TR-4955: Notfallwiederherstellung mit FSx ONTAP und VMC (AWS VMware Cloud)

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-aws-vmc-dro.html on August 18, 2025. Always check docs.netapp.com for the latest.

Inhalt

TR-4955: Notfallwiederherstellung mit FSx ONTAP und VMC (AWS VMware Cloud) . . . 1
Überblick . . . 1
Erste Schritte . . . 1
Bereitstellen und Konfigurieren von VMware Cloud auf AWS . . . 2
Bereitstellen und Konfigurieren von FSx ONTAP . . . 2
Bereitstellen und Konfigurieren von SnapMirror für FSx ONTAP . . . 2
DRO-Installation . . . 3
Voraussetzungen . . . 3
OS Anforderungen . . . 3
Installieren des Pakets . . . 3
DRO-Konfiguration . . . 4
Ressourcengruppierungen . . . 6
Replikationspläne . . . 7
Ransomware-Wiederherstellung . . . 15
Vorteile . . . 15

TR-4955: Notfallwiederherstellung mit FSx ONTAP und VMC (AWS VMware Cloud)

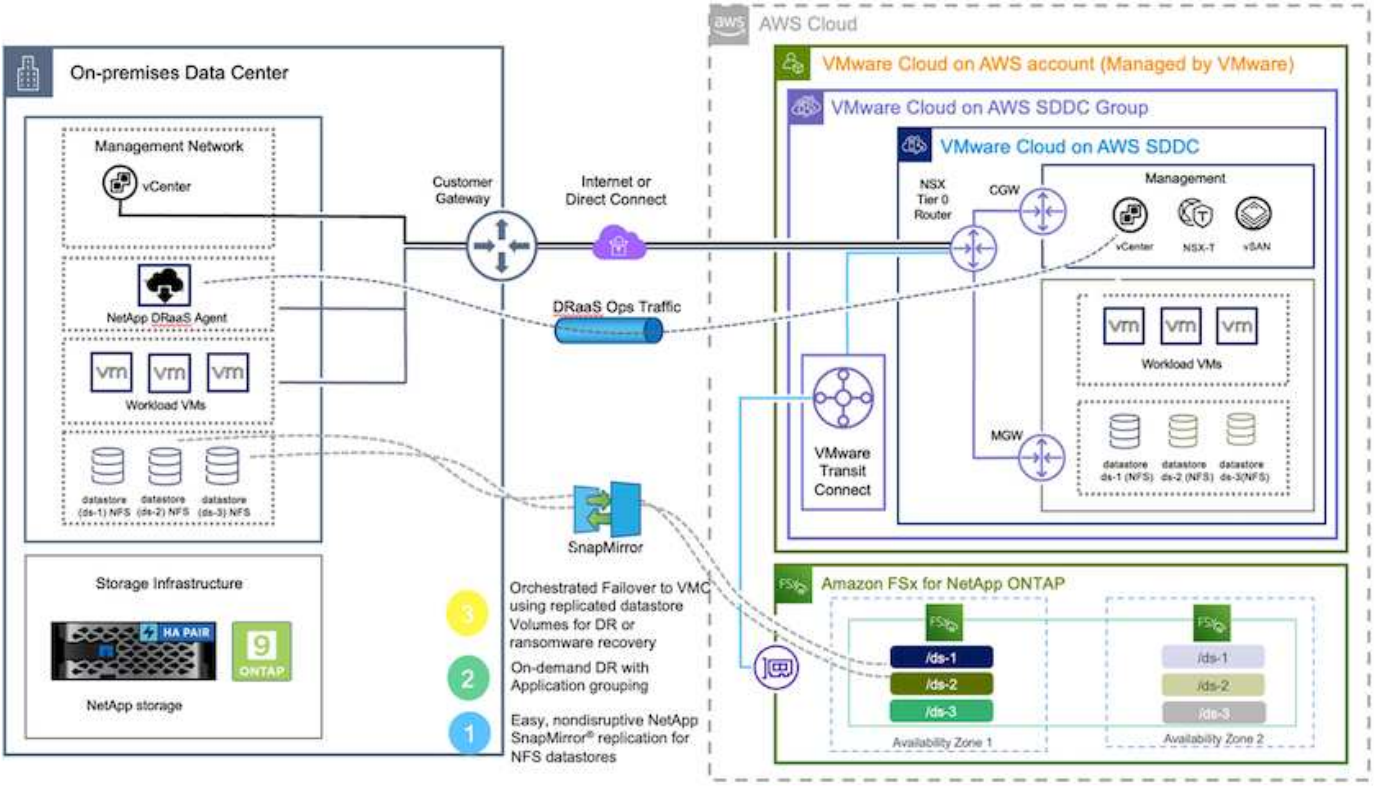
Mit Disaster Recovery Orchestrator (DRO; eine Skriptlösung mit Benutzeroberfläche) können Workloads, die vor Ort auf FSx ONTAP repliziert wurden, nahtlos wiederhergestellt werden. DRO automatisiert die Wiederherstellung von der SnapMirror Ebene über die VM-Registrierung bei VMC bis hin zu Netzwerkzuordnungen direkt auf NSX-T. Diese Funktion ist in allen VMC-Umgebungen enthalten.

Niyaz Mohamed, NetApp

Überblick

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Site-Ausfällen und Datenbeschädigungen (z. B. Ransomware) zu schützen. Mit der NetApp SnapMirror -Technologie können lokale VMware-Workloads auf FSx ONTAP repliziert werden, das in AWS ausgeführt wird.

Mit Disaster Recovery Orchestrator (DRO; eine Skriptlösung mit Benutzeroberfläche) können Workloads, die vor Ort auf FSx ONTAP repliziert wurden, nahtlos wiederhergestellt werden. DRO automatisiert die Wiederherstellung von der SnapMirror Ebene über die VM-Registrierung bei VMC bis hin zu Netzwerkzuordnungen direkt auf NSX-T. Diese Funktion ist in allen VMC-Umgebungen enthalten.



Erste Schritte

Bereitstellen und Konfigurieren von VMware Cloud auf AWS

"VMware Cloud auf AWS"bietet eine Cloud-native Erfahrung für VMware-basierte Workloads im AWS-Ökosystem. Jedes VMware Software-Defined Data Center (SDDC) läuft in einer Amazon Virtual Private Cloud (VPC) und bietet einen vollständigen VMware-Stack (einschließlich vCenter Server), NSX-T Software-Defined Networking, vSAN Software-Defined Storage und einen oder mehrere ESXi-Hosts, die den Workloads Rechen- und Speicherressourcen bereitstellen. Um eine VMC-Umgebung auf AWS zu konfigurieren, folgen Sie den Schritten hier"Link" . Ein Pilotlichtcluster kann auch für DR-Zwecke verwendet werden.

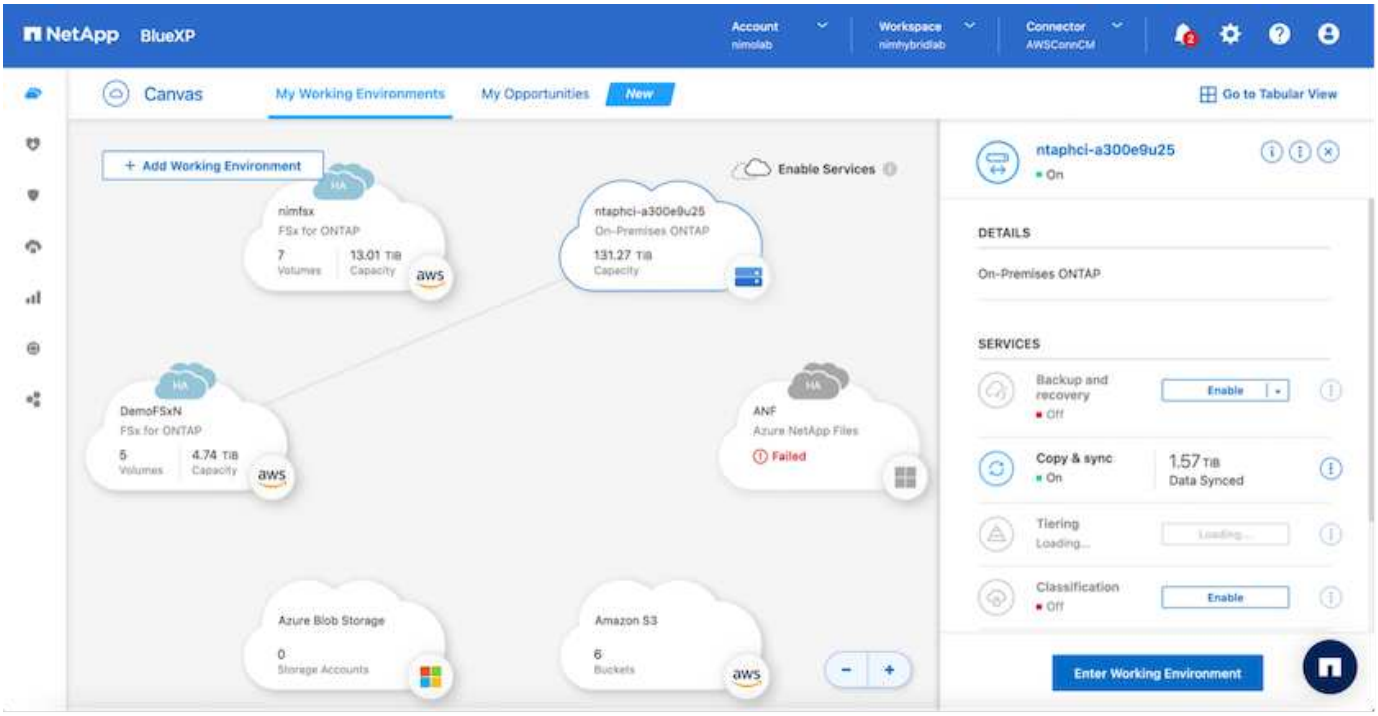
> In der ersten Version unterstützt DRO einen vorhandenen Pilotlichtcluster. Die On-Demand-SDDC-Erstellung wird in einer kommenden Version verfügbar sein.

