TR-4955: Notfallwiederherstellung mit Azure NetApp Files (ANF) und Azure VMware Solution (AVS)

NetApp public and hybrid cloud solutions

NetApp
August 18, 2025

Inhalt

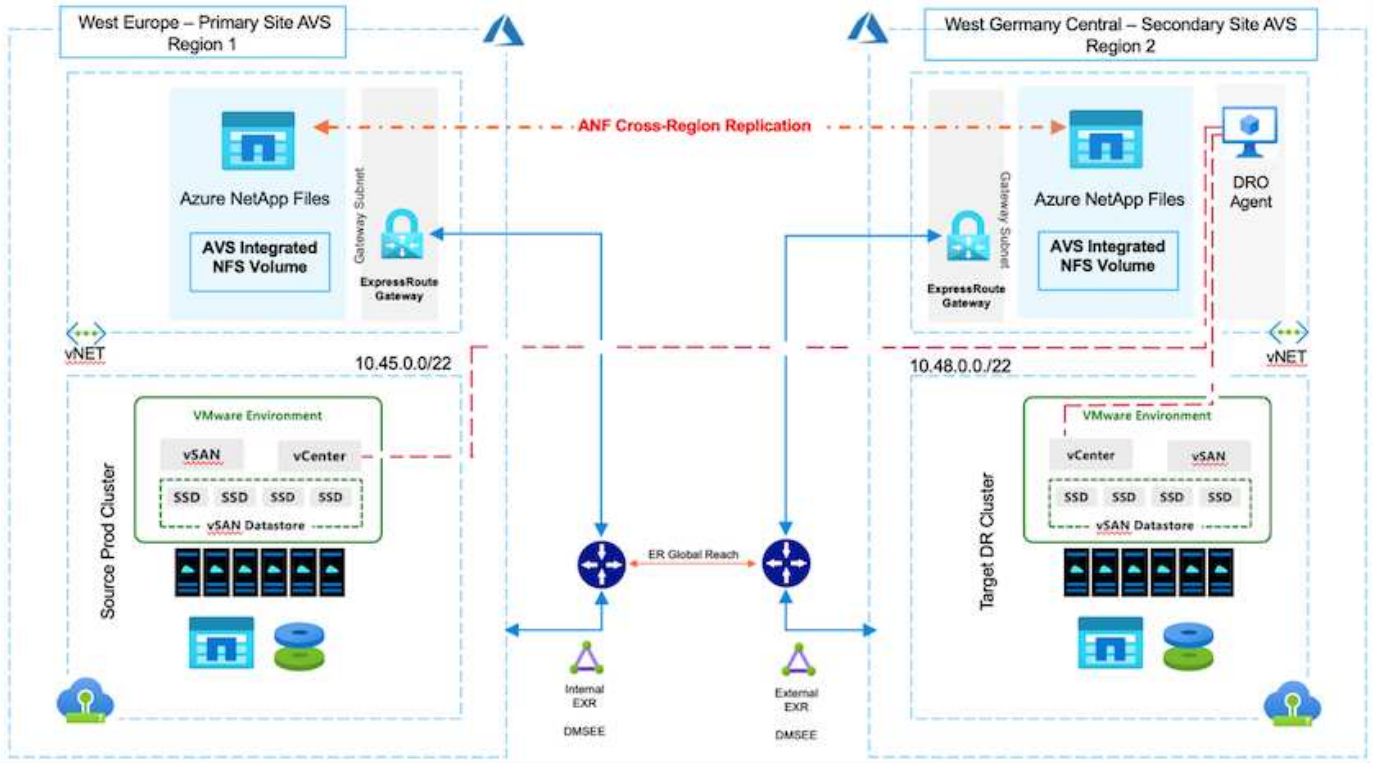
TR-4955: Notfallwiederherstellung mit Azure NetApp Files (ANF) und Azure VMware Solution (AVS)

Die Notfallwiederherstellung mithilfe der Replikation auf Blockebene zwischen Regionen innerhalb der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen.

Überblick

Mit der regionsübergreifenden Volumereplikation von Azure NetApp Files (ANF) können VMware-Workloads, die auf einem Azure VMware Solution (AVS) SDDC-Standort ausgeführt werden und Azure NetApp Files-Volumes als NFS-Datenspeicher auf dem primären AVS-Standort verwenden, auf einen bestimmten sekundären AVS-Standort in der Zielwiederherstellungsregion repliziert werden.

Mit Disaster Recovery Orchestrator (DRO) (einer Skriptlösung mit Benutzeroberfläche) können Sie Workloads, die von einem AVS SDDC auf ein anderes repliziert wurden, nahtlos wiederherstellen. DRO automatisiert die Wiederherstellung, indem es das Replikations-Peering unterbricht und dann das Zielvolume als Datenspeicher bereitstellt, über die VM-Registrierung bei AVS bis hin zu Netzwerkzuordnungen direkt auf NSX-T (in allen privaten AVS-Clouds enthalten).



Voraussetzungen und allgemeine Empfehlungen

- Stellen Sie sicher, dass Sie die regionsübergreifende Replikation aktiviert haben, indem Sie ein Replikations-Peering erstellen. Sehen "Erstellen einer Volumereplikation für Azure NetApp Files" .
- Sie müssen ExpressRoute Global Reach zwischen den privaten Quell- und Ziel-Clouds der Azure VMware Solution konfigurieren.

- Sie müssen über einen Dienstprinzipal verfügen, der auf Ressourcen zugreifen kann.
- Die folgende Topologie wird unterstützt: primärer AVS-Standort zu sekundärem AVS-Standort.
- Konfigurieren Sie die "Replikation" Planen Sie für jedes Volume entsprechend den Geschäftsanforderungen und der Datenänderungsrate.

Kaskadierungs- und Fan-In- und Fan-Out-Topologien werden nicht unterstützt.

Erste Schritte

Bereitstellen der Azure VMware-Lösung

Der "Azure VMware-Lösung" (AVS) ist ein Hybrid-Cloud-Dienst, der voll funktionsfähige VMware SDDCs innerhalb einer öffentlichen Microsoft Azure-Cloud bereitstellt. AVS ist eine First-Party-Lösung, die vollständig von Microsoft verwaltet und unterstützt und von VMware verifiziert wird und die Azure-Infrastruktur nutzt. Daher erhalten Kunden VMware ESXi für die Computervirtualisierung, vSAN für hyperkonvergenten Speicher und NSX für Netzwerke und Sicherheit und profitieren gleichzeitig von der globalen Präsenz von Microsoft Azure, den erstklassigen Rechenzentrumseinrichtungen und der Nähe zum umfangreichen Ökosystem nativer Azure-Dienste und -Lösungen. Eine Kombination aus Azure VMware Solution SDDC und Azure NetApp Files bietet die beste Leistung bei minimaler Netzwerklatenz.

Um eine AVS-Private-Cloud auf Azure zu konfigurieren, folgen Sie den Schritten in diesem"Link" für NetApp Dokumentation und in diesem "Link" für Microsoft-Dokumentation. Eine Pilotlichtumgebung mit minimaler Konfiguration kann für DR-Zwecke verwendet werden. Dieses Setup enthält nur Kernkomponenten zur Unterstützung kritischer Anwendungen und kann skaliert werden, sodass im Falle eines Failovers weitere Hosts bereitgestellt werden können, um den Großteil der Last zu übernehmen.

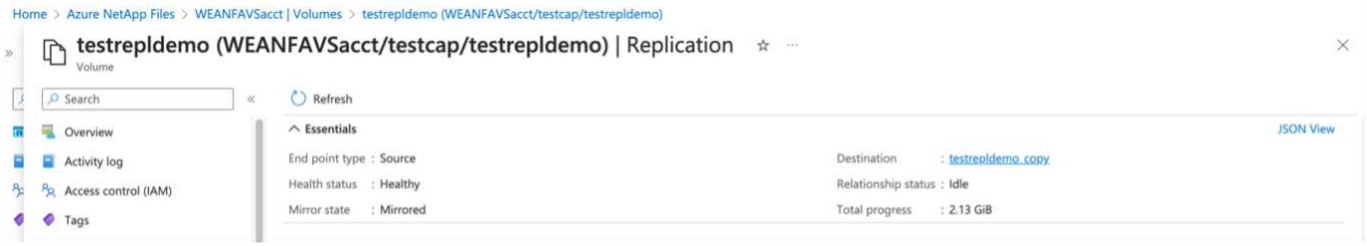
In der ersten Version unterstützt DRO einen vorhandenen AVS SDDC-Cluster. Die On-Demand-SDDC-Erstellung wird in einer kommenden Version verfügbar sein.

Bereitstellen und Konfigurieren von Azure NetApp Files

"Azure NetApp Files"ist ein leistungsstarker, gebührenpflichtiger Dateispeicherdienst der Enterprise-Klasse. Befolgen Sie die Schritte in diesem "Link" zum Bereitstellen und Konfigurieren von Azure NetApp Files als NFS-Datenspeicher zur Optimierung der AVS-Bereitstellungen in privaten Clouds.

Erstellen einer Volumereplikation für Azure NetApp Files-basierte Datenspeichervolumes

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



Befolgen Sie die Schritte in diesem "Link" um eine regionsübergreifende Replikation durch Erstellen eines Replikations-Peerings einzurichten. Das Servicelevel für den Zielkapazitätspool kann mit dem des

Quellkapazitätspools übereinstimmen. Für diesen speziellen Anwendungsfall können Sie jedoch das Standard-Service-Level auswählen und dann "Ändern Sie den Service-Level" im Falle einer echten Katastrophe oder DR-Simulationen.

