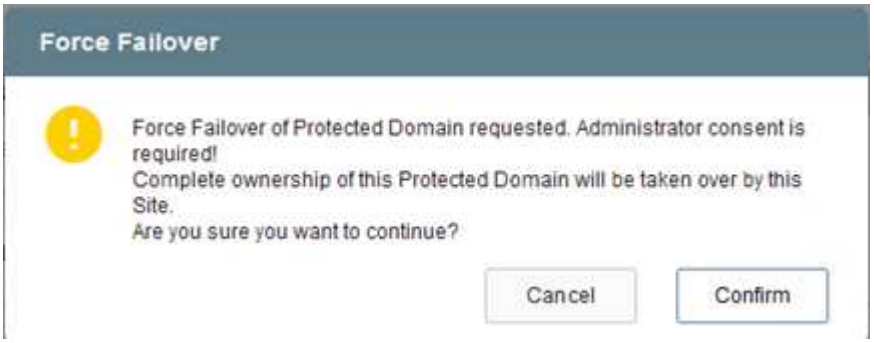
2. Greifen Sie auf die Jetstream-Benutzeroberfläche auf AVS SDDC (Zielseite) zu und lösen Sie die Failover-Option aus, um das Failover abzuschließen. Die Taskleiste zeigt den Fortschritt der Failover-Aktivitäten an.

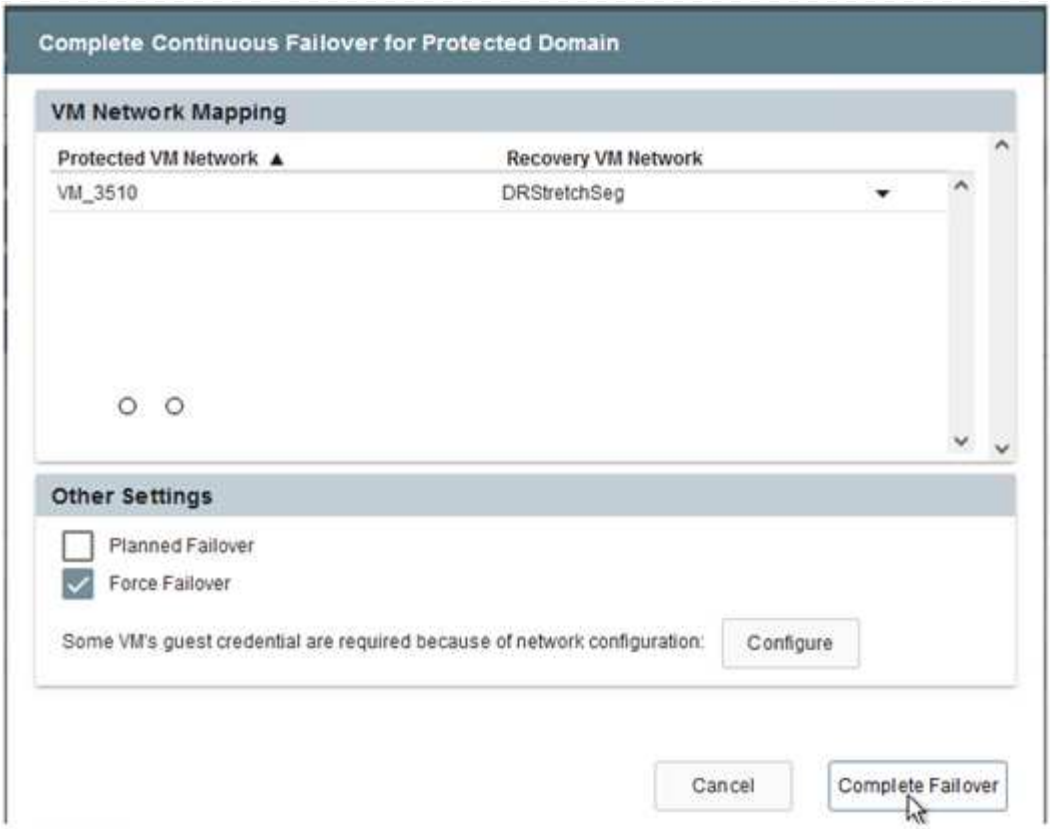
   Im Dialogfenster, das nach Abschluss des Failovers angezeigt wird, kann die Failover-Aufgabe als geplant angegeben oder als erzwungen angenommen werden.





Beim erzwungenen Failover wird davon ausgegangen, dass auf den primären Standort nicht mehr zugegriffen werden kann und der Besitz der geschützten Domäne direkt vom Wiederherstellungsstandort übernommen werden sollte.



