BlueXP Disaster Recovery

NetApp Solutions

NetApp
December 19, 2024

This PDF was generated from https://docs.netapp.com/de-de/netapp-solutions/ehc/bxp-scv-hybrid-solution.html on December 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

BlueXP Disaster Recovery

3-2-1 Datensicherung für VMware mit SnapCenter Plug-in und BlueXP Backup und Recovery für VMs

Die 3-2-1-1-Backup-Strategie ist eine in der Branche anerkannte Datenschutzmethode, die einen umfassenden Ansatz für den Schutz wertvoller Daten bietet. Diese Strategie ist zuverlässig und stellt sicher, dass auch bei unerwarteten Notfällen weiterhin eine Kopie der Daten verfügbar ist.

Autor: Josh Powell – NetApp Solutions Engineering

Überblick

Die Strategie setzt sich aus drei Grundregeln zusammen:

1. Bewahren Sie mindestens drei Kopien Ihrer Daten auf. Dadurch wird sichergestellt, dass selbst wenn eine Kopie verloren geht oder beschädigt ist, noch mindestens zwei Kopien vorhanden sind, auf die Sie zurückfallen können.
2. Speichern Sie zwei Sicherungskopien auf verschiedenen Speichermedien oder Geräten. Durch die Diversifizierung von Storage-Medien werden Geräte- oder medienspezifische Ausfälle geschützt. Wenn ein Gerät beschädigt wird oder ein Medientyp ausfällt, bleibt die andere Sicherungskopie davon unberührt.
3. Außerdem muss mindestens eine Backup-Kopie extern aufbewahrt werden. Externer Storage dient als ausfallsicher bei lokalen Katastrophen wie Bränden oder Überschwemmungen, bei denen Kopien vor Ort nicht mehr verwendet werden können.

Dieses Lösungsdokument umfasst eine 3-2-1-1-Backup-Lösung mit dem SnapCenter Plug-in für VMware vSphere (SCV) zur Erstellung primärer und sekundärer Backups unserer lokalen Virtual Machines sowie BlueXP Backup und Recovery für Virtual Machines, um eine Kopie unserer Daten im Cloud Storage oder StorageGRID zu sichern.

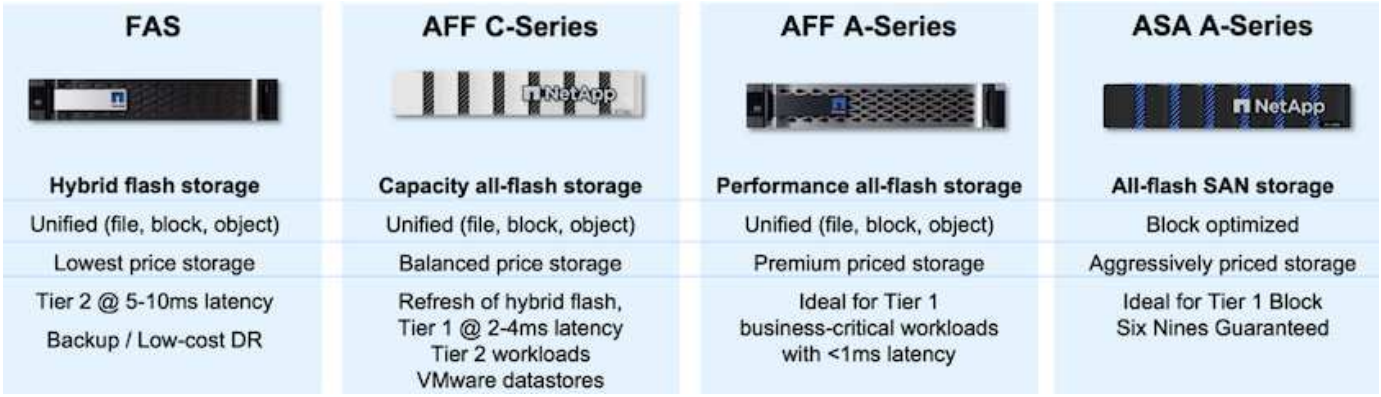
Anwendungsfälle

Diese Lösung eignet sich für folgende Anwendungsfälle:

- Backup und Restore von lokalen Virtual Machines und Datastores mit dem SnapCenter Plug-in für VMware vSphere
- Backup und Restore von lokalen Virtual Machines und Datastores, die auf ONTAP Clustern gehostet und mit BlueXP Backup und Recovery für Virtual Machines in Objekt-Storage gesichert werden.

NetApp ONTAP Datenspeicher

ONTAP ist die branchenführende Storage-Lösung von NetApp mit Unified Storage, auch wenn der Zugriff über SAN- oder NAS-Protokolle erfolgt. Die 3-2-1-1-Backup-Strategie stellt sicher, dass lokale Daten auf mehr als einem Medientyp geschützt sind. NetApp bietet Plattformen von Hochgeschwindigkeits-Flash bis hin zu kostengünstigeren Medien.



Weitere Informationen zu allen Hardware-Plattformen von NetApp finden Sie im Checkout "NetApp Datenspeicher".

SnapCenter Plug-in für VMware vSphere

Das SnapCenter Plug-in für VMware vSphere ist ein Datensicherangebot, das eng in VMware vSphere integriert ist und das ein einfaches Management von Backup und Restore für Virtual Machines ermöglicht. Als Teil dieser Lösung bietet SnapMirror eine schnelle und zuverlässige Methode zur Erstellung einer zweiten unveränderlichen Backup-Kopie der Daten von Virtual Machines auf einem sekundären ONTAP Storage Cluster. Dank dieser Architektur können Wiederherstellungen für Virtual Machines problemlos von primären oder sekundären Backup-Standorten aus initiiert werden.

SCV wird als virtuelle linux-Appliance mit einer OVA-Datei bereitgestellt. Das Plug-in verwendet jetzt ein Remote-Plug-in
Der NetApp Architektur sind. Das Remote-Plug-in läuft außerhalb des vCenter-Servers und wird auf der virtuellen SCV-Appliance gehostet.

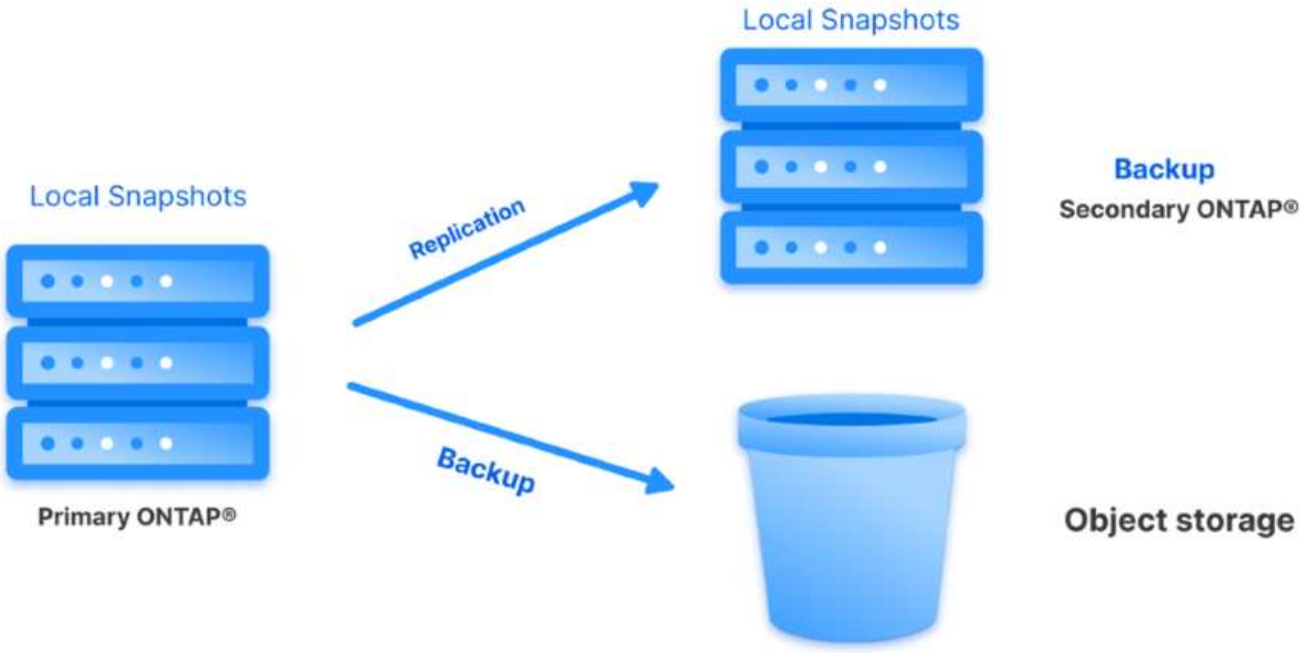
Ausführliche Informationen zu SCV finden Sie unter "Dokumentation zum SnapCenter Plug-in für VMware vSphere".

BlueXP Backup und Recovery für Virtual Machines

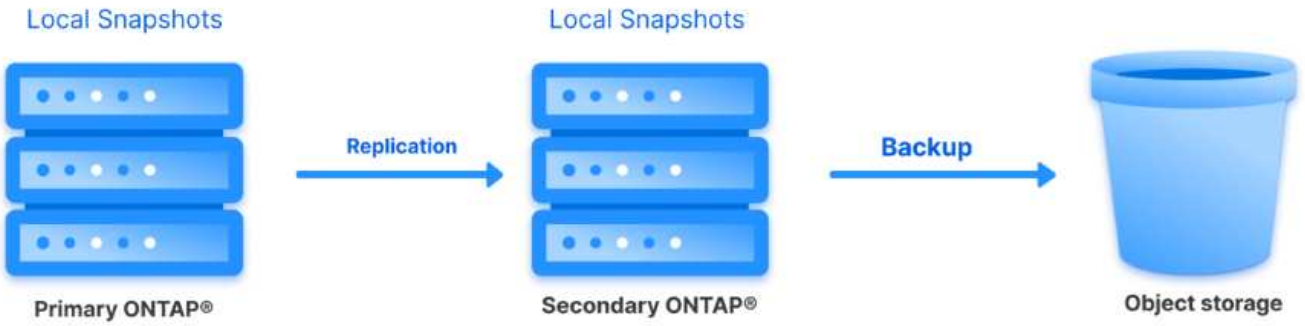
BlueXP Backup und Recovery ist ein Cloud-basiertes Tool für das Datenmanagement. Es bietet eine zentrale Managementoberfläche für eine Vielzahl von Backup- und Recovery-Vorgängen sowohl in On-Premises- als auch in Cloud-Umgebungen. Ein Bestandteil der NetApp BlueXP Backup und Recovery Suite ist eine Funktion, die in das SnapCenter Plug-in für VMware vSphere (lokal) integriert werden kann, um eine Kopie der Daten auf den Objekt-Storage in der Cloud zu erweitern. Auf diese Weise wird eine dritte Kopie der Daten an einem externen Standort erstellt, die aus den primären oder sekundären Storage-Backups stammt. Mit BlueXP Backup und Recovery lassen sich Storage-Richtlinien zur Übertragung von Datenkopien von beiden lokalen Standorten ganz einfach festlegen.

Wenn Sie sich für die primären und sekundären Backups als Quelle in BlueXP Backup und Recovery entscheiden, werden Sie eines von zwei Topologien implementieren:

Fan-out-Topologie – Wenn ein Backup vom SnapCenter-Plugin für VMware vSphere initiiert wird, wird sofort ein lokaler Snapshot erstellt. SCV initiiert dann einen SnapMirror-Vorgang, der den letzten Snapshot auf den sekundären ONTAP-Cluster repliziert. In BlueXP Backup und Recovery gibt eine Richtlinie das primäre ONTAP-Cluster als Quelle für eine Snapshot Kopie der Daten an einen Objektspeicher Ihres gewünschten Cloud-Providers an.



Kaskadierung der Topologie – die Erstellung der primären und sekundären Datenkopien mittels SCV ist identisch mit der oben genannten Fan-out-Topologie. Diesmal wird jedoch in BlueXP Backup und Recovery eine Richtlinie erstellt, die angibt, dass das Backup in Objektspeicher vom sekundären ONTAP-Cluster stammen soll.



Mit BlueXP Backup und Recovery können Backup-Kopien von lokalen ONTAP Snapshots in AWS Glacier, Azure Blob und GCP Archiv-Storage erstellt werden.

AWS Glacier and Deep Glacier

Azure Blob Archive

GCP Archive Storage

Außerdem kann NetApp StorageGRID als Objekt-Storage-Backup-Ziel verwendet werden. Weitere Informationen zu StorageGRID finden Sie im "StorageGRID Landing Page".

Übersicht Zur Lösungsimplementierung

Diese Liste enthält die allgemeinen Schritte, die erforderlich sind, um diese Lösung zu konfigurieren und Backup- und Restore-Vorgänge von SCV und BlueXP Backup- und Recovery-Vorgängen auszuführen:

1. Konfiguration der SnapMirror Beziehung zwischen den ONTAP Clustern, die für primäre und sekundäre Datenkopien verwendet werden soll
2. Konfigurieren Sie das SnapCenter-Plug-in für VMware vSphere.
   a. Fügen Sie Storage-Systeme Hinzu
   b. Backup-Richtlinien erstellen
   c. Erstellen von Ressourcengruppen
   d. Führen Sie die ersten Backup-Jobs aus
3. Konfigurieren Sie BlueXP Backup und Recovery für Virtual Machines
   a. Arbeitsumgebung hinzufügen
   b. Erkennen von SCV- und vCenter-Appliances
   c. Backup-Richtlinien erstellen
   d. Aktivieren Sie Backups
4. Stellen Sie virtuelle Maschinen aus dem primären und sekundären Speicher mithilfe von SCV wieder her.
5. Wiederherstellung von Virtual Machines aus Objekt-Storage mithilfe von BlueXP Backup und Restore

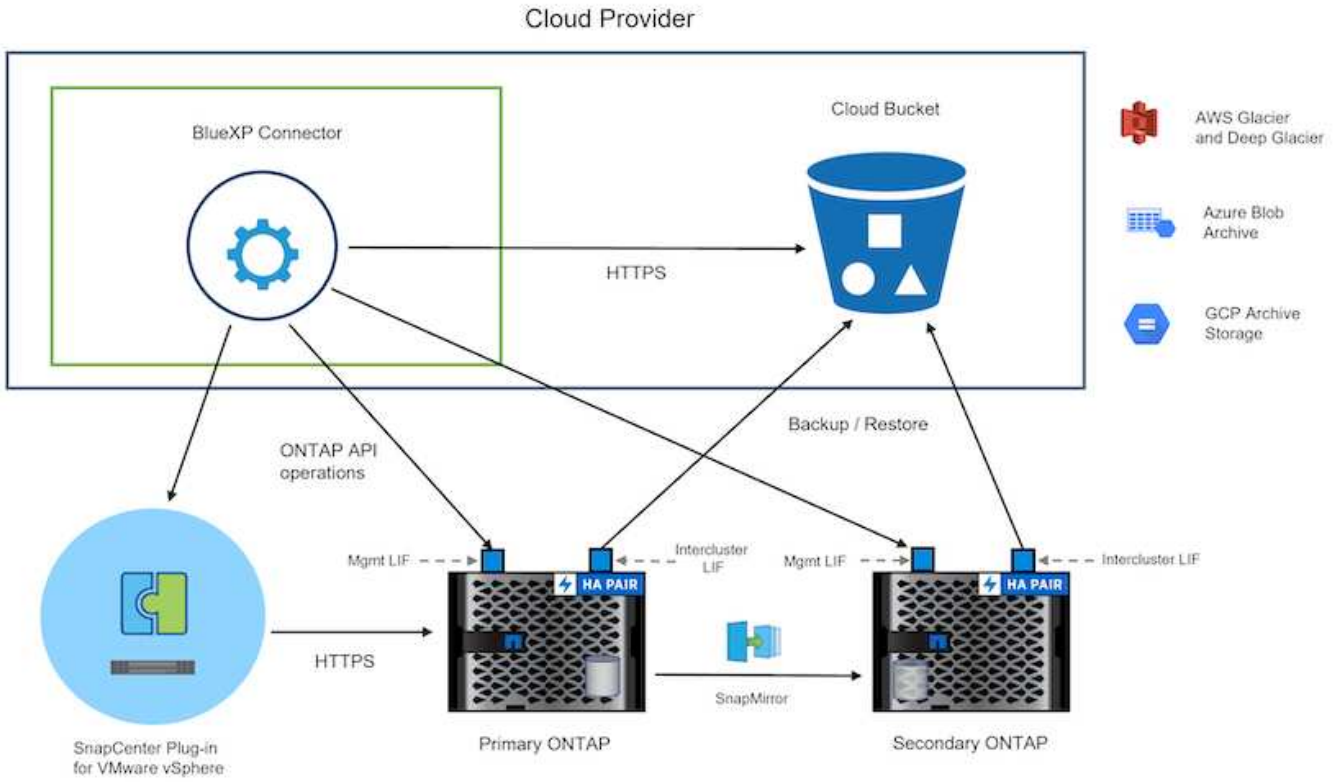
Voraussetzungen

Mit dieser Lösung soll die Datensicherung von Virtual Machines demonstriert werden, die in VMware vSphere ausgeführt werden und sich in NFS-Datenspeichern befinden, die von NetApp ONTAP gehostet werden. Bei dieser Lösung wird vorausgesetzt, dass die folgenden Komponenten konfiguriert und einsatzbereit sind:

1. ONTAP Storage-Cluster mit NFS- oder VMFS-Datenspeichern, die mit VMware vSphere verbunden sind. Sowohl NFS- als auch VMFS-Datastores werden unterstützt. Für diese Lösung wurden NFS-Datenspeicher verwendet.
2. Sekundärer ONTAP Storage-Cluster mit SnapMirror Beziehungen, die für Volumes erstellt werden, die für NFS-Datastores verwendet werden.
3. Für Objekt-Storage-Backups installierter BlueXP Connector beim Cloud-Provider
4. Zu sichernde Virtual Machines befinden sich in NFS-Datenspeichern auf dem primären ONTAP-Storage-Cluster.
5. Netzwerkkonnektivität zwischen dem BlueXP Connector und den lokalen ONTAP Storage-Cluster-Managementschnittstellen
6. Netzwerkverbindung zwischen dem BlueXP Connector und der lokalen SCV Appliance VM und zwischen dem BlueXP Konnektor und vCenter.
7. Netzwerkverbindung zwischen den lokalen ONTAP Intercluster LIFs und dem Objekt-Storage-Service
8. Für Management-SVM auf primären und sekundären ONTAP Storage-Clustern konfigurierter DNS Weitere Informationen finden Sie unter "Konfigurieren Sie DNS für die Auflösung des Host-Namens".

Übergeordnete Architektur

Die Test-/Validierung dieser Lösung wurde in einem Labor durchgeführt, das in der endgültigen Implementierungsumgebung eventuell nicht übereinstimmt.



Lösungsimplementierung

In dieser Lösung stellen wir detaillierte Anweisungen für die Implementierung und Validierung einer Lösung bereit, die das SnapCenter Plug-in für VMware vSphere zusammen mit Backup und Recovery von BlueXP nutzt. Damit können Backup und Recovery von Windows und Linux Virtual Machines innerhalb eines VMware vSphere Clusters in einem lokalen Datacenter durchgeführt werden. Die Virtual Machines in diesem Setup werden auf NFS-Datenspeichern gespeichert, die von einem ONTAP A300 Storage-Cluster gehostet werden. Darüber hinaus dient ein separates ONTAP A300 Storage-Cluster als sekundäres Ziel für mit SnapMirror replizierte Volumes. Darüber hinaus wurde Objekt-Storage, der auf Amazon Web Services und Azure Blob gehostet wird, als Ziele für eine dritte Kopie der Daten genutzt.

Wir werden über die Erstellung von SnapMirror Beziehungen für sekundäre Kopien unserer durch SCV gemanagten Backups und die Konfiguration von Backup-Jobs in SCV und BlueXP Backup und Recovery hinweggehen.

Detaillierte Informationen zum SnapCenter-Plug-in für VMware vSphere finden Sie im "Dokumentation zum SnapCenter Plug-in für VMware vSphere".

Detaillierte Informationen zu Backup und Recovery von BlueXP finden Sie im "BlueXP Backup- und Recovery-Dokumentation".

Einrichten von SnapMirror Beziehungen zwischen ONTAP Clustern

Das SnapCenter Plug-in für VMware vSphere nutzt ONTAP SnapMirror Technologie zum Management des Transports von sekundären SnapMirror bzw. SnapVault Kopien zu einem sekundären ONTAP Cluster.

SCV Backup-Richtlinien haben die Möglichkeit, SnapMirror oder SnapVault Beziehungen zu verwenden. Der Hauptunterschied liegt darin, dass der für Backups in der Richtlinie konfigurierte Aufbewahrungszeitplan am primären und sekundären Standort identisch ist. SnapVault wurde für die Archivierung entwickelt. Bei Verwendung dieser Option kann mit der SnapMirror Beziehung ein separater Aufbewahrungszeitplan für die

Snapshot-Kopien auf dem sekundären ONTAP Storage-Cluster aufgestellt werden.

Sie können SnapMirror Beziehungen in BlueXP einrichten, wo viele der Schritte automatisiert sind oder dies mit System Manager und der ONTAP CLI möglich ist. Alle diese Methoden werden im Folgenden erläutert.

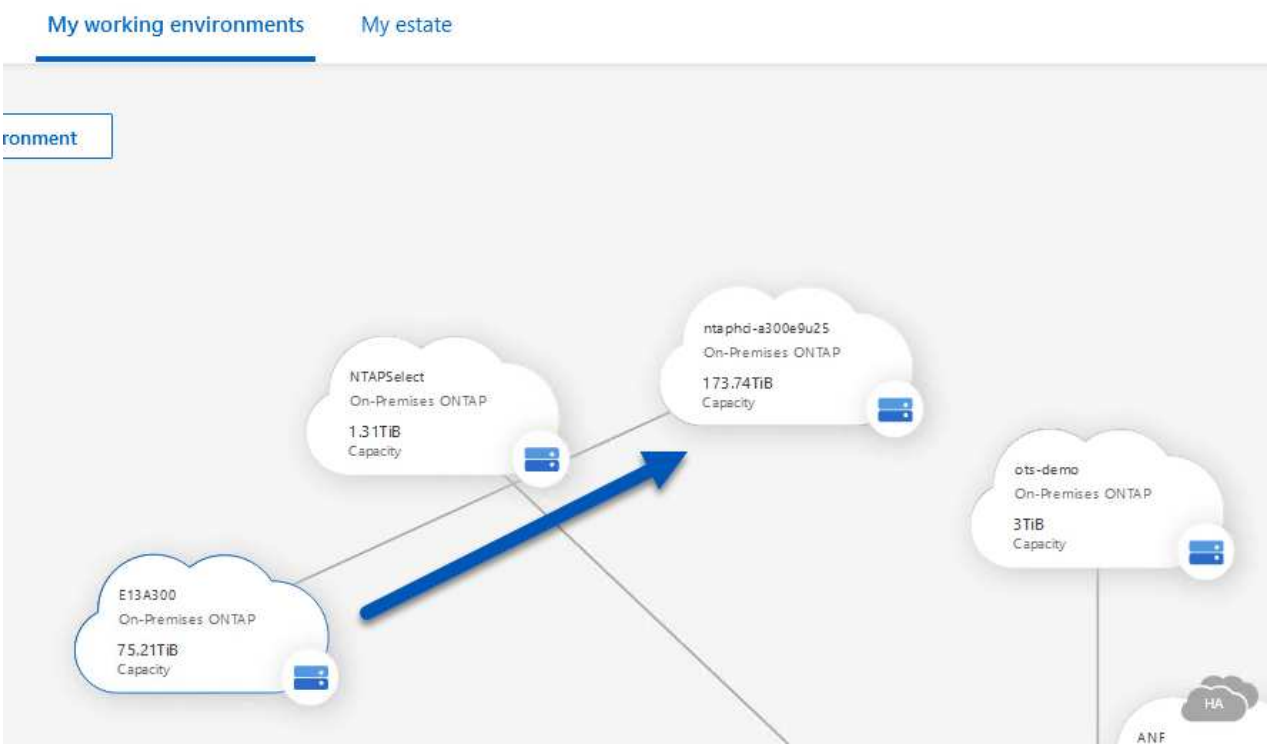
SnapMirror Beziehungen mit BlueXP aufbauen

Folgende Schritte müssen über die BlueXP Webkonsole durchgeführt werden:

Einrichtung der Replizierung für primäre und sekundäre ONTAP Storage-Systeme

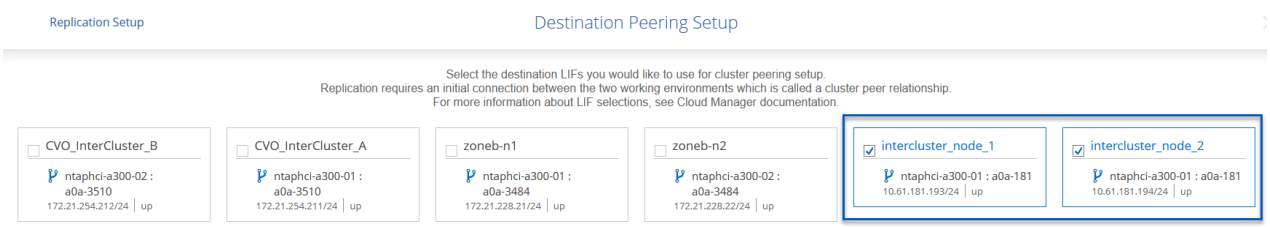
Melden Sie sich zunächst bei der BlueXP Webkonsole an und navigieren Sie zu den Leinwand.