Eine regionsübergreifende Replikationsbeziehung ist Voraussetzung und muss vorher erstellt werden.

DRO-Installation

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

Voraussetzungen:

- Dienstprinzipal, der auf Ressourcen zugreifen kann.
- Stellen Sie sicher, dass eine entsprechende Verbindung zu den Quell- und Ziel-SDDC- und Azure NetApp Files Instanzen besteht.
- Wenn Sie DNS-Namen verwenden, sollte eine DNS-Auflösung vorhanden sein. Verwenden Sie andernfalls IP-Adressen für vCenter.

Betriebssystemanforderungen:

- Ubuntu Focal 20.04 (LTS)Die folgenden Pakete müssen auf der vorgesehenen virtuellen Agent-Maschine installiert werden:
- Docker
- Docker-Compose
- JqChange `docker.sock` zu dieser neuen Berechtigung: `sudo chmod 666 /var/run/docker.sock`.

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

Die Schritte sind wie folgt:

1. Laden Sie das Installationspaket auf die angegebene virtuelle Maschine herunter:

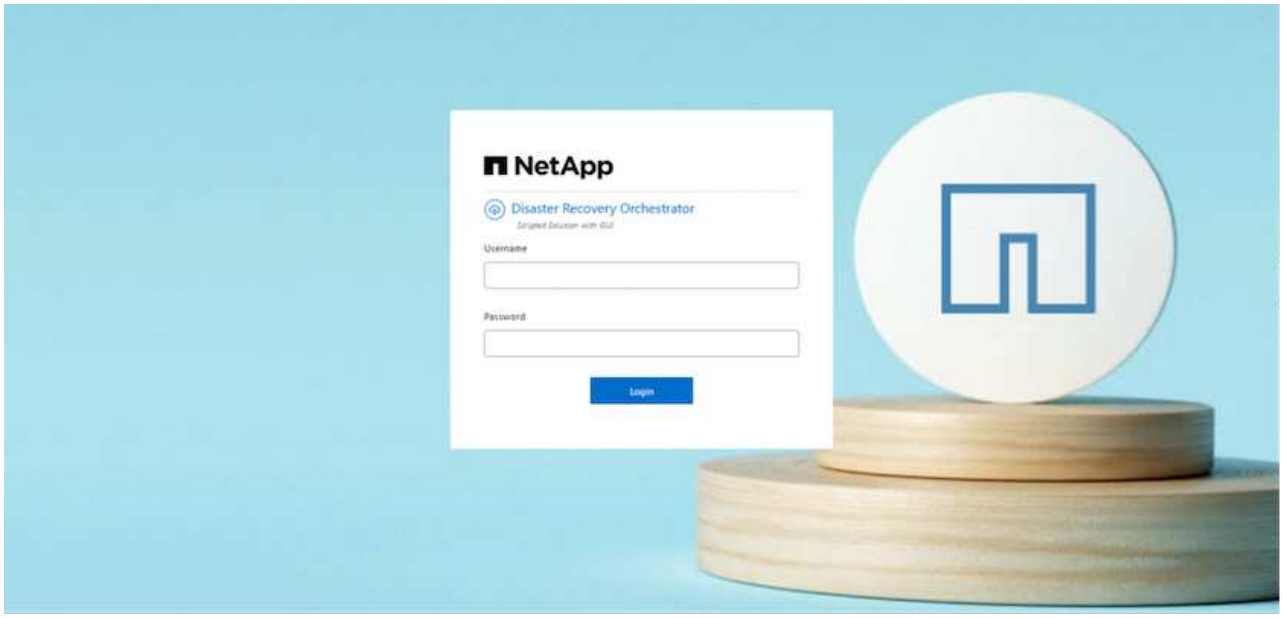
```
git clone https://github.com/NetApp/DRO-Azure.git
```

Der Agent muss in der sekundären AVS-Standortregion oder in der primären AVS-Standortregion in einer anderen 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 Anmeldeinformationen auf die Benutzeroberfläche zu:
    - Benutzername: `admin`
    - Passwort: `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-Agenten am sekundären AVS-Standort bereitzustellen und die ExpressRoute-Gateway-Verbindung so zu konfigurieren, dass der DRO-Agent über das Netzwerk mit den entsprechenden AVS- und Azure NetApp Files Komponenten kommunizieren kann.

Der erste Schritt besteht darin, Anmeldeinformationen hinzuzufügen. DRO benötigt die Berechtigung zum Erkennen von Azure NetApp Files und der Azure VMware-Lösung. Sie können einem Azure-Konto die erforderlichen Berechtigungen erteilen, indem Sie eine Azure Active Directory (AD)-Anwendung erstellen und einrichten und die von DRO benötigten Azure-Anmeldeinformationen abrufen. Sie müssen den Dienstprinzipal 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 mit dem Dienstprinzipal verknüpften Anmeldeinformationen auszuwählen. Sie müssen diese Anmeldeinformationen zu DRO hinzufügen, bevor Sie auf „Neue Site hinzufügen“ klicken können.

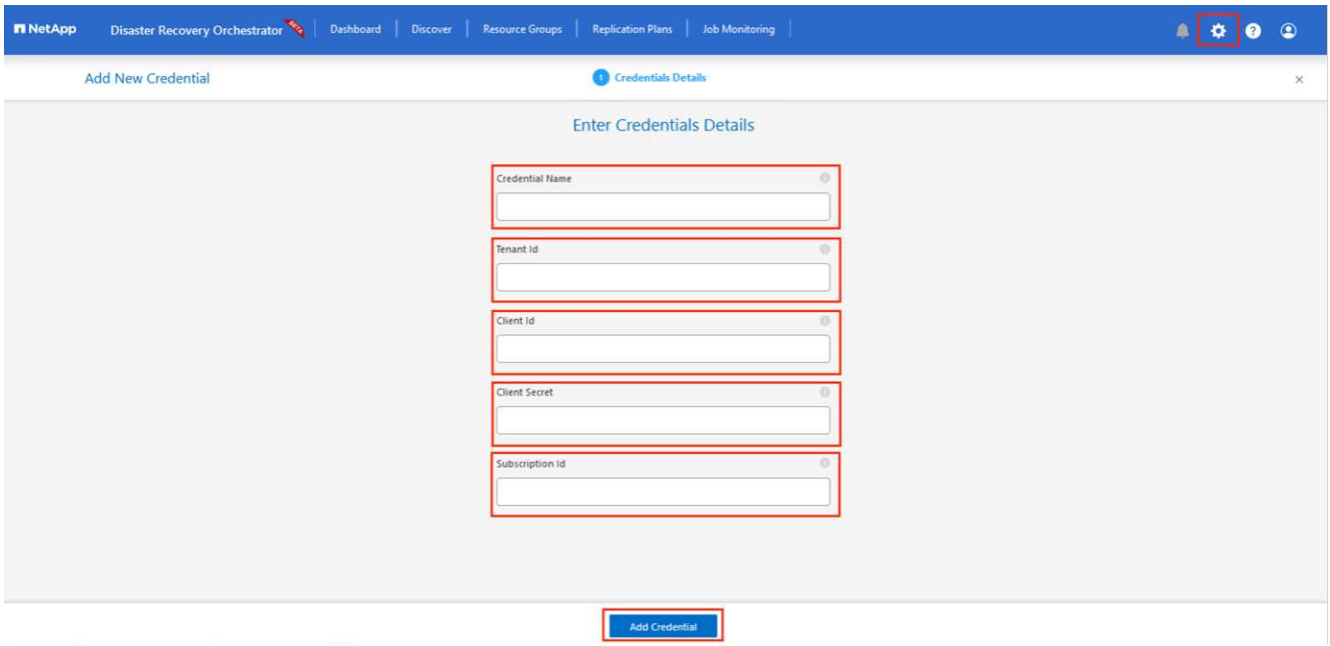
Führen Sie zum Ausführen dieses Vorgangs die folgenden Schritte aus:

1. Öffnen Sie DRO in einem unterstützten Browser und verwenden Sie den Standardbenutzernamen und das Standardkennwort/`admin`/`admin`). Das Passwort kann nach der ersten Anmeldung über die Option „Passwort ändern“ zurückgesetzt werden.
2. Klicken Sie oben rechts in der DRO-Konsole auf das Symbol **Einstellungen** und wählen Sie **Anmeldeinformationen** aus.
3. Klicken Sie auf „Neue Anmeldeinformationen hinzufügen“ und folgen Sie den Schritten des Assistenten.
4. Um die Anmeldeinformationen zu definieren, geben Sie Informationen zum Azure Active Directory-Dienstprinzipal ein, der die erforderlichen Berechtigungen erteilt:

- Anmeldeinformationsname
- Mandanten-ID
- Client-ID
- Clientgeheimnis
- Abonnement-ID