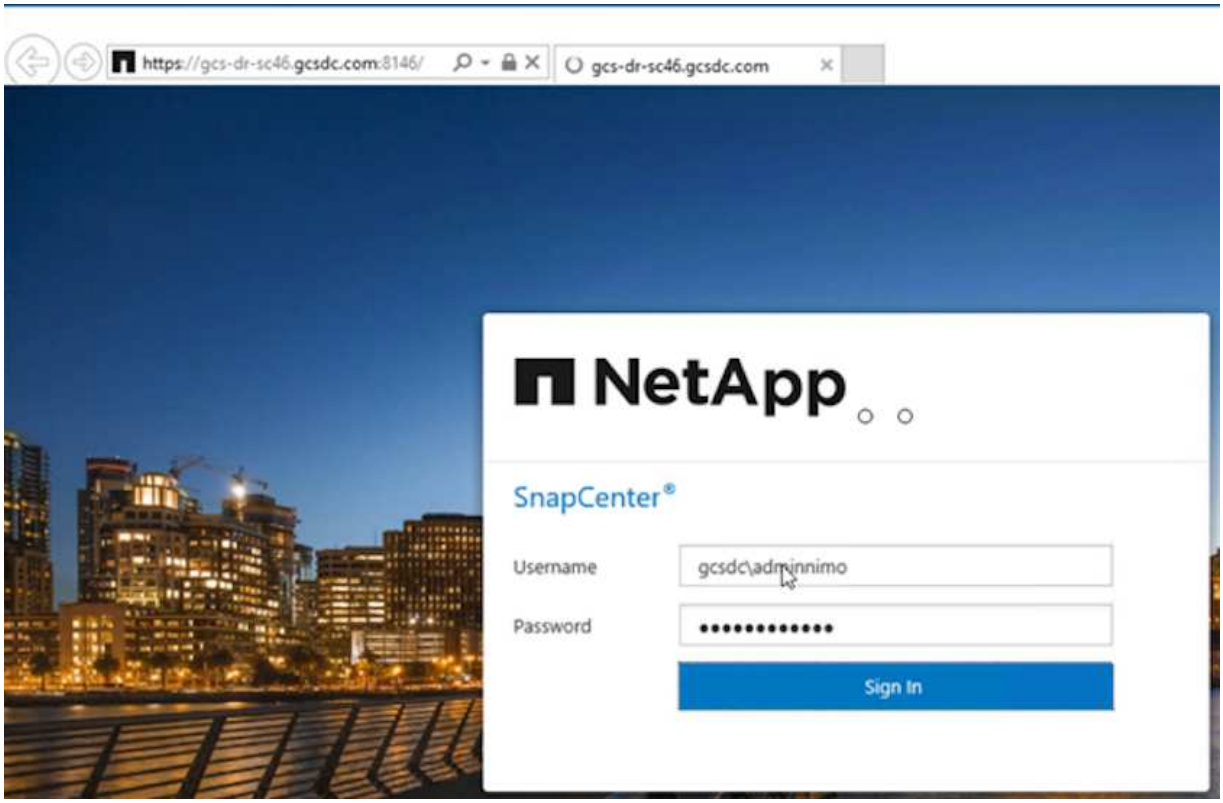


3. Nach Abschluss des kontinuierlichen Failovers wird eine Meldung angezeigt, die den Abschluss der Aufgabe bestätigt. Wenn die Aufgabe abgeschlossen ist, greifen Sie auf die wiederhergestellten VMs zu, um ISCSI- oder NFS-Sitzungen zu konfigurieren.

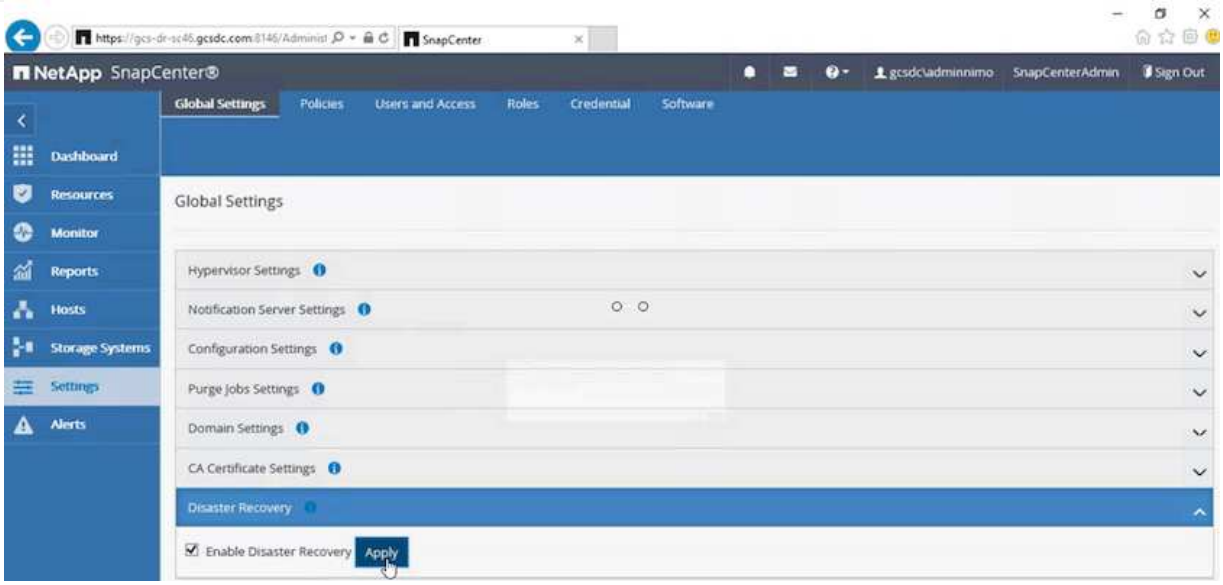
Der Failover-Modus ändert sich in „Wird im Failover ausgeführt“ und der VM-Status ist „Wiederherstellbar“. Alle VMs der geschützten Domäne werden jetzt am Wiederherstellungsstandort in dem durch die Failover-Runbook-Einstellungen angegebenen Zustand ausgeführt.

Um die Failover-Konfiguration und -Infrastruktur zu überprüfen, kann JetStream DR im Testmodus (Option „Test-Failover“) betrieben werden, um die Wiederherstellung virtueller Maschinen und ihrer Daten aus dem Objektspeicher in eine Testwiederherstellungsumgebung zu beobachten. Wenn ein Failover-Verfahren im Testmodus ausgeführt wird, ähnelt sein Ablauf einem tatsächlichen Failover-Prozess.

4. Nachdem die virtuellen Maschinen wiederhergestellt wurden, verwenden Sie die Speicher-Notfallwiederherstellung für den In-Guest-Speicher. Um diesen Prozess zu demonstrieren, wird in diesem Beispiel ein SQL-Server verwendet.
5. Melden Sie sich bei der wiederhergestellten SnapCenter VM auf AVS SDDC an und aktivieren Sie den DR-Modus.
   a. Greifen Sie über den Browser auf die SnapCenter -Benutzeroberfläche zu.