1. Ziehen Sie das (primäre) ONTAP Quell-Storage-System per Drag & Drop auf das (sekundäre) ONTAP Ziel-Storage-System.

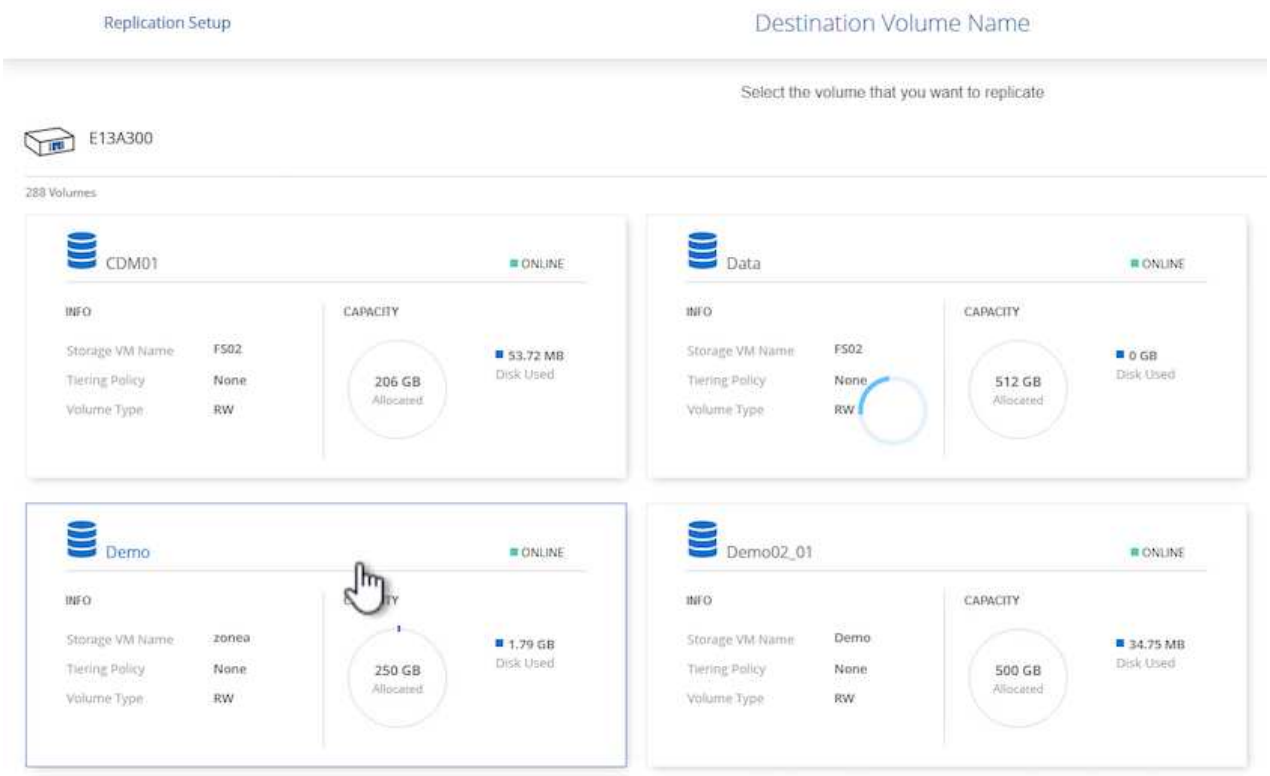


2. Wählen Sie aus dem angezeigten Menü **Replikation**.

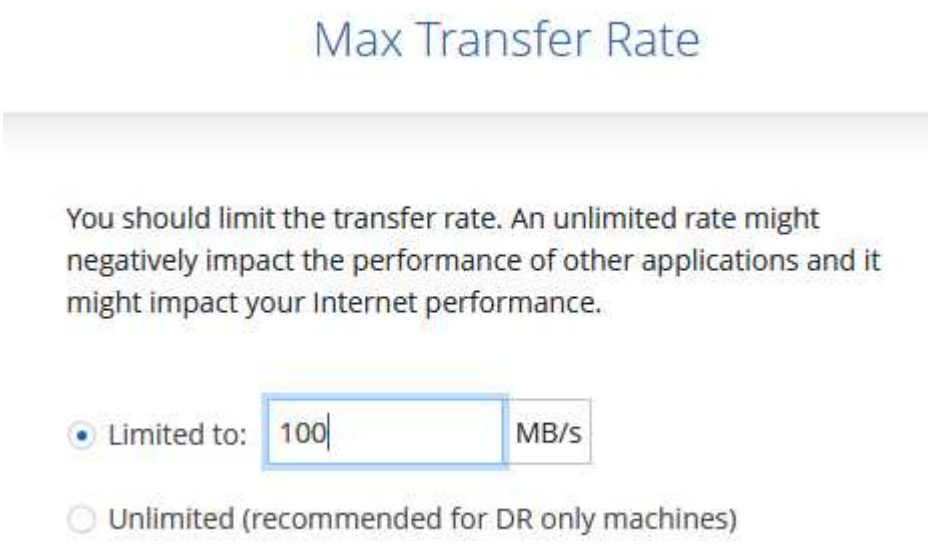
3. Wählen Sie auf der Seite **Destination Peering Setup** die Ziel-Intercluster-LIFs aus, die für die Verbindung zwischen Speichersystemen verwendet werden sollen.



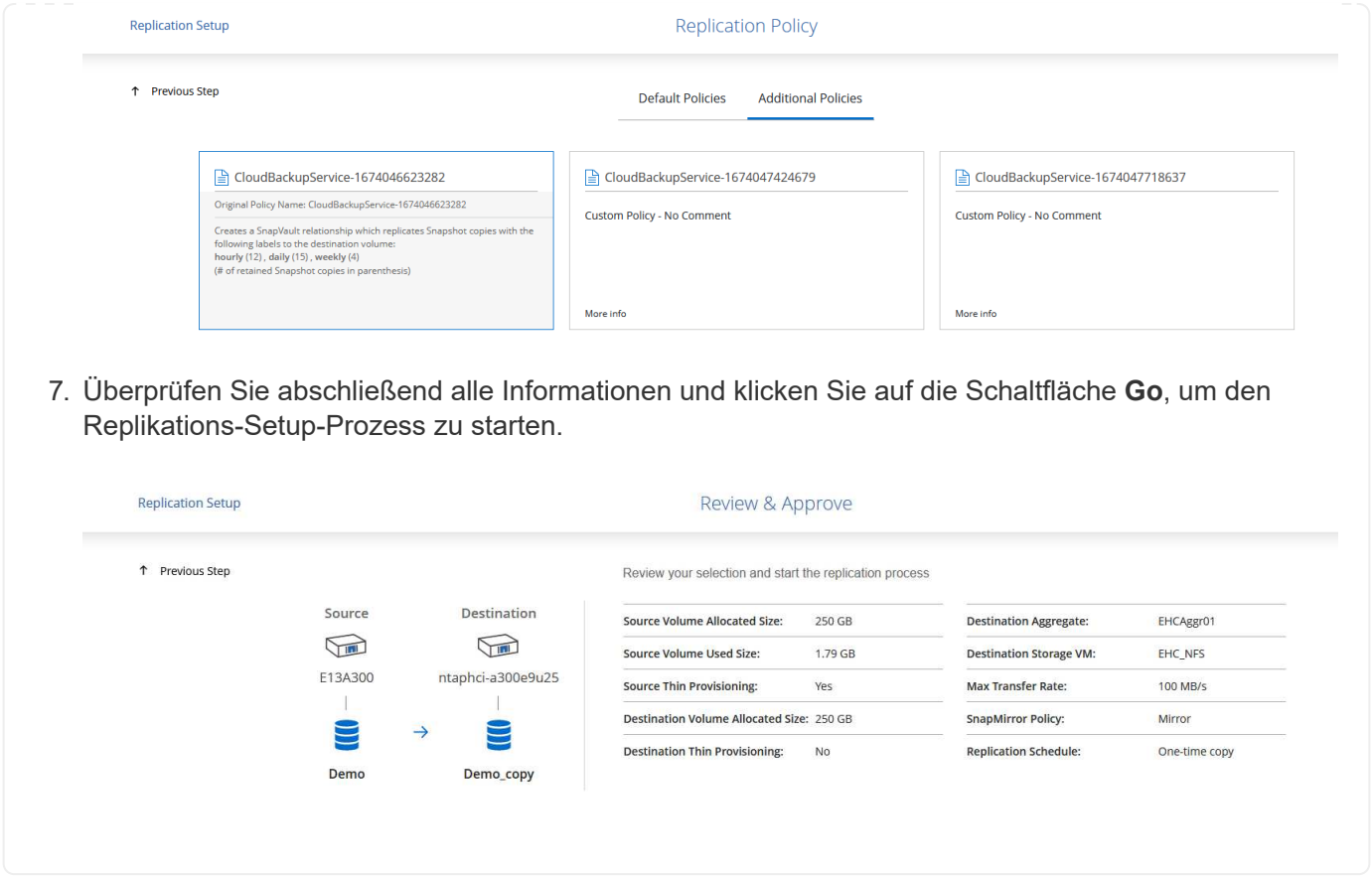
4. Wählen Sie auf der Seite **Destination Volume Name** zunächst das Quell-Volume aus, füllen Sie dann den Namen des Ziel-Volumes aus und wählen Sie die Ziel-SVM und das Aggregat aus. Klicken Sie auf **Weiter**, um fortzufahren.



5. Wählen Sie die maximale Übertragungsrate für die Replikation aus.



6. Wählen Sie die Richtlinie aus, die den Aufbewahrungsplan für sekundäre Backups bestimmt. Diese Policy kann im Vorfeld erstellt werden (siehe den manuellen Prozess unten im Schritt **Create a Snapshot Retention Policy**) oder nach Bedarf geändert werden.



7. Überprüfen Sie abschließend alle Informationen und klicken Sie auf die Schaltfläche **Go**, um den Replikations-Setup-Prozess zu starten.

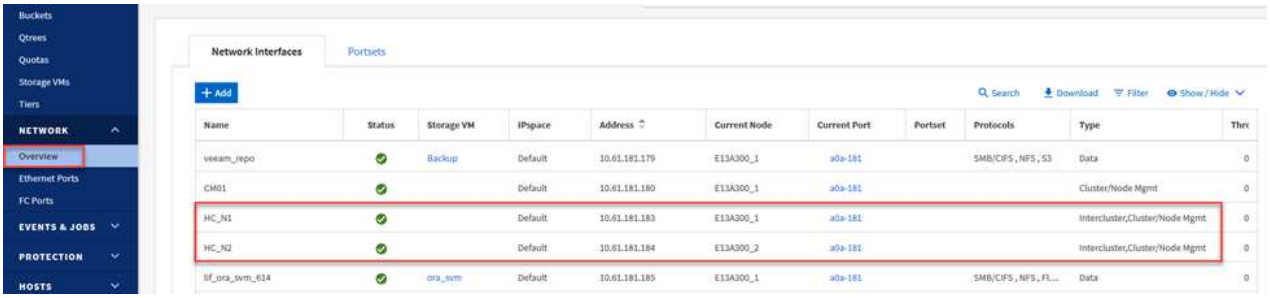
Einrichten von SnapMirror Beziehungen mit System Manager und ONTAP CLI

Alle erforderlichen Schritte zum Aufbau von SnapMirror Beziehungen können mit System Manager oder der ONTAP CLI durchgeführt werden. Im folgenden Abschnitt finden Sie detaillierte Informationen zu beiden Methoden:

Zeichnen Sie die logischen Schnittstellen von Intercluster und Ziel auf

Sie können die logischen Inter-Cluster-Informationen für die ONTAP Quell- und Ziel-Cluster aus System Manager oder aus der CLI abrufen.

1. Wechseln Sie in ONTAP System Manager zur Seite „Netzwerkübersicht“ und rufen Sie die IP-Adressen des Typs „Intercluster“ ab, die für die Kommunikation mit der AWS VPC konfiguriert sind, bei der FSX installiert ist.



2. Um die Intercluster-IP-Adressen über die CLI abzurufen, führen Sie den folgenden Befehl aus:

```
ONTAP-Dest::> network interface show -role intercluster
```

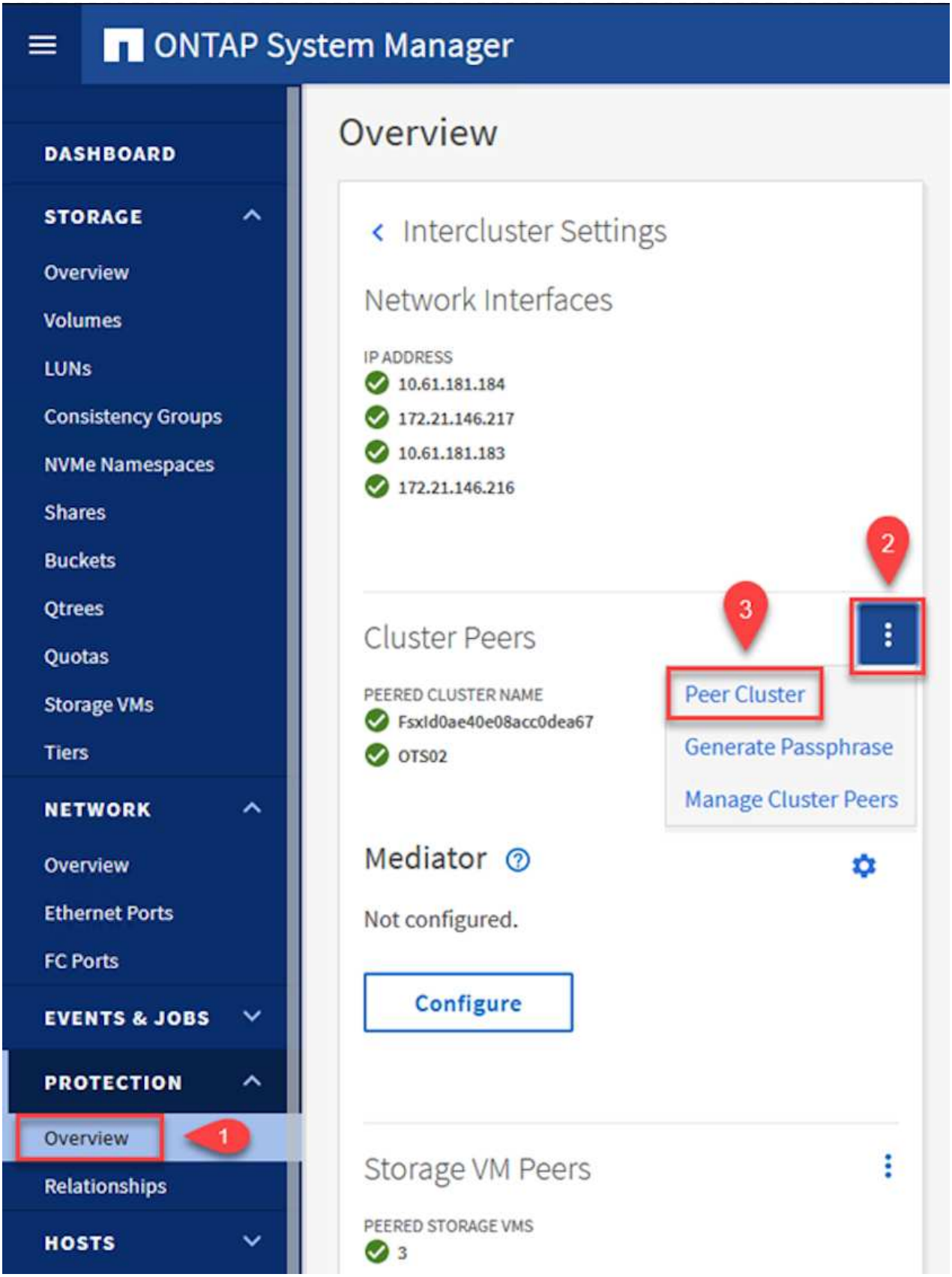
Cluster-Peering zwischen ONTAP Clustern einrichten

Zum Erstellen von Cluster-Peering zwischen ONTAP Clustern muss im anderen Peer-Cluster eine eindeutige Passphrase bestätigt werden, die beim Initiierung des ONTAP-Clusters eingegeben wurde.

1. Richten Sie Peering auf dem Ziel-ONTAP-Cluster mit ein `cluster peer create` Befehl. Wenn Sie dazu aufgefordert werden, geben Sie eine eindeutige Passphrase ein, die später im Quellcluster verwendet wird, um den Erstellungsprozess abzuschließen.

```
ONTAP-Dest::> cluster peer create -address-family ipv4 -peer-addrs
source_intercluster_1, source_intercluster_2
Enter the passphrase:
Confirm the passphrase:
```

2. Im Quell-Cluster können Sie die Cluster-Peer-Beziehung entweder mit ONTAP System Manager oder der CLI einrichten. Navigieren Sie im ONTAP System Manager zu Schutz > Übersicht, und wählen Sie Peer Cluster aus.

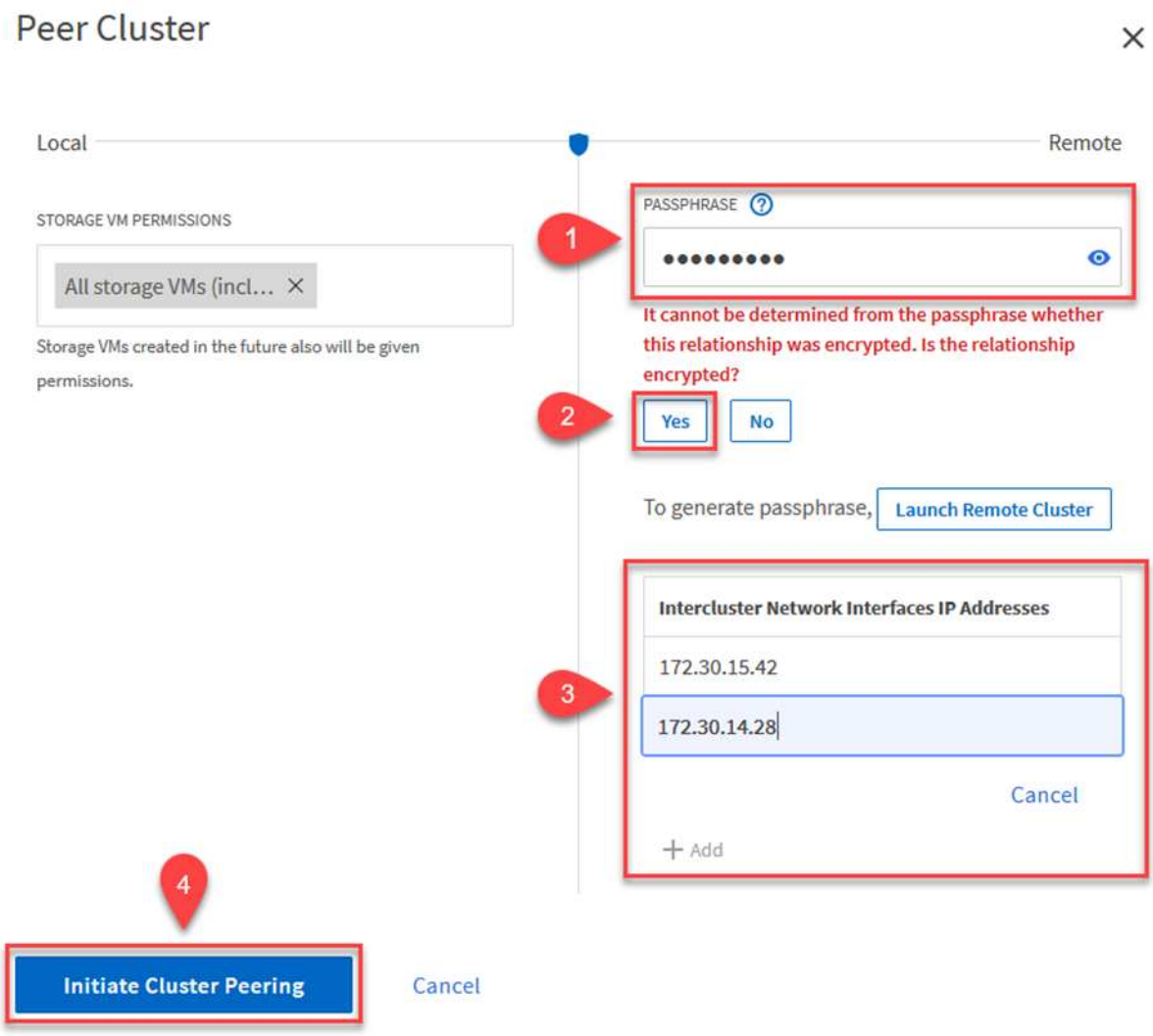


3. Füllen Sie im Dialogfeld Peer Cluster die erforderlichen Informationen aus:
   a. Geben Sie die Passphrase ein, um die Peer-Cluster-Beziehung auf dem Ziel-ONTAP-Cluster herzustellen.

b. Wählen Sie `Yes` Um eine verschlüsselte Beziehung aufzubauen.

c. Geben Sie die Intercluster LIF IP-Adresse(n) des ONTAP Ziel-Clusters ein.

d. Klicken Sie auf Cluster Peering initiieren, um den Prozess abzuschließen.



4. Überprüfen Sie mit dem folgenden Befehl den Status der Cluster-Peer-Beziehung vom ONTAP-Zielcluster:

```
ONTAP-Dest::> cluster peer show
```

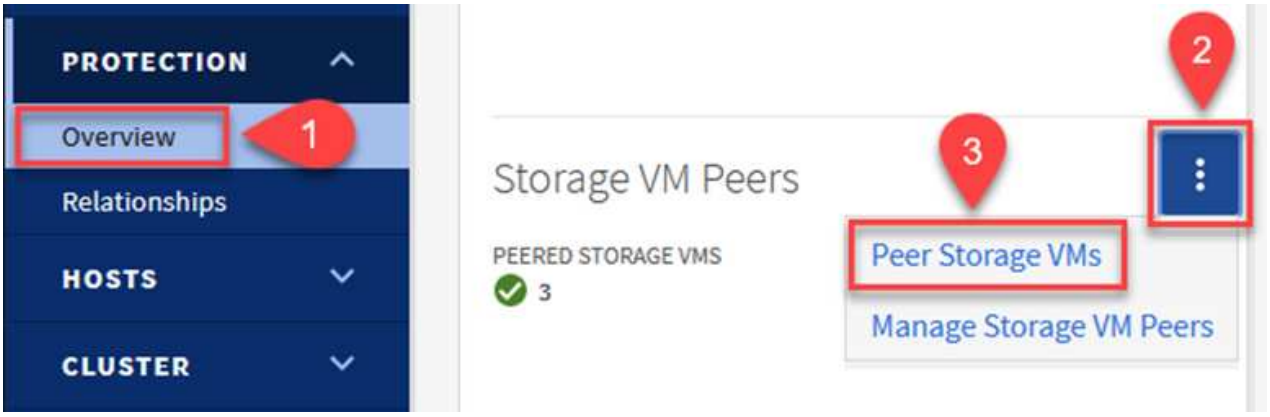
SVM-Peering-Beziehung einrichten

Im nächsten Schritt werden eine SVM-Beziehung zwischen den Ziel- und Quell-Storage Virtual Machines eingerichtet, die die Volumes enthalten, die sich in den SnapMirror Beziehungen befinden.

1. Verwenden Sie aus dem ONTAP-Zielcluster den folgenden Befehl in der CLI, um die SVM-Peer-Beziehung zu erstellen:

```
ONTAP-Dest::> vserver peer create -vserver DestSVM -peer-vserver
Backup -peer-cluster OnPremSourceSVM -applications snapmirror
```

2. Akzeptieren Sie vom ONTAP-Quellcluster die Peering-Beziehung entweder mit dem ONTAP System Manager oder der CLI.
3. Wählen Sie im ONTAP System Manager unter „Protection > Overview“ die Option „Peer Storage VMs“ unter „Storage VM Peers“ aus.