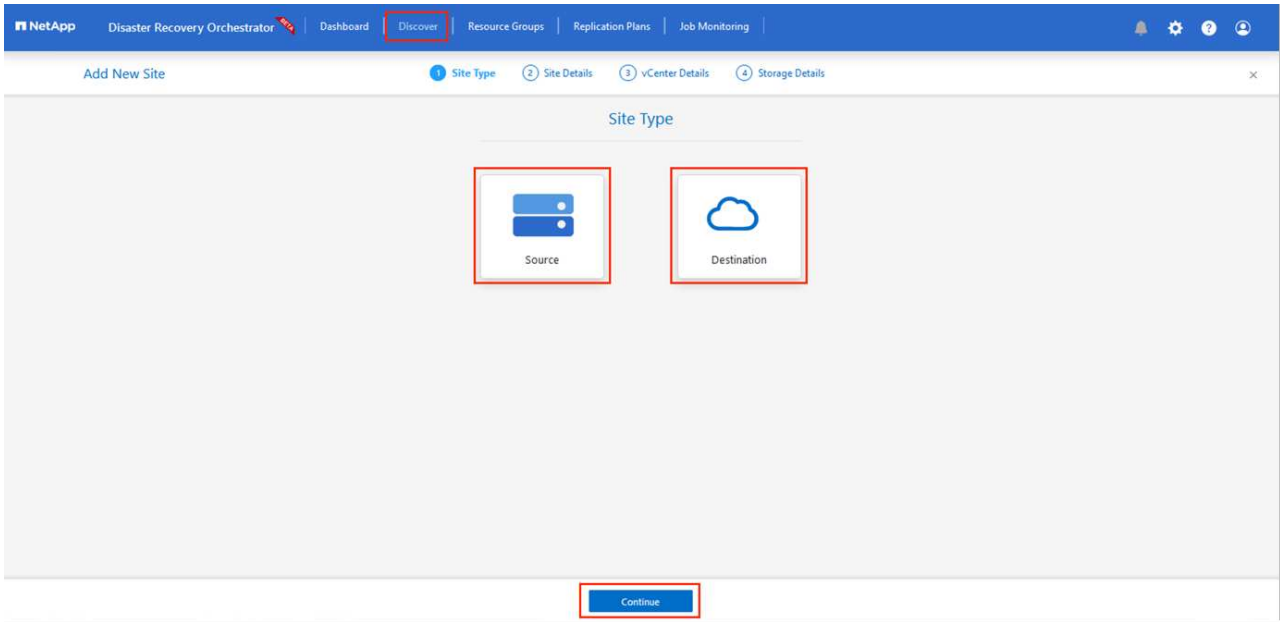
  Sie sollten diese Informationen beim Erstellen der AD-Anwendung erfasst haben.

5. Bestätigen Sie die Angaben zu den neuen Anmeldeinformationen und klicken Sie auf „Anmeldeinformationen hinzufügen“.



Nachdem Sie die Anmeldeinformationen hinzugefügt haben, ist es an der Zeit, die primären und sekundären AVS-Sites (sowohl vCenter als auch das Azure NetApp Dateispeicherkonto) zu ermitteln und zu DRO hinzuzufügen. Führen Sie die folgenden Schritte aus, um die Quell- und Zielsite hinzuzufügen:

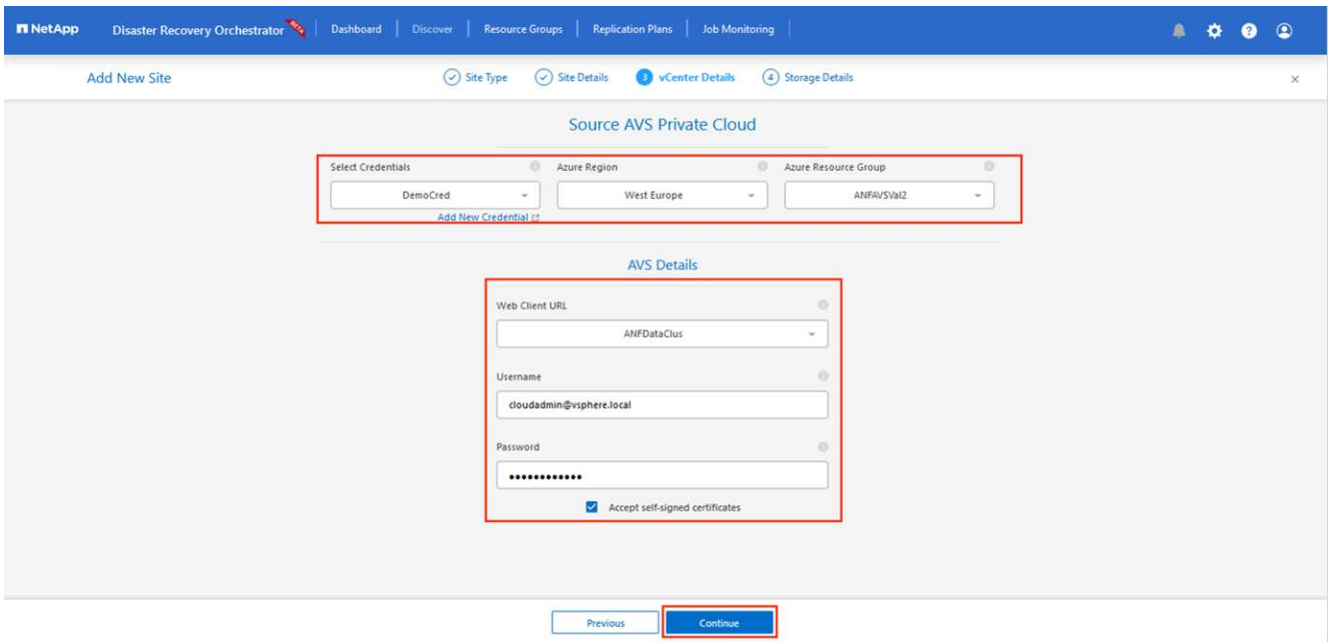
6. Gehen Sie zur Registerkarte **Entdecken**.
7. Klicken Sie auf **Neue Site hinzufügen**.
8. Fügen Sie die folgende primäre AVS-Site hinzu (in der Konsole als **Quelle** bezeichnet).
   - SDDC vCenter
   - Azure NetApp Files Speicherkonto
9. Fügen Sie die folgende sekundäre AVS-Site hinzu (in der Konsole als **Ziel** bezeichnet).
   - SDDC vCenter
   - Azure NetApp Files Speicherkonto



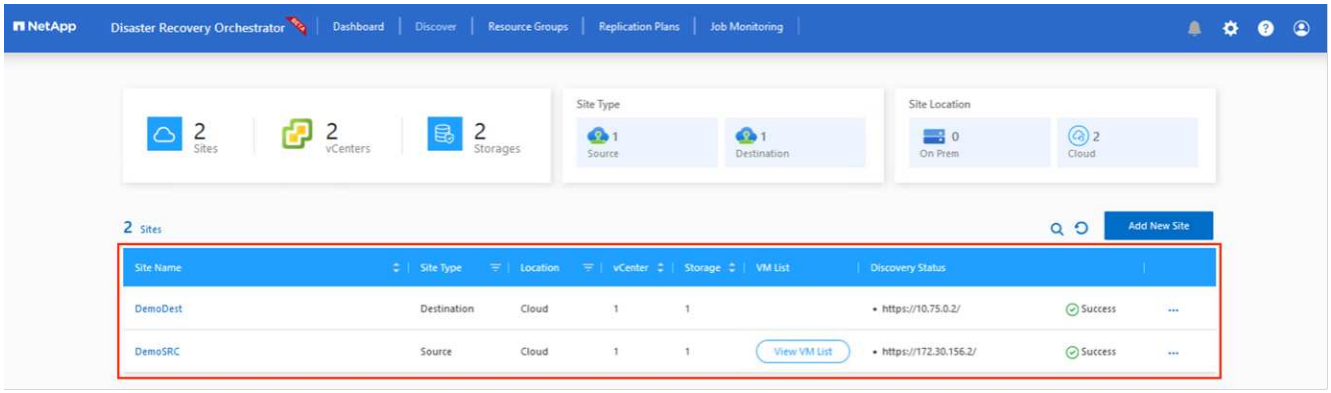
10. Fügen Sie Sitedetails hinzu, indem Sie auf **Quelle** klicken, einen aussagekräftigen Sitenamen eingeben und den Connector auswählen. Klicken Sie dann auf **Weiter**.

> Zu Demonstrationszwecken wird in diesem Dokument das Hinzufügen einer Quellsite behandelt.