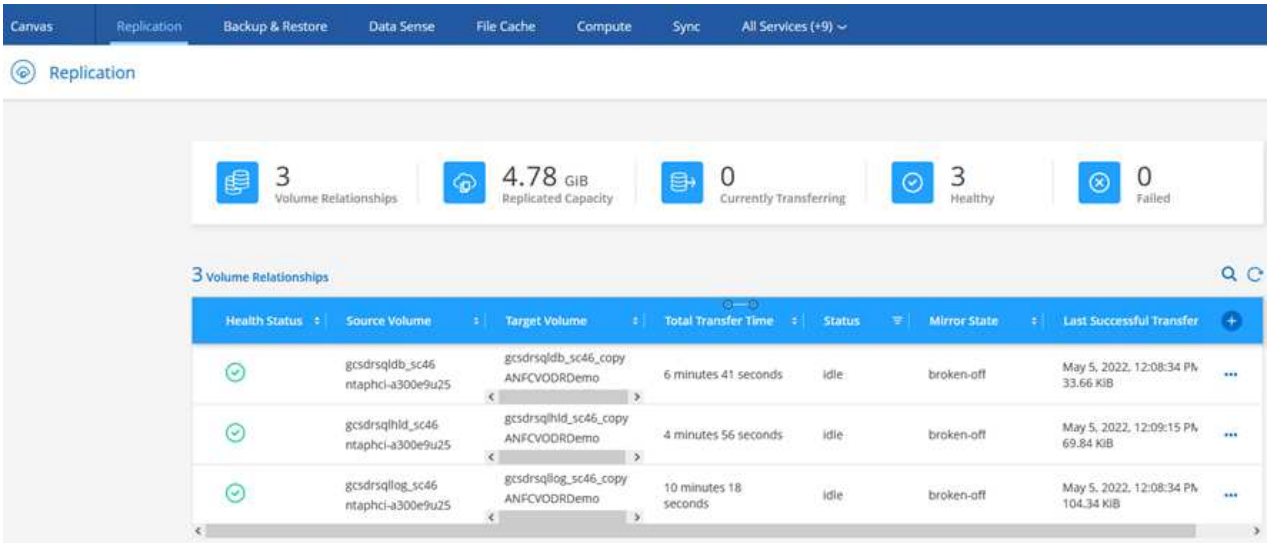
   b. Navigieren Sie auf der Seite „Einstellungen“ zu „Einstellungen > Globale Einstellungen > Notfallwiederherstellung“.
   c. Wählen Sie „Notfallwiederherstellung aktivieren“ aus.
   d. Klicken Sie auf „Übernehmen“.



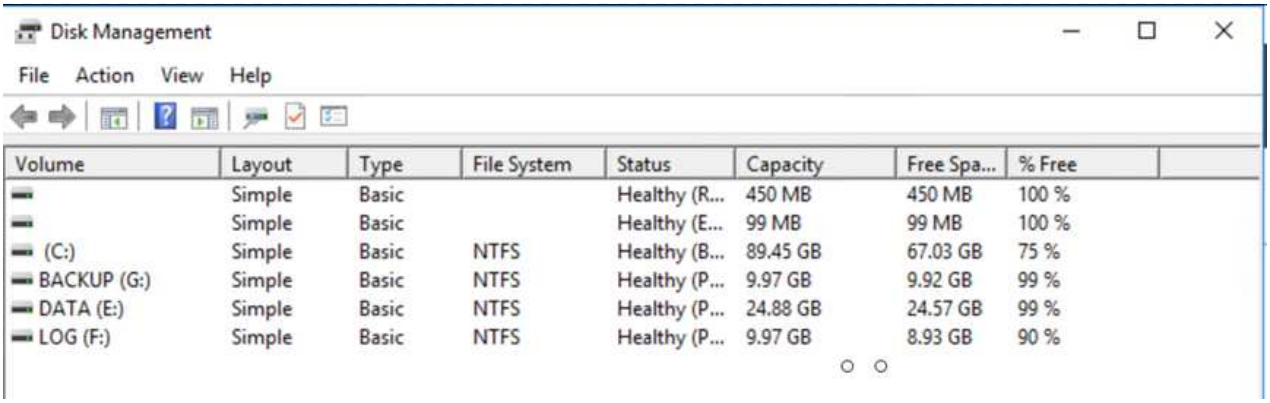
e. Überprüfen Sie, ob der DR-Job aktiviert ist, indem Sie auf Überwachen > Jobs klicken.

> Für die Speicher-Notfallwiederherstellung sollte NetApp SnapCenter 4.6 oder höher verwendet werden. Für frühere Versionen sollten anwendungskonsistente Snapshots (mit SnapMirror repliziert) verwendet und eine manuelle Wiederherstellung durchgeführt werden, falls frühere Sicherungen am Notfallwiederherstellungsstandort wiederhergestellt werden müssen.