Bereitstellen und Konfigurieren von FSx ONTAP

Amazon FSx ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem beliebten NetApp ONTAP Dateisystem basiert. Befolgen Sie die Schritte in diesem"Link" zum Bereitstellen und Konfigurieren von FSx ONTAP.

Bereitstellen und Konfigurieren von SnapMirror für FSx ONTAP

Der nächste Schritt besteht darin, NetApp BlueXP zu verwenden, die bereitgestellte FSx ONTAP Instanz auf AWS zu ermitteln und die gewünschten Datenspeichervolumes mit der entsprechenden Häufigkeit und Aufbewahrung der NetApp Snapshot-Kopien aus einer lokalen Umgebung auf FSx ONTAP zu replizieren:



Befolgen Sie die Schritte unter diesem Link, um BlueXP zu konfigurieren. Sie können die Replikation auch über die NetApp ONTAP CLI planen, indem Sie diesem Link folgen.

> Eine SnapMirror -Beziehung ist Voraussetzung und muss vorher erstellt werden.

DRO-Installation

Um mit DRO zu beginnen, verwenden Sie das Ubuntu-Betriebssystem auf einer bestimmten EC2-Instance oder virtuellen Maschine, um sicherzustellen, dass Sie die Voraussetzungen erfüllen. Installieren Sie dann das Paket.

Voraussetzungen

- Stellen Sie sicher, dass eine Verbindung zum Quell- und Ziel-vCenter und den Speichersystemen besteht.
- Wenn Sie DNS-Namen verwenden, sollte eine DNS-Auflösung vorhanden sein. Andernfalls sollten Sie IP-Adressen für das vCenter und die Speichersysteme verwenden.
- Erstellen Sie einen Benutzer mit Root-Berechtigungen. Sie können sudo auch mit einer EC2-Instanz verwenden.

OS Anforderungen

- Ubuntu 20.04 (LTS) mit mindestens 2 GB und 4 vCPUs
- Die folgenden Pakete müssen auf der vorgesehenen Agent-VM installiert werden:
  - Docker
  - Docker-Compose
  - Jq

Berechtigungen ändern für `docker.sock`: `sudo chmod 666 /var/run/docker.sock`.

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

Installieren des Pakets

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

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

   > Der Agent kann vor Ort oder in einem AWS VPC 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 DRO-prereq.tar
   ```

3. Navigieren Sie zum Verzeichnis und führen Sie das Bereitstellungsskript wie folgt aus:

   ```
   sudo sh deploy.sh
   ```

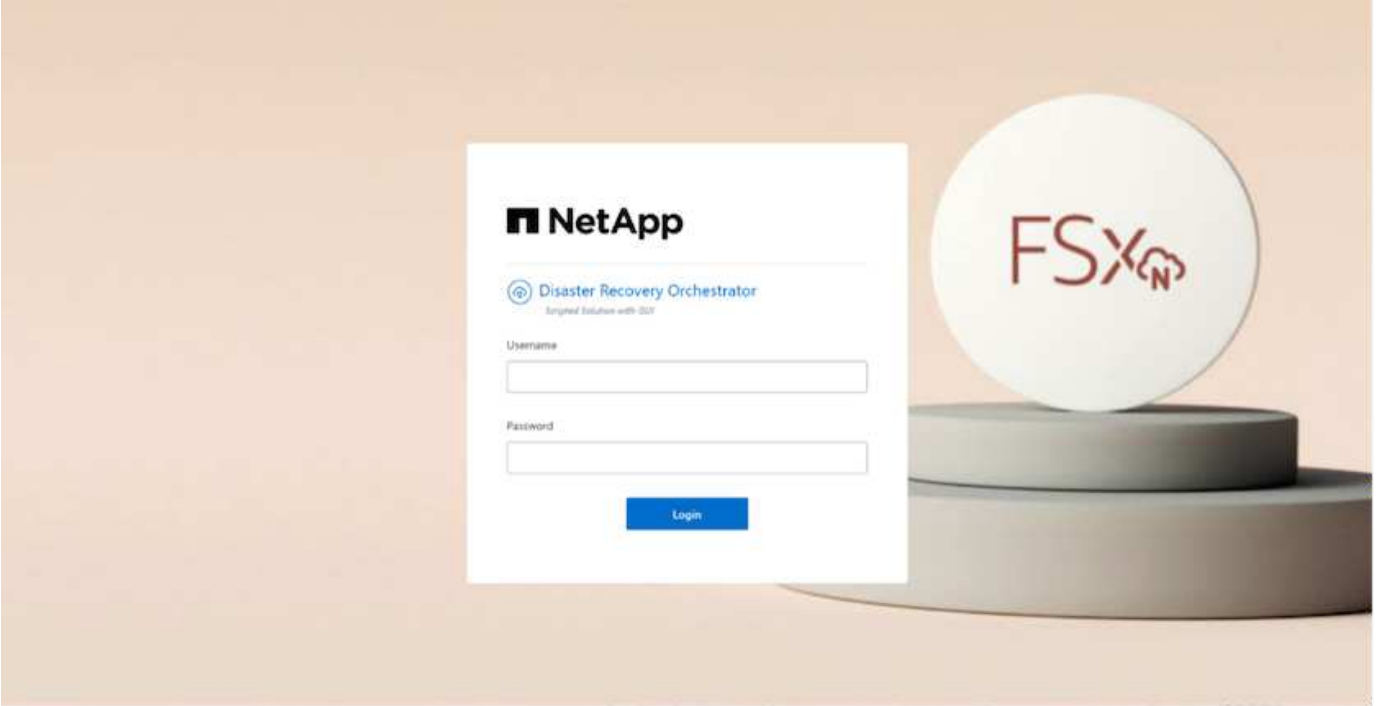
4. Greifen Sie auf die Benutzeroberfläche zu, indem Sie Folgendes verwenden:

```
https://<host-ip-address>
```

mit den folgenden Standardanmeldeinformationen:

```
Username: admin
Password: admin
```

Das Passwort kann über die Option „Passwort ändern“ geändert werden.



DRO-Konfiguration

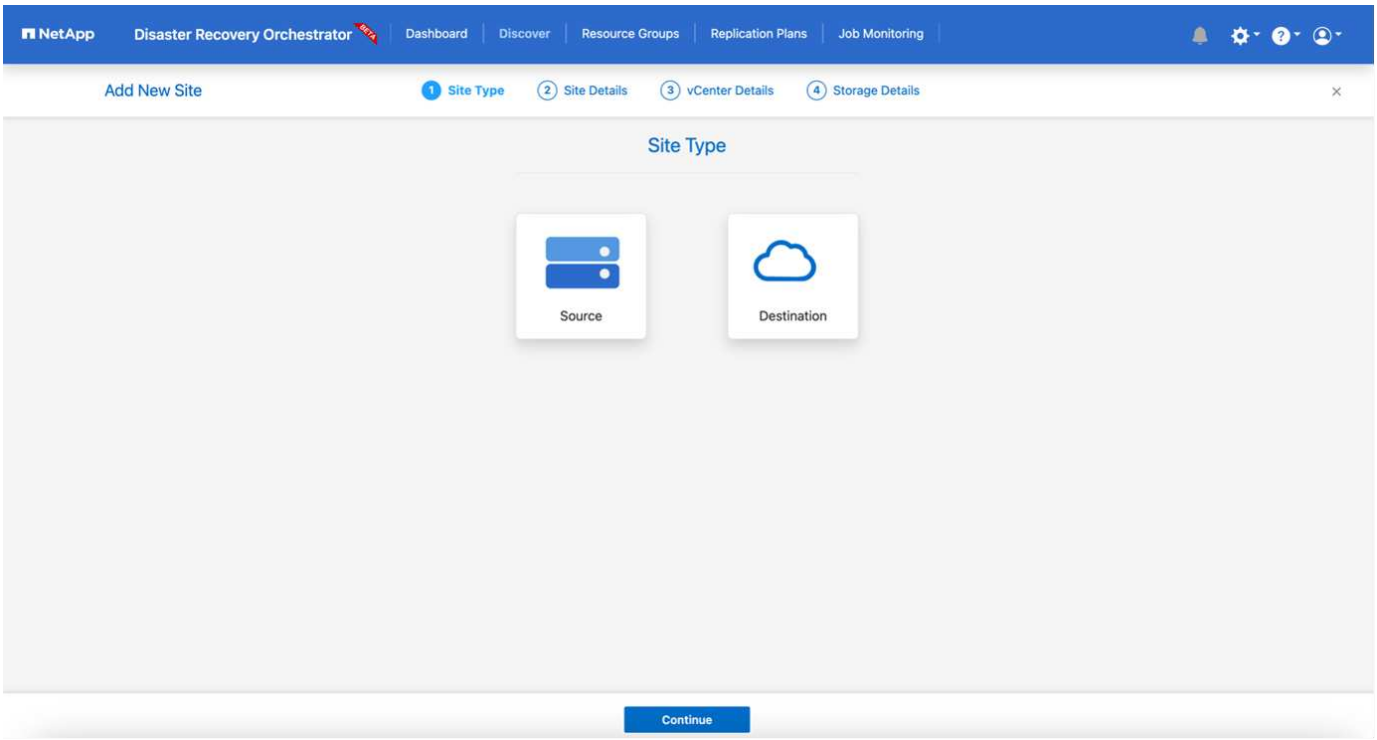
Nachdem FSx ONTAP und VMC ordnungsgemäß konfiguriert wurden, können Sie mit der Konfiguration von DRO beginnen, um die Wiederherstellung lokaler Workloads auf VMC mithilfe der schreibgeschützten SnapMirror -Kopien auf FSx ONTAP zu automatisieren.

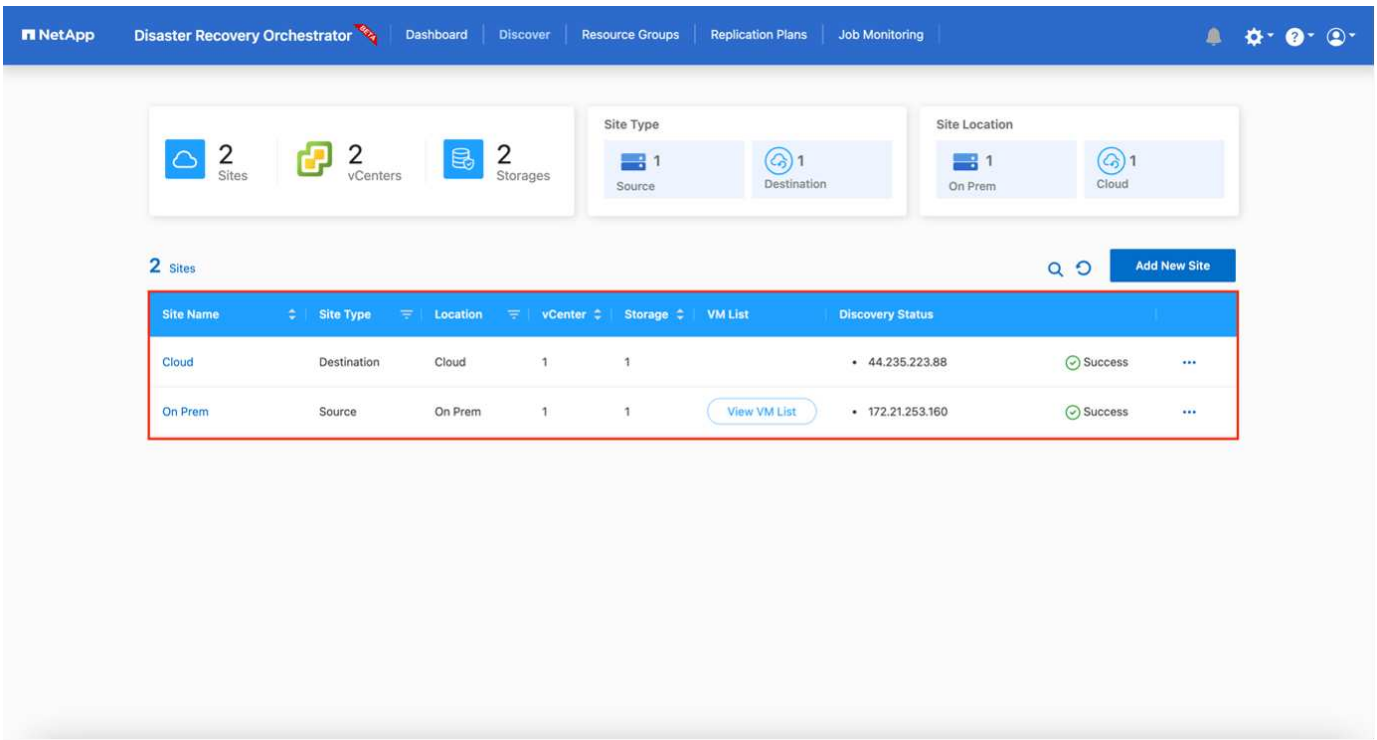
NetApp empfiehlt, den DRO-Agenten in AWS und auch in derselben VPC bereitzustellen, in der FSx ONTAP bereitgestellt wird (es kann auch eine Peer-Verbindung bestehen), damit der DRO-Agent über das Netzwerk mit Ihren lokalen Komponenten sowie mit den FSx ONTAP und VMC-Ressourcen kommunizieren kann.

Der erste Schritt besteht darin, die lokalen und Cloud-Ressourcen (sowohl vCenter als auch Speicher) zu ermitteln und zu DRO hinzuzufügen. Öffnen Sie DRO in einem unterstützten Browser, verwenden Sie den Standardbenutzernamen und das Standardkennwort (admin/admin) und fügen Sie Sites hinzu. Websites können auch mithilfe der Option „Entdecken“ hinzugefügt werden. Fügen Sie die folgenden Plattformen hinzu:

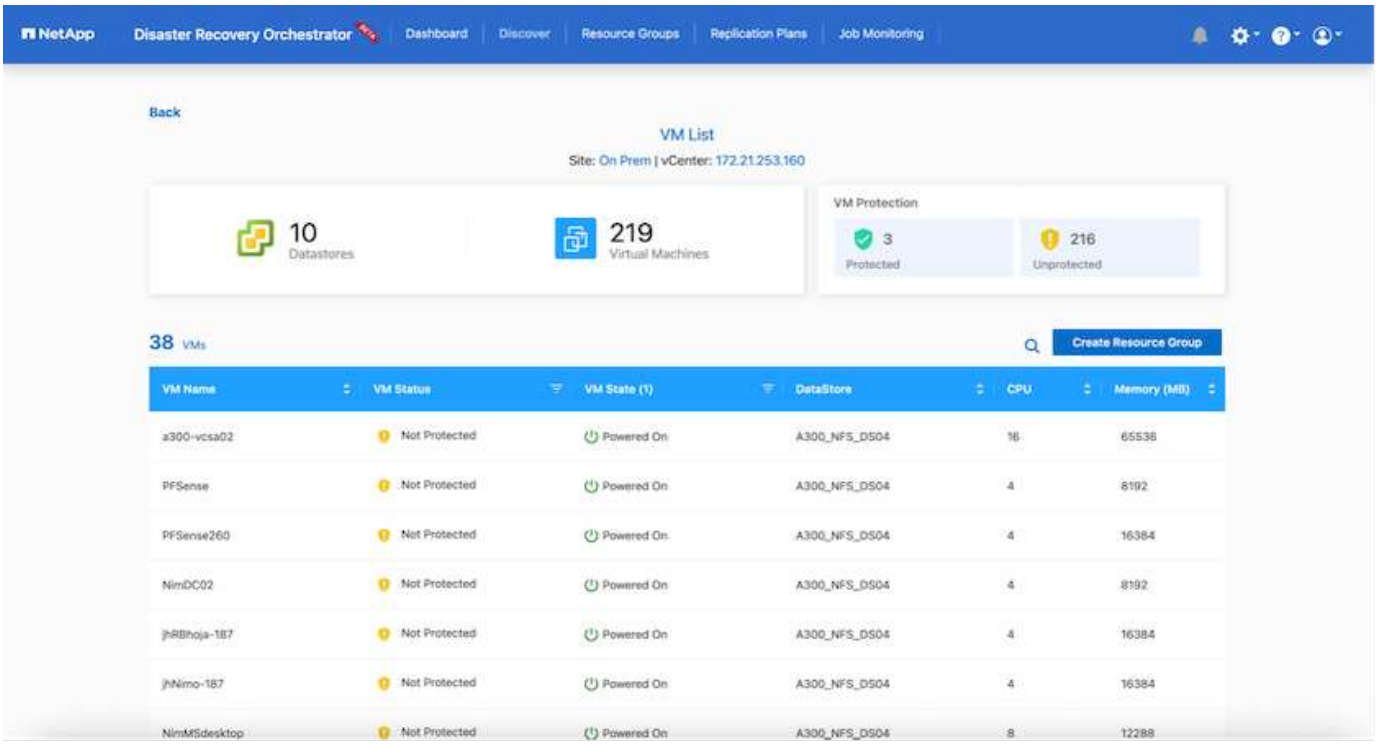
- Vor Ort
  - Lokales vCenter

    - ONTAP -Speichersystem
- Wolke
    - VMC vCenter
    - FSx ONTAP





Nach dem Hinzufügen führt DRO eine automatische Erkennung durch und zeigt die VMs an, die über entsprechende SnapMirror Replikate vom Quellspeicher bis zu FSx ONTAP verfügen. DRO erkennt automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.