4. Füllen Sie im Dialogfeld Peer Storage VM die erforderlichen Felder aus:
   - Der Quell-Storage-VM
   - Dem Ziel-Cluster
   - Der Ziel-Storage-VM

5. Klicken Sie auf Peer Storage VMs, um den SVM-Peering-Prozess abzuschließen.

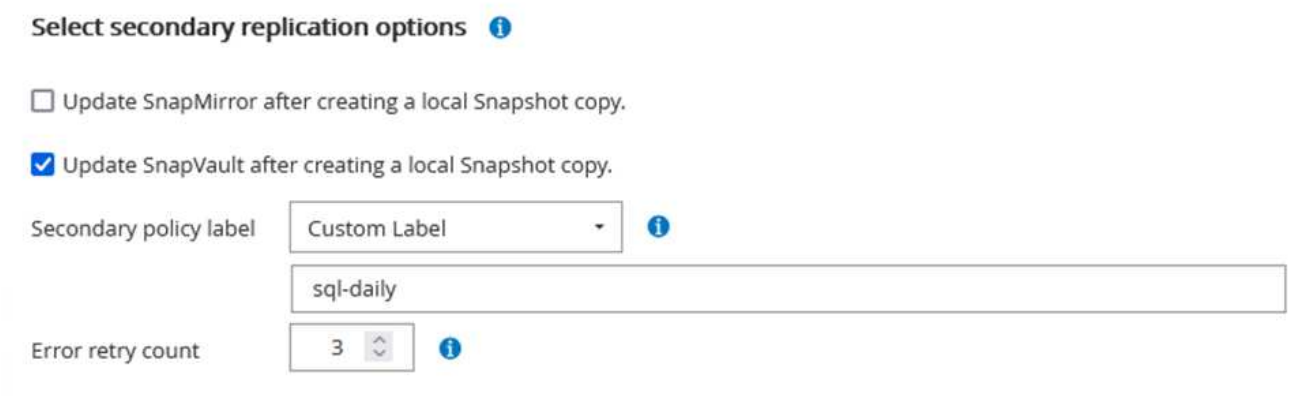
Erstellen einer Snapshot Aufbewahrungsrichtlinie

SnapCenter managt Aufbewahrungszeitpläne für Backups, die als Snapshot Kopien auf dem primären Storage-System existieren. Dies wird beim Erstellen einer Richtlinie in SnapCenter festgelegt. SnapCenter managt keine Aufbewahrungsrichtlinien für Backups, die in sekundären Storage-Systemen aufbewahrt werden. Diese Richtlinien werden separat durch eine SnapMirror Richtlinie gemanagt, die auf dem sekundären FSX-Cluster erstellt wurde und mit den Ziel-Volumes in einer SnapMirror Beziehung zum Quell-Volume verknüpft ist.

Beim Erstellen einer SnapCenter-Richtlinie haben Sie die Möglichkeit, ein sekundäres Richtlinienetikett anzugeben, das der SnapMirror-Kennzeichnung von jedem Snapshot hinzugefügt wird, der beim Erstellen eines SnapCenter-Backups generiert wird.

> Auf dem sekundären Storage werden diese Kennungen mit Richtliniensegeln abgeglichen, die mit dem Ziel-Volume verbunden sind, um die Aufbewahrung von Snapshots zu erzwingen.

Das folgende Beispiel zeigt ein SnapMirror-Etikett, das an allen Snapshots vorhanden ist, die im Rahmen einer Richtlinie erzeugt wurden, die für die täglichen Backups unserer SQL Server-Datenbank und der Protokoll-Volumes verwendet wird.



Weitere Informationen zum Erstellen von SnapCenter-Richtlinien für eine SQL Server-Datenbank finden Sie im "SnapCenter-Dokumentation".

Sie müssen zuerst eine SnapMirror-Richtlinie mit Regeln erstellen, die die Anzahl der beizubehaltenden Snapshot-Kopien vorschreiben.

1. Erstellen Sie die SnapMirror-Richtlinie auf dem FSX-Cluster.

```
ONTAP-Dest::> snapmirror policy create -vserver DestSVM -policy
PolicyName -type mirror-vault -restart always
```

2. Fügen Sie der Richtlinie Regeln mit SnapMirror-Labels hinzu, die zu den in den SnapCenter-Richtlinien angegebenen sekundären Richtlinienbezeichnungen passen.

```
ONTAP-Dest::> snapmirror policy add-rule -vserver DestSVM -policy
PolicyName -snapmirror-label SnapMirrorLabelName -keep
#ofSnapshotsToRetain
```

Das folgende Skript enthält ein Beispiel für eine Regel, die einer Richtlinie hinzugefügt werden kann:

```
ONTAP-Dest::> snapmirror policy add-rule -vserver sql_svm_dest
-policy Async_SnapCenter_SQL -snapmirror-label sql-ondemand -keep 15
```

Erstellen Sie für jedes SnapMirror Label zusätzliche Regeln und die Anzahl der zu behaltenden Snapshots (Aufbewahrungszeitraum).

Erstellung von Ziel-Volumes

Um ein Ziel-Volume auf ONTAP zu erstellen, das der Empfänger von Snapshot-Kopien aus unseren Quell-Volumes sein wird, führen Sie den folgenden Befehl auf dem Ziel-ONTAP-Cluster aus:

```
ONTAP-Dest::> volume create -vserver DestSVM -volume DestVolName
-aggregate DestAggrName -size VolSize -type DP
```

SnapMirror Beziehungen zwischen Quell- und Ziel-Volumes erstellen

Führen Sie den folgenden Befehl auf dem Ziel-ONTAP-Cluster aus, um eine SnapMirror Beziehung zwischen einem Quell- und Ziel-Volume zu erstellen:

```
ONTAP-Dest::> snapmirror create -source-path
OnPremSourceSVM:OnPremSourceVol -destination-path DestSVM:DestVol -type
XDP -policy PolicyName
```

SnapMirror Beziehungen initialisieren

Initialisieren Sie die SnapMirror-Beziehung. Bei diesem Prozess wird ein neuer Snapshot initiiert, der vom Quell-Volume erzeugt wird und in das Ziel-Volume kopiert.

Führen Sie zum Erstellen eines Volumes den folgenden Befehl auf dem ONTAP-Zielcluster aus:

```
ONTAP-Dest::> snapmirror initialize -destination-path DestSVM:DestVol
```

Konfigurieren Sie das SnapCenter-Plug-in für VMware vSphere

Nach der Installation kann das SnapCenter-Plug-in für VMware vSphere über die vCenter Server Appliance Management-Schnittstelle aufgerufen werden. SCV verwaltet Backups für die NFS-Datastores, die auf den ESXi-Hosts gemountet sind und die die Windows- und Linux-VMs enthalten.

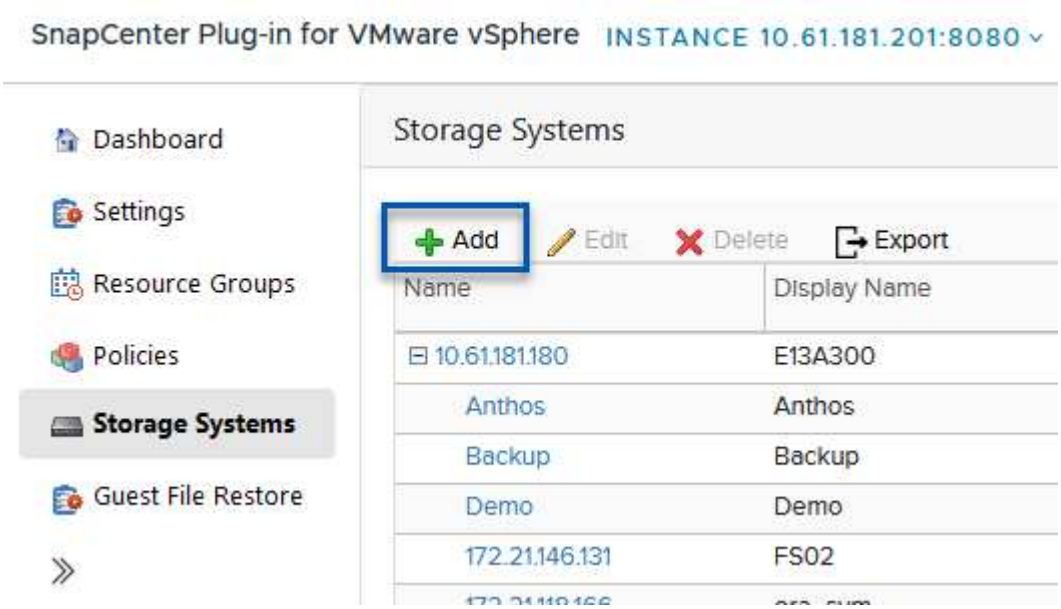
Überprüfen Sie die "Datensicherungs-Workflow" Abschnitt der SCV-Dokumentation enthält weitere Informationen zu den Schritten, die bei der Konfiguration von Backups erforderlich sind.

Um Backups Ihrer virtuellen Maschinen und Datenspeicher zu konfigurieren, müssen die folgenden Schritte über die Plug-in-Schnittstelle durchgeführt werden.

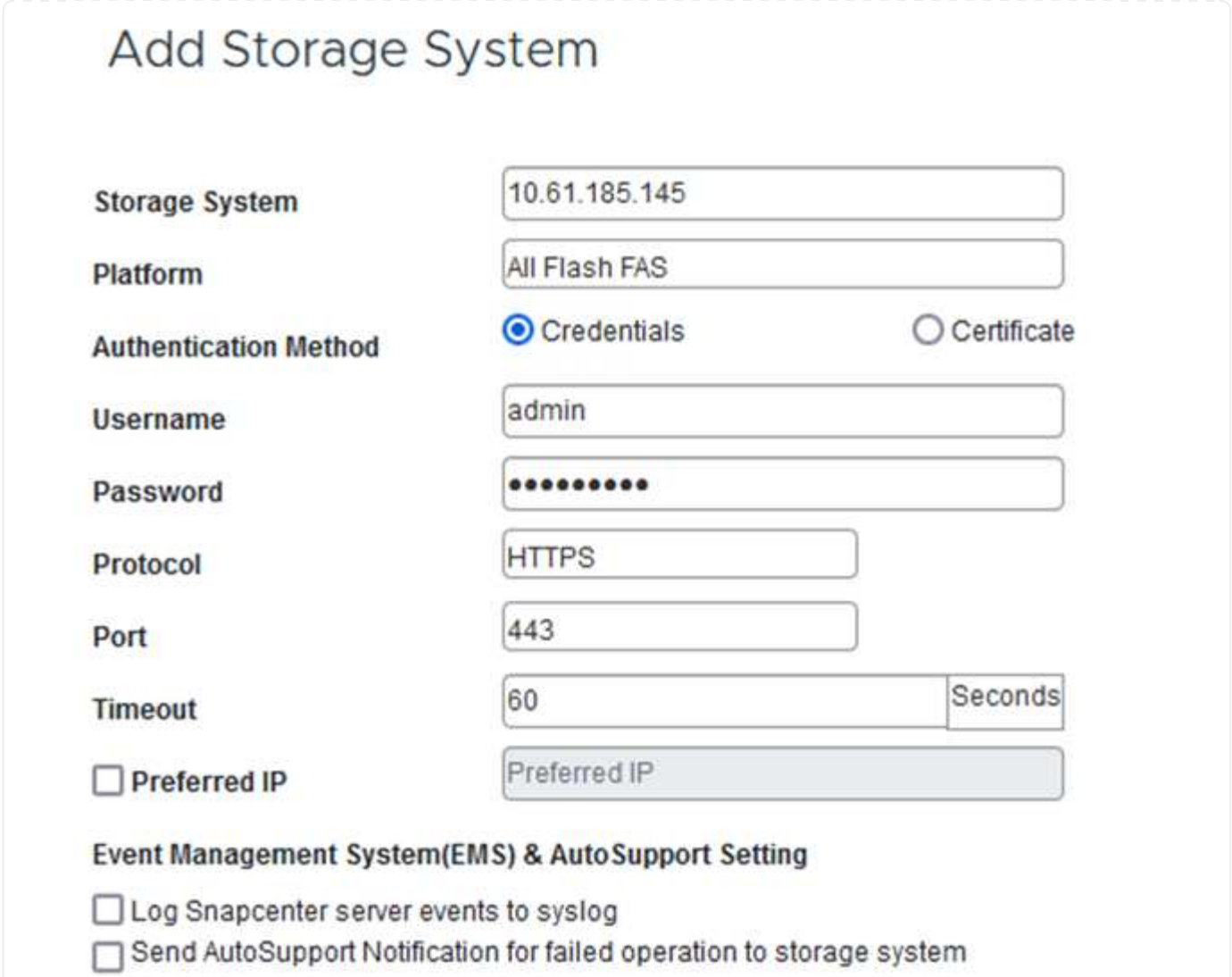
ONTAP Storage-Systeme ermitteln

Die ONTAP Storage-Cluster ermitteln, die für primäre und sekundäre Backups verwendet werden können.

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Speichersysteme** und klicken Sie auf die Schaltfläche **Hinzufügen**.



2. Geben Sie die Zugangsdaten und den Plattformtyp für das primäre ONTAP-Speichersystem ein und klicken Sie auf **Hinzufügen**.



3. Wiederholen Sie diesen Vorgang für das sekundäre ONTAP-Speichersystem.

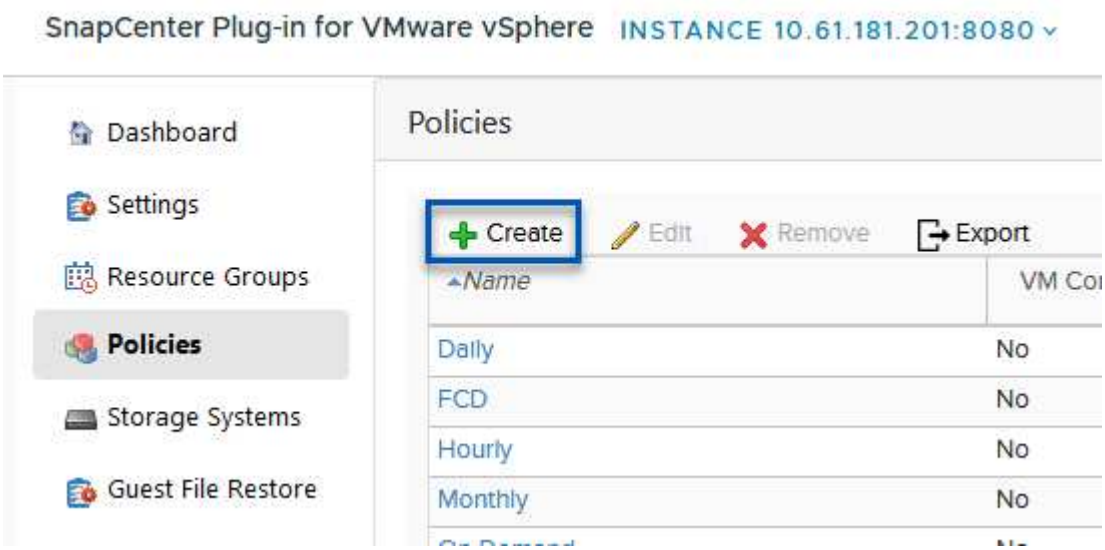
Erstellen Sie SCV-Backup-Richtlinien

Richtlinien legen den Aufbewahrungszeitraum, die Häufigkeit und die Replikationsoptionen für die von SCV verwalteten Backups fest.

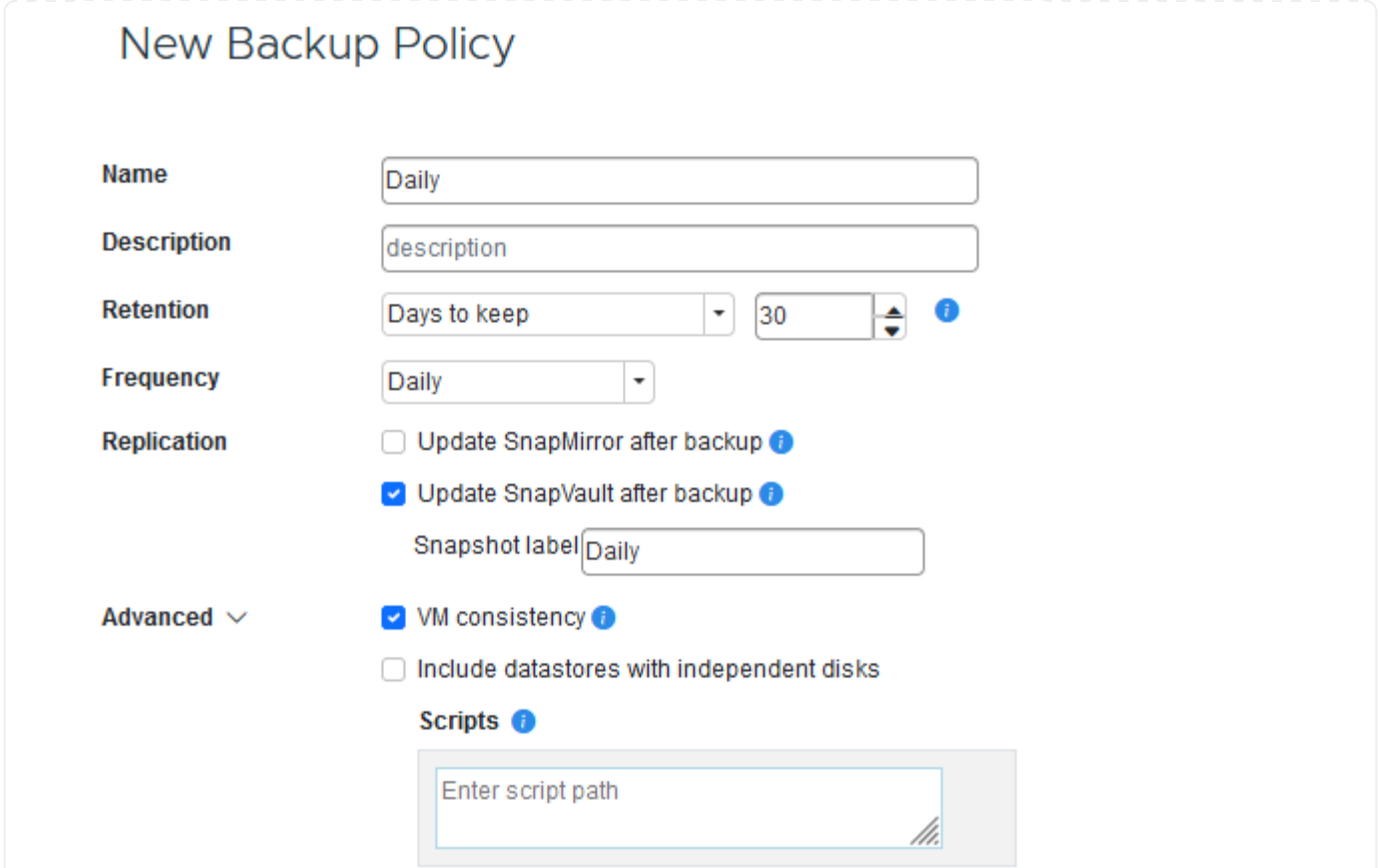
Überprüfen Sie die "Erstellen von Backup-Richtlinien für VMs und Datastores" Weitere Informationen finden Sie in der Dokumentation.

Führen Sie die folgenden Schritte aus, um Backup-Richtlinien zu erstellen:

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Richtlinien** und klicken Sie auf die Schaltfläche **Erstellen**.



2. Geben Sie einen Namen für die Richtlinie, den Aufbewahrungszeitraum, die Häufigkeit und die Replikationsoptionen sowie die Snapshot-Bezeichnung an.



Beim Erstellen einer Richtlinie im SnapCenter-Plug-in werden Optionen für SnapMirror und SnapVault angezeigt. Wenn Sie SnapMirror wählen, ist der in der Richtlinie angegebene Zeitplan für die Aufbewahrung sowohl für die primären als auch für die sekundären Snapshots identisch. Wenn Sie SnapVault wählen, wird der Aufbewahrungszeitplan für den sekundären Snapshot auf einem separaten Zeitplan basieren, der mit der SnapMirror Beziehung implementiert wurde. Dies ist nützlich, wenn Sie längere Aufbewahrungsfristen für sekundäre Backups wünschen.

Snapshot-Labels sind nützlich, da sie verwendet werden können, um Richtlinien mit einem bestimmten Aufbewahrungszeitraum für die SnapVault Kopien, die auf das sekundäre ONTAP Cluster repliziert werden, durchzuführen. Wenn SCV in Verbindung mit BlueXP Backup und Restore verwendet wird, muss das Feld „Snapshot“ entweder leer sein oder match das in der BlueXP Backup-Richtlinie angegebene Label aufweisen.

3. Wiederholen Sie das Verfahren für jede Richtlinie. Zum Beispiel separate Richtlinien für tägliche, wöchentliche und monatliche Backups.

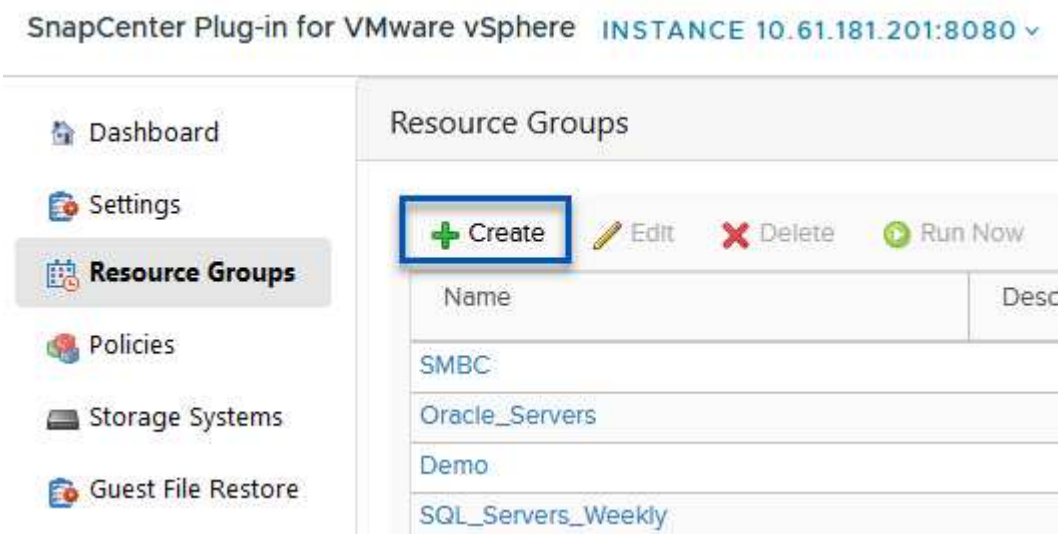
Erstellen von Ressourcengruppen

Ressourcengruppen enthalten die Datastores und virtuellen Maschinen, die in einen Backup-Job aufgenommen werden sollen, sowie die zugehörige Richtlinie und den Backup-Zeitplan.

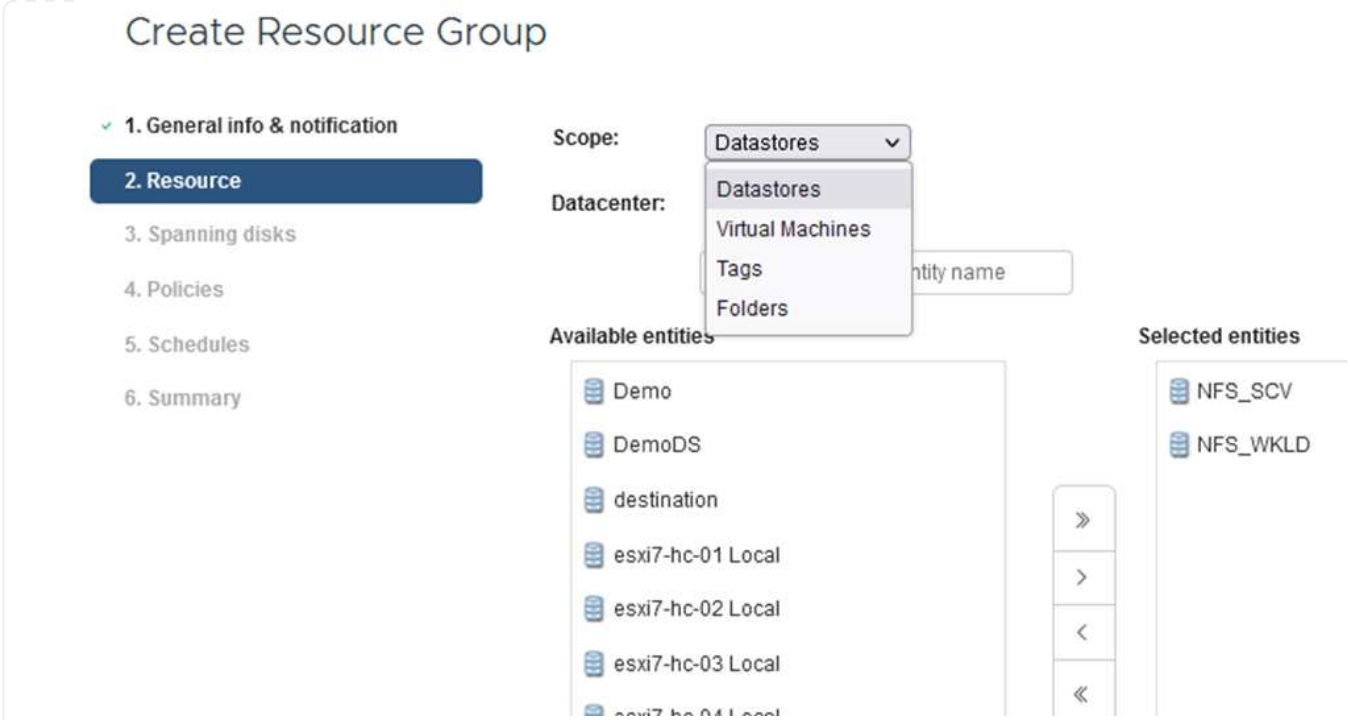
Überprüfen Sie die "Erstellen von Ressourcengruppen" Weitere Informationen finden Sie in der Dokumentation.