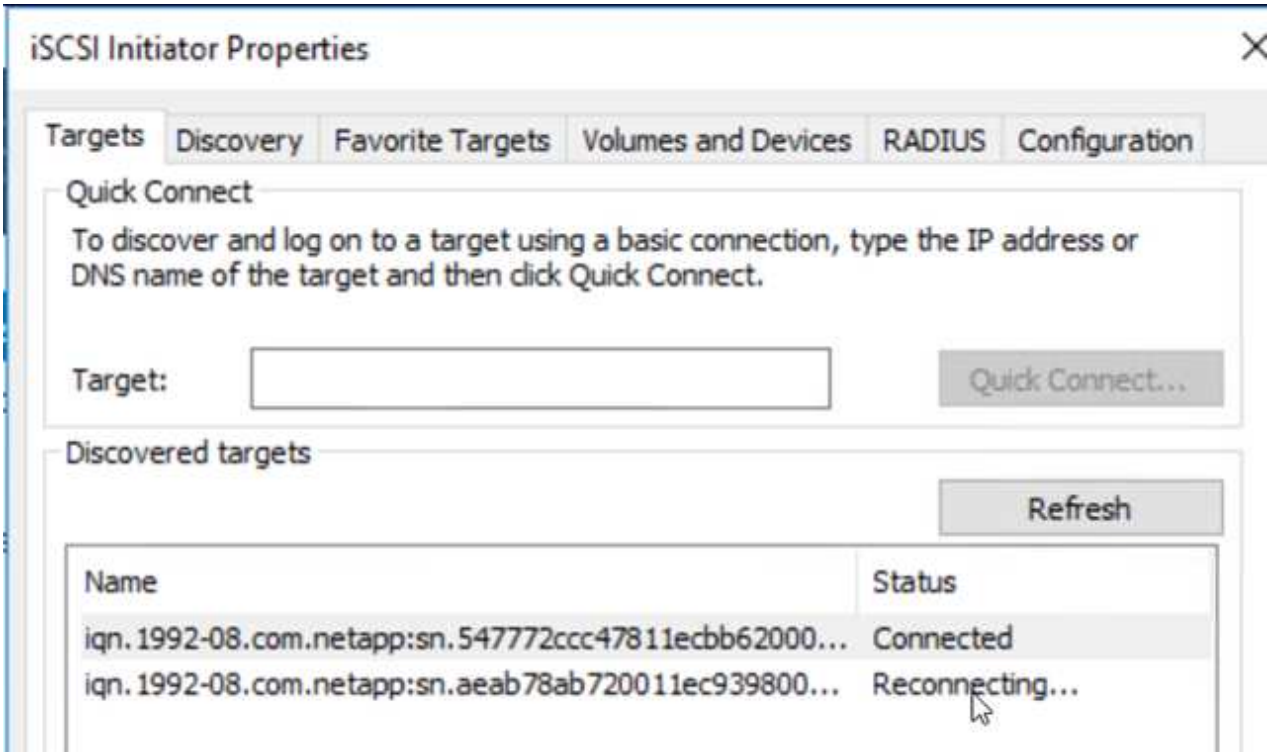
6. Stellen Sie sicher, dass die SnapMirror -Beziehung unterbrochen ist.



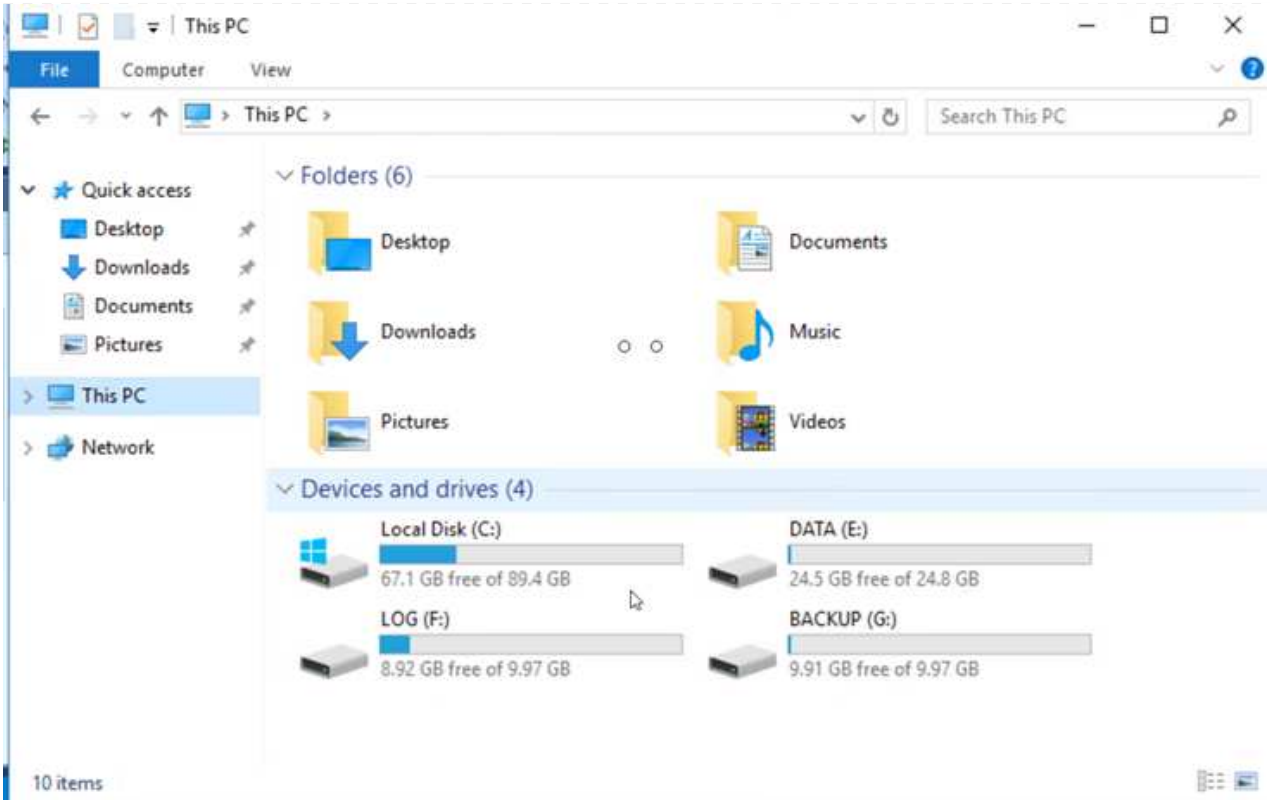
7. Fügen Sie die LUN von Cloud Volumes ONTAP mit denselben Laufwerksbuchstaben an die wiederhergestellte SQL-Gast-VM an.