Der nächste Schritt besteht darin, die erforderlichen VMs in Funktionsgruppen zu gruppieren, die als Ressourcengruppen dienen.

Ressourcengruppierungen

Nachdem die Plattformen hinzugefügt wurden, können Sie die VMs, die Sie wiederherstellen möchten, in Ressourcengruppen gruppieren. 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.

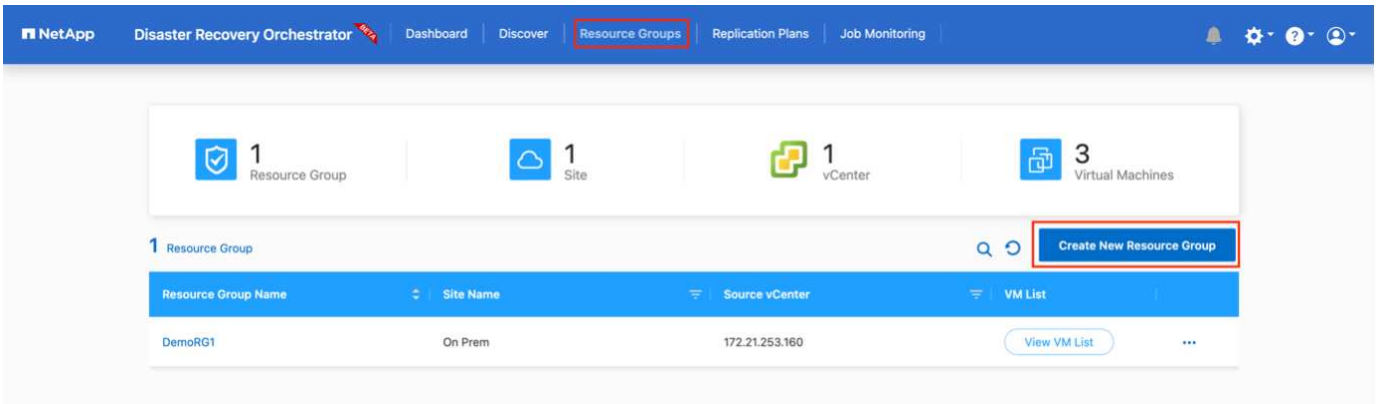
Führen Sie die folgenden Schritte aus, um mit der Erstellung von Ressourcengruppen zu beginnen:

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 **Ressourcengruppendetails** ein und klicken Sie auf **Weiter**.
4. Wählen Sie mithilfe der Suchoption die entsprechenden VMs aus.
5. Wählen Sie die Startreihenfolge und Startverzögerung (Sek.) für die ausgewählten VMs aus. Legen Sie die Reihenfolge der Einschaltsequenz fest, indem Sie jede VM auswählen und die Priorität dafür festlegen. Drei ist der Standardwert für alle VMs.

   Die Optionen sind wie folgt:

   1 – Die erste virtuelle Maschine, die eingeschaltet wird. 3 – Standard. 5 – Die letzte virtuelle Maschine, die eingeschaltet wird.

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

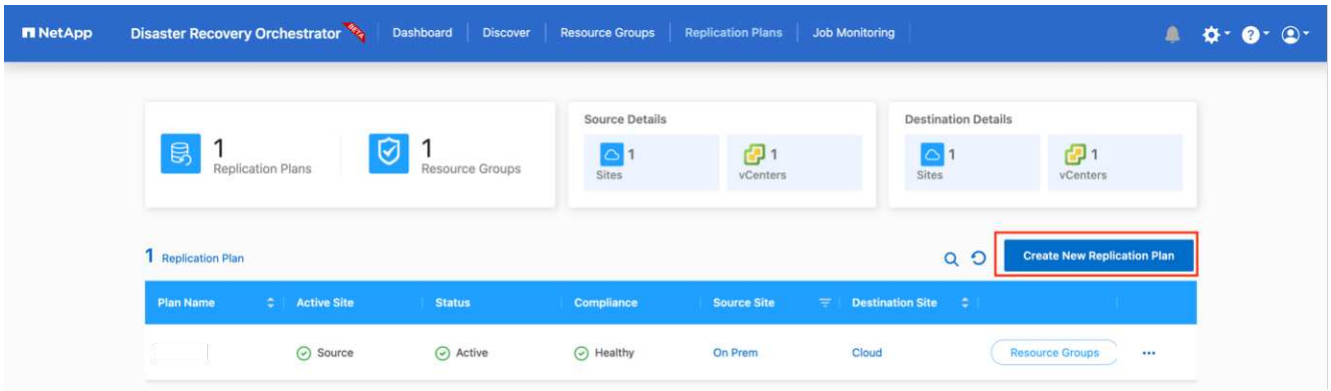


Replikationspläne

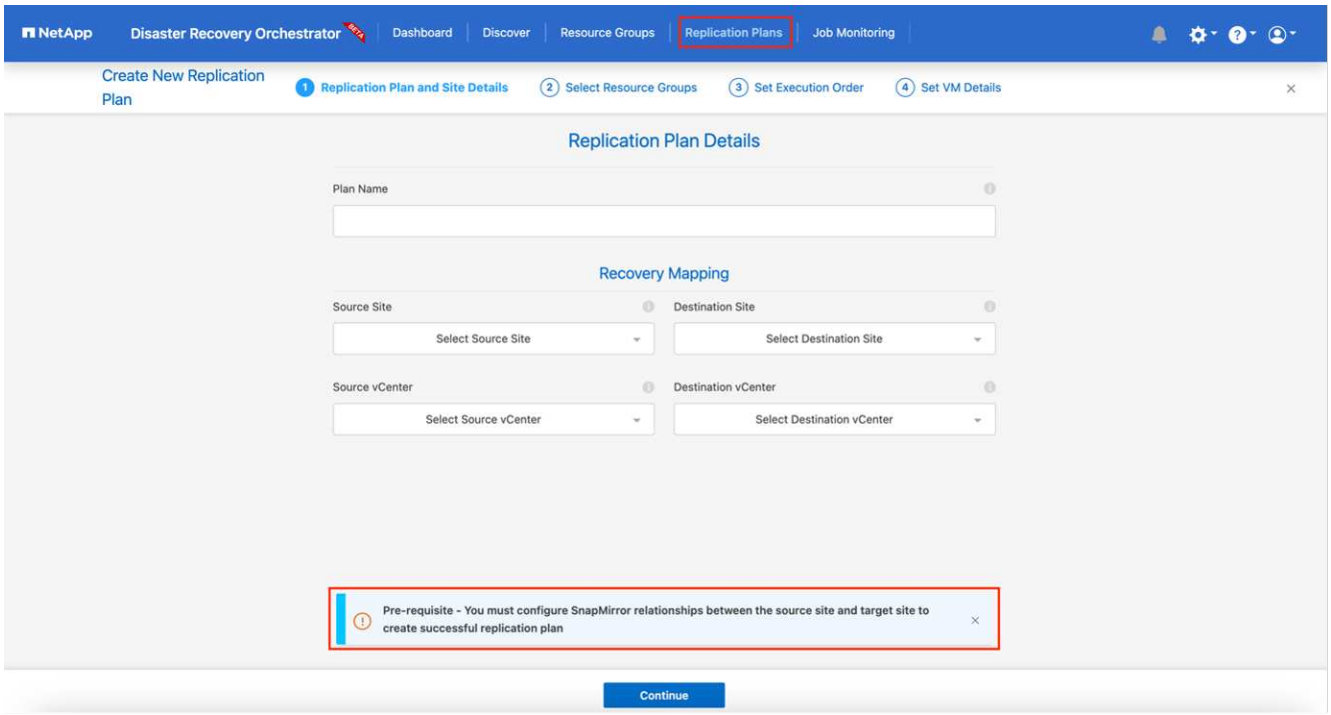
Sie benötigen einen Plan zur Wiederherstellung von Anwendungen im Katastrophenfall. Wählen Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste aus und wählen Sie die Ressourcengruppen aus, die in diesen Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen (z. B. Domänencontroller, dann Tier-1, dann Tier-2 usw.). Solche Pläne werden manchmal 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:

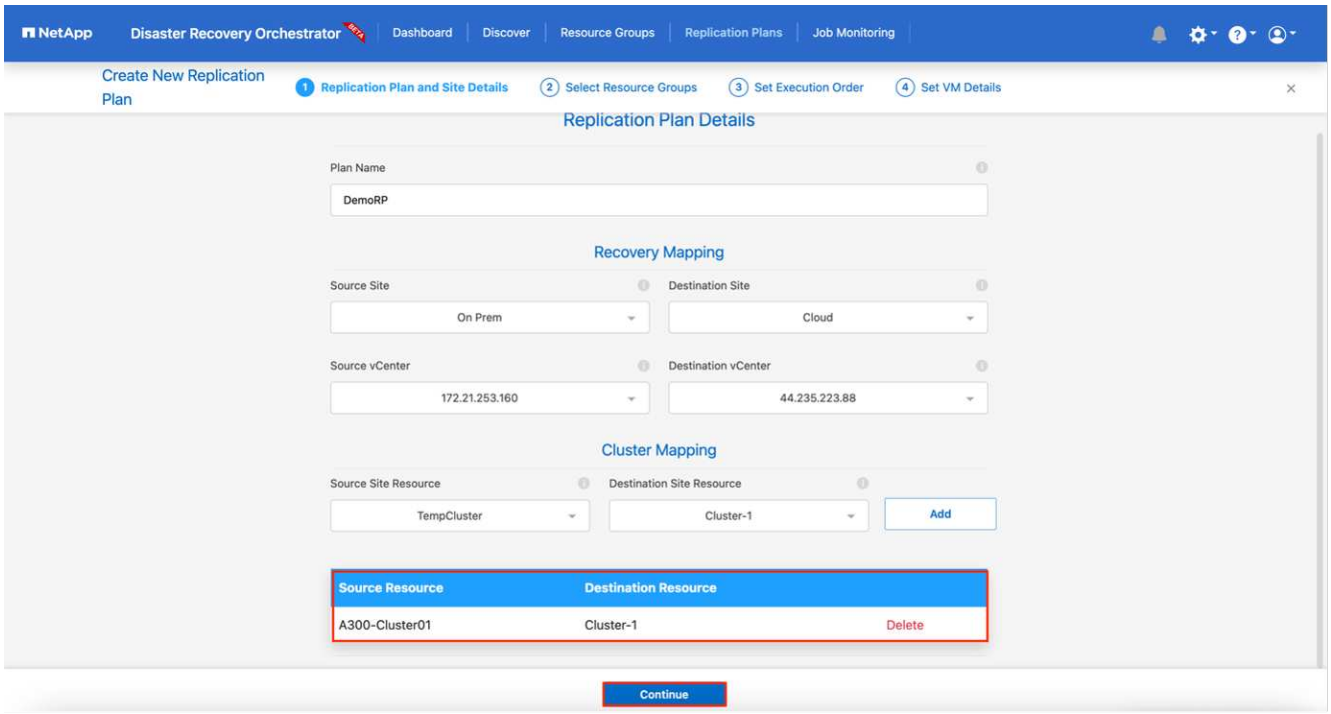
1. Greifen Sie auf **Replikationspläne** zu und klicken Sie auf **Neuen Replikationsplan erstellen**.



2. Geben Sie unter **Neuer 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.

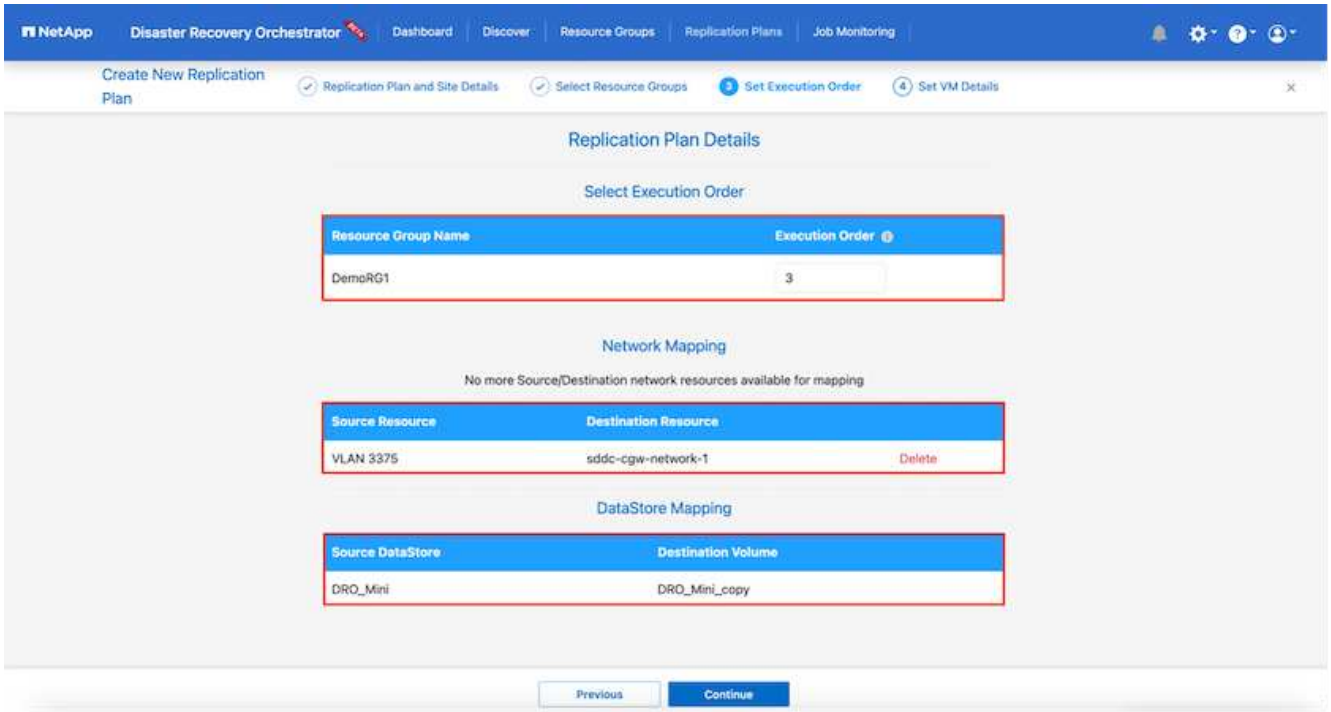


3. Wählen Sie nach Abschluss der Wiederherstellungszuordnung die Clusterzuordnung aus.

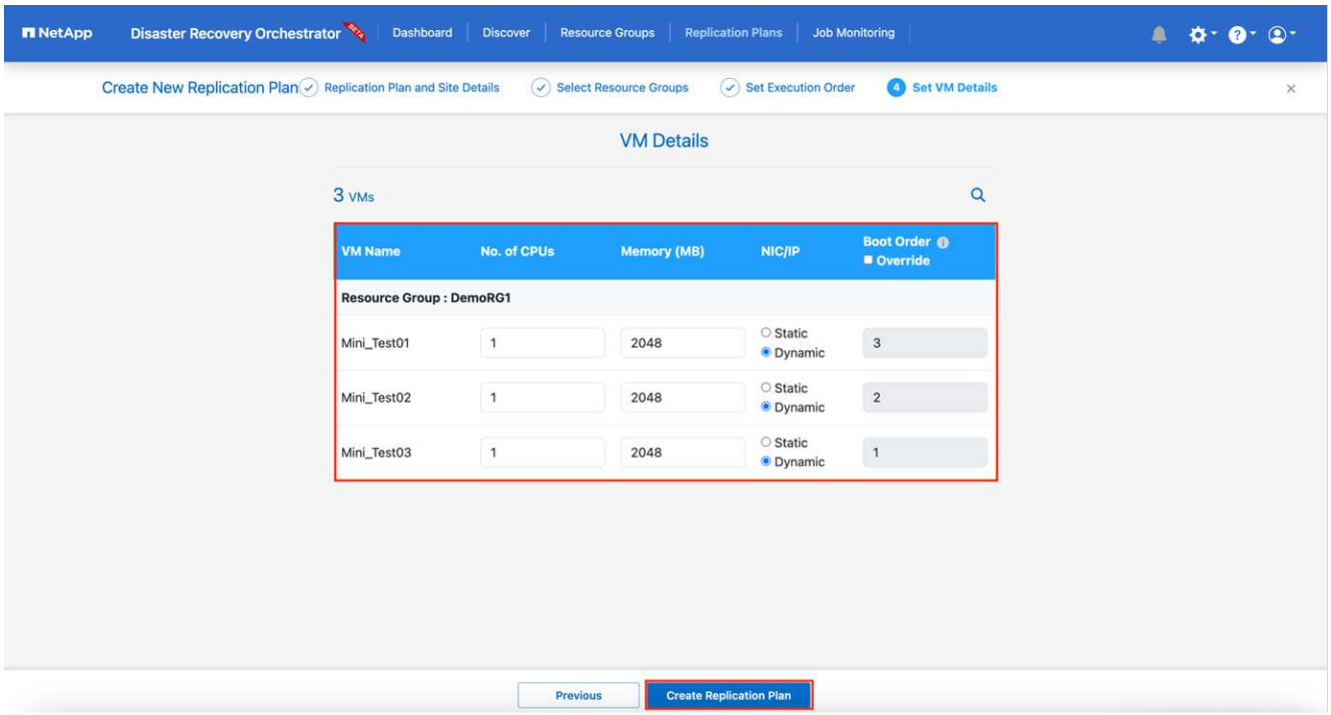


4. Wählen Sie **Ressourcengruppendetails** und klicken Sie auf **Weiter**.
5. Legen Sie die Ausführungsreihenfolge für die Ressourcengruppe fest. Mit dieser Option können Sie die Reihenfolge der Vorgänge auswählen, wenn mehrere Ressourcengruppen vorhanden sind.
6. Wenn Sie fertig sind, wählen Sie die Netzwerkzuordnung zum entsprechenden Segment aus. Die Segmente sollten bereits in VMC bereitgestellt sein. Wählen Sie daher das entsprechende Segment aus, um die VM zuzuordnen.
7. Basierend auf der Auswahl der VMs werden Datenspeicherzuordnungen automatisch ausgewählt.

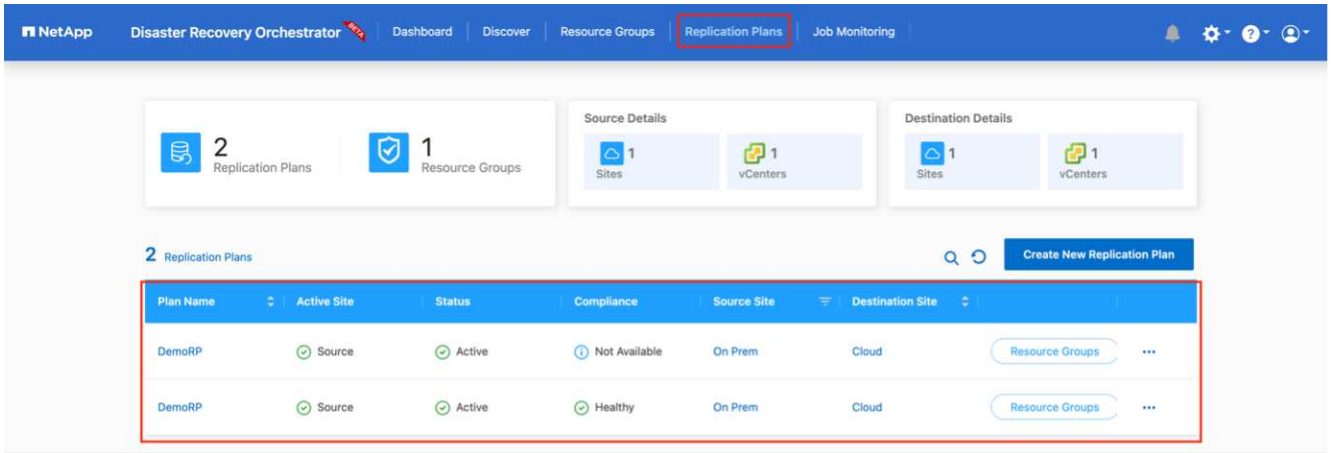
SnapMirror ist auf Lautstärke eingestellt. Daher werden alle VMs zum Replikationsziel repliziert. Stellen Sie sicher, dass Sie alle VMs auswählen, die Teil des Datenspeichers sind. Wenn sie nicht ausgewählt sind, werden nur die VMs verarbeitet, die Teil des Replikationsplans sind.



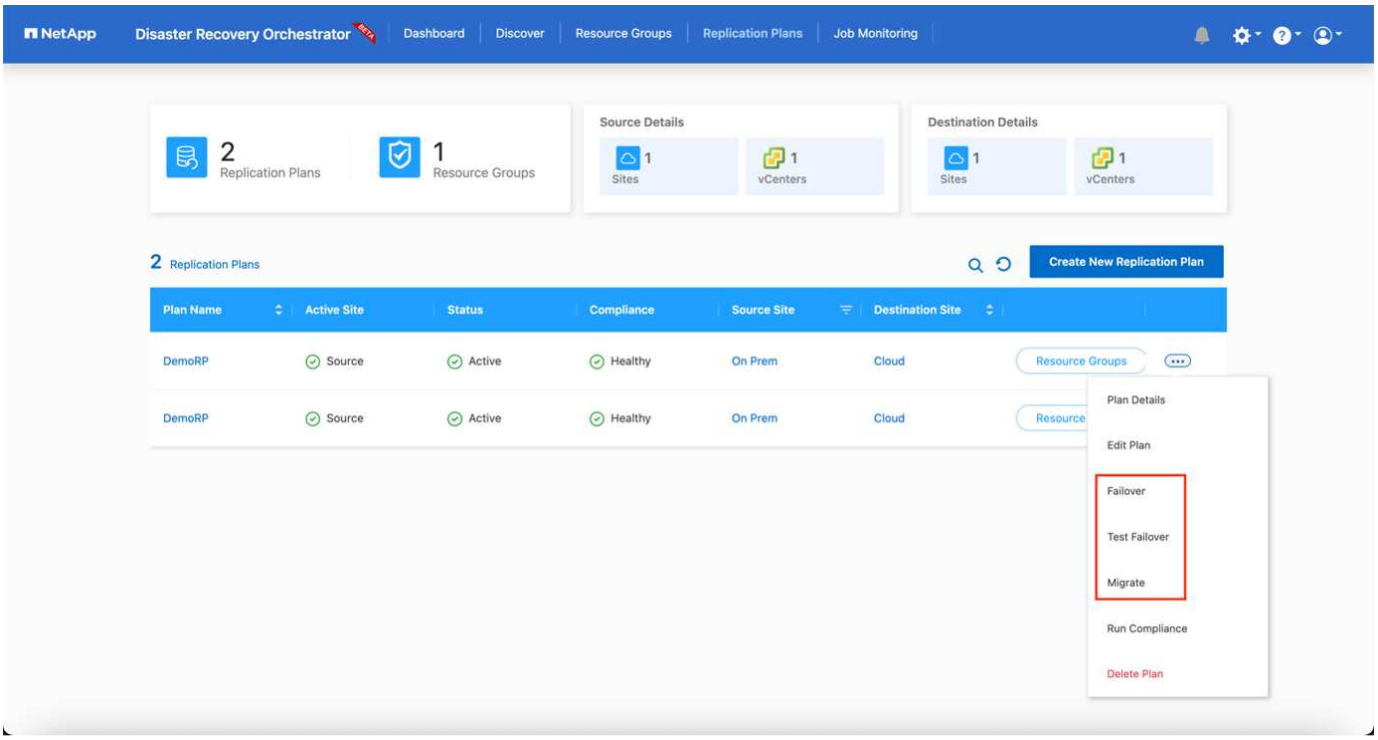