Führen Sie die folgenden Schritte aus, um Ressourcengruppen zu erstellen.

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Ressourcengruppen** und klicken Sie auf die Schaltfläche **Erstellen**.

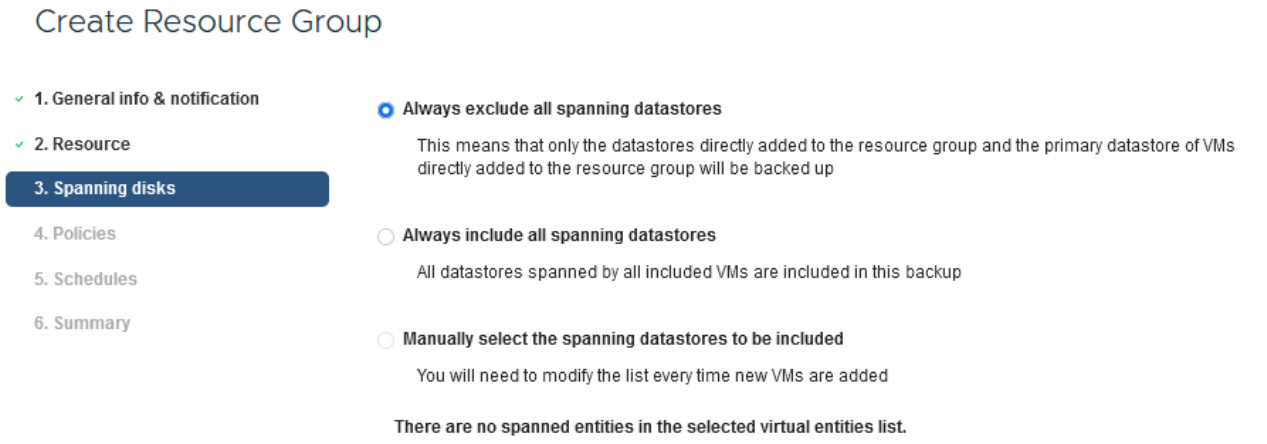


2. Geben Sie im Assistenten Ressourcengruppe erstellen einen Namen und eine Beschreibung für die Gruppe sowie Informationen ein, die für den Empfang von Benachrichtigungen erforderlich sind. Klicken Sie auf **Weiter**
3. Wählen Sie auf der nächsten Seite die Datastores und virtuellen Maschinen aus, die in den Backup-Job aufgenommen werden sollen, und klicken Sie dann auf **Weiter**.



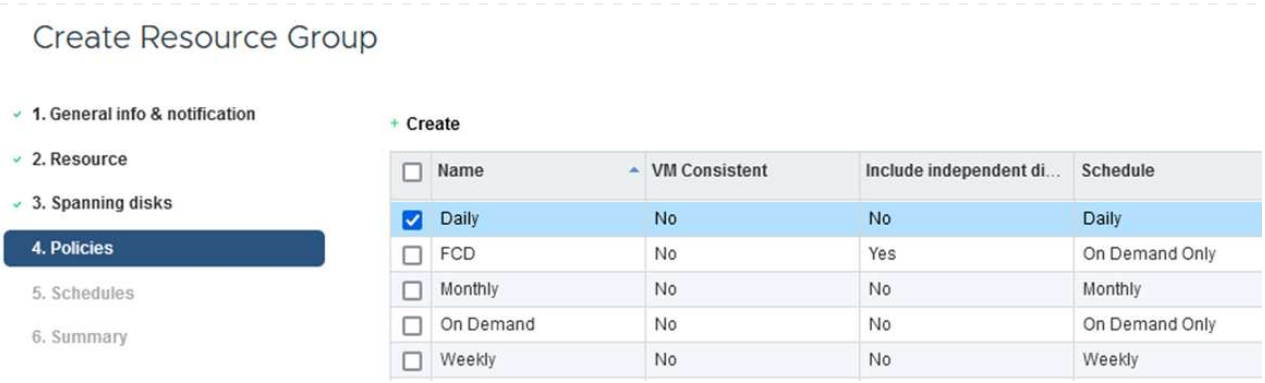
Es besteht die Möglichkeit, spezifische VMs oder vollständige Datastores auszuwählen. Unabhängig davon, welchen Sie wählen, wird das gesamte Volume (und Datastore) gesichert, da der Backup das Ergebnis der Erstellung eines Snapshots des zugrunde liegenden Volumes ist. In den meisten Fällen ist es am einfachsten, den gesamten Datastore auszuwählen. Wenn Sie jedoch beim Wiederherstellen die Liste der verfügbaren VMs begrenzen möchten, können Sie nur eine Teilmenge der VMs für das Backup auswählen.

4. Wählen Sie Optionen für das Spanning von Datastores für VMs mit VMDKs, die sich auf mehreren Datastores befinden, und klicken Sie dann auf **Weiter**.



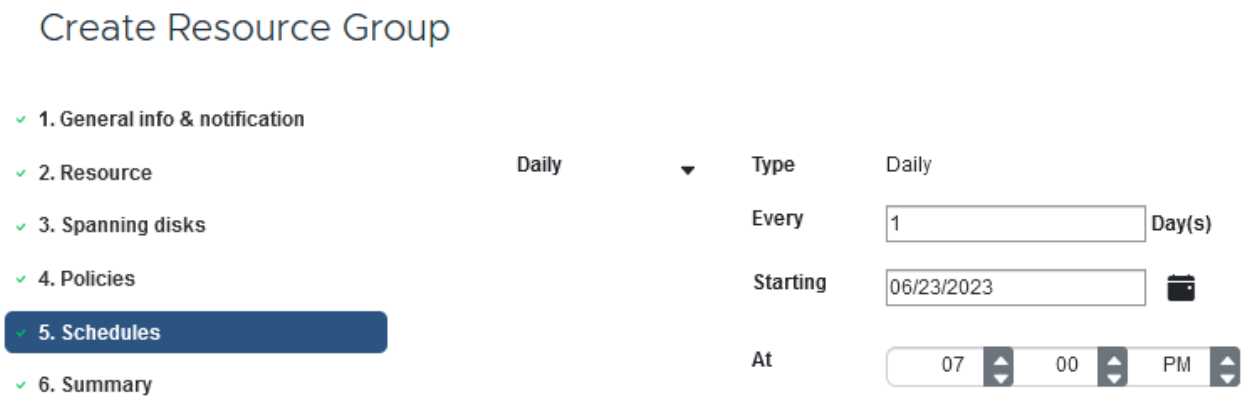
BlueXP Backup und Recovery unterstützt derzeit nicht die Sicherung von VMs mit VMDKs, die mehrere Datastores umfassen.

5. Wählen Sie auf der nächsten Seite die Richtlinien aus, die der Ressourcengruppe zugeordnet werden sollen, und klicken Sie auf **Weiter**.



Beim Backup von über SCV gemanagten Snapshots in Objektspeicher mithilfe von BlueXP Backup und Recovery kann jede Ressourcengruppe nur einer einzigen Richtlinie zugeordnet werden.

6. Wählen Sie einen Zeitplan aus, der bestimmt, zu welchem Zeitpunkt die Backups ausgeführt werden. Klicken Sie auf **Weiter**.

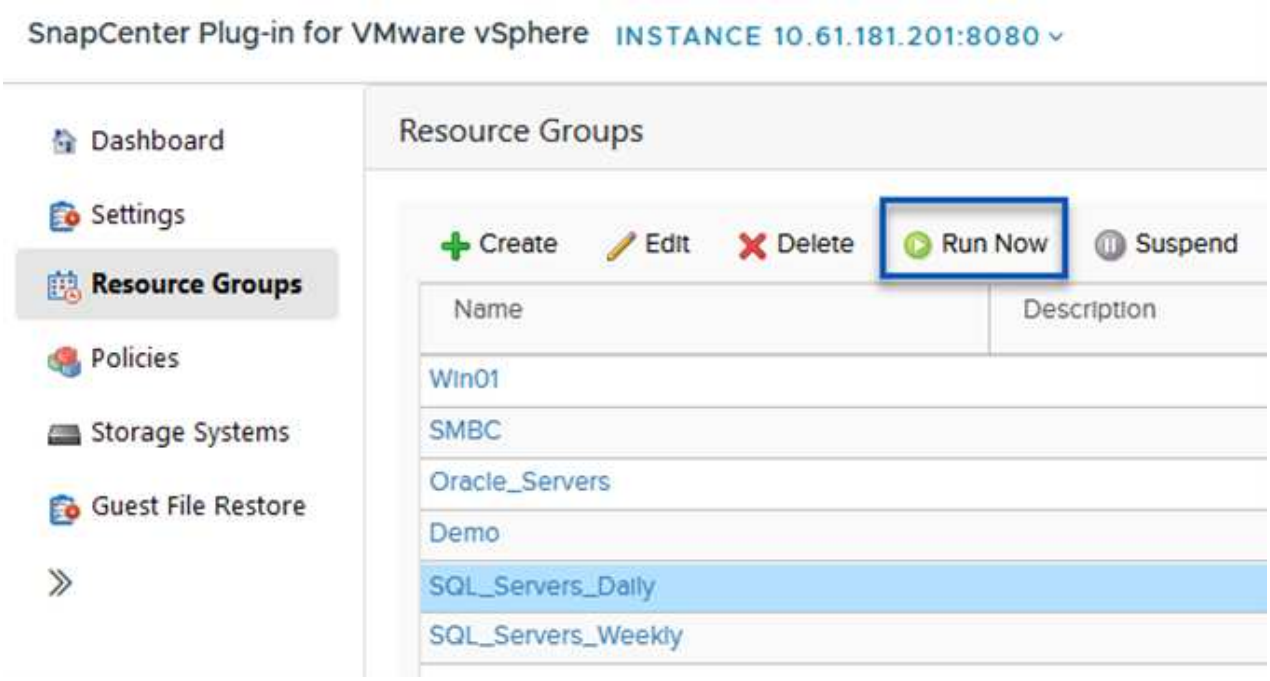


7. Überprüfen Sie abschließend die Übersichtsseite und dann auf **Finish**, um die Erstellung der Ressourcengruppe abzuschließen.

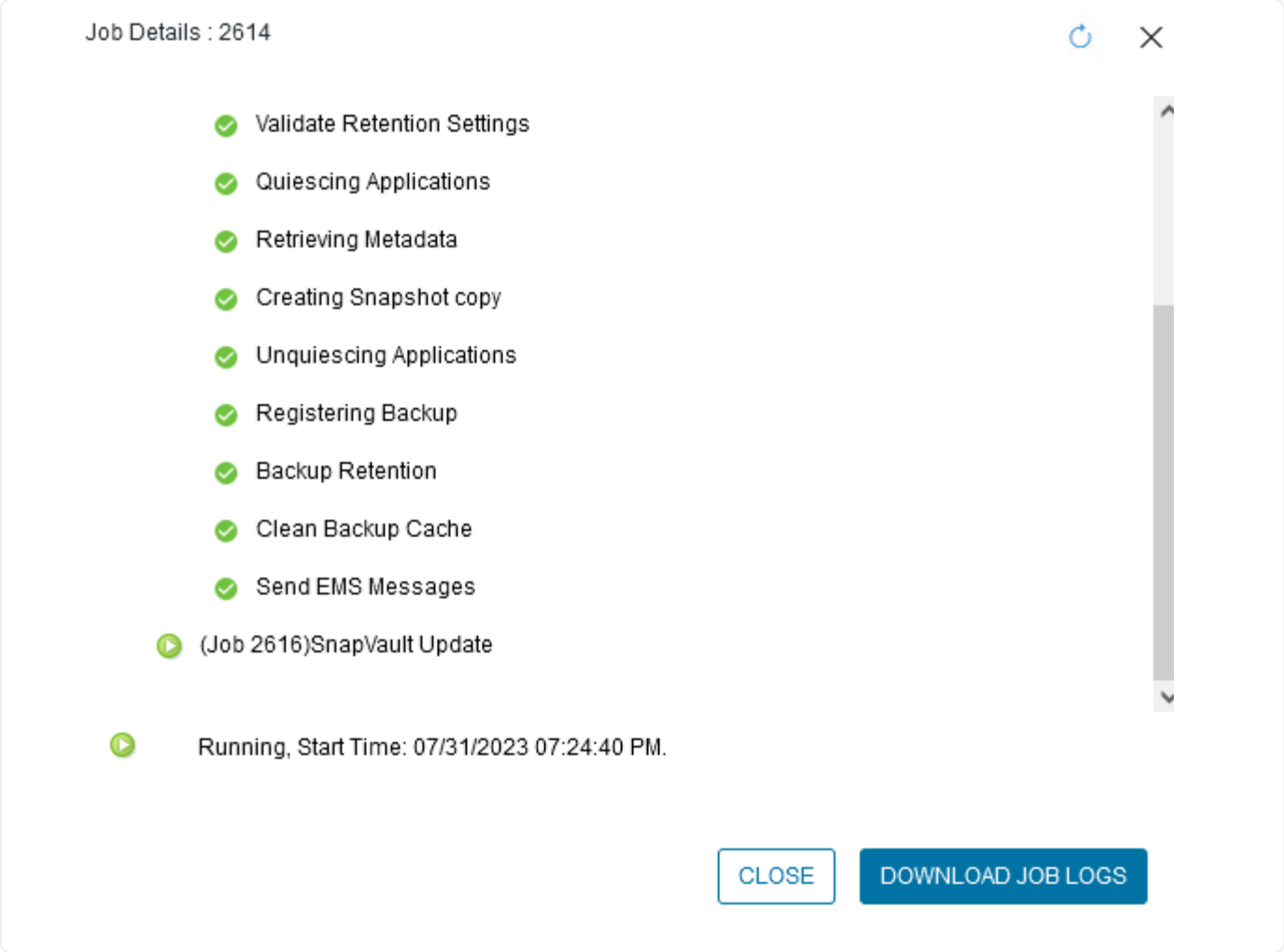
Führen Sie einen Backupjob aus

Führen Sie in diesem letzten Schritt einen Backupjob aus und überwachen Sie dessen Fortschritt. Mindestens ein Backup-Job muss in SCV erfolgreich abgeschlossen werden, bevor Ressourcen von BlueXP Backup und Recovery erkannt werden können.

1. Navigieren Sie im SnapCenter Plug-in für VMware vSphere im linken Menü zu **Ressourcengruppen**.
2. Um einen Backup-Job zu starten, wählen Sie die gewünschte Ressourcengruppe aus und klicken Sie auf die Schaltfläche **Jetzt ausführen**.



3. Um den Sicherungsauftrag zu überwachen, navigieren Sie im linken Menü zu **Dashboard**. Klicken Sie unter **Recent Job Activities** auf die Job-ID-Nummer, um den Job-Fortschritt zu überwachen.



Konfigurieren Sie Backups auf Objekt-Storage in BlueXP Backup und Recovery

Damit BlueXP die Dateninfrastruktur effektiv managen kann, ist die vorherige Installation eines Connectors erforderlich. Der Connector führt die Aktionen aus, die für die Erkennung von Ressourcen und das Management von Datenvorgängen erforderlich sind.

Weitere Informationen zu BlueXP Connector finden Sie unter "Erfahren Sie mehr über Steckverbinder" In der BlueXP Dokumentation.

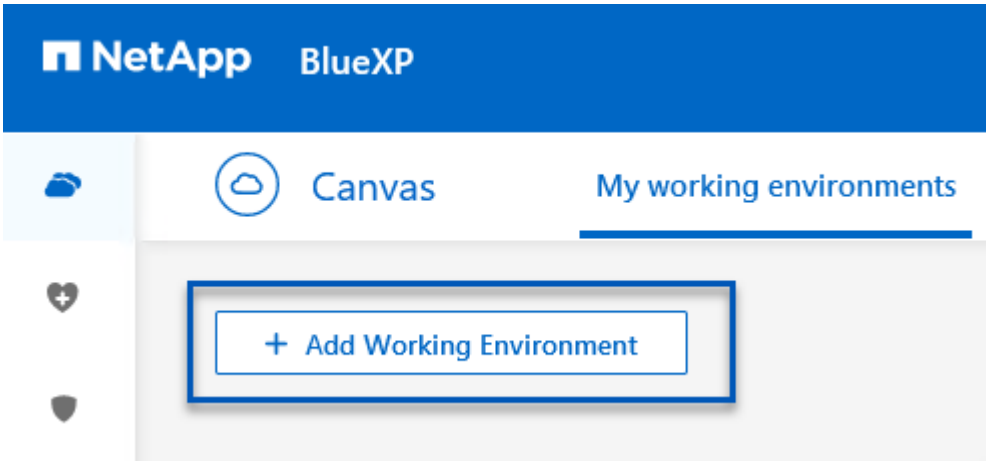
Sobald der Connector für den verwendeten Cloud-Provider installiert ist, wird eine grafische Darstellung des Objektspeichers im Bildschirm angezeigt.

Gehen Sie wie folgt vor, um BlueXP Backup und Recovery für Backup-Daten zu konfigurieren, die durch SCV On-Premises gemanagt werden:

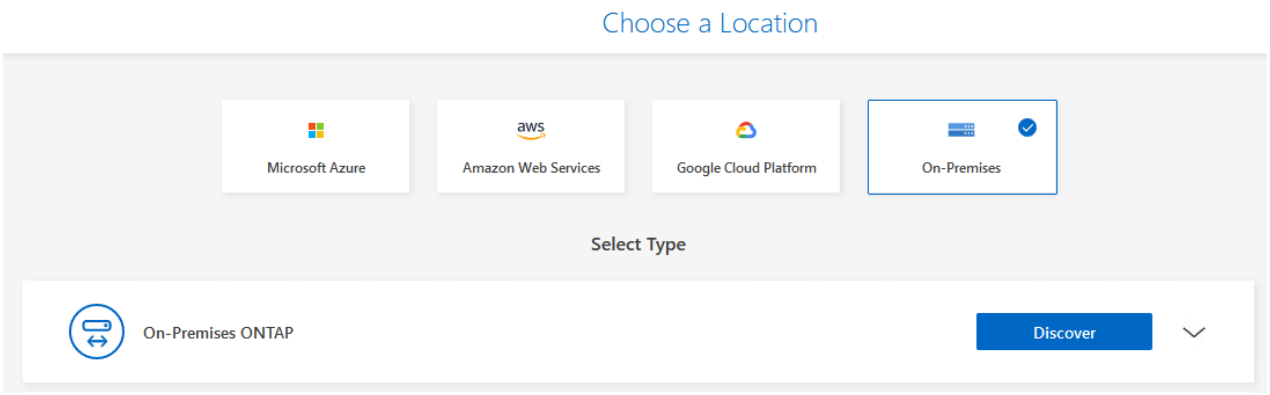
Arbeitsumgebungen zum Bildschirm hinzufügen

In einem ersten Schritt fügen Sie die lokalen ONTAP Storage-Systeme zu BlueXP hinzu

1. Wählen Sie auf dem Bildschirm **Arbeitsumgebung hinzufügen**, um zu beginnen.



2. Wählen Sie **On-Premises** aus der Wahl der Standorte und klicken Sie dann auf die Schaltfläche **Discover**.



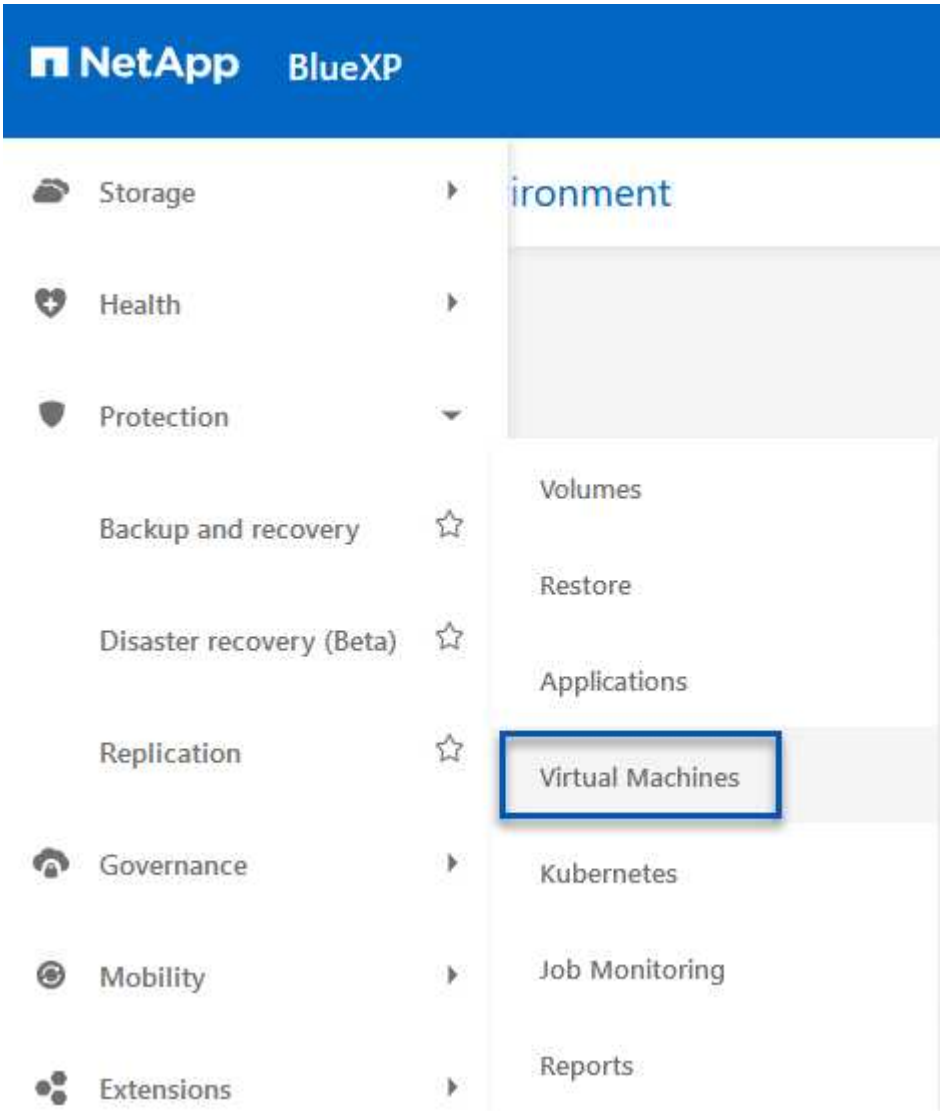
3. Geben Sie die Anmeldeinformationen für das ONTAP-Speichersystem ein, und klicken Sie auf die Schaltfläche **Entdecken**, um die Arbeitsumgebung hinzuzufügen.


ONTAP Cluster IP
10.61.181.180
User Name
admin
Password

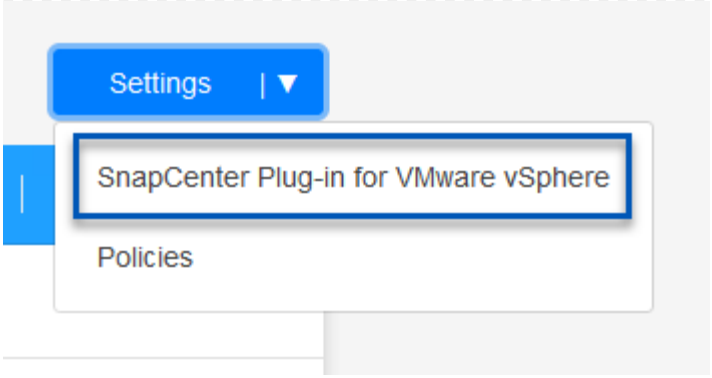
Erkennen Sie lokale SCV-Appliance und vCenter

Um den lokalen Datastore und die Ressourcen der virtuellen Maschine zu ermitteln, fügen Sie Informationen für den SCV-Daten-Broker und Anmeldeinformationen für die vCenter Management-Appliance hinzu.