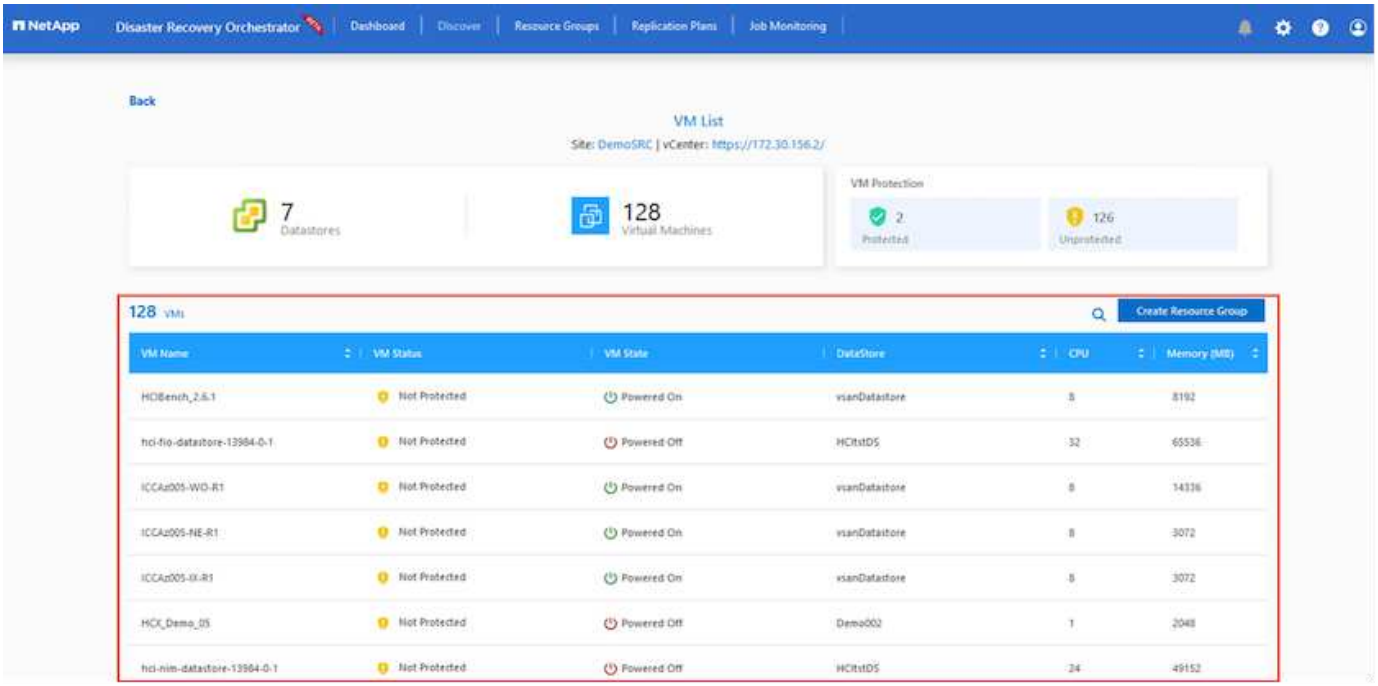
11. Aktualisieren Sie die vCenter-Details. Wählen Sie dazu die Anmeldeinformationen, die Azure-Region und die Ressourcengruppe aus der Dropdown-Liste für das primäre AVS SDDC aus.
12. DRO listet alle verfügbaren SDDCs innerhalb der Region auf. Wählen Sie die gewünschte private Cloud-URL aus der Dropdown-Liste aus.
13. Geben Sie den `cloudadmin@vsphere.local` Benutzeranmeldeinformationen. Der Zugriff ist über das Azure-Portal möglich. Befolgen Sie die in diesem Dokument beschriebenen Schritte "Link" . Klicken Sie anschließend auf **Weiter**.



14. Wählen Sie die Quellspeicherdetails (ANF) aus, indem Sie die Azure-Ressourcengruppe und das NetApp -Konto auswählen.
15. Klicken Sie auf **Site erstellen**.



Nach dem Hinzufügen führt DRO eine automatische Erkennung durch und zeigt die VMs an, die über entsprechende regionsübergreifende Replikate vom Quell- zum Zielstandort verfügen. DRO erkennt automatisch die von den VMs verwendeten Netzwerke und Segmente und füllt sie.



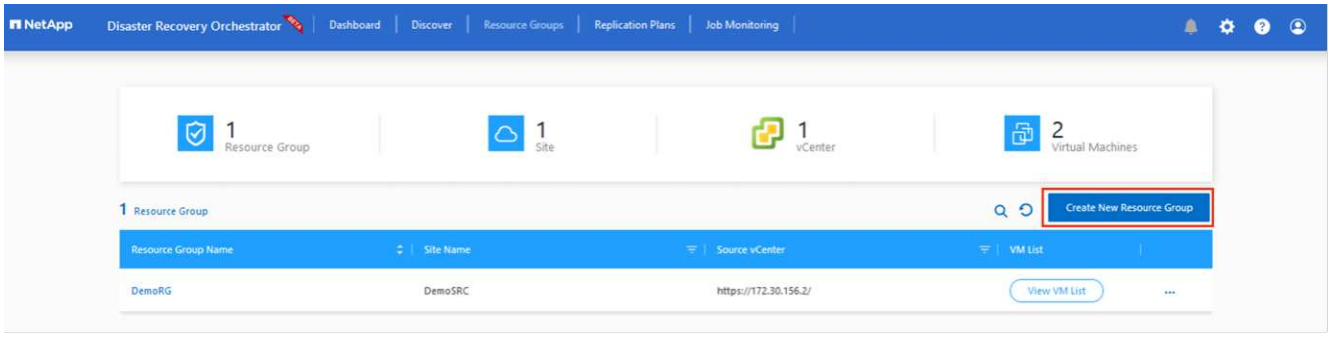
Der nächste Schritt besteht darin, die benötigten VMs in ihren Funktionsgruppen als Ressourcengruppen zu gruppieren.

Ressourcengruppierungen

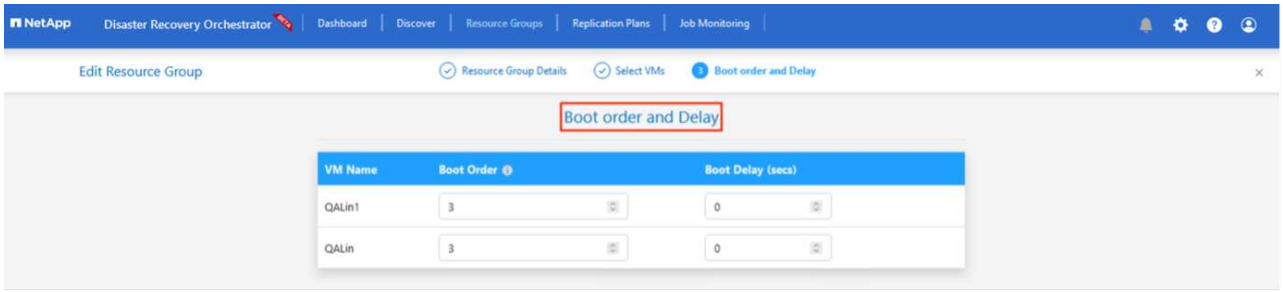
Nachdem die Plattformen hinzugefügt wurden, gruppieren Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen. Mit DRO-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen, Startverzögerungen und optionalen Anwendungsvalidierungen enthalten, die bei der Wiederherstellung ausgeführt werden können.

Um mit der Erstellung von Ressourcengruppen zu beginnen, klicken Sie auf das Menüelement **Neue Ressourcengruppe erstellen**.

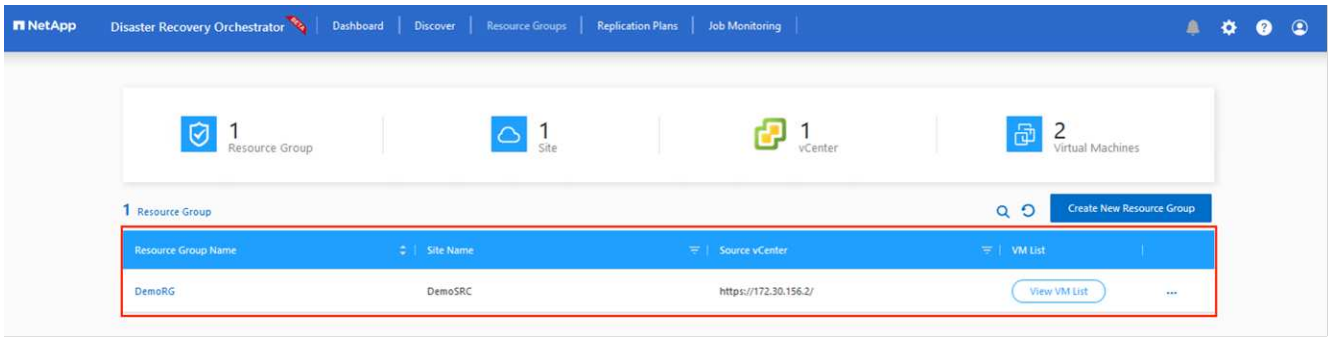
1. Greifen Sie auf **Ressourcengruppen** zu und klicken Sie auf **Neue Ressourcengruppe erstellen**.