8. Unter den VM-Details können Sie optional die CPU- und RAM-Parameter der VM anpassen. Dies kann sehr hilfreich sein, wenn Sie große Umgebungen auf kleineren Zielclustern wiederherstellen oder DR-Tests durchführen, ohne eine 1:1-physikalische VMware-Infrastruktur bereitstellen zu müssen. Darüber hinaus können Sie die Startreihenfolge und die Startverzögerung (Sekunden) für alle ausgewählten VMs in den Ressourcengruppen ändern. Es gibt eine zusätzliche Option zum Ändern der Startreihenfolge, wenn Änderungen an den bei der Auswahl der Startreihenfolge der Ressourcengruppe ausgewählten vorgenommen werden müssen. Standardmäßig wird die bei der Ressourcengruppenauswahl festgelegte Startreihenfolge verwendet. In dieser Phase können jedoch beliebige Änderungen vorgenommen werden.

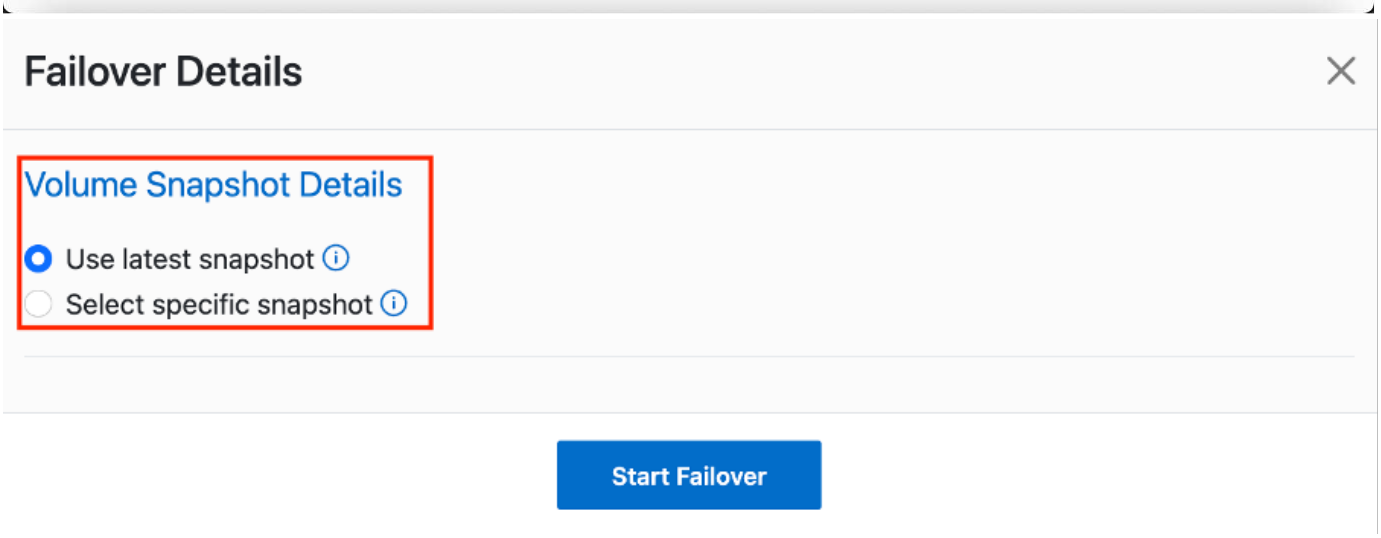


9. Klicken Sie auf **Replikationsplan erstellen**.

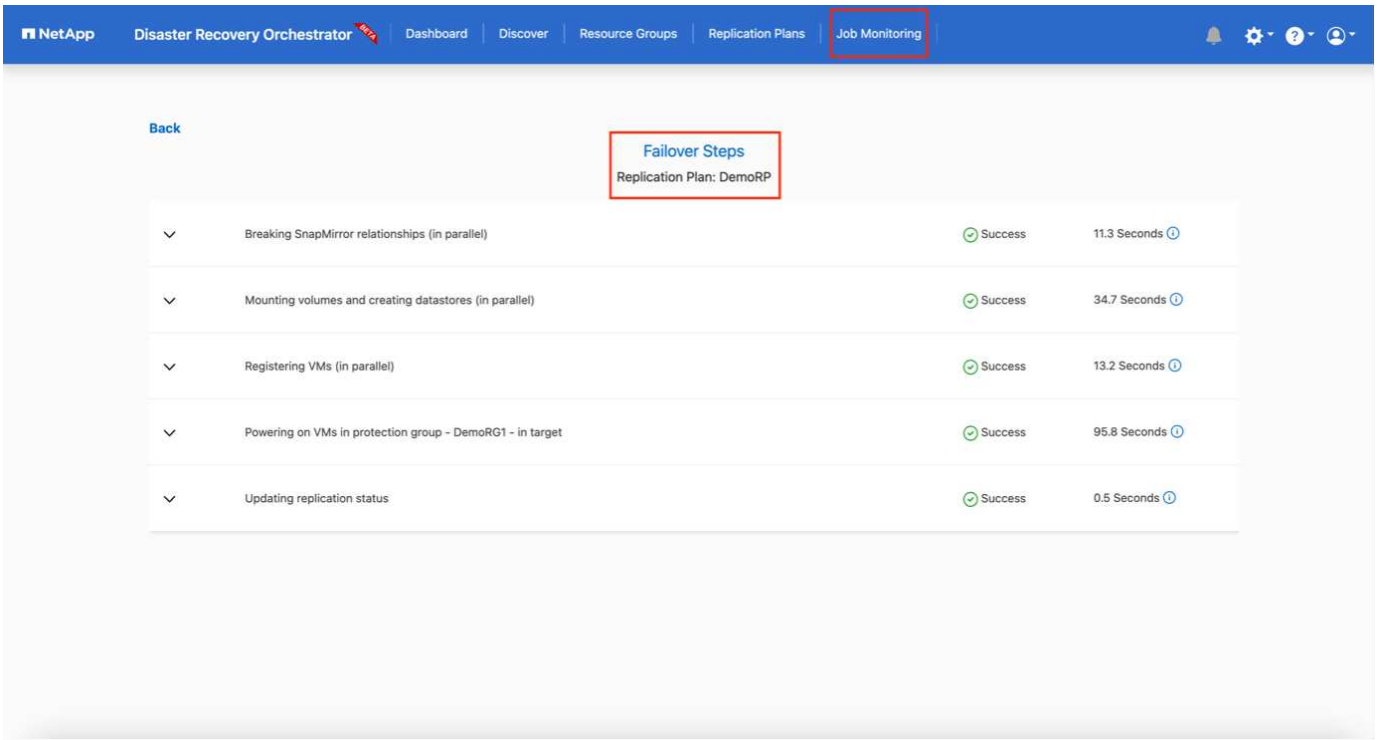


Nachdem der Replikationsplan erstellt wurde, kann je nach Bedarf die Failover-Option, die Test-Failover-Option oder die Migrationsoption ausgeführt werden. Während der Failover- und Test-Failover-Optionen wird die aktuellste SnapMirror -Snapshot-Kopie verwendet, oder es kann eine bestimmte Snapshot-Kopie aus einer Point-in-Time-Snapshot-Kopie ausgewählt werden (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann sehr hilfreich 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.

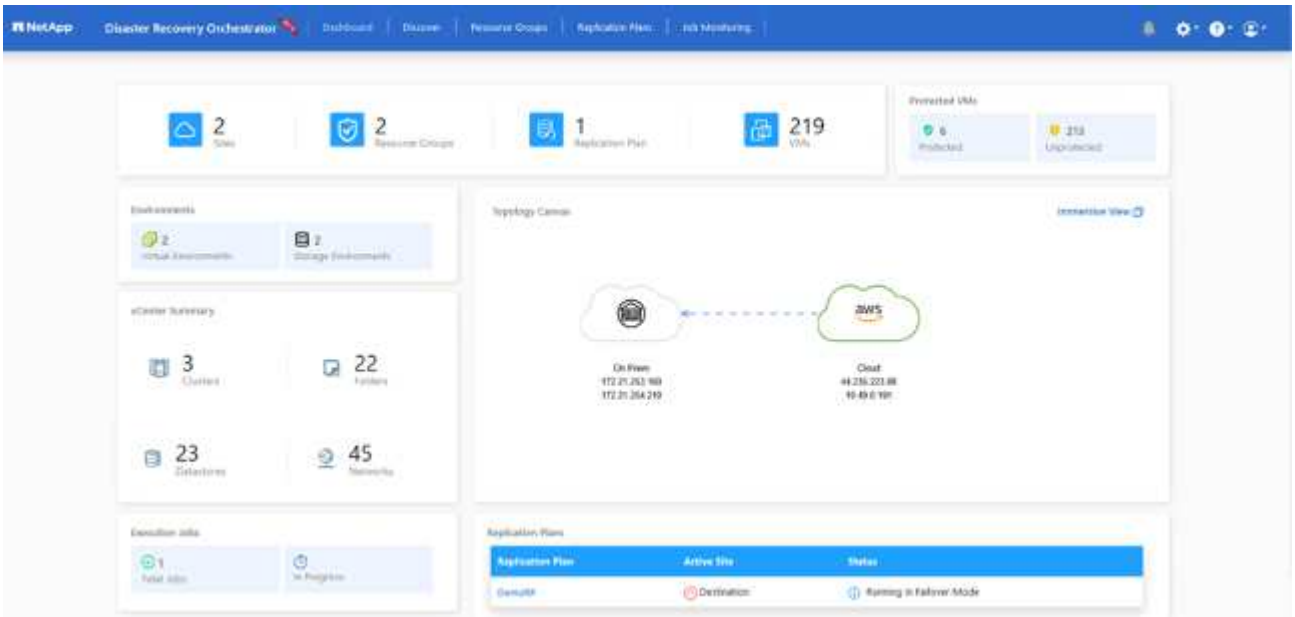




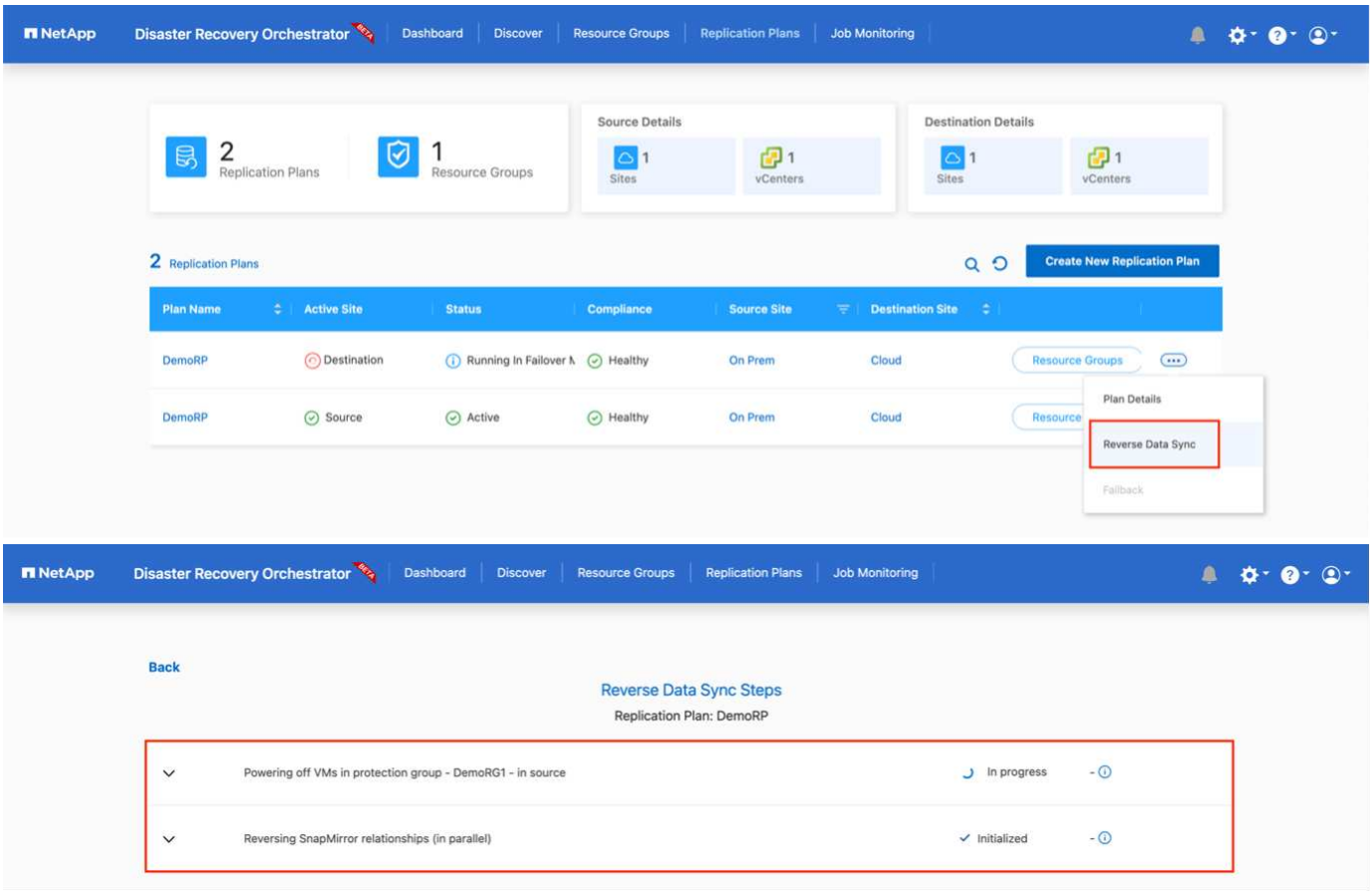
Der Replikationsplan kann im Aufgabenmenü überwacht werden:



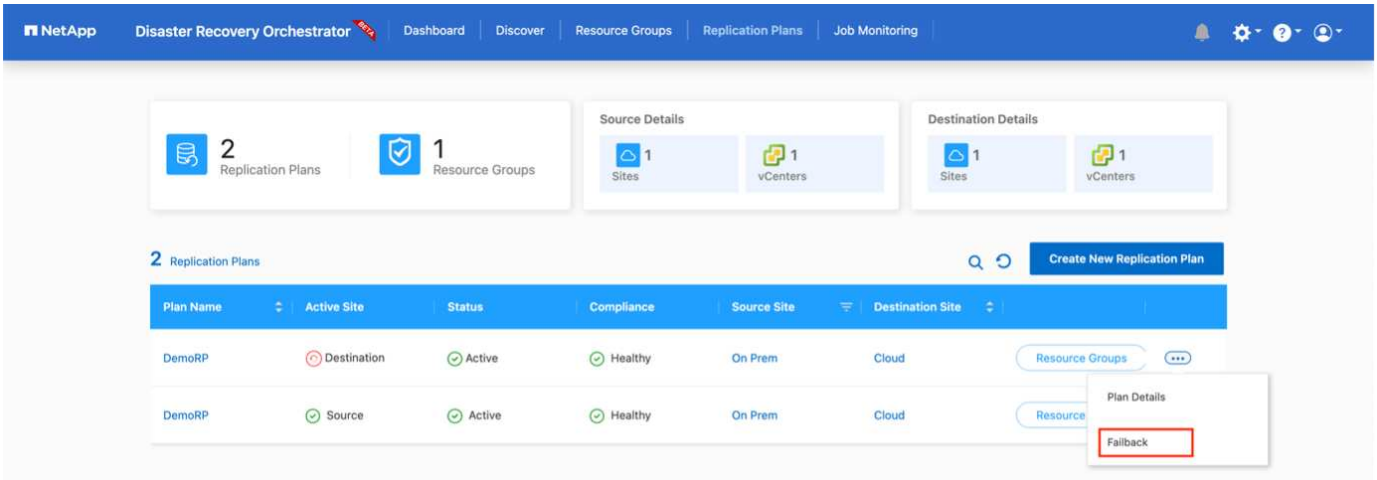
Nachdem das Failover ausgelöst wurde, können die wiederhergestellten Elemente im VMC vCenter (VMs, Netzwerke, Datenspeicher) angezeigt werden. Standardmäßig werden die VMs im Workload-Ordner wiederhergestellt.