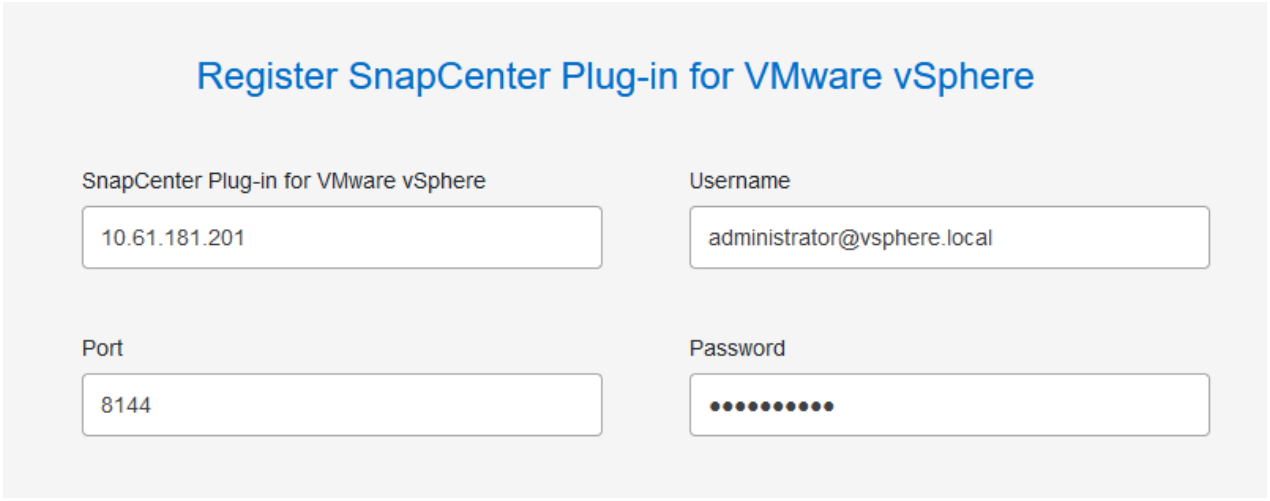
1. Wählen Sie im linken Menü von BlueXP die Option **Schutz > Backup und Recovery > Virtual Machines**



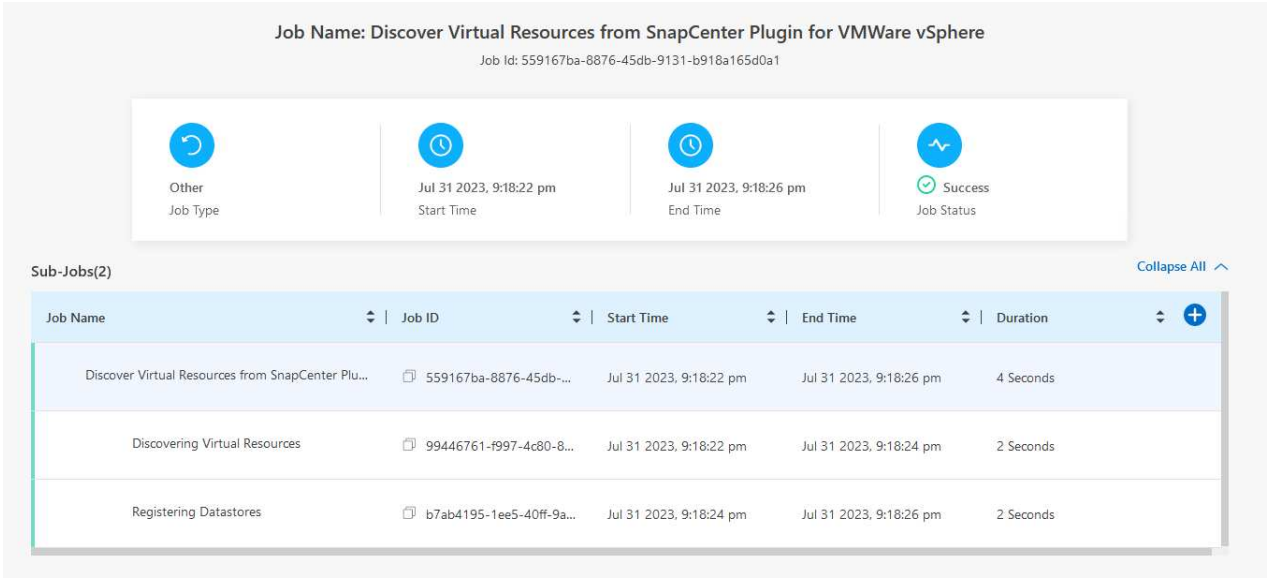
2. Rufen Sie im Hauptbildschirm der virtuellen Maschinen das Dropdown-Menü **Einstellungen** auf und wählen Sie **SnapCenter Plug-in für VMware vSphere**.



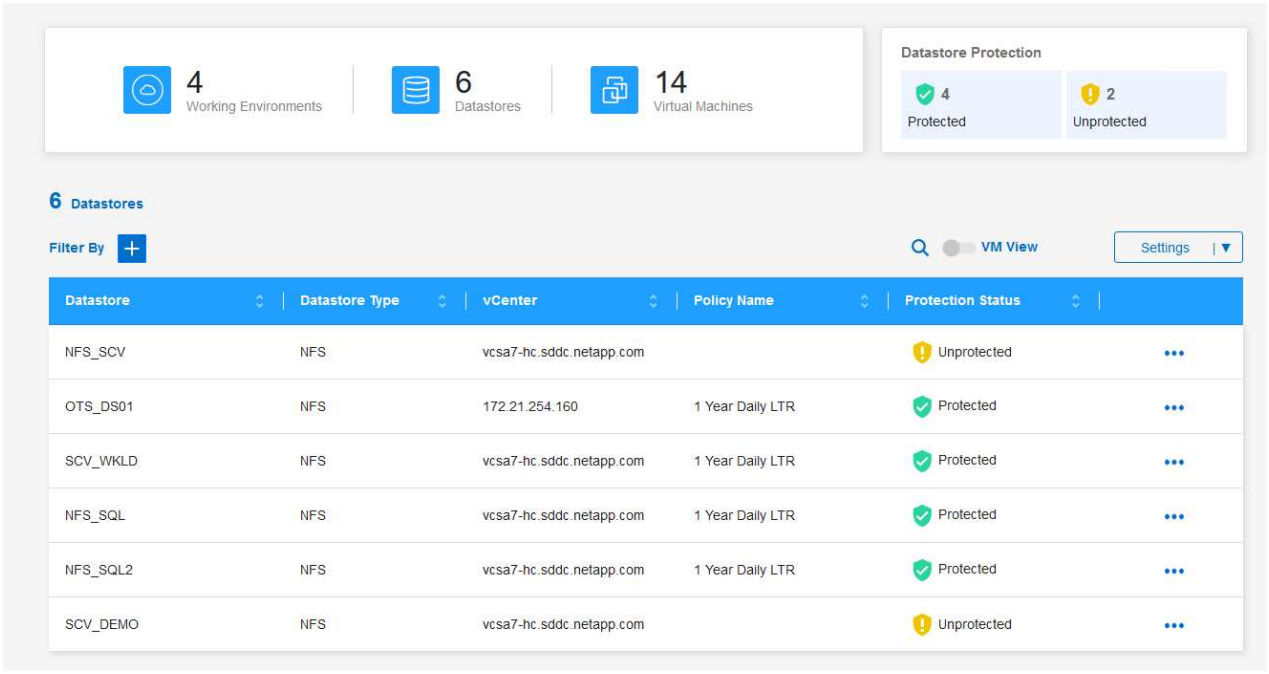
3. Klicken Sie auf die Schaltfläche **Registrieren** und geben Sie dann die IP-Adresse und die Portnummer für die SnapCenter-Plug-in-Appliance sowie den Benutzernamen und das Passwort für die vCenter-Management-Appliance ein. Klicken Sie auf die Schaltfläche **Registrieren**, um den Ermittlungsvorgang zu starten.



4. Der Fortschritt von Jobs kann über die Registerkarte Jobüberwachung überwacht werden.



5. Sobald die Erkennung abgeschlossen ist, können Sie die Datenspeicher und virtuellen Maschinen in allen erkannten SCV-Appliances anzeigen.

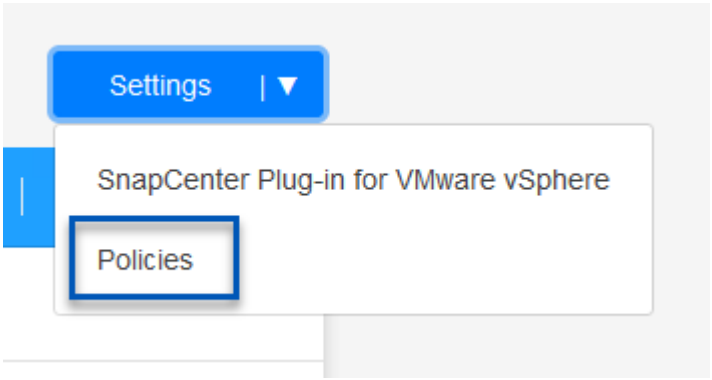

4
Working Environments
6
Datastores
14
Virtual Machines
Datastore Protection
4
Protected
2
Unprotected
6 Datastores
Filter By
VM View
Settings
Datastore
Datastore Type
vCenter
Policy Name
Protection Status
NFS_SCV
NFS
vcsa7-hc.sddc.netapp.com
Unprotected
OTS_DS01
NFS
172.21.254.160
1 Year Daily LTR
Protected
SCV_WKLD
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
NFS_SQL2
NFS
vcsa7-hc.sddc.netapp.com
1 Year Daily LTR
Protected
SCV_DEMO
NFS
vcsa7-hc.sddc.netapp.com
Unprotected

BlueXP Backup-Richtlinien erstellen

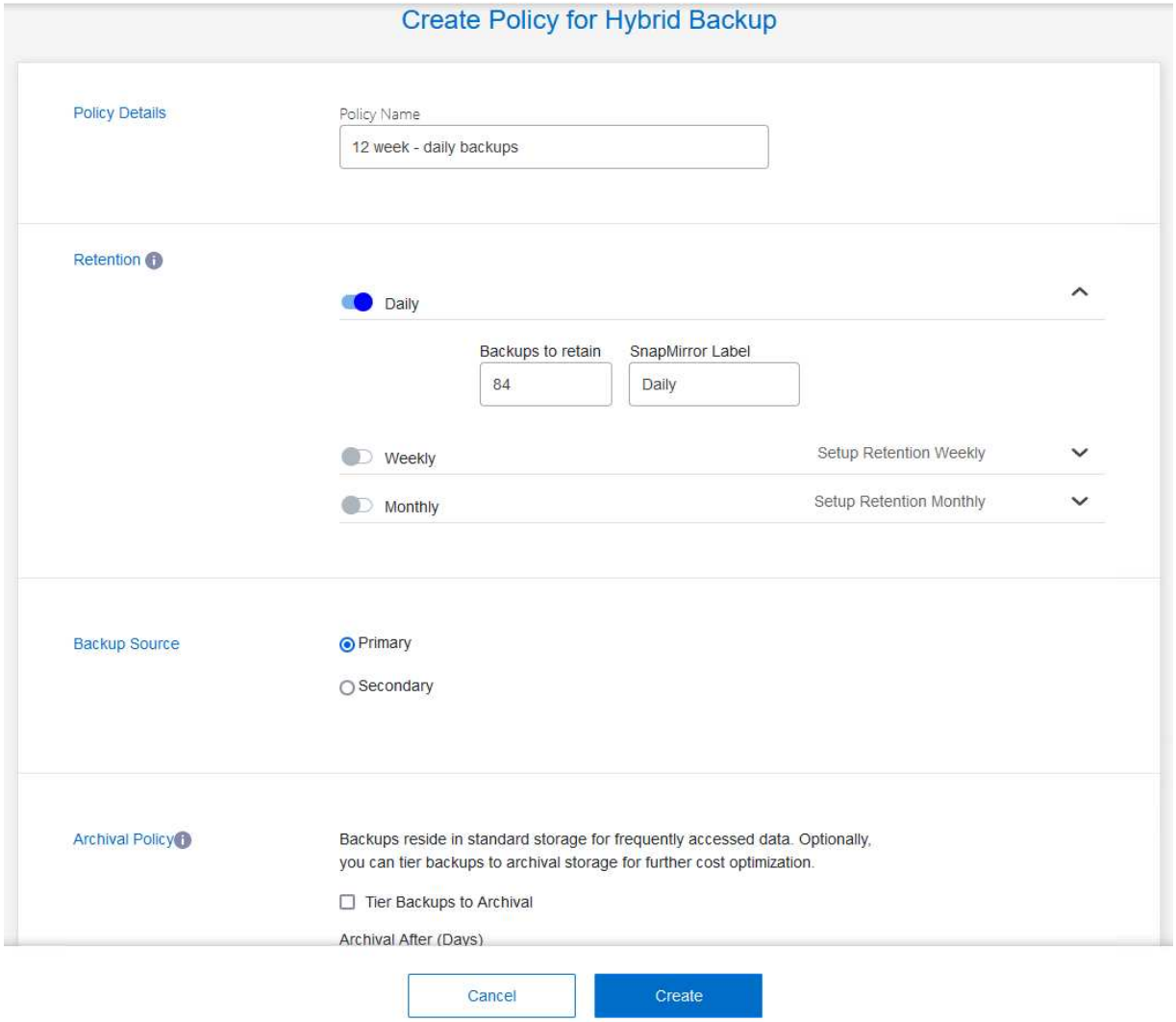
Erstellen Sie in BlueXP Backup und Recovery für Virtual Machines Richtlinien zur Angabe des Aufbewahrungszeitraums, der Backup-Quelle und der Archivierungsrichtlinie.

Weitere Informationen zum Erstellen von Richtlinien finden Sie unter "Erstellen Sie eine Richtlinie zum Backup von Datastores".

1. Rufen Sie auf der Hauptseite von BlueXP Backup und Recovery für virtuelle Maschinen das Dropdown-Menü **Einstellungen** auf und wählen Sie **Richtlinien** aus.



2. Klicken Sie auf **Create Policy**, um auf das Fenster **Create Policy for Hybrid Backup** zuzugreifen.
   a. Fügen Sie einen Namen für die Richtlinie hinzu
   b. Wählen Sie die gewünschte Aufbewahrungsfrist aus
   c. Legen Sie fest, ob Backups vom primären oder sekundären lokalen ONTAP Storage-System bezogen werden
   d. Geben Sie optional an, nach welcher Zeitspanne Backups auf Archiv-Storage verschoben werden sollen, um zusätzliche Kosteneinsparungen zu erzielen.



Das hier eingegebene SnapMirror-Label wird verwendet, um zu ermitteln, welche Backups die Richtlinie auch anwenden sollen. Der Name der Beschriftung muss mit dem Namen der Beschriftung in der entsprechenden On-Premises-SCV-Richtlinie übereinstimmen.

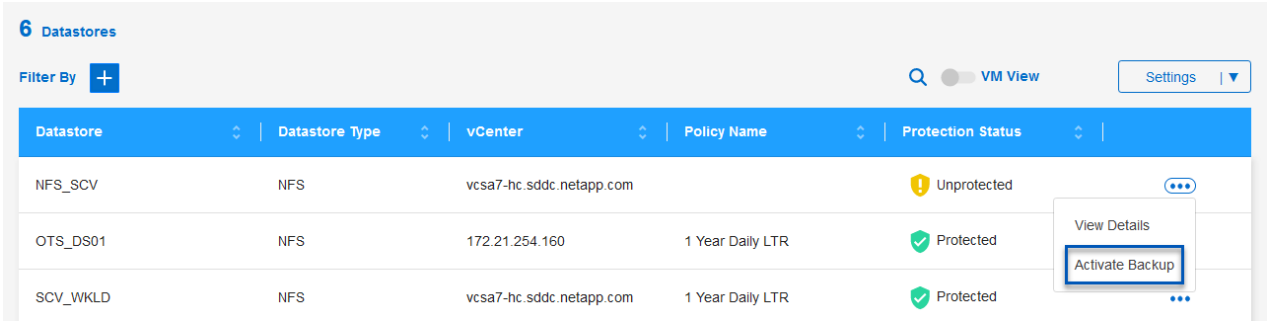
3. Klicken Sie auf **Create**, um die Erstellung der Richtlinie abzuschließen.

Backup von Datastores auf Amazon Web Services

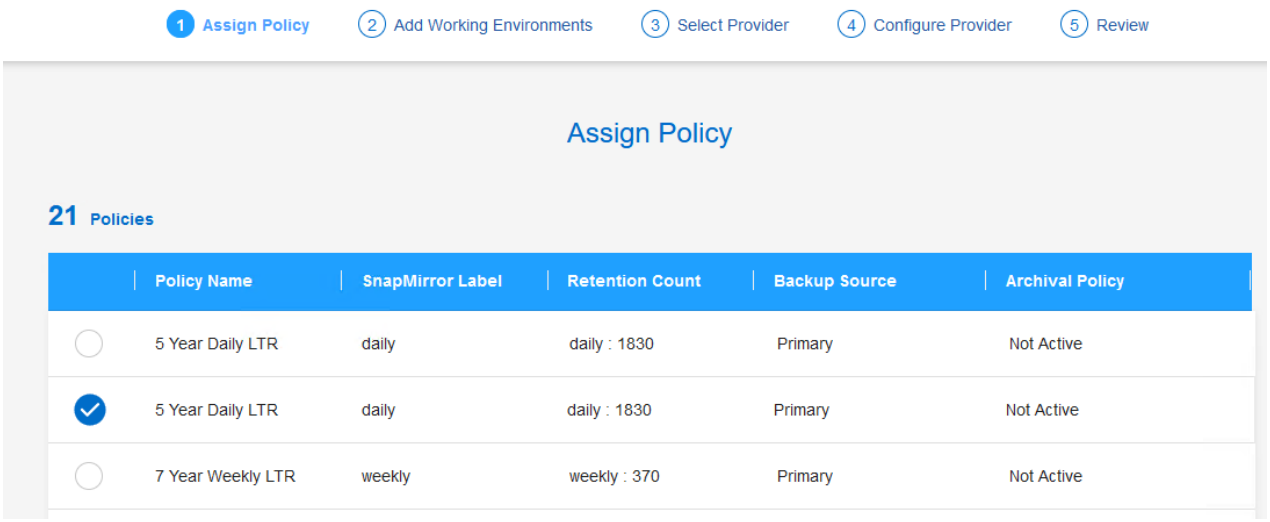
Im letzten Schritt aktivieren Sie die Datensicherung für einzelne Datenspeicher und Virtual Machines. Im folgenden Schritt wird die Aktivierung von Backups auf AWS beschrieben.

Weitere Informationen finden Sie unter "Erstellen Sie Backups von Datastores in Amazon Web Services".

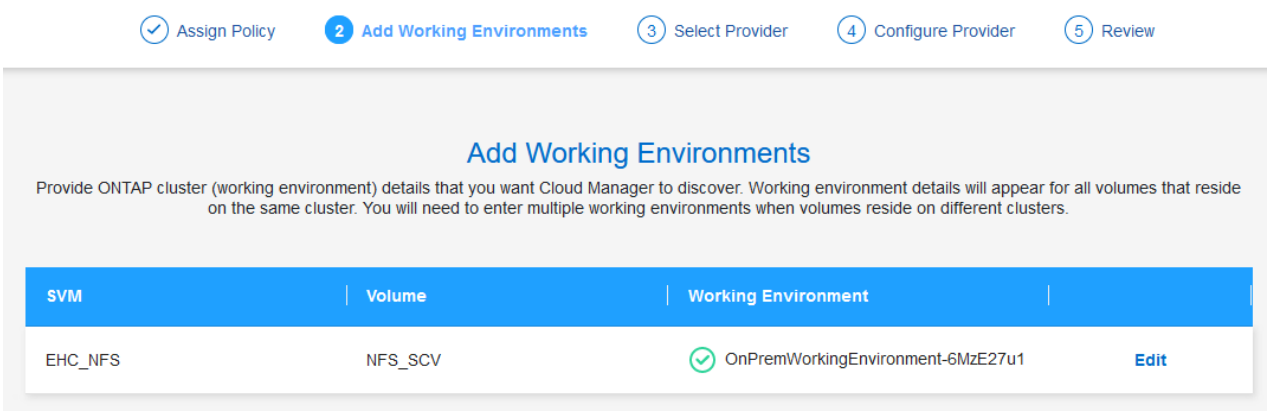
1. Rufen Sie auf der Hauptseite von BlueXP Backup und Recovery für Virtual Machines das Dropdown-Menü Einstellungen für den zu sichernden Datastore auf und wählen Sie **Backup aktivieren** aus.



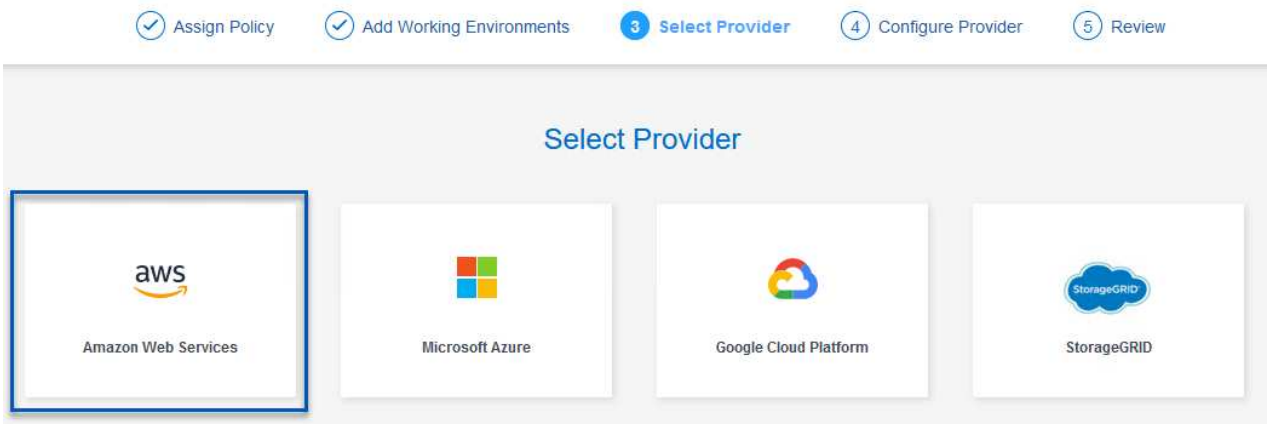
2. Weisen Sie die für den Datenschutzvorgang zu verwendende Richtlinie zu und klicken Sie auf **Weiter**.



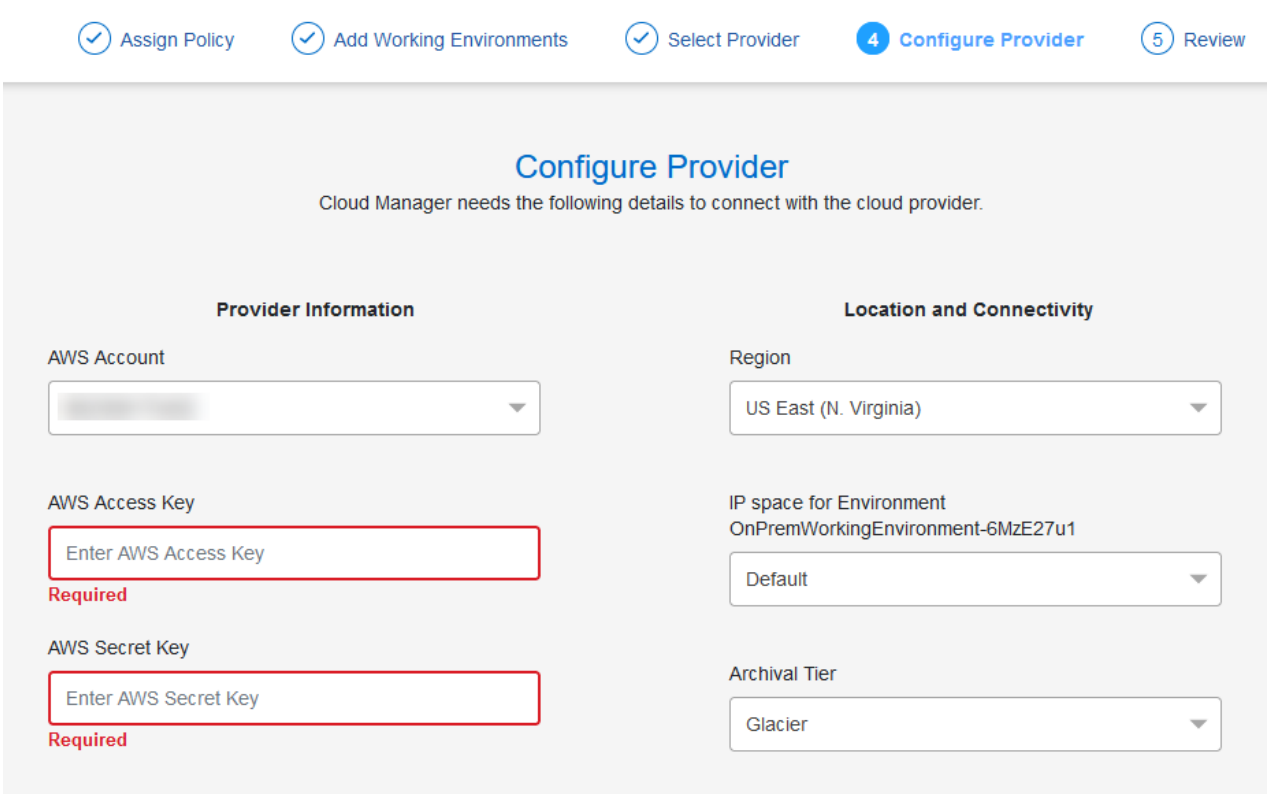
3. Auf der Seite **Add working Environments** sollten der Datastore und die Arbeitsumgebung mit einem Häkchen angezeigt werden, wenn die Arbeitsumgebung zuvor erkannt wurde. Wenn die Arbeitsumgebung noch nicht erkannt wurde, können Sie sie hier hinzufügen. Klicken Sie auf **Weiter**, um fortzufahren.