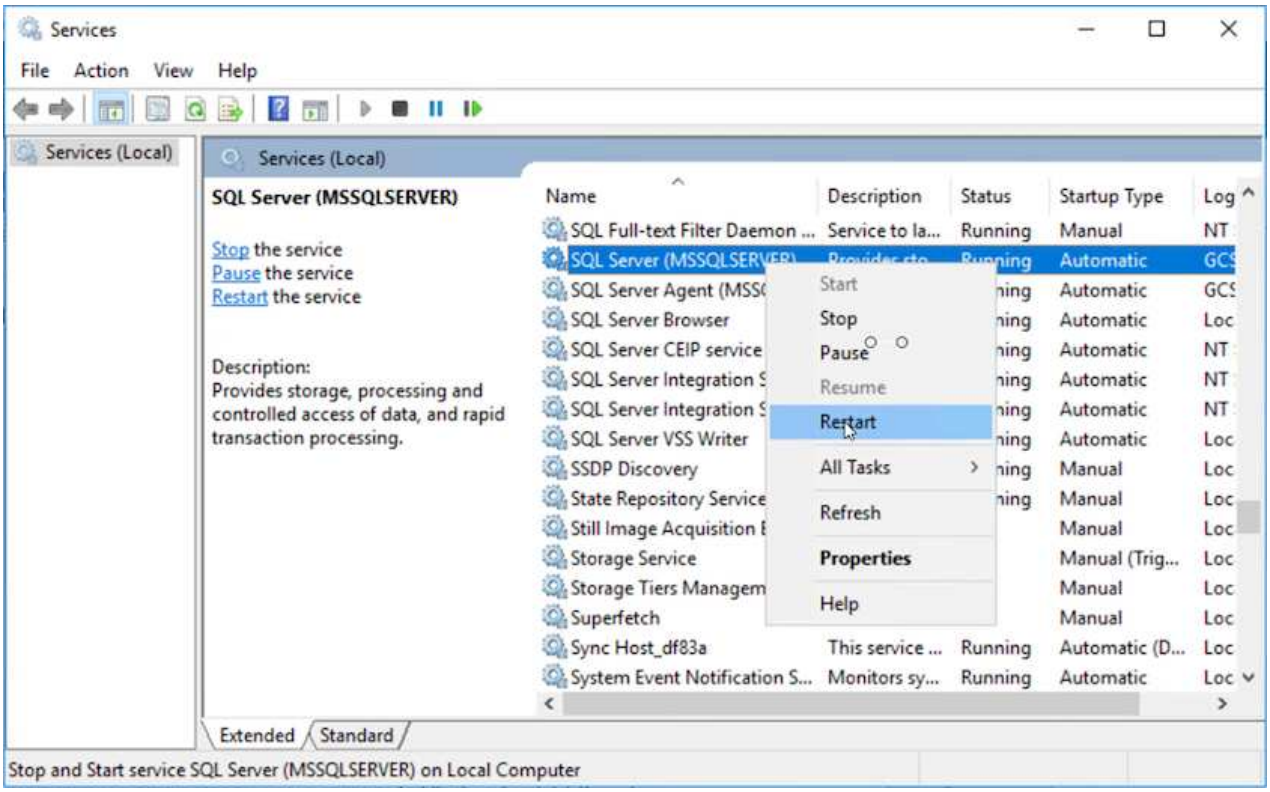
8. Öffnen Sie den iSCSI-Initiator, löschen Sie die vorherige getrennte Sitzung und fügen Sie das neue Ziel zusammen mit Multipath für die replizierten Cloud Volumes ONTAP Volumes hinzu.



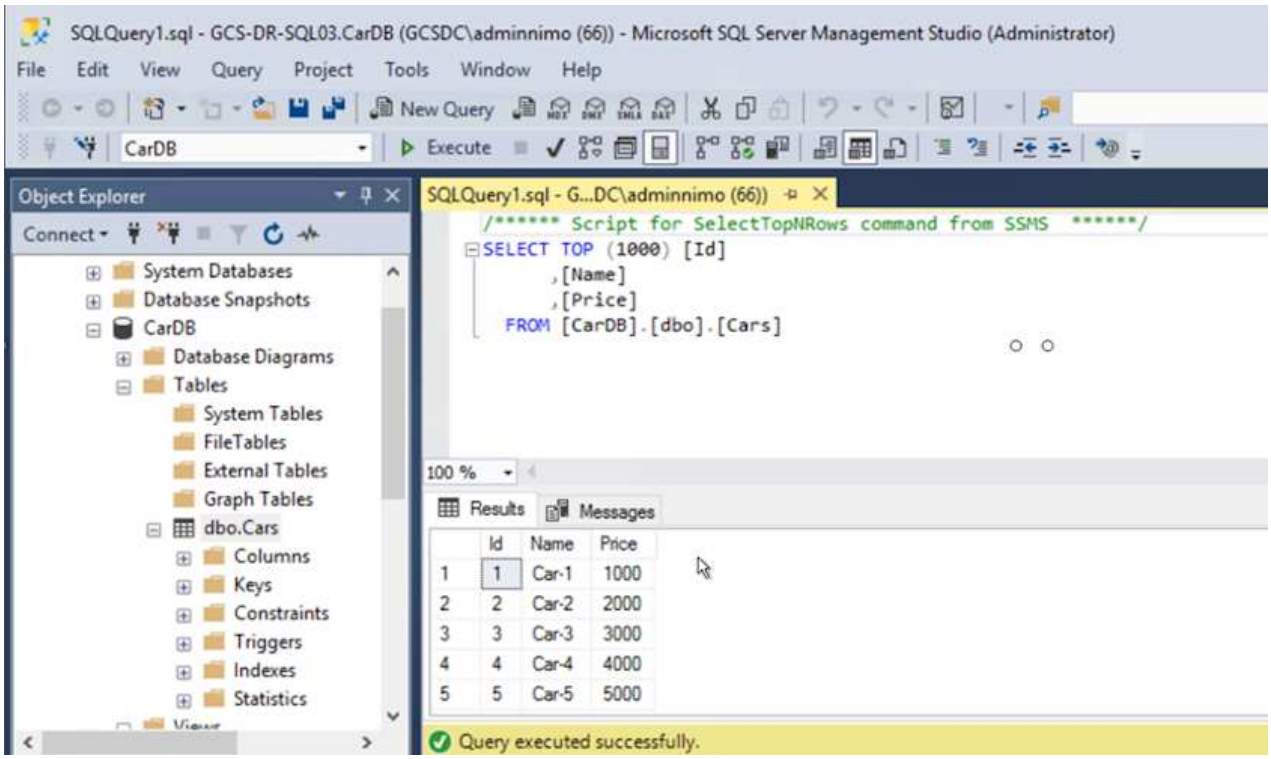
9. Stellen Sie sicher, dass alle Festplatten mit denselben Laufwerksbuchstaben verbunden sind, die vor DR verwendet wurden.