2. Wählen Sie unter „Neue Ressourcengruppe“ die Quellsite aus der Dropdown-Liste aus und klicken Sie auf „Erstellen“.
3. Geben Sie die Details der Ressourcengruppe ein und klicken Sie auf **Weiter**.
4. Wählen Sie mithilfe der Suchoption geeignete VMs aus.
5. Wählen Sie die **Startreihenfolge** und **Startverzögerung** (Sek.) für alle ausgewählten VMs aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede virtuelle Maschine auswählen und die Priorität dafür festlegen. Der Standardwert für alle virtuellen Maschinen ist 3. Die Optionen sind wie folgt:
   - Die erste virtuelle Maschine, die eingeschaltet wird
   - Standard
   - Die letzte eingeschaltete virtuelle Maschine



6. Klicken Sie auf **Ressourcengruppe erstellen**.



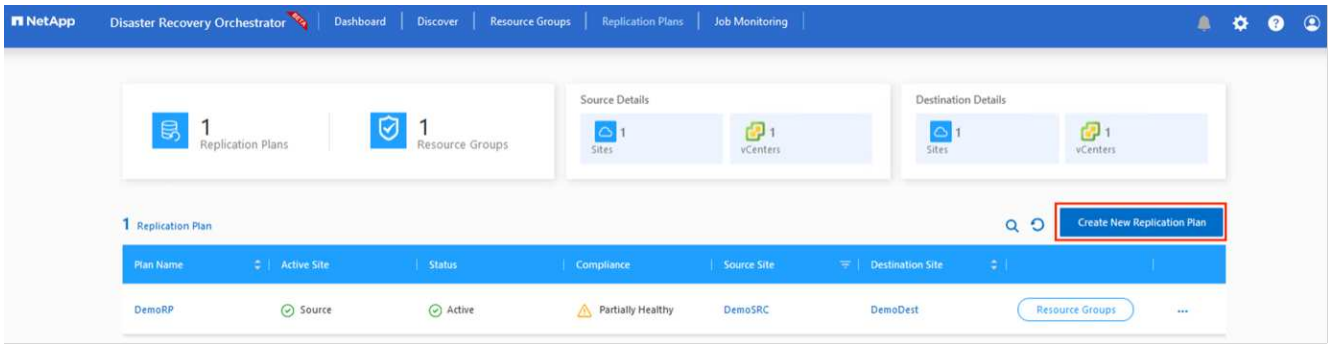
Replikationspläne

Sie müssen über einen Plan zur Wiederherstellung von Anwendungen im Katastrophenfall verfügen. Wählen Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste aus, wählen Sie die Ressourcengruppen aus, die in diesen Plan aufgenommen werden sollen, und geben Sie auch die Gruppierung an, wie

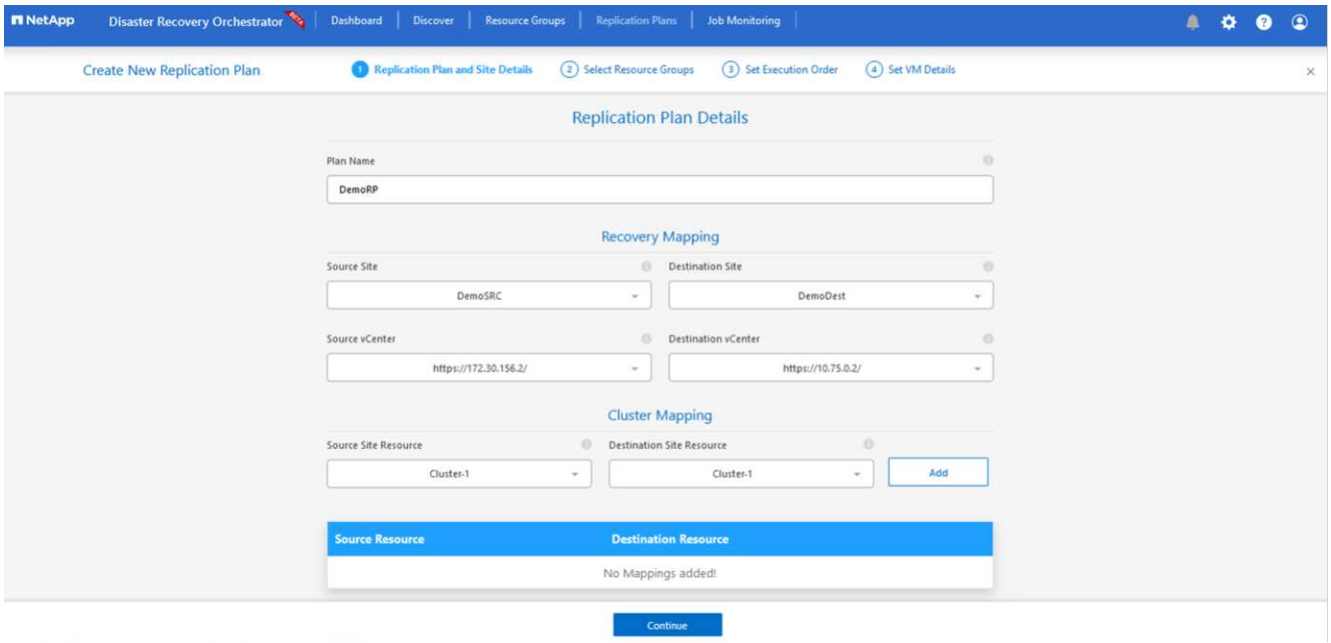
Anwendungen wiederhergestellt und eingeschaltet werden sollen (z. B. Domänencontroller, Tier-1, Tier-2 usw.). Pläne werden oft auch als Blaupausen bezeichnet. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte „Replikationsplan“ und klicken Sie auf **Neuer Replikationsplan**.

Führen Sie die folgenden Schritte aus, um mit der Erstellung eines Replikationsplans zu beginnen:

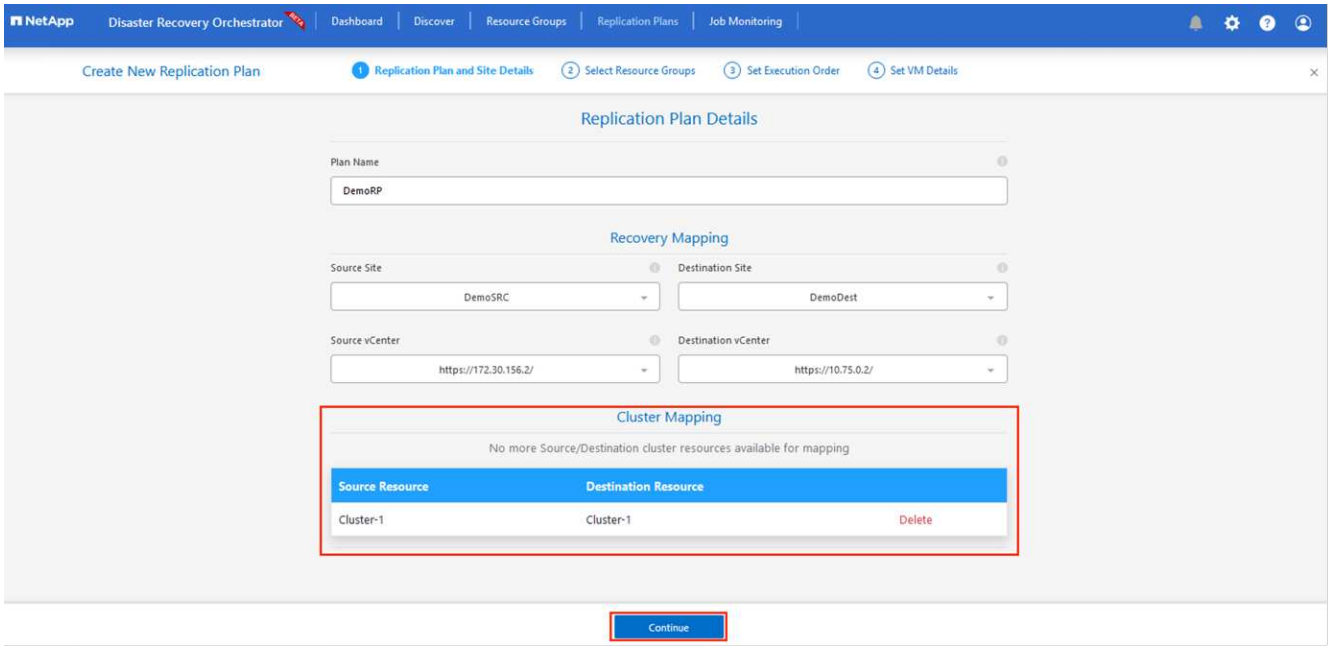
1. Navigieren Sie zu **Replikationsplänen** und klicken Sie auf **Neuen Replikationsplan erstellen**.



2. Geben Sie im **Neuen Replikationsplan** einen Namen für den Plan ein und fügen Sie Wiederherstellungszuordnungen hinzu, indem Sie die Quellsite, das zugehörige vCenter, die Zielsite und das zugehörige vCenter auswählen.