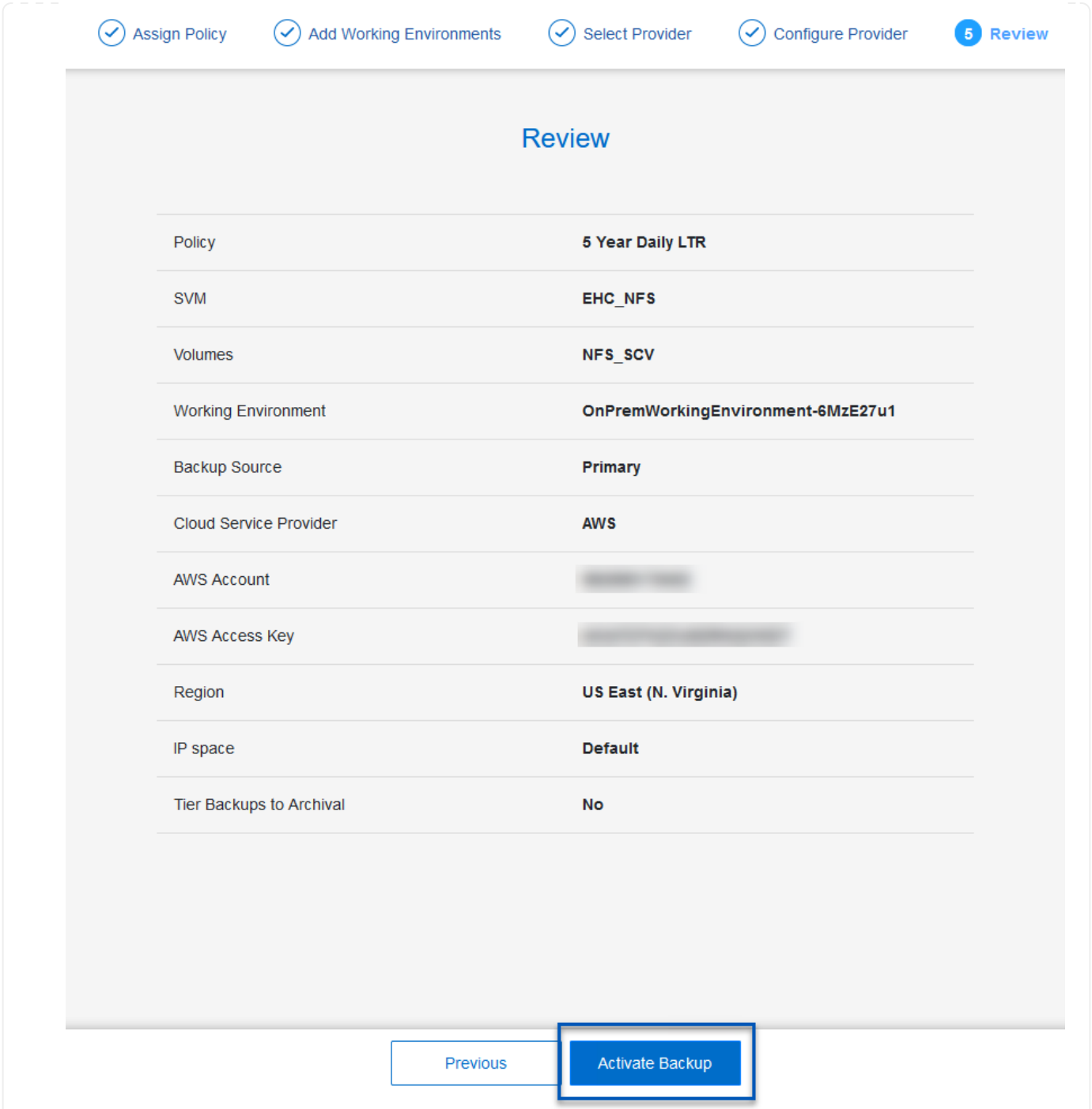
4. Klicken Sie auf der Seite **Select Provider** auf AWS und klicken Sie dann auf die Schaltfläche **Next**, um fortzufahren.



5. Geben Sie die Provider-spezifischen Anmeldeinformationen für AWS an, einschließlich des zu verwendenden AWS Zugriffsschlüssels und des geheimen Schlüssels, der Region und der Archiv-Tier. Wählen Sie außerdem den ONTAP IP-Speicherplatz für das lokale ONTAP Storage-System aus. Klicken Sie auf **Weiter**.



6. Überprüfen Sie abschließend die Details des Backup-Jobs und klicken Sie auf die Schaltfläche **Backup aktivieren**, um den Datenschutz des Datastore zu initiieren.



An diesem Punkt kann die Datenübertragung nicht sofort beginnen. Bei BlueXP Backup und Recovery werden stündlich nach herausragenden Snapshots durchsucht und diese anschließend an den Objekt-Storage übertragen.

Wiederherstellung von Virtual Machines bei Datenverlust

Der Schutz Ihrer Daten zu gewährleisten, ist nur ein Aspekt umfassenden Datenschutzes. Ebenso wichtig ist die Fähigkeit, Daten bei Datenverlust oder Ransomware-Angriffen von jedem Standort aus umgehend wiederherzustellen. Diese Funktion ist von entscheidender Bedeutung für die Aufrechterhaltung eines nahtlosen Geschäftsbetriebs und die Einhaltung von Recovery-Zeitpunkten.

NetApp bietet eine äußerst anpassungsfähige 3-2-1-1-Strategie und bietet individuelle Kontrolle über Aufbewahrungszeitpläne am primären, sekundären und Objekt-Storage. Diese Strategie bietet die Flexibilität, Datensicherungsansätze an spezifische Anforderungen anzupassen.

Dieser Abschnitt bietet einen Überblick über den Datenwiederherstellungsprozess sowohl über das SnapCenter Plug-in für VMware vSphere als auch über das BlueXP Backup und Recovery für Virtual Machines.

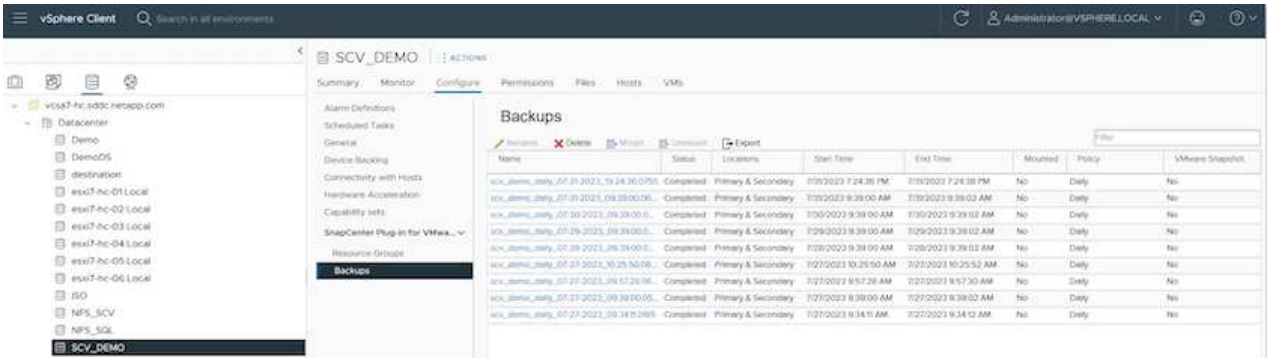
Wiederherstellen virtueller Maschinen aus dem SnapCenter Plug-in für VMware vSphere

Für diese Lösung wurden virtuelle Maschinen an ursprünglichen und alternativen Standorten wiederhergestellt. In dieser Lösung werden nicht alle Aspekte der Datenwiederherstellungsfunktionen von SCV behandelt. Ausführliche Informationen zu allen Angeboten von SCV finden Sie im "Wiederherstellung von VMs aus Backups" In der Produktdokumentation.

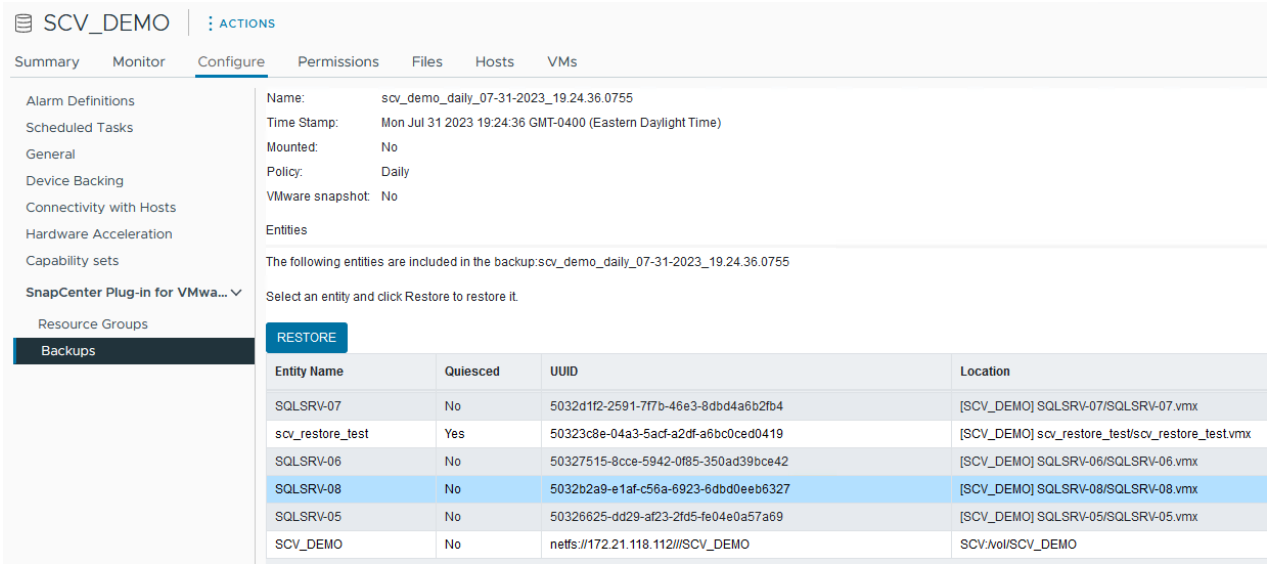
Stellen Sie virtuelle Maschinen über SCV wieder her

Führen Sie die folgenden Schritte aus, um eine VM-Wiederherstellung aus dem primären oder sekundären Speicher wiederherzustellen.

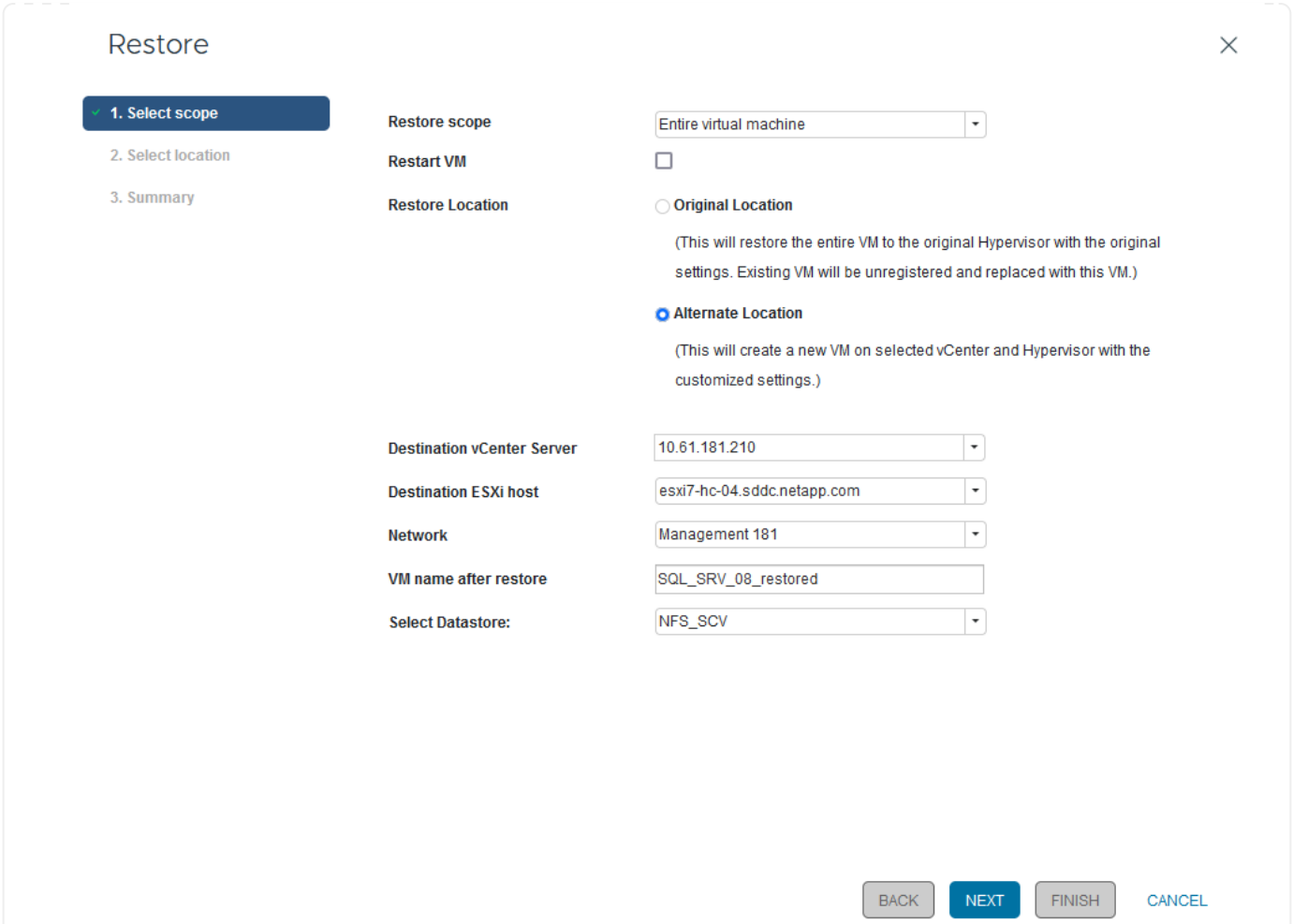
1. Navigieren Sie im vCenter-Client zu **Inventar > Speicher** und klicken Sie auf den Datenspeicher, der die virtuellen Maschinen enthält, die Sie wiederherstellen möchten.
2. Klicken Sie auf der Registerkarte **Configure** auf **Backups**, um die Liste der verfügbaren Backups aufzurufen.



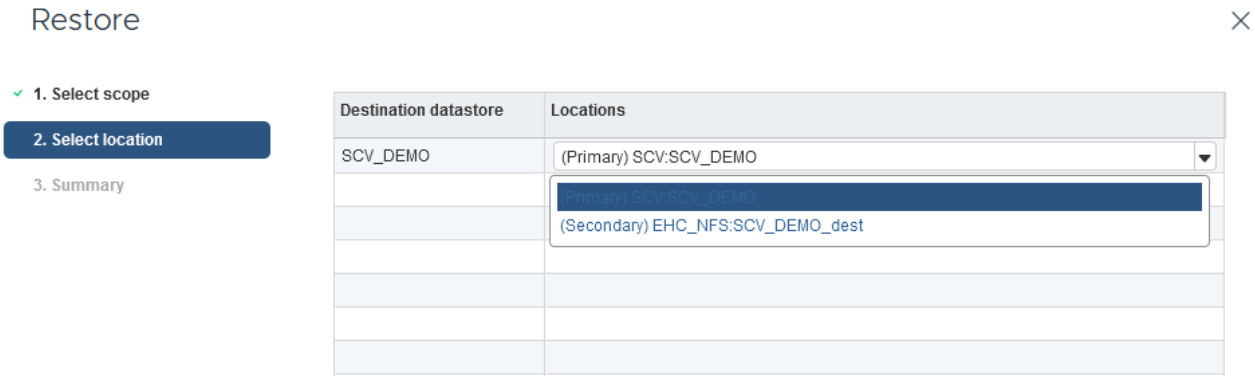
3. Klicken Sie auf ein Backup, um auf die Liste der VMs zuzugreifen, und wählen Sie dann eine wiederherzustellende VM aus. Klicken Sie auf **Wiederherstellen**.



4. Wählen Sie im Wiederherstellungsassistenten aus, um die gesamte virtuelle Maschine oder eine bestimmte VMDK wiederherzustellen. Wählen Sie diese Option aus, um sie am ursprünglichen Speicherort oder an einem alternativen Speicherort zu installieren, geben Sie nach der Wiederherstellung den VM-Namen und den Zieldatenspeicher an. Klicken Sie Auf **Weiter**.



5. Wählen Sie die Option zum Backup vom primären oder sekundären Speicherort aus.



6. Überprüfen Sie abschließend eine Zusammenfassung des Backupjobs, und klicken Sie auf Fertig stellen, um den Wiederherstellungsprozess zu starten.

Wiederherstellung von Virtual Machines aus BlueXP Backup und Recovery für Virtual Machines

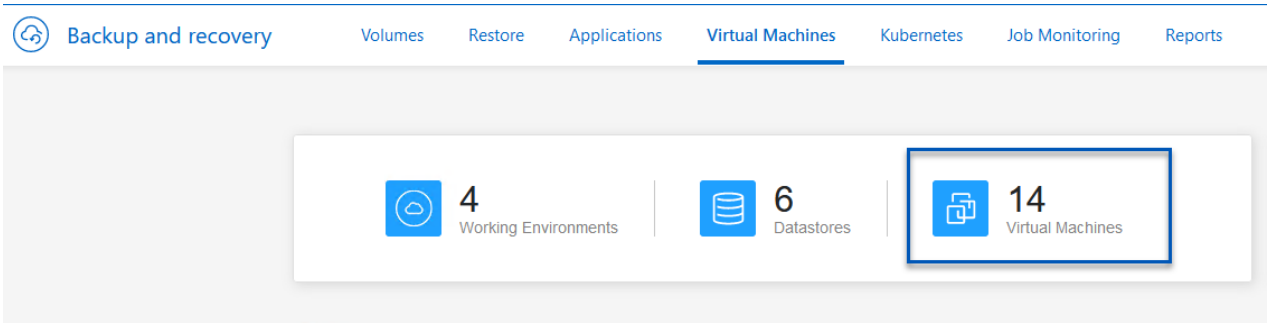
Mit BlueXP Backup und Recovery für Virtual Machines können Virtual Machines an ihrem ursprünglichen Speicherort wiederhergestellt werden. Der Zugriff auf Restore-Funktionen erfolgt über die Web-Konsole von BlueXP.

Weitere Informationen finden Sie unter "Wiederherstellung der Daten von Virtual Machines aus der Cloud".

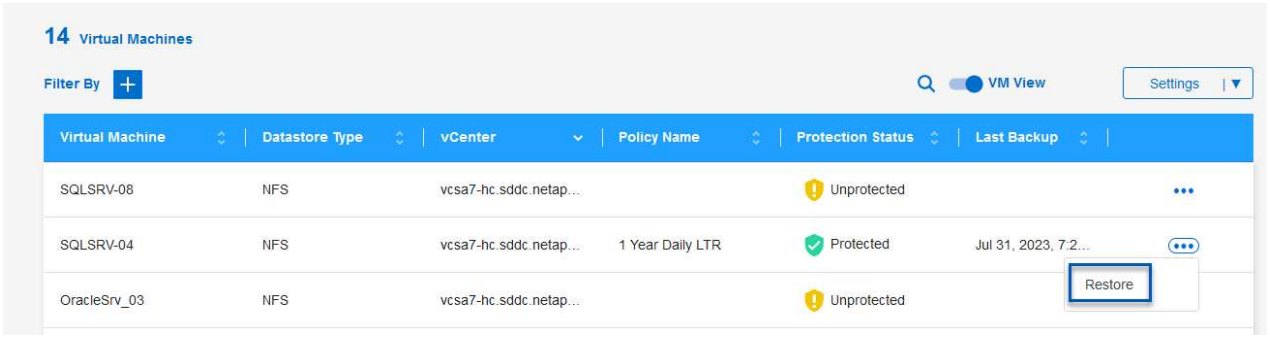
Wiederherstellung von Virtual Machines aus BlueXP Backup und Recovery

Führen Sie die folgenden Schritte aus, um eine Virtual Machine aus dem Backup- und Recovery-Verfahren von BlueXP wiederherzustellen.

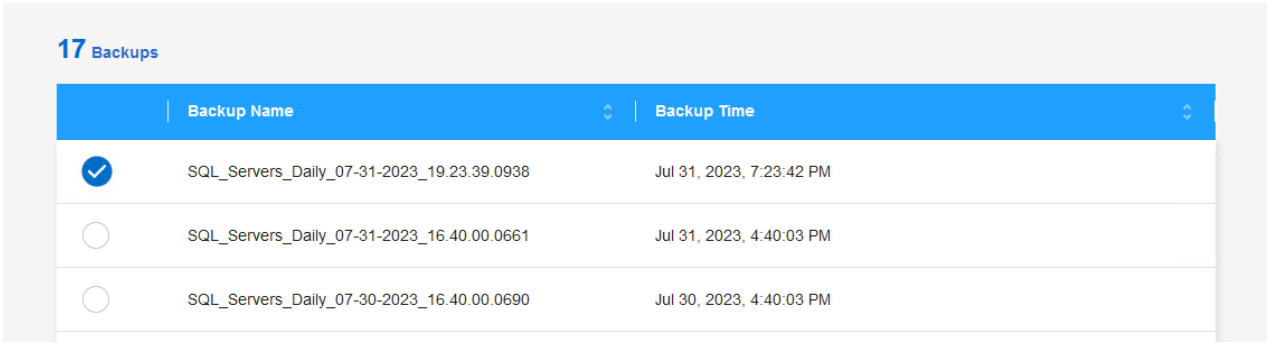
1. Navigieren Sie zu **Schutz > Sicherung und Wiederherstellung > Virtuelle Maschinen** und klicken Sie auf Virtuelle Maschinen, um die Liste der virtuellen Maschinen anzuzeigen, die wiederhergestellt werden können.