10. Starten Sie den MSSQL-Serverdienst neu.



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



Im Falle von NFS hängen Sie die Volumes mit dem Mount-Befehl an und aktualisieren Sie die `/etc/fstab` Einträge.

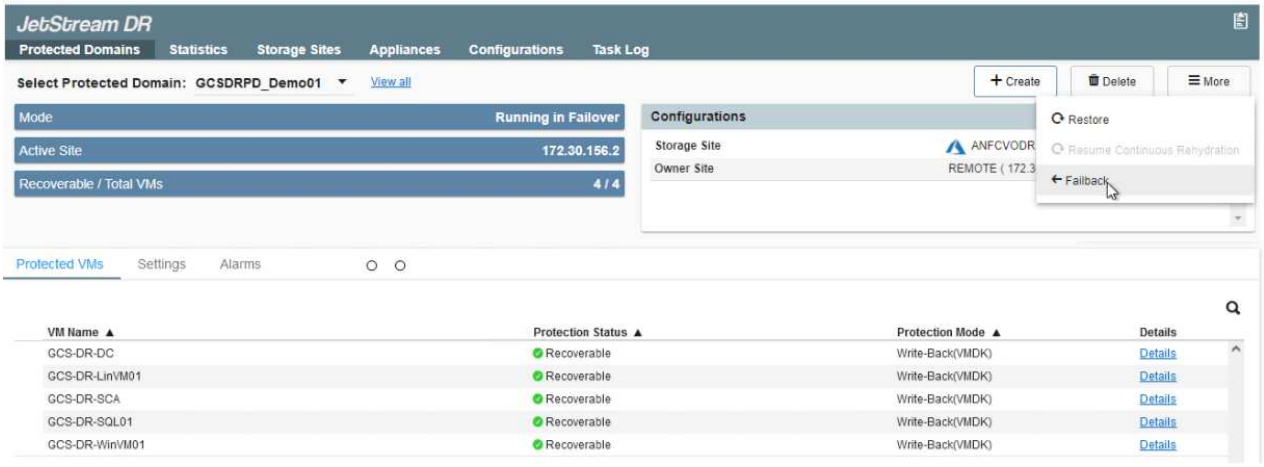
Ab diesem Zeitpunkt kann der Betrieb wieder aufgenommen werden und das Geschäft kann normal weiterlaufen.

Auf der NSX-T-Seite kann ein separates dediziertes Tier-1-Gateway zum Simulieren von Failover-Szenarien erstellt werden. Dadurch wird sichergestellt, dass alle Workloads miteinander kommunizieren können, jedoch kein Datenverkehr in die Umgebung hinein oder aus ihr heraus geleitet werden kann, sodass alle Triage-, Eindämmungs- oder Härtungsaufgaben ohne das Risiko einer Kreuzkontamination durchgeführt werden können. Dieser Vorgang liegt außerhalb des Rahmens dieses Dokuments, kann jedoch problemlos zur Simulation der Isolation durchgeführt werden.

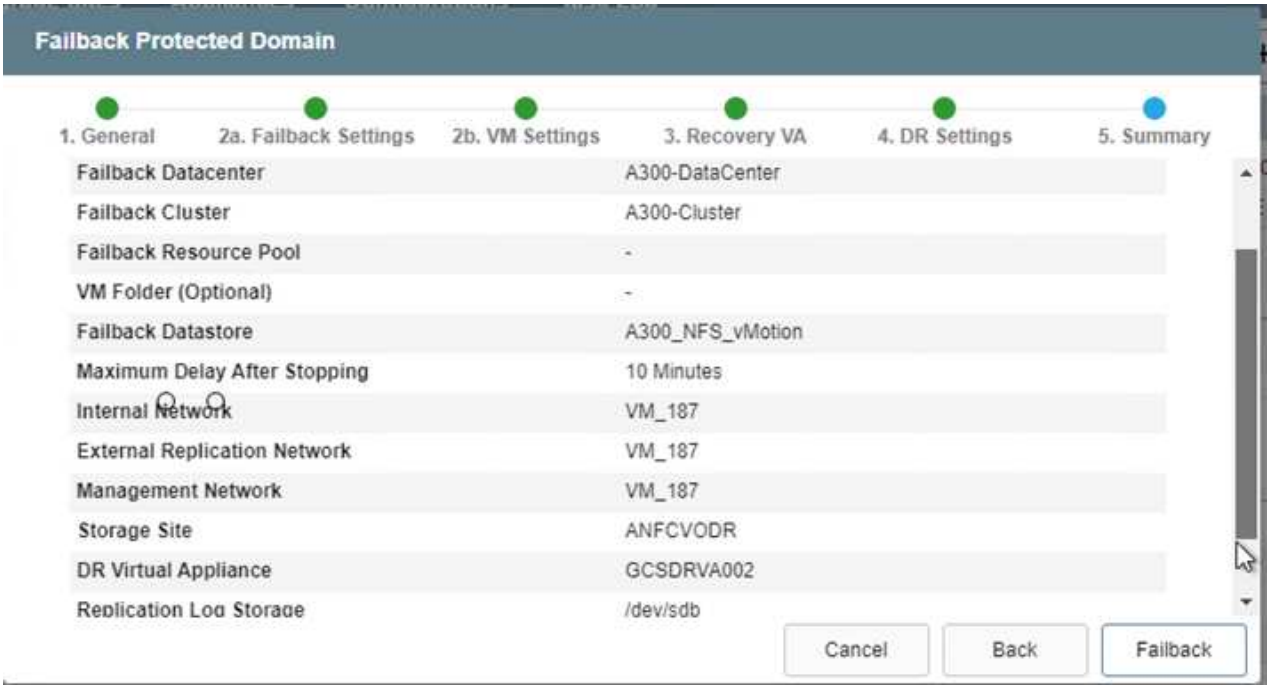
Nachdem die primäre Site wieder betriebsbereit ist, können Sie ein Failback durchführen. Der VM-Schutz wird von Jetstream wieder aufgenommen und die SnapMirror -Beziehung muss umgekehrt werden.