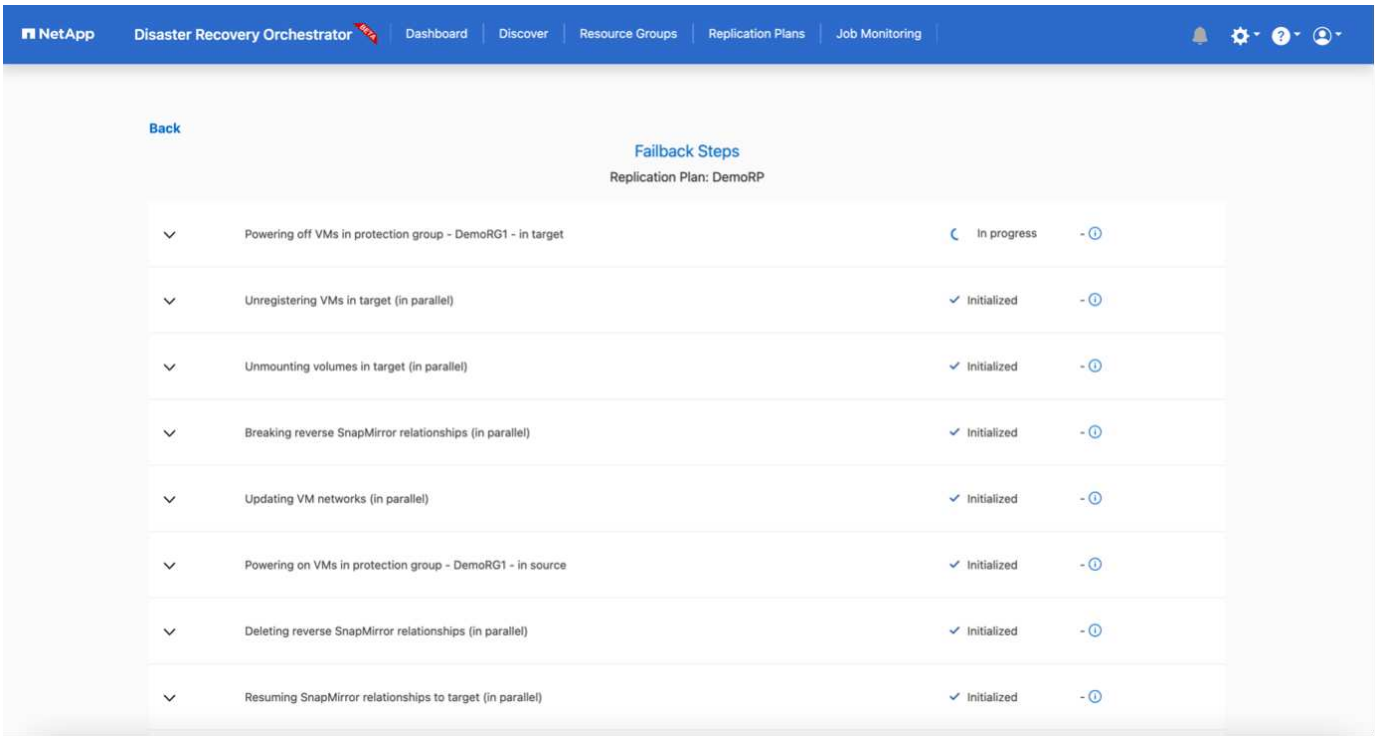


Failback kann auf Replikationsplanebene ausgelöst werden. Für ein Test-Failover kann die Teardown-Option verwendet werden, um die Änderungen rückgängig zu machen und die FlexClone -Beziehung zu entfernen. Das mit dem Failover verbundene Failback ist ein zweistufiger Prozess. Wählen Sie den Replikationsplan und dann **Datensynchronisierung umkehren** aus.

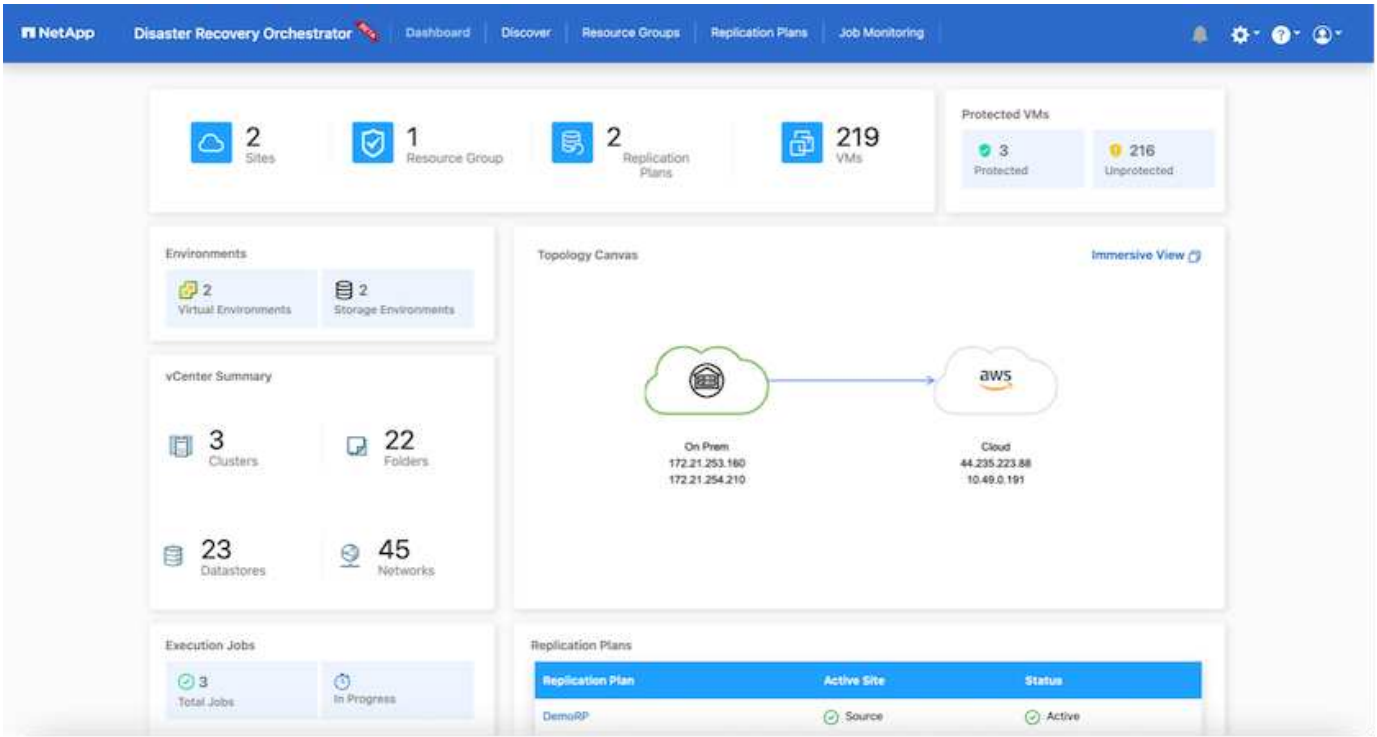


Nach Abschluss können Sie ein Failback auslösen, um zum ursprünglichen Produktionsstandort zurückzukehren.





In NetApp BlueXP können wir sehen, dass die Replikationsintegrität für die entsprechenden Volumes (diejenigen, die VMC als Lese-/Schreib-Volumes zugeordnet wurden) abgebrochen wurde. Während des Test-Failovers ordnet DRO das Ziel- oder Replikat-Volume nicht zu. Stattdessen erstellt es eine FlexClone Kopie der erforderlichen SnapMirror (oder Snapshot-)Instanz und stellt die FlexClone -Instanz bereit, die keine zusätzliche physische Kapazität für FSx ONTAP verbraucht. Dieser Prozess stellt sicher, dass das Volume nicht geändert wird und Replikationsaufträge auch während DR-Tests oder Triage-Workflows fortgesetzt werden können. Darüber hinaus stellt dieser Prozess sicher, dass bei auftretenden Fehlern oder der Wiederherstellung beschädigter Daten die Wiederherstellung bereinigt werden kann, ohne dass die Gefahr besteht, dass das Replikat zerstört wird.



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, wiederhergestellte Workloads vor wiederkehrenden Angriffen beispielsweise durch ruhende Malware oder anfällige Anwendungen zu schützen.