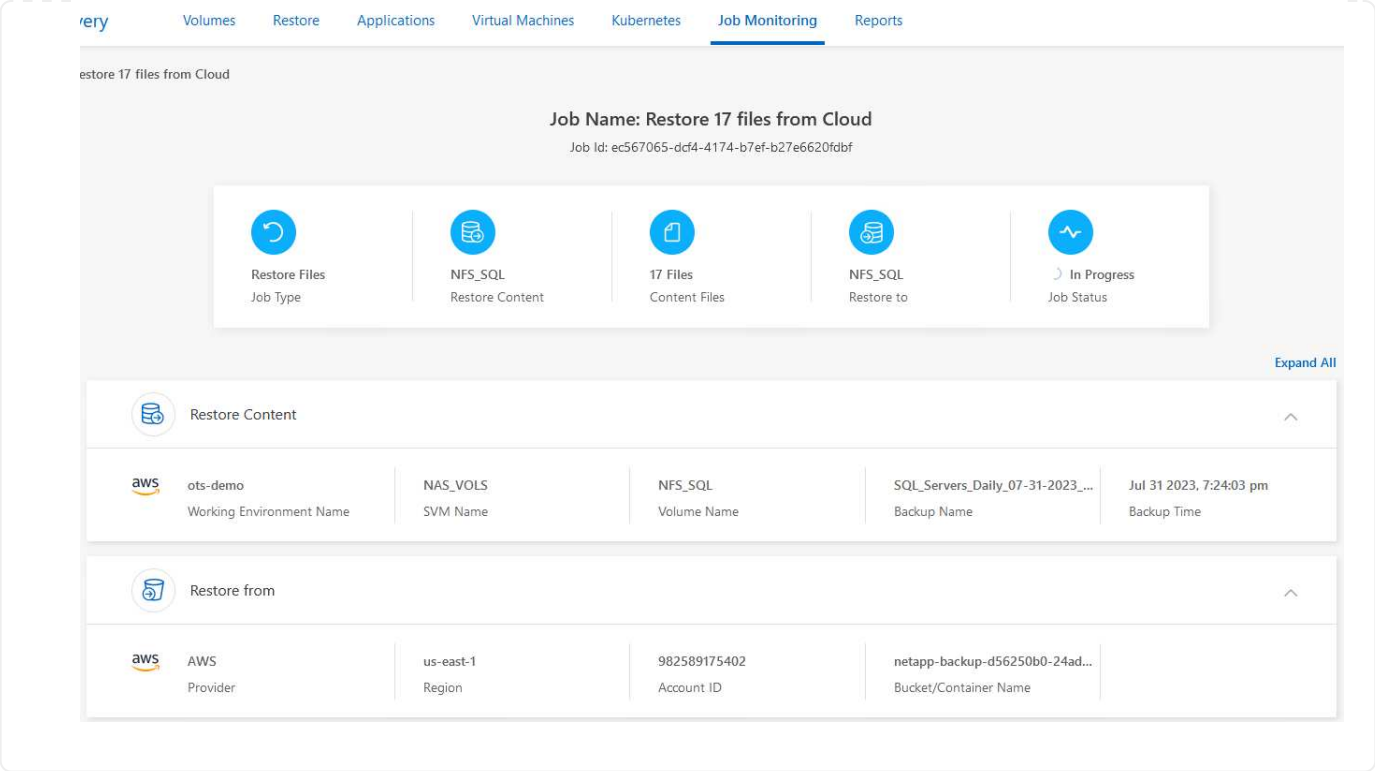
2. Öffnen Sie das Dropdown-Menü Einstellungen für die wiederherzustellende VM, und wählen Sie aus



3. Wählen Sie das zu wiederherstellende Backup aus und klicken Sie auf **Weiter**.



4. Überprüfen Sie eine Zusammenfassung des Backup-Jobs und klicken Sie auf **Wiederherstellen**, um den Wiederherstellungsprozess zu starten.
5. Überwachen Sie den Fortschritt des Wiederherstellungsjobs über die Registerkarte **Job Monitoring**.



Schlussfolgerung

Die 3-2-1-1-Backup-Strategie nach Implementierung mit dem SnapCenter Plug-in für VMware vSphere und BlueXP Backup- und Recovery-Lösungen für Virtual Machines stellt eine robuste, zuverlässige und kostengünstige Lösung für die Datensicherung dar. Diese Strategie gewährleistet nicht nur Datenredundanz und -Verfügbarkeit, sondern bietet auch die Flexibilität, Daten von jedem Standort aus wiederherzustellen – sowohl aus On-Premises-ONTAP-Storage-Systemen als auch aus Cloud-basiertem Objektspeicher.

Der in dieser Dokumentation präsentierte Anwendungsfall konzentriert sich auf bewährte Datensicherungstechnologien, die die Integration von NetApp, VMware und den führenden Cloud-Providern hervorheben. Das SnapCenter Plug-in für VMware vSphere ermöglicht die nahtlose Integration in VMware vSphere und ermöglicht so ein effizientes und zentralisiertes Management von Datensicherungsvorgängen. Diese Integration optimiert die Backup- und Recovery-Prozesse für Virtual Machines und ermöglicht so einfache Planung, Überwachung und flexible Restore-Vorgänge innerhalb des VMware Ökosystems. BlueXP Backup und Recovery für Virtual Machines bietet das eine (1) in 3-2-1 durch sichere Backups der Daten von Virtual Machines mit Air-Gap-Separierung in Cloud-basiertem Objekt-Storage. Die intuitive Benutzeroberfläche und der logische Workflow bilden eine sichere Plattform für die langfristige Archivierung geschäftskritischer Daten.

Weitere Informationen

Weitere Informationen zu den in dieser Lösung vorgestellten Technologien finden Sie in den folgenden zusätzlichen Informationen.

- "Dokumentation zum SnapCenter Plug-in für VMware vSphere"
- "BlueXP-Dokumentation"

DR mit BlueXP DRaaS

Überblick

Disaster Recovery steht allen VMware Administratoren an erster Stelle. Da VMware ganze Server in eine Reihe von Dateien einkapselt, aus denen die Virtual Machine besteht, nutzen Administratoren blockspeicherbasierte Techniken wie Klone, Snapshots und Replikate, um diese VMs zu sichern. ONTAP Arrays bieten integrierte Replizierung für die Übertragung von Volume-Daten und damit der Virtual Machines auf den designierten Datastore-LUNs von einem Standort zum anderen. BlueXP DRaaS lässt sich in vSphere integrieren und automatisiert den gesamten Workflow für nahtloses Failover und Failback bei einem Notfall. Durch die Kombination von Storage-Replizierung mit intelligenter Automatisierung verfügen Administratoren jetzt über einfaches Management. So können sie Disaster Recovery-Pläne nicht nur konfigurieren, automatisieren und testen, sondern auch im Notfall problemlos ausführen.

In einer VMware vSphere Umgebung sind die zeitaufwändigsten Teile eines DR-Failover durch die Ausführung der erforderlichen Schritte zum Inventarisieren, Registrieren, Neukonfigurieren und Hochfahren der VMs am DR-Standort. Eine ideale Lösung bietet sowohl niedrige RPOs (wie in Minuten gemessen) als auch ein niedriges RTO (in Minuten bis Stunden gemessen). Ein Faktor, der in einer DR-Lösung oft übersehen wird, ist die Möglichkeit, die DR-Lösung effizient und in regelmäßigen Abständen zu testen.

Für die Erstellung einer DR-Lösung sollten folgende Faktoren berücksichtigt werden:

- Die Recovery-Zeitvorgabe (RTO). Die RTO beschreibt, wie schnell ein Unternehmen nach einem Ausfall eine Wiederherstellung durchführen kann, genauer gesagt, wie lange es dauert, bis Business Services wieder verfügbar sind.
- Der Recovery-Zeitpunkt (RPO). Der RPO gibt an, wie alt die wiederhergestellten Daten sind, nachdem sie verfügbar gemacht wurden, relativ zum Zeitpunkt des Notfalls.
- Skalierbarkeit und Anpassungsfähigkeit: Zu diesem Faktor gehört auch die Möglichkeit, Storage-Ressourcen bei steigender Nachfrage inkrementell zu erweitern.

Weitere technische Informationen zu den verfügbaren Lösungen finden Sie unter:

- "DR unter Verwendung von BlueXP DRaaS für NFS-Datastores"
- "DR, die BlueXP DRaaS für VMFS-Datastores verwendet"

DR unter Verwendung von BlueXP DRaaS für NFS-Datastores

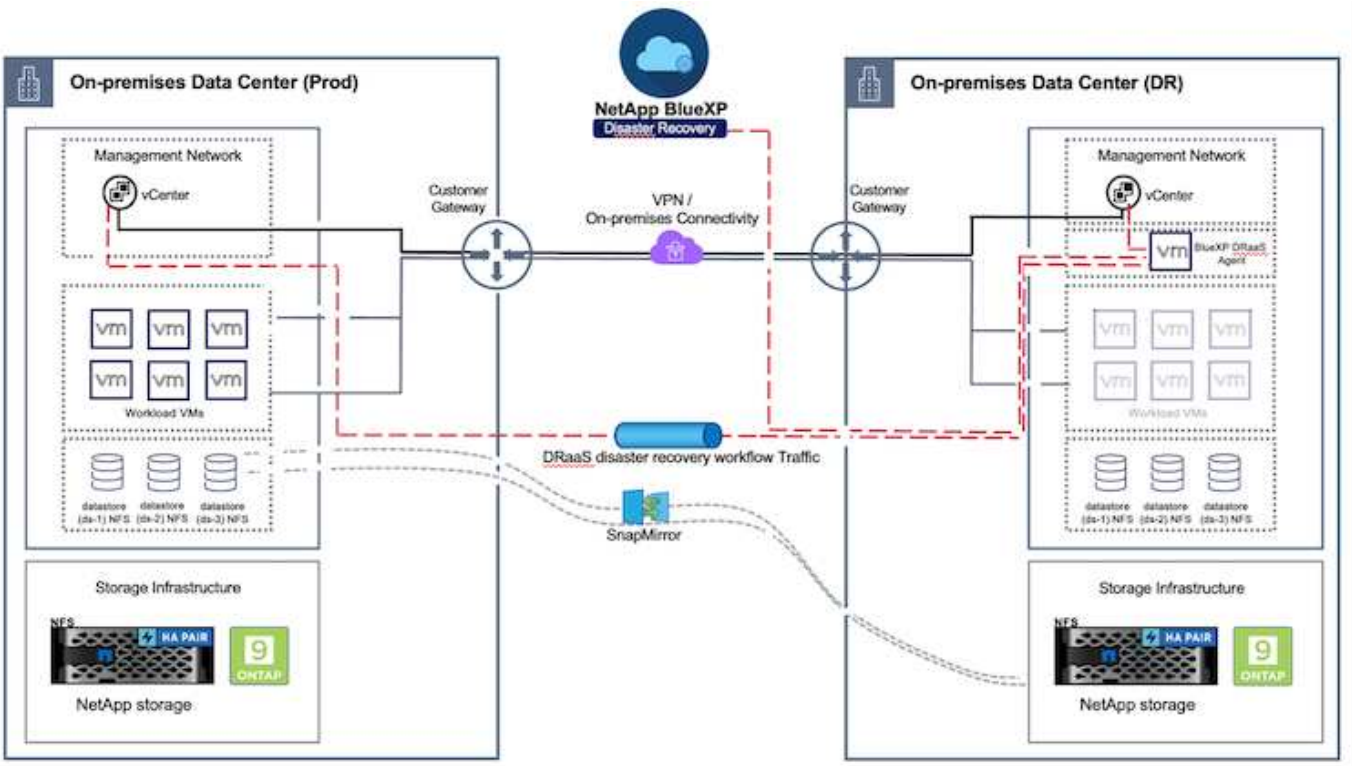
Disaster Recovery durch Replizierung auf Blockebene vom Produktionsstandort zum Disaster-Recovery-Standort ist eine ausfallsichere und kostengünstige Methode, um Workloads vor Standortausfällen und Datenbeschädigungen, z. B. durch Ransomware-Angriffe, zu schützen. Mithilfe der NetApp SnapMirror Replizierung können VMware Workloads, die auf lokalen ONTAP Systemen mit NFS-Datastore ausgeführt werden, auf ein anderes ONTAP Storage-System repliziert werden, das sich in einem festgelegten Recovery-Datacenter befindet, in dem auch VMware implementiert wird.

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zur Einrichtung von Disaster

Recovery für lokale VMware VMs an einem anderen designierten Standort beschrieben. Als Teil dieser Einrichtung, das BlueXP Konto, BlueXP Connector, die ONTAP-Arrays in BlueXP Workspace hinzugefügt, die erforderlich sind, um die Kommunikation von VMware vCenter zum ONTAP Storage zu ermöglichen. Darüber hinaus wird in diesem Dokument beschrieben, wie die Replikation zwischen Standorten konfiguriert und ein Recovery-Plan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Standort-Failover und zum Failback, wenn der primäre Standort wiederhergestellt und online gekauft wird.

Durch den BlueXP Disaster Recovery Service, der in die NetApp BlueXP Konsole integriert ist, können Unternehmen ihre lokalen VMware vCenter und ONTAP Storage mühelos erkennen. Auf diese Weise können Unternehmen Ressourcengruppen erstellen, einen Disaster-Recovery-Plan erstellen, diesen Ressourcengruppen zuordnen und Failover und Failback testen oder ausführen. SnapMirror bietet Block-Replizierung auf Storage-Ebene, sodass die beiden Standorte mit inkrementellen Änderungen aktualisiert werden können, was zu einem Recovery Point Objective (RPO) von bis zu 5 Minuten führt. Außerdem lassen sich Disaster Recovery-Verfahren simulieren, ohne dabei die Produktion zu beeinträchtigen oder zusätzliche Storage-Kosten zu verursachen.

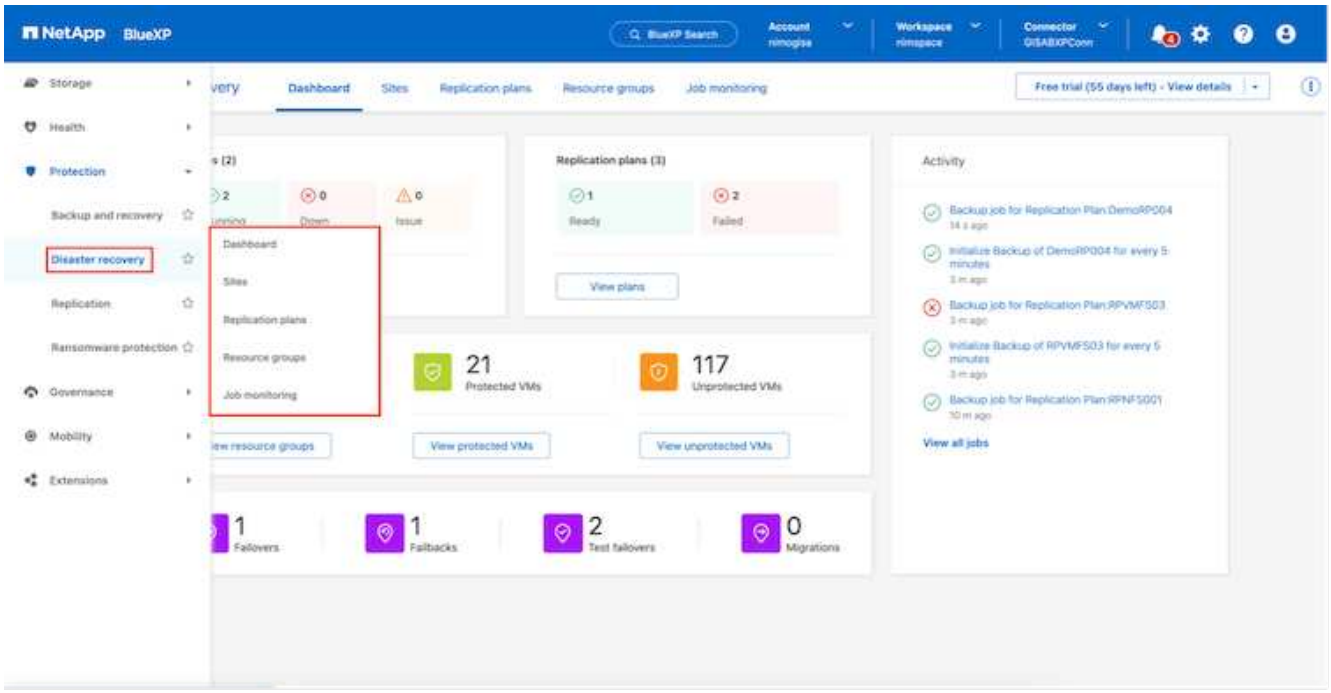
Bei der BlueXP Disaster Recovery wird mithilfe der FlexClone Technologie von ONTAP eine platzsparende Kopie des NFS-Datenspeichers aus dem letzten replizierten Snapshot am Disaster Recovery-Standort erstellt. Nach Abschluss des Disaster-Recovery-Tests können Kunden die Testumgebung einfach löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Wenn ein Failover tatsächlich erfolgt, orchestriert der BlueXP Disaster Recovery Service alle erforderlichen Schritte, um die geschützten Virtual Machines mit nur wenigen Klicks automatisch am designierten Disaster Recovery-Standort zu aktivieren. Der Service umkehrt auch die SnapMirror-Beziehung zum primären Standort und repliziert bei Bedarf alle Änderungen vom sekundären zum primären für einen Failback-Vorgang. All diese Funktionen verursachen jedoch nur einen Bruchteil der Kosten, die andere bekannte Alternativen bieten.



Erste Schritte

Um die BlueXP Disaster Recovery zu starten, verwenden Sie die BlueXP Konsole und greifen Sie dann auf den Service zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste des BlueXP die Option Schutz > Notfallwiederherstellung.
3. Das BlueXP Disaster Recovery Dashboard wird angezeigt.

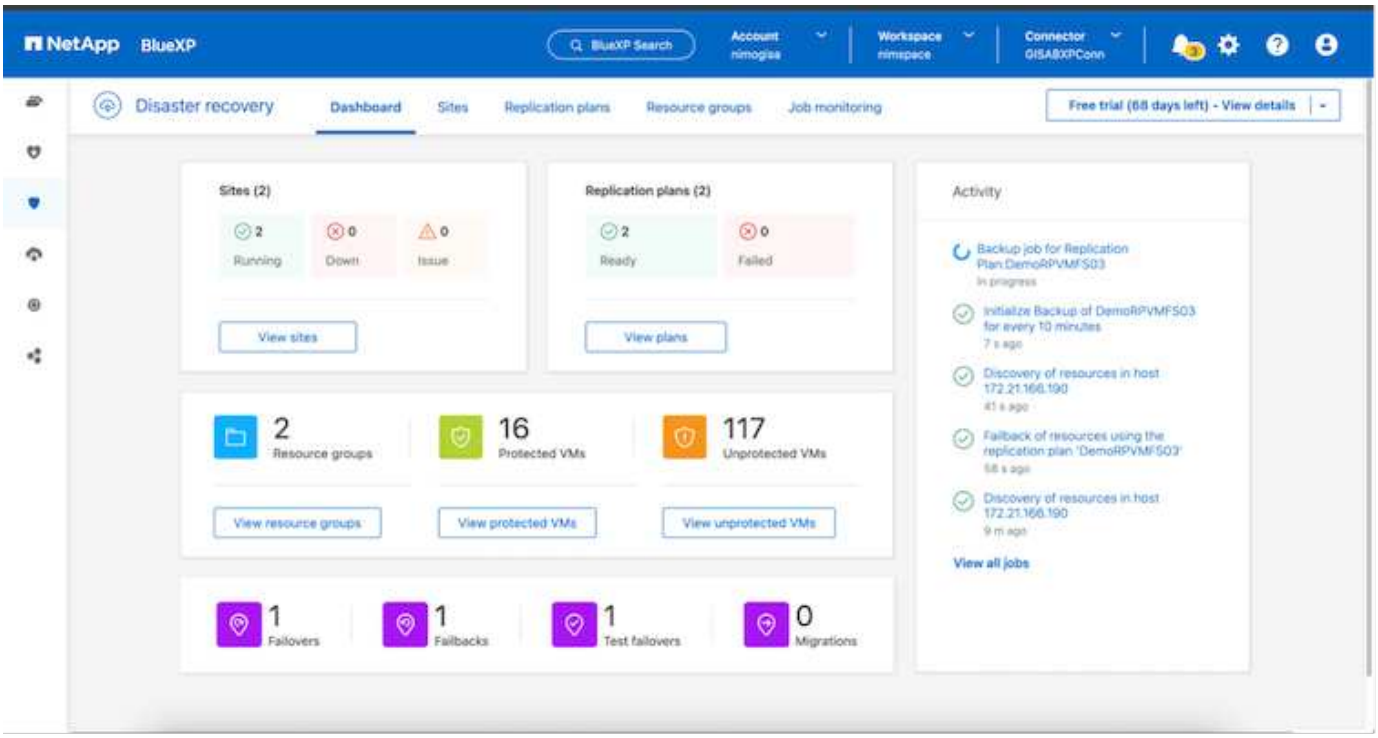


Stellen Sie vor der Konfiguration des Disaster Recovery-Plans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der BlueXP -Anschluss ist in NetApp BlueXP eingerichtet.
- Die BlueXP Connector-Instanz ist mit dem Quell- und Ziel-vCenter sowie mit den Storage-Systemen verbunden.
- NetApp Data ONTAP-Cluster für die Bereitstellung von Storage-NFS-Datastores.
- Lokale NetApp Storage-Systeme, die NFS-Datastores für VMware hosten, werden in BlueXP hinzugefügt.
- Bei der Verwendung von DNS-Namen sollte die DNS-Auflösung vorhanden sein. Verwenden Sie andernfalls IP-Adressen für vCenter.
- Die SnapMirror-Replizierung ist für die designierten NFS-basierten Datenspeicher-Volumes konfiguriert.
- Stellen Sie sicher, dass die Umgebung Versionen von vCenter Server und ESXi-Servern unterstützt.

Sobald die Verbindung zwischen dem Quell- und dem Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte ein paar Klicks und ca. 3 bis 5 Minuten dauern.

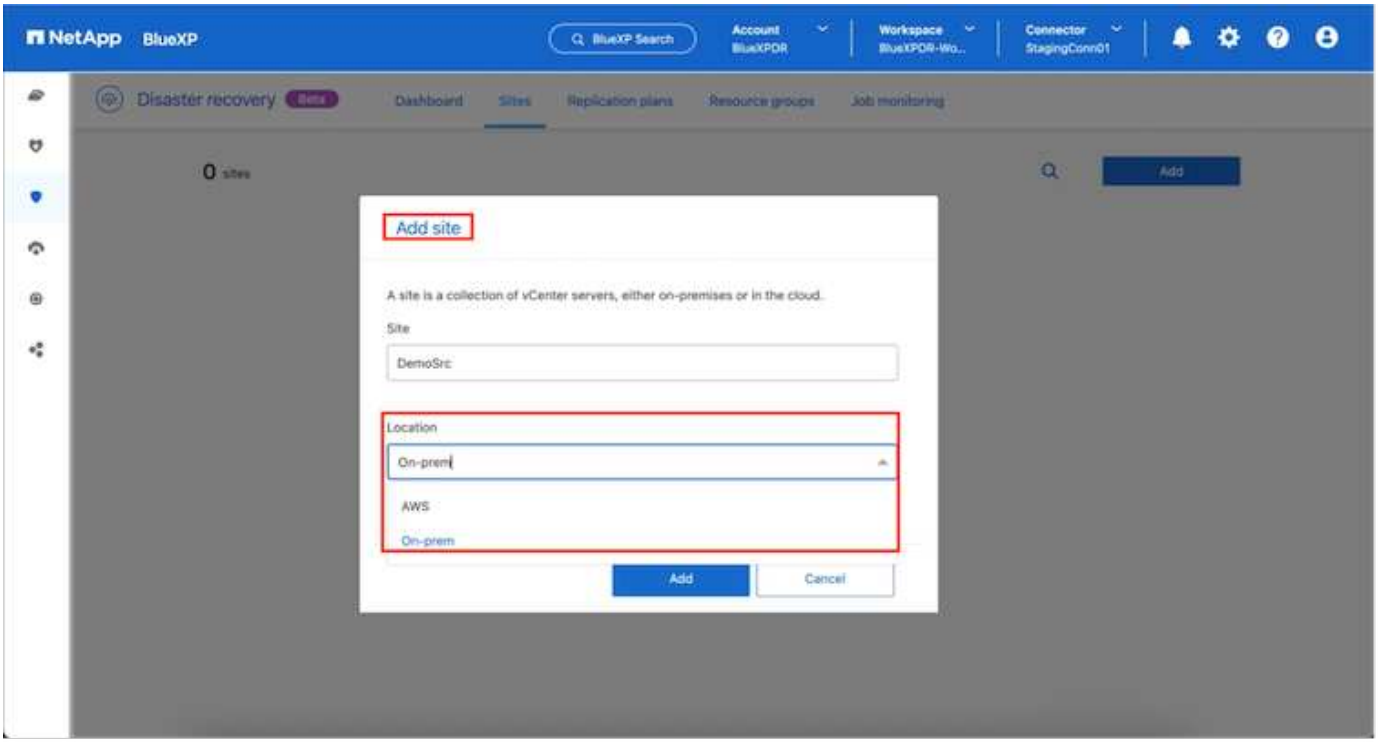
NetApp empfiehlt die Implementierung des BlueXP Connectors am Zielstandort oder an einem dritten Standort, damit der BlueXP Connector über das Netzwerk mit den Quell- und Zielressourcen kommunizieren kann.