1. 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.
2. 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.

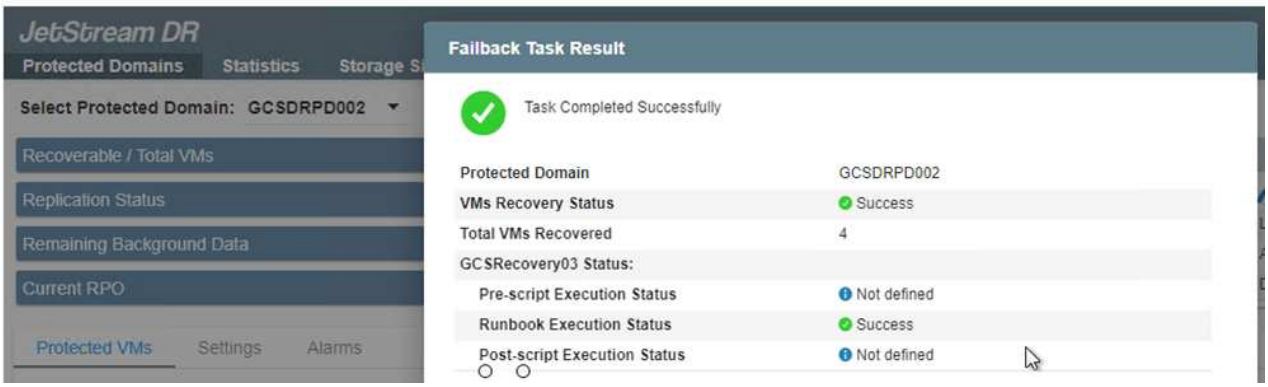
Der vom CPT generierte Failback-Plan kann auch verwendet werden, um die Rückgabe der VMs und ihrer Daten aus dem Objektspeicher zurück in die ursprüngliche VMware-Umgebung zu initiieren.



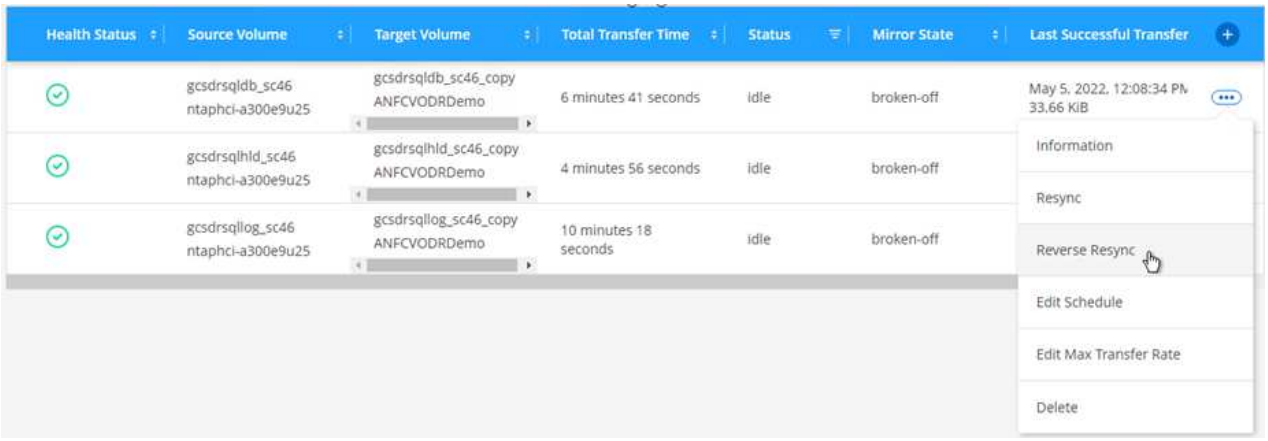
Geben Sie die maximale Verzögerung an, nachdem die VMs am Wiederherstellungsstandort angehalten und am geschützten Standort neu gestartet wurden. Die für diesen Vorgang benötigte Zeit umfasst die Fertigstellung der Replikation nach dem Stoppen der Failover-VMs, die zum Bereinigen der Wiederherstellungssite benötigte Zeit und die zum Neuerstellen der VMs auf der geschützten Site benötigte Zeit. NetApp empfiehlt 10 Minuten.

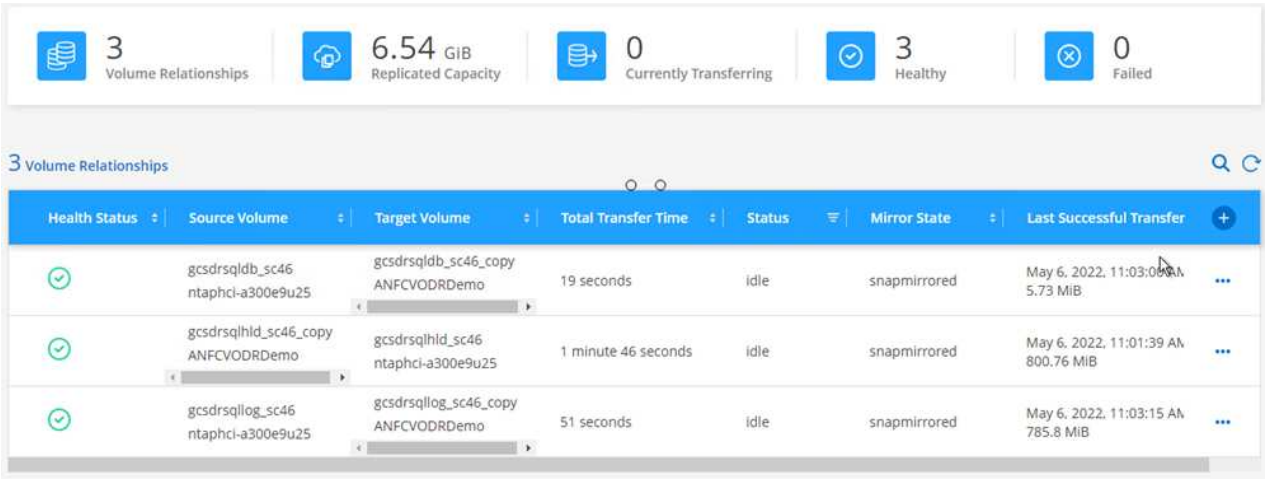


3. Schließen Sie den Failback-Prozess ab und bestätigen Sie anschließend die Wiederaufnahme des VM-Schutzes und der Datenkonsistenz.