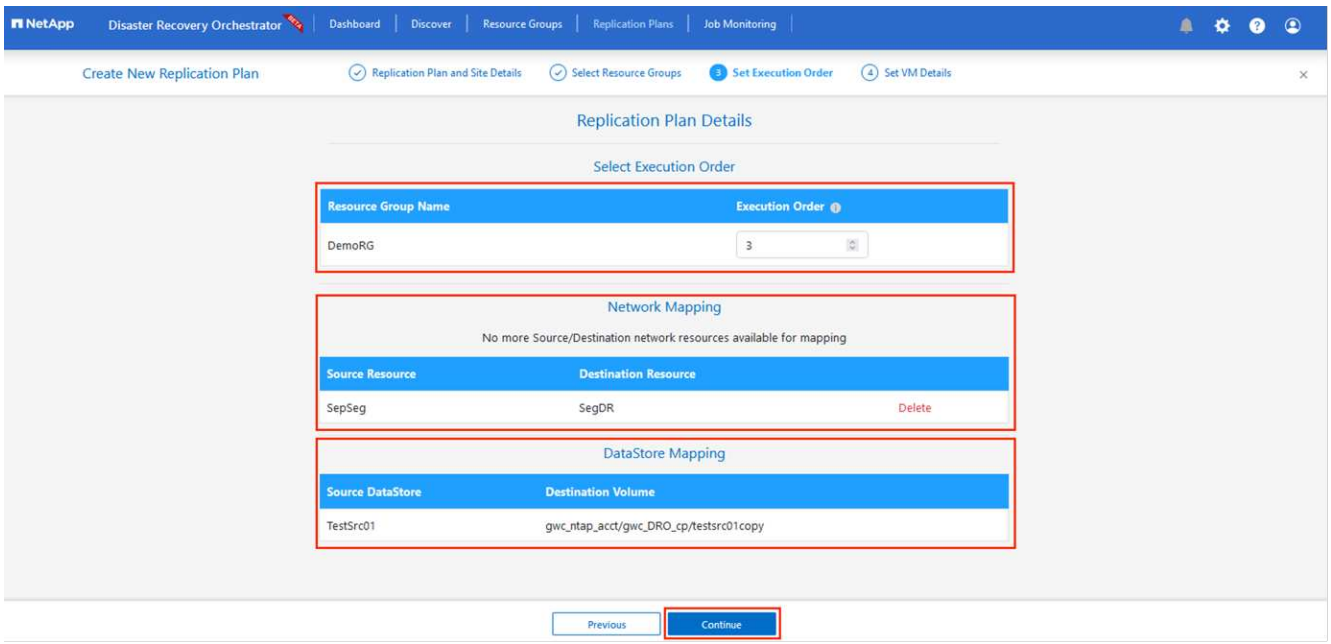


3. Wählen Sie nach Abschluss der Wiederherstellungszuordnung die **Clusterzuordnung** aus.

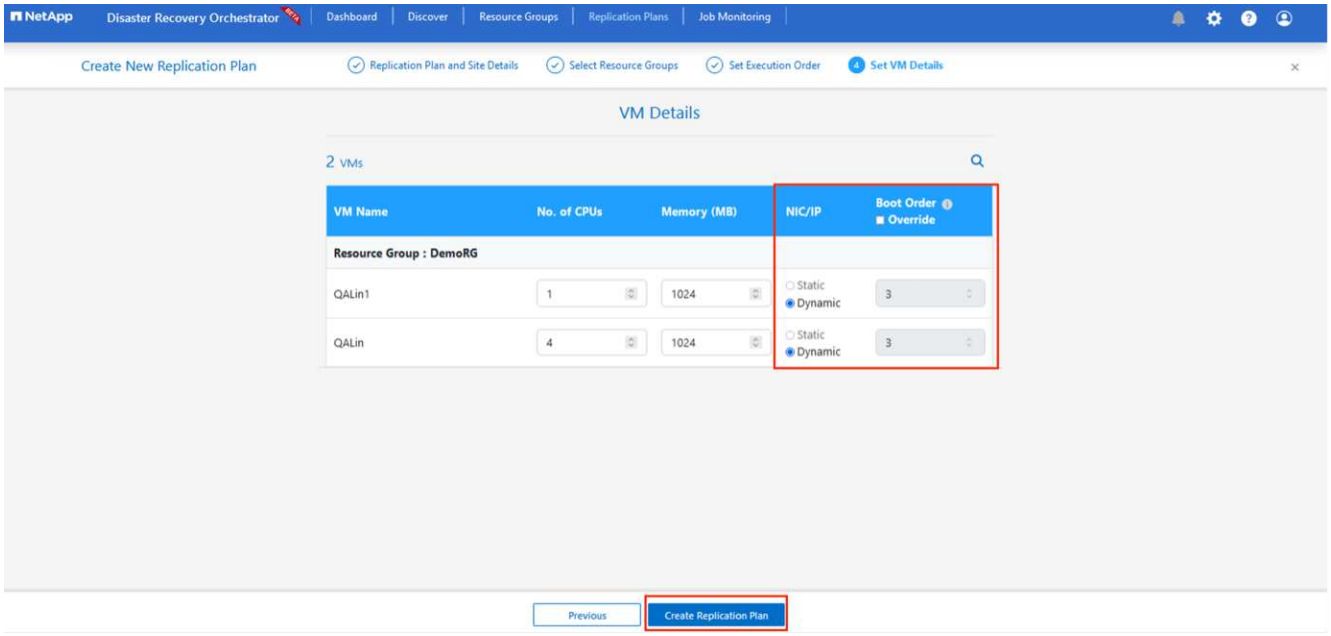


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Sobald dies erledigt ist, legen Sie die Netzwerkzuordnung auf das entsprechende Segment fest. Die Segmente sollten bereits auf dem sekundären AVS-Cluster bereitgestellt sein. Um die VMs diesen zuzuordnen, wählen Sie das entsprechende Segment aus.
7. Datenspeicherzuordnungen werden automatisch basierend auf der Auswahl der VMs ausgewählt.

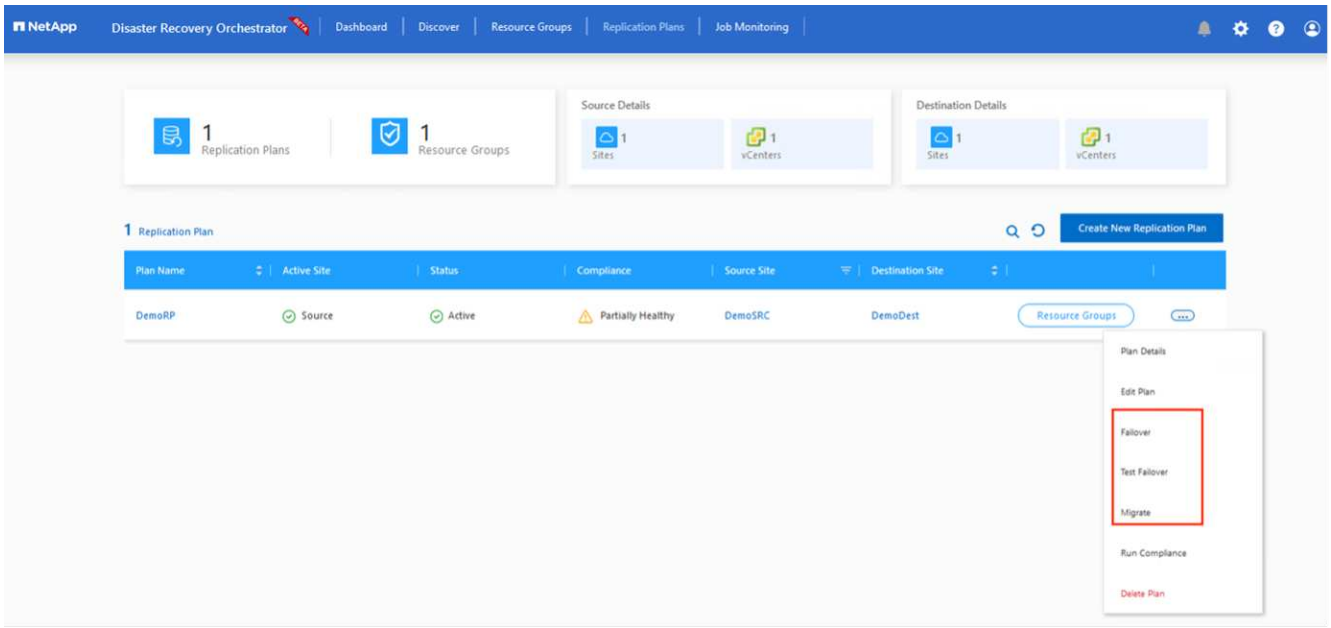
> ⓘ Die regionsübergreifende Replikation (CRR) erfolgt auf Volumeebene. Daher werden alle auf dem jeweiligen Volume befindlichen VMs zum CRR-Ziel repliziert. Achten Sie darauf, alle VMs auszuwählen, die Teil des Datenspeichers sind, da nur virtuelle Maschinen verarbeitet werden, die Teil des Replikationsplans sind.



8. Unter VM-Details können Sie optional die CPU- und RAM-Parameter der VMs ändern. Dies kann sehr hilfreich sein, wenn Sie große Umgebungen auf kleineren Zielclustern wiederherstellen oder DR-Tests durchführen, ohne eine physische Eins-zu-eins-VMware-Infrastruktur bereitstellen zu müssen. Ändern Sie außerdem die Startreihenfolge und die Startverzögerung (Sek.) für alle ausgewählten VMs in den Ressourcengruppen. Es gibt eine zusätzliche Option zum Ändern der Startreihenfolge, wenn Änderungen an der von Ihnen bei der Auswahl der Startreihenfolge der Ressourcengruppe ausgewählten Reihenfolge erforderlich sind. Standardmäßig wird die bei der Ressourcengruppenauswahl festgelegte Startreihenfolge verwendet. In dieser Phase können jedoch beliebige Änderungen vorgenommen werden.