DRO geht auf diese Probleme ein, indem es Ihnen ermöglicht, Ihr System von jedem verfügbaren Zeitpunkt aus wiederherzustellen. Sie können Workloads auch in funktionsfähige und dennoch isolierte Netzwerke zurückverlagern, sodass Anwendungen an einem Standort funktionieren und miteinander kommunizieren können, an dem sie keinem Nord-Süd-Verkehr ausgesetzt sind. Dies bietet Ihrem Sicherheitsteam einen sicheren Ort, um forensische Untersuchungen durchzuführen und sicherzustellen, dass keine versteckte oder schlafende Malware vorhanden ist.

Vorteile

- Nutzung der effizienten und belastbaren SnapMirror -Replikation.
- Wiederherstellung zu jedem verfügbaren Zeitpunkt mit Aufbewahrung der Snapshot-Kopie.
- Vollständige Automatisierung aller erforderlichen Schritte zur Wiederherstellung von Hunderten bis Tausenden von VMs aus den Schritten zur Speicher-, Rechen-, Netzwerk- und Anwendungsvalidierung.
- Workload-Wiederherstellung mit ONTAP FlexClone -Technologie unter Verwendung einer Methode, die das replizierte Volume nicht ändert.
  - Vermeidet das Risiko einer Datenbeschädigung bei Volumes oder Snapshot-Kopien.
  - Vermeidet Replikationsunterbrechungen während DR-Test-Workflows.
  - Mögliche Verwendung von DR-Daten mit Cloud-Computing-Ressourcen für Workflows über DR hinaus, wie z. B. DevTest, Sicherheitstests, Patch- oder Upgrade-Tests und Fehlerbehebungstests.
- CPU- und RAM-Optimierung zur Senkung der Cloud-Kosten durch die Möglichkeit der Wiederherstellung auf kleineren Computerclustern.

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.