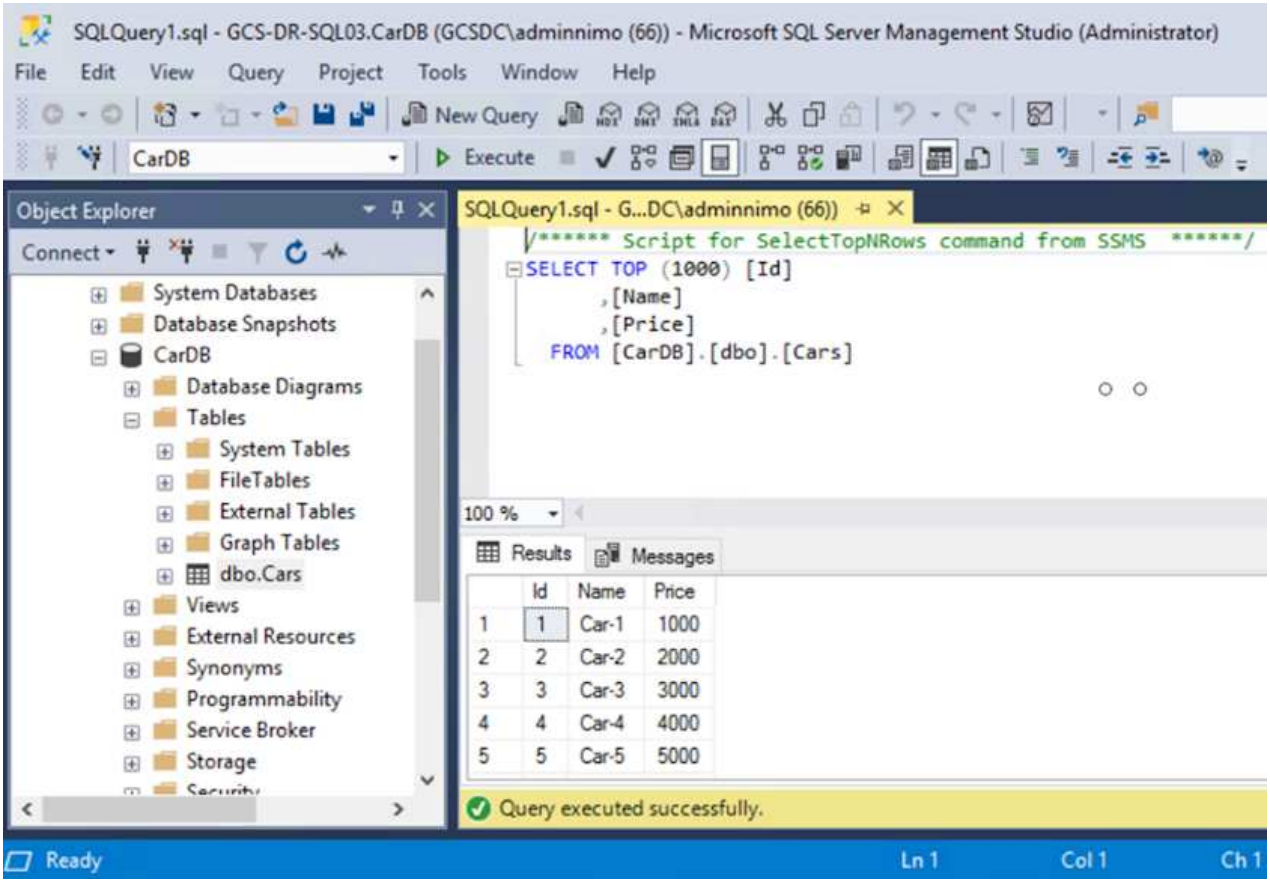


4. Nachdem die VMs wiederhergestellt wurden, trennen Sie den sekundären Speicher vom Host und stellen Sie eine Verbindung zum primären Speicher her.





5. Starten Sie den MSSQL-Serverdienst neu.
6. Überprüfen Sie, ob die SQL-Ressourcen wieder online sind.



Um ein Failback zum primären Speicher durchzuführen, stellen Sie sicher, dass die Beziehungsrichtung dieselbe bleibt wie vor dem Failover, indem Sie einen umgekehrten Resynchronisierungsvorgang durchführen.

Um die Rollen des primären und sekundären Speichers nach dem umgekehrten Resynchronisierungsvorgang beizubehalten, führen Sie den umgekehrten Resynchronisierungsvorgang erneut durch.

Dieser Prozess ist auf andere Anwendungen wie Oracle, ähnliche Datenbankvarianten und alle anderen Anwendungen anwendbar, die über den Gast verbundenen Speicher verwenden.

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

Vorteile dieser Lösung

- Verwendet die effiziente und stabile Replikation von SnapMirror.
- Stellt mit ONTAP Snapshot-Aufbewahrung alle verfügbaren Zeitpunkte wieder her.
- Für alle erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs ist eine vollständige Automatisierung verfügbar, angefangen bei den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung.
- SnapCenter verwendet Klonmechanismen, die das replizierte Volume nicht ändern.
  - Dadurch wird das Risiko einer Datenbeschädigung bei Volumes und Snapshots vermieden.

    - Vermeidet Replikationsunterbrechungen während DR-Test-Workflows.
    - Nutzt die DR-Daten für Workflows, die über DR hinausgehen, wie etwa Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests und Fehlerbehebungstests.
- Durch die CPU- und RAM-Optimierung können die Cloud-Kosten gesenkt werden, indem die Wiederherstellung auf kleineren Computerclustern ermöglicht wird.