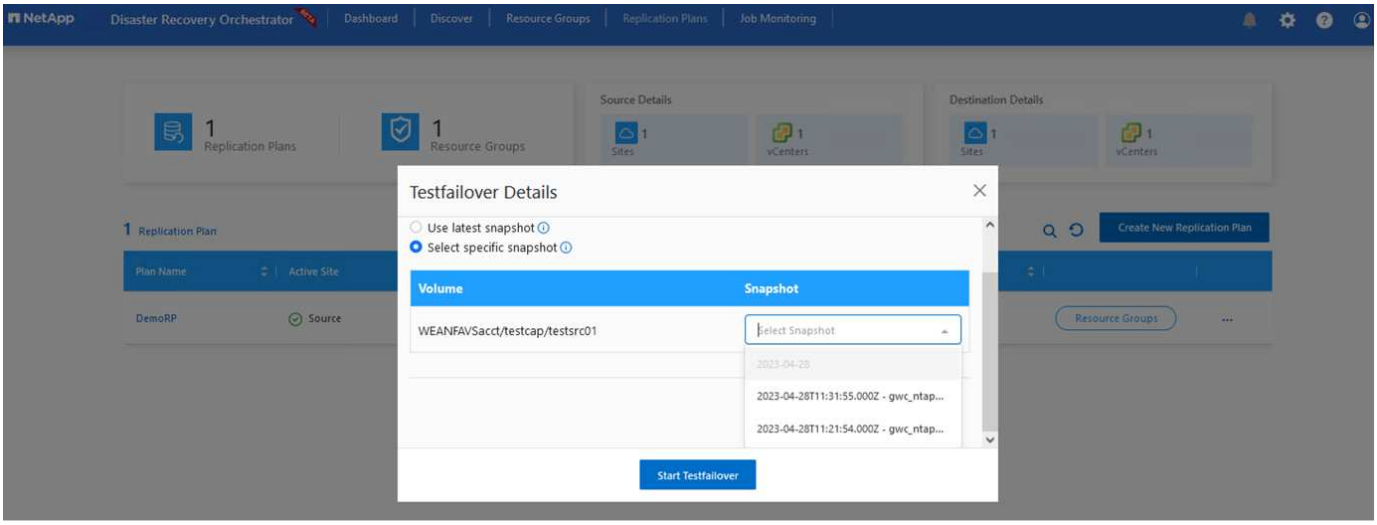


9. Klicken Sie auf **Replikationsplan erstellen**. Nachdem der Replikationsplan erstellt wurde, können Sie je nach Ihren Anforderungen die Optionen Failover, Testfailover oder Migration ausführen.

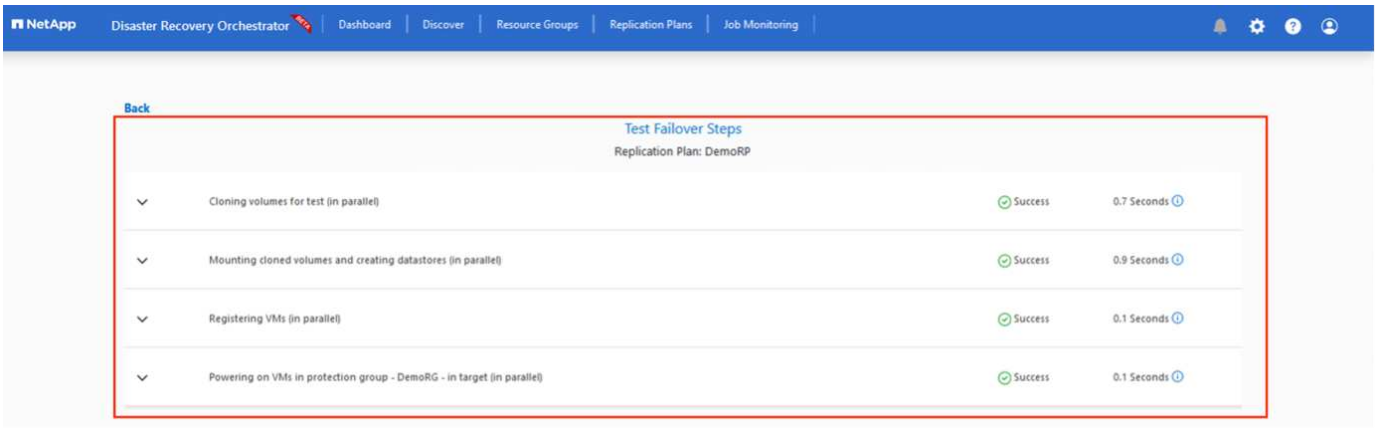


Bei den Failover- und Test-Failover-Optionen wird der aktuellste Snapshot verwendet oder es kann ein bestimmter Snapshot aus einem Point-in-Time-Snapshot ausgewählt werden. Die Point-in-Time-Option kann sehr nützlich sein, wenn Sie mit einem Korruptionsereignis wie Ransomware konfrontiert sind, bei dem die

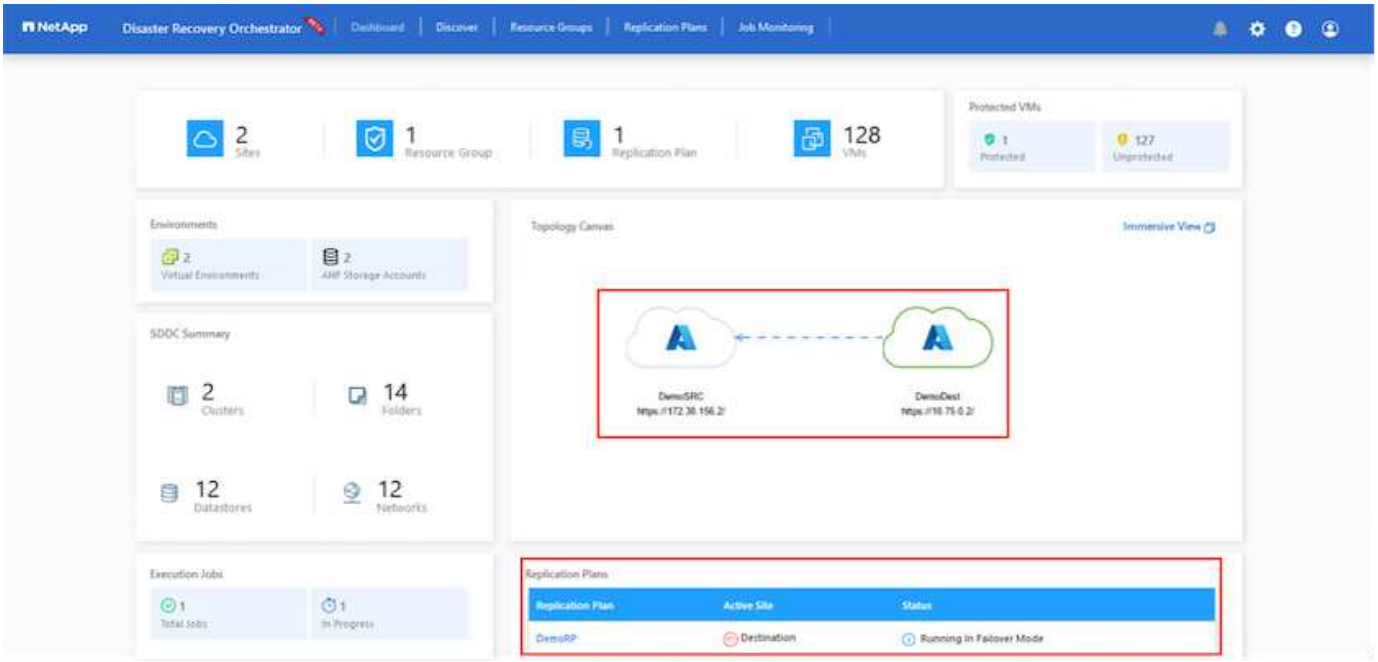
aktuellsten Replikate bereits kompromittiert oder verschlüsselt sind. DRO zeigt alle verfügbaren Zeitpunkte an.



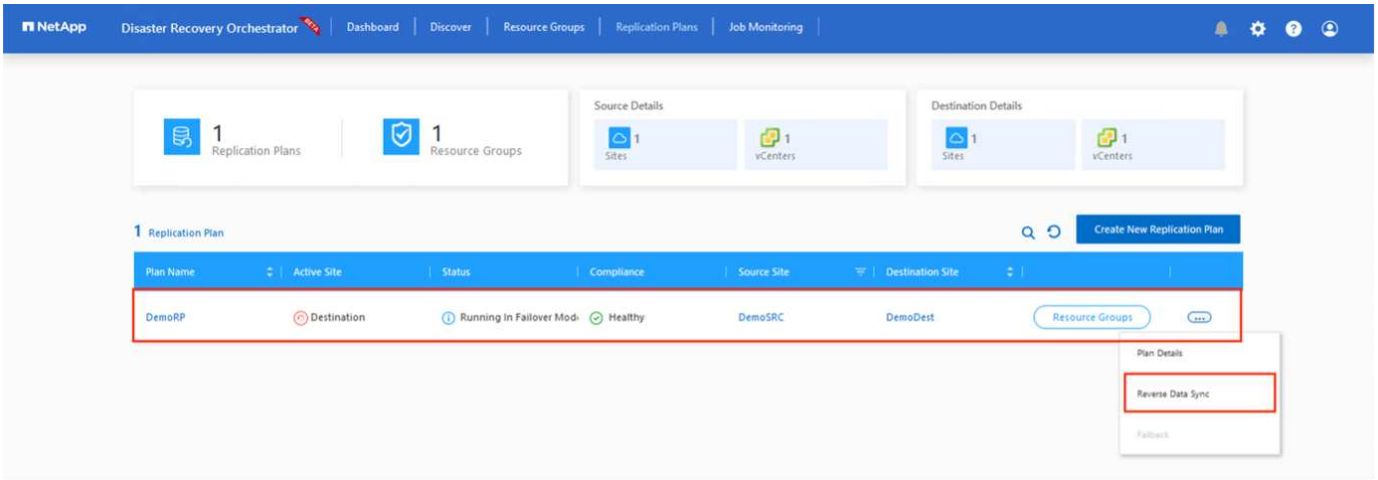
Um ein Failover auszulösen oder ein Failover mit der im Replikationsplan angegebenen Konfiguration zu testen, können Sie auf **Failover** oder **Failover testen** klicken. Sie können den Replikationsplan im Aufgabenmenü überwachen.



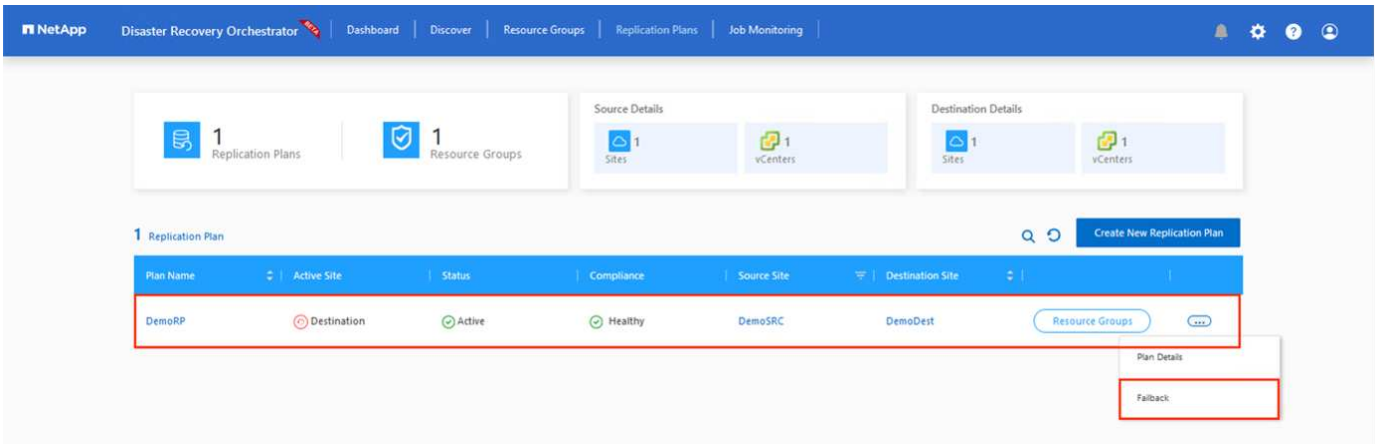
Nachdem das Failover ausgelöst wurde, können die wiederhergestellten Elemente im AVS SDDC vCenter (VMs, Netzwerke und Datenspeicher) des sekundären Standorts angezeigt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.

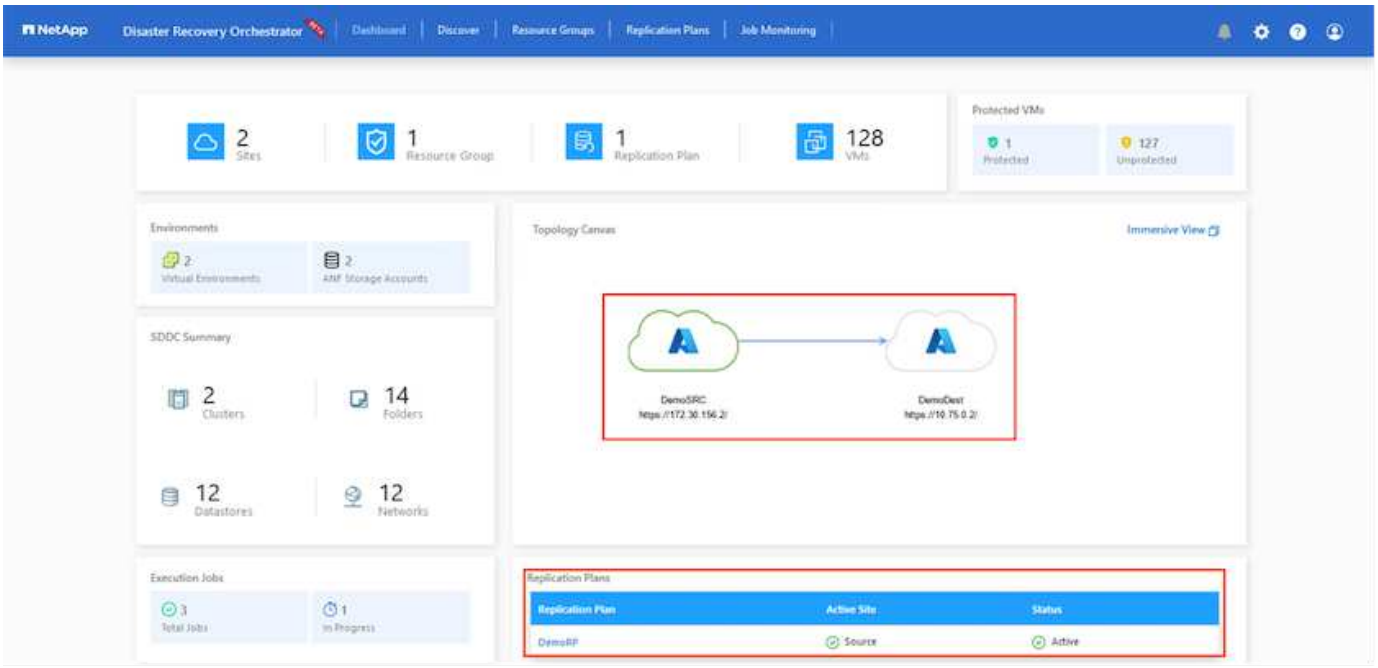


Failback kann auf der Ebene des Replikationsplans ausgelöst werden. Im Falle eines Test-Failovers kann die Teardown-Option verwendet werden, um die Änderungen rückgängig zu machen und das neu erstellte Volume zu entfernen. Failbacks im Zusammenhang mit Failover sind ein zweistufiger Prozess. Wählen Sie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



Nachdem dieser Schritt abgeschlossen ist, lösen Sie ein Failback aus, um zur primären AVS-Site zurückzukehren.





Im Azure-Portal können wir sehen, dass die Replikationsintegrität für die entsprechenden Volumes unterbrochen wurde, die dem AVS SDDC des sekundären Standorts als Lese-/Schreibvolumes zugeordnet wurden. Während des Test-Failovers ordnet DRO das Ziel- oder Replikat-Volume nicht zu. Stattdessen wird ein neues Volume des erforderlichen regionsübergreifenden Replikations-Snapshots erstellt und das Volume als Datenspeicher bereitgestellt, wodurch zusätzliche physische Kapazität aus dem Kapazitätspool verbraucht wird und sichergestellt wird, dass das Quellvolume nicht geändert wird. Insbesondere können Replikationsaufträge während DR-Tests oder Triage-Workflows fortgesetzt werden. 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.

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, sobald dieser ermittelt ist, sicherzustellen, dass wiederhergestellte Workloads vor erneuten Angriffen (beispielsweise durch ruhende Malware oder anfällige Anwendungen) geschützt sind.

DRO geht auf diese Bedenken ein, indem es Unternehmen die Wiederherstellung von jedem verfügbaren Zeitpunkt aus ermöglicht. Anschließend werden die Arbeitslasten in funktionsfähige und dennoch isolierte Netzwerke zurückgeführt, sodass die Anwendungen funktionieren und miteinander kommunizieren können,

aber keinem Nord-Süd-Verkehr ausgesetzt sind. Dieser Prozess bietet Sicherheitsteams einen sicheren Ort, um forensische Untersuchungen durchzuführen und versteckte oder schlafende Malware zu identifizieren.

Abschluss

Die Notfallwiederherstellungslösung Azure NetApp Files und Azure VMware bietet Ihnen die folgenden Vorteile:

- Nutzen Sie die effiziente und stabile regionsübergreifende Replikation von Azure NetApp Files .
- Stellen Sie mit Snapshot-Aufbewahrung einen beliebigen verfügbaren Zeitpunkt wieder her.
- Automatisieren Sie alle erforderlichen Schritte vollständig, um Hunderte bis Tausende von VMs aus den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung wiederherzustellen.
- Bei der Workload-Wiederherstellung wird der Prozess „Neue Volumes aus den aktuellsten Snapshots erstellen“ genutzt, bei dem das replizierte Volume nicht manipuliert wird.
- Vermeiden Sie jegliches Risiko einer Datenbeschädigung auf den Volumes oder Snapshots.
- Vermeiden Sie Replikationsunterbrechungen während DR-Test-Workflows.
- Nutzen Sie DR-Daten und Cloud-Rechenressourcen für Workflows, die über DR hinausgehen, wie etwa Entwicklung/Test, Sicherheitstests, Patch- und Upgrade-Tests sowie Fehlerbehebungstests.
- Durch die CPU- und RAM-Optimierung können die Cloud-Kosten gesenkt werden, da die Wiederherstellung auf kleineren Computerclustern möglich ist.

Wo Sie weitere Informationen finden

Weitere Informationen zu den in diesem Dokument beschriebenen Informationen finden Sie in den folgenden Dokumenten und/oder auf den folgenden Websites:

- Erstellen einer Volumereplikation für Azure NetApp Files

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

- Regionenübergreifende Replikation von Azure NetApp Files -Volumes

  "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"

- Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf Azure

  "AVS auf Azure einrichten"

- Bereitstellen und Konfigurieren der Azure VMware-Lösung

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