BlueXP Disaster Recovery-Konfiguration

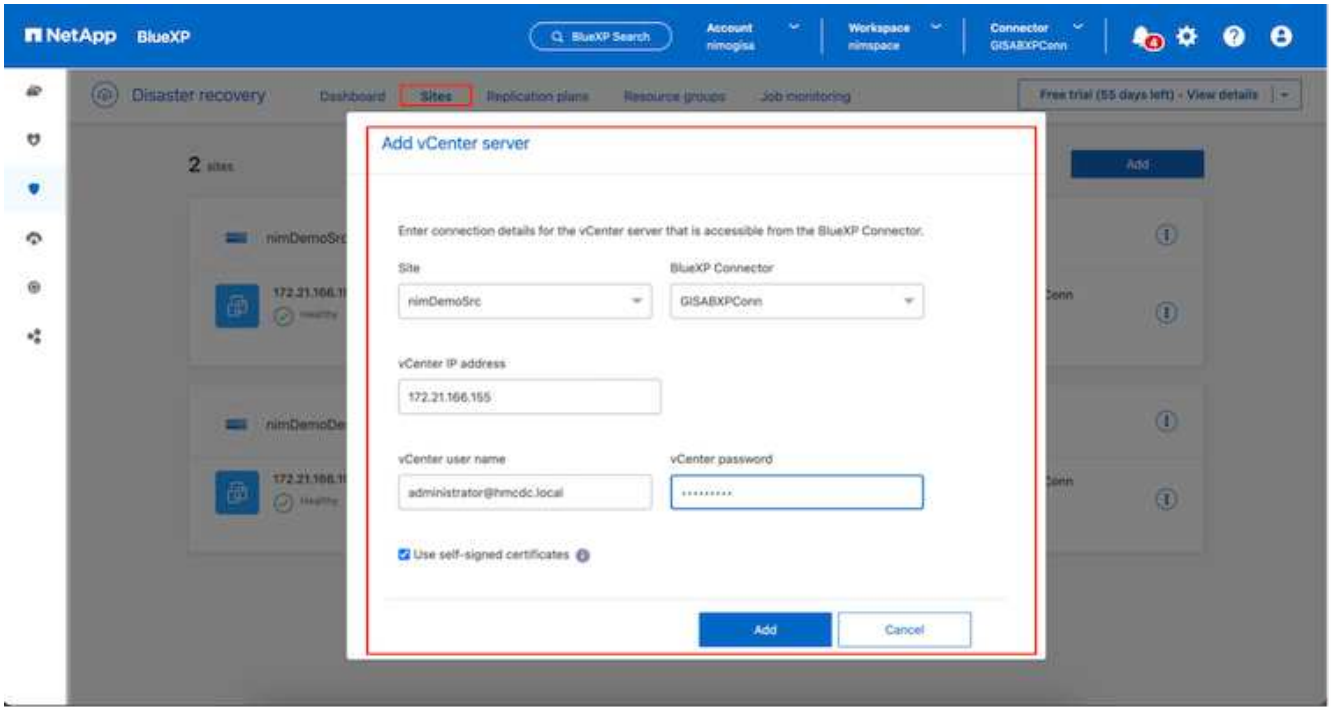
Der erste Schritt zur Vorbereitung auf Disaster Recovery besteht darin, die lokalen vCenter und Storage-Ressourcen zu erkennen und zu BlueXP Disaster Recovery hinzuzufügen.

Öffnen Sie die BlueXP -Konsole, und wählen Sie aus der linken Navigation **Schutz > Notfallwiederherstellung** aus. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü, Wählen Sie **Standorte > Hinzufügen > vCenter hinzufügen**.

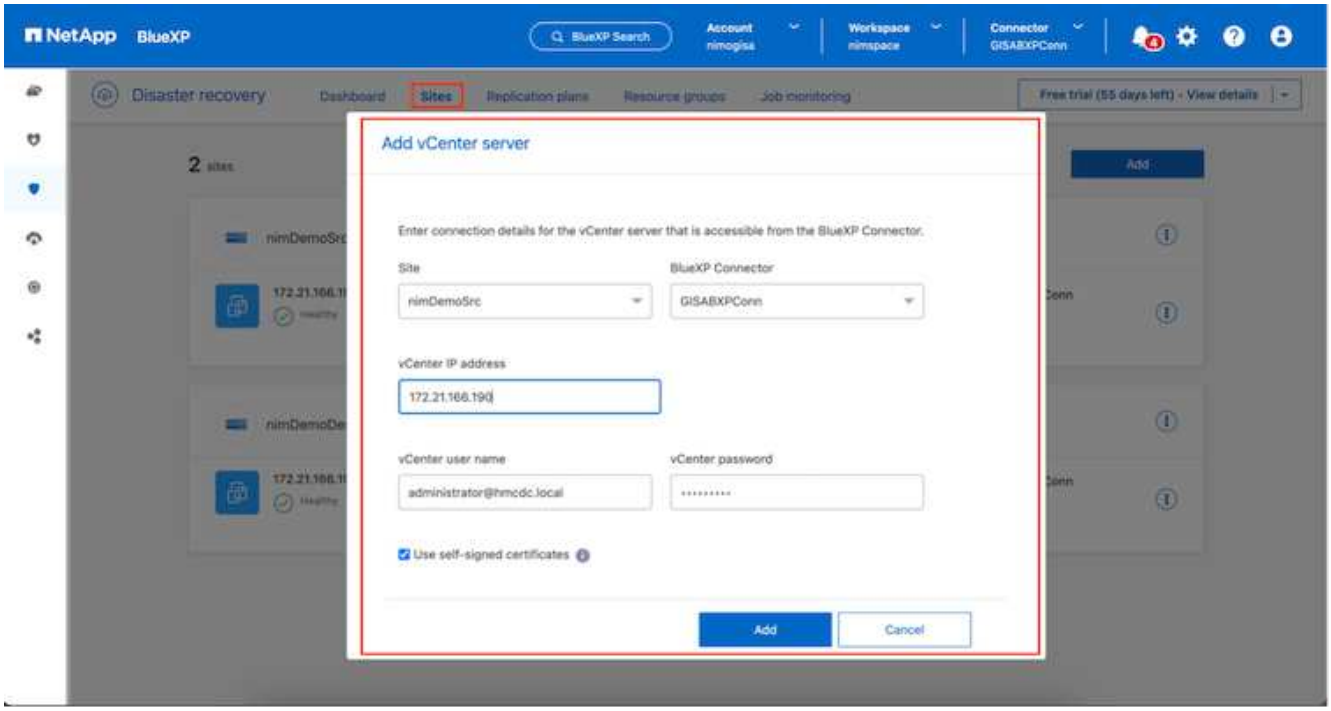


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle**. VCenter vor Ort.



- **Ziel**. VMC SDDC vCenter:



Sobald die vCenters hinzugefügt wurden, wird eine automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen dem Quell-Standort-Array und dem Ziel-Standort-Array

SnapMirror bietet Datenreplizierung in einer NetApp-Umgebung. Die SnapMirror-Replikation basiert auf NetApp Snapshot®-Technologie und ist äußerst effizient, da sie nur die Blöcke repliziert, die seit dem letzten Update geändert oder hinzugefügt wurden. SnapMirror lässt sich einfach über den NetApp OnCommand®

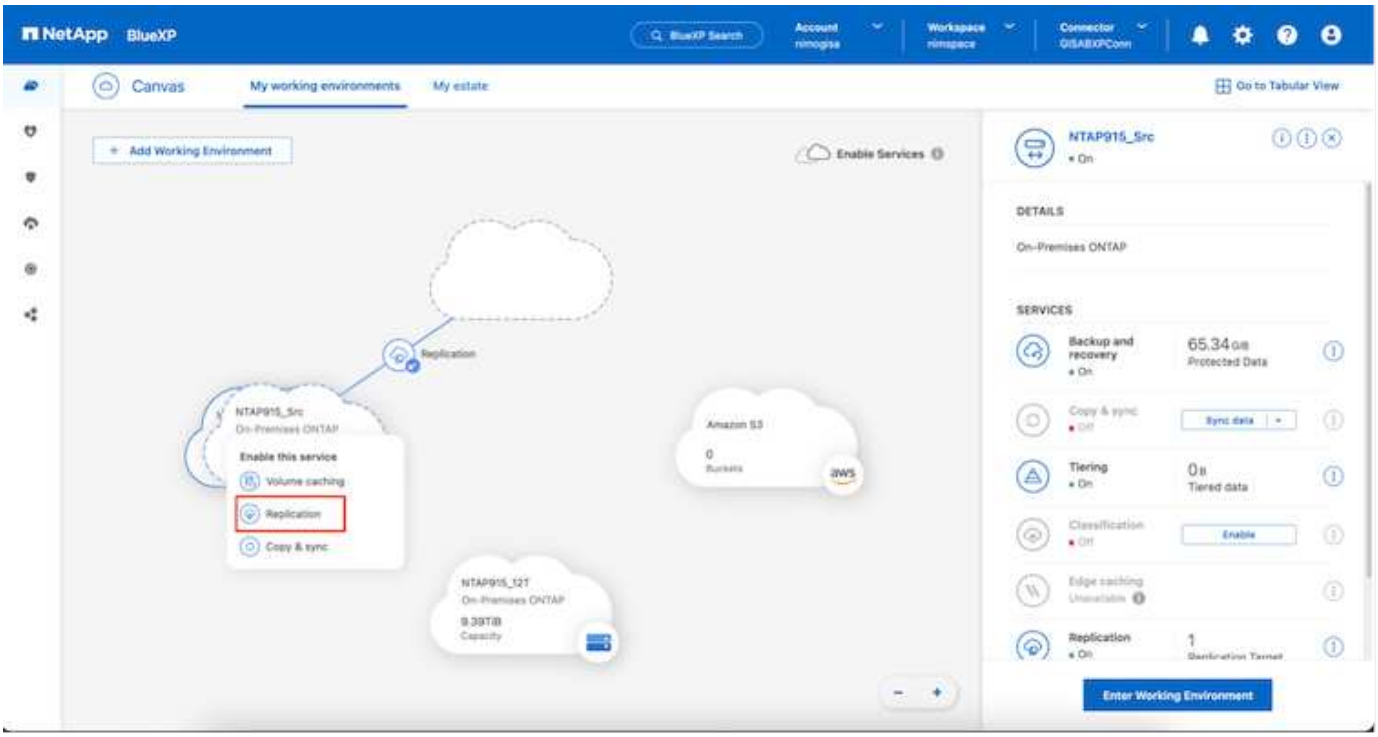
System Manager oder die ONTAP CLI konfigurieren. BlueXP DRaaS erstellt außerdem das über die SnapMirror-Beziehung bereitgestellte Cluster und SVM-Peering wird vorab konfiguriert.

In Fällen, in denen der primäre Storage nicht komplett verloren geht, bietet SnapMirror eine effiziente Möglichkeit zur Neusynchronisierung des primären und DR-Standorts. SnapMirror kann die beiden Standorte neu synchronisieren. Dabei werden nur die geänderten oder neuen Daten vom DR-Standort zum primären Standort übertragen, indem die SnapMirror Beziehungen einfach umgekehrt werden. Das bedeutet, dass Replikationspläne in BlueXP DRaaS nach einem Failover in beide Richtungen resynchronisiert werden können, ohne das gesamte Volume neu zu erstellen. Wenn eine Beziehung in umgekehrter Richtung neu synchronisiert wird, werden nur neue Daten zurück zum Ziel gesendet, die seit der letzten erfolgreichen Synchronisierung der Snapshot Kopie geschrieben wurden.

Wenn die SnapMirror-Beziehung bereits über CLI oder System Manager für das Volume konfiguriert ist, nimmt BlueXP DRaaS die Beziehung auf und fährt mit den restlichen Workflow-Operationen fort.

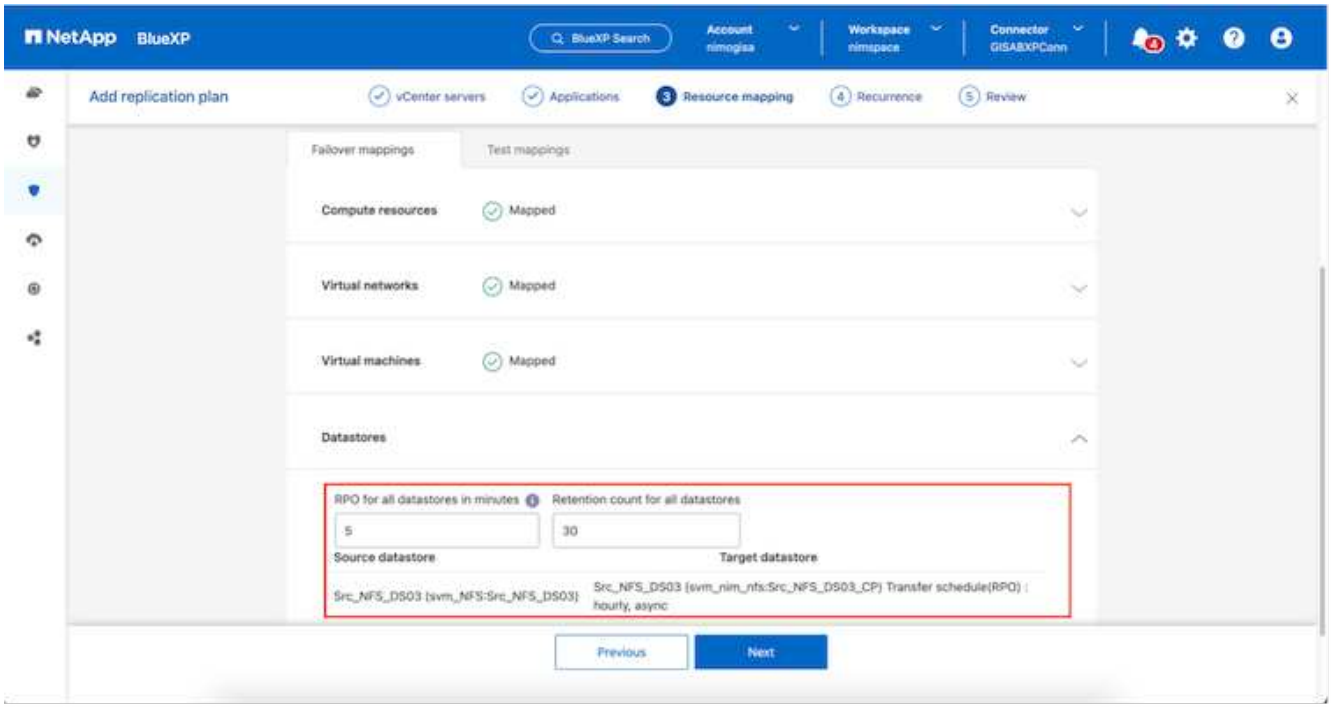
Wie Sie es für VMware Disaster Recovery einrichten

Der Prozess zur Erstellung der SnapMirror-Replizierung bleibt für jede Applikation unverändert. Der Prozess kann manuell oder automatisiert werden. Am einfachsten lässt sich BlueXP zur Konfiguration der SnapMirror Replizierung nutzen, indem das ONTAP Quell-System der Umgebung einfach per Drag & Drop auf das Ziel gezogen wird, um den Assistenten zu starten, der den Rest des Prozesses durchläuft.



Auch BlueXP DRaaS kann dasselbe automatisieren, wenn die folgenden beiden Kriterien erfüllt sind:

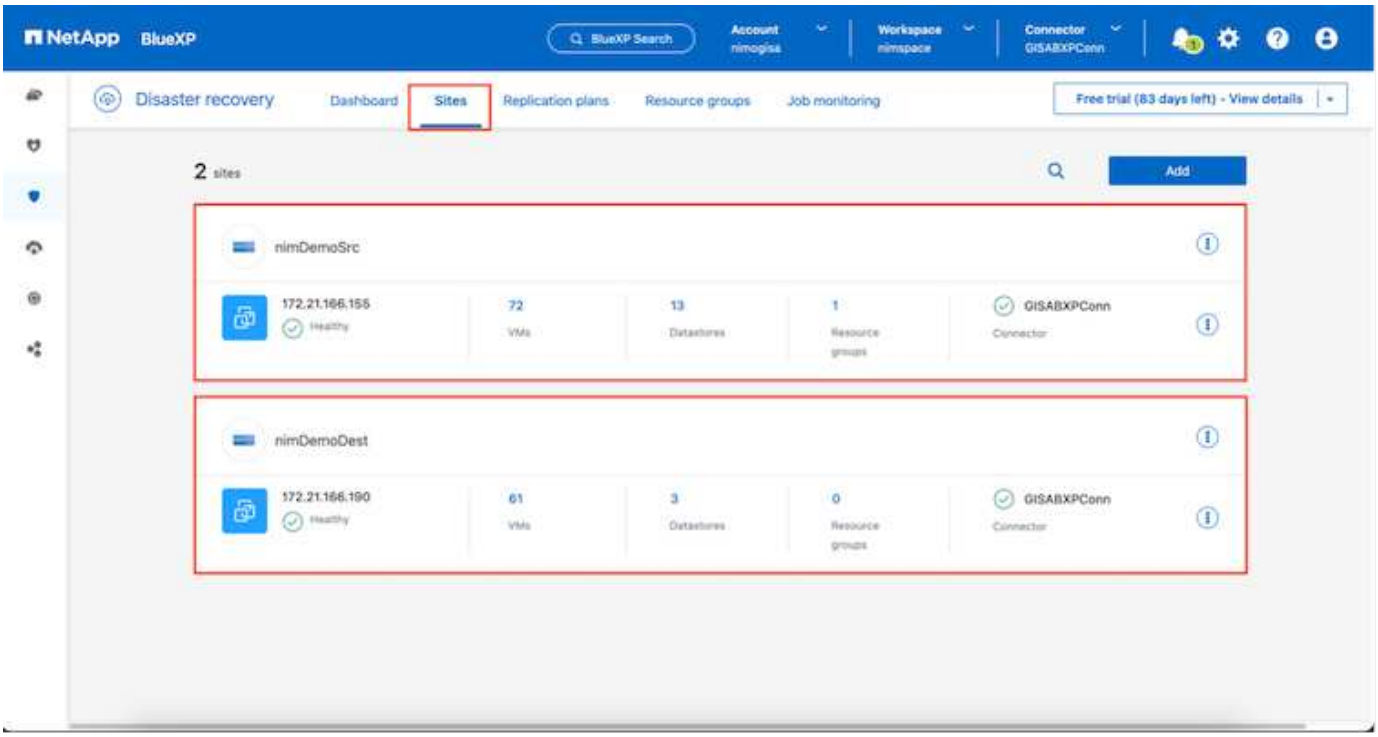
- Quell- und Ziel-Cluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



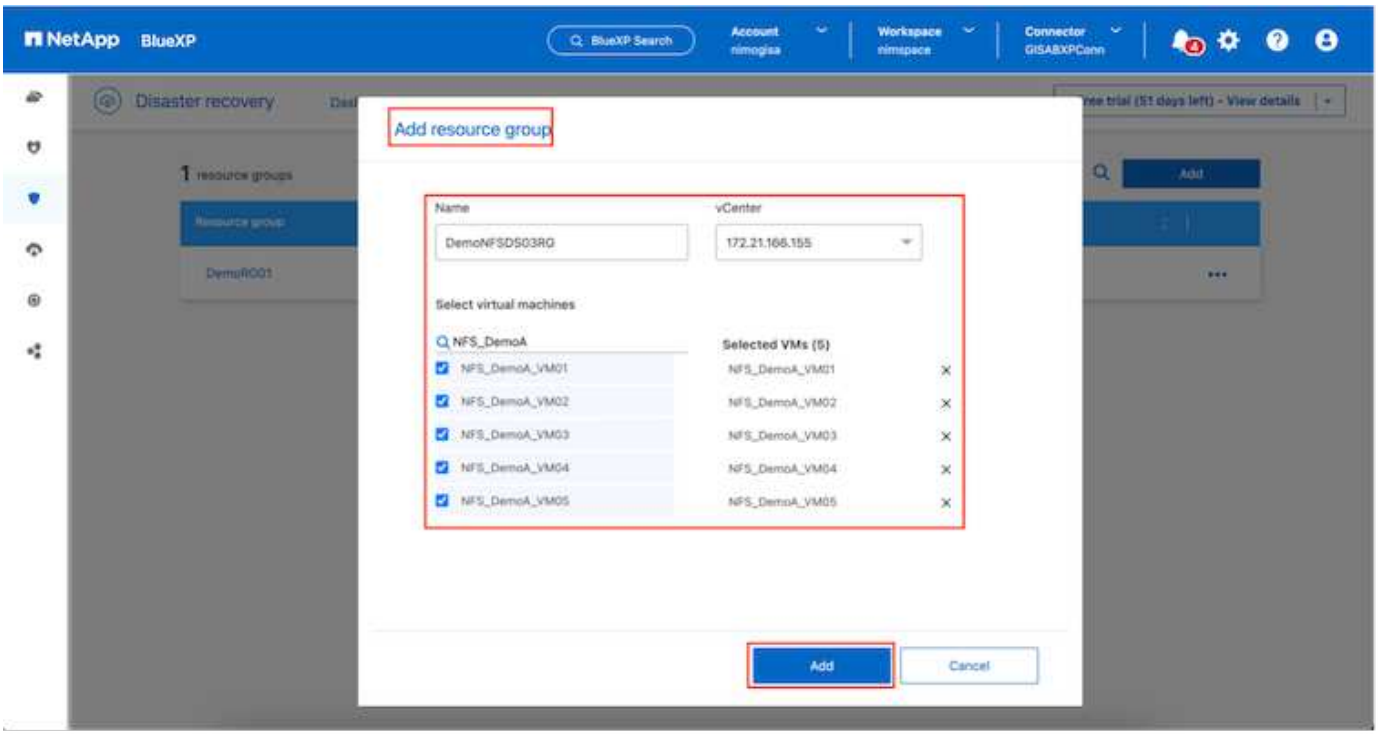
Wenn die SnapMirror-Beziehung bereits über CLI für das Volume konfiguriert ist, nimmt BlueXP DRaaS die Beziehung auf und fährt mit den restlichen Workflow-Operationen fort.

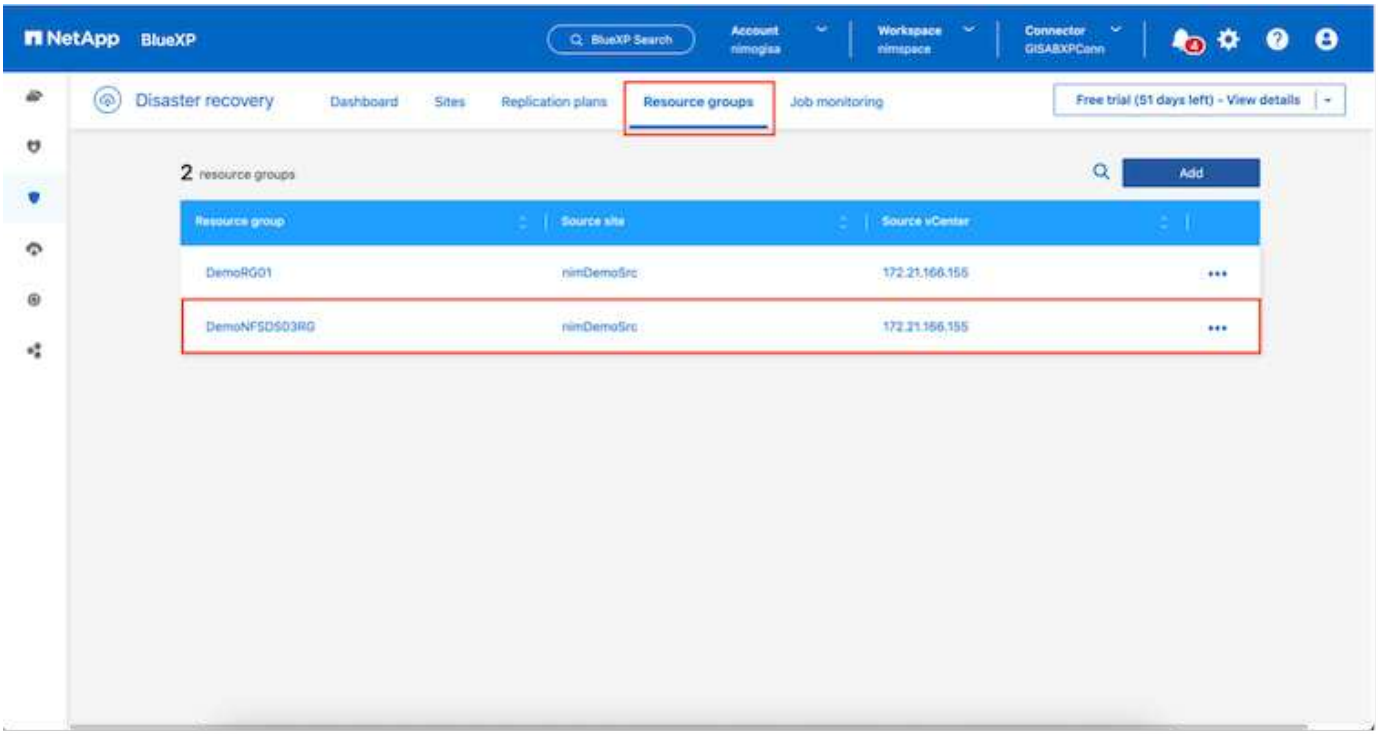
Welche Vorteile bietet BlueXP Disaster Recovery für Sie?

Nachdem die Quell- und Zielstandorte hinzugefügt wurden, führt die BlueXP Disaster Recovery automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. BlueXP Disaster Recovery erkennt auch automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt diese aus.



Nach dem Hinzufügen der Standorte können VMs zu Ressourcengruppen zusammengefasst werden. Mit den BlueXP Disaster Recovery-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logischen Gruppen gruppieren, die ihre Boot-Aufträge und Boot-Verzögerungen enthalten, die bei der Recovery ausgeführt werden können. Um Ressourcengruppen zu erstellen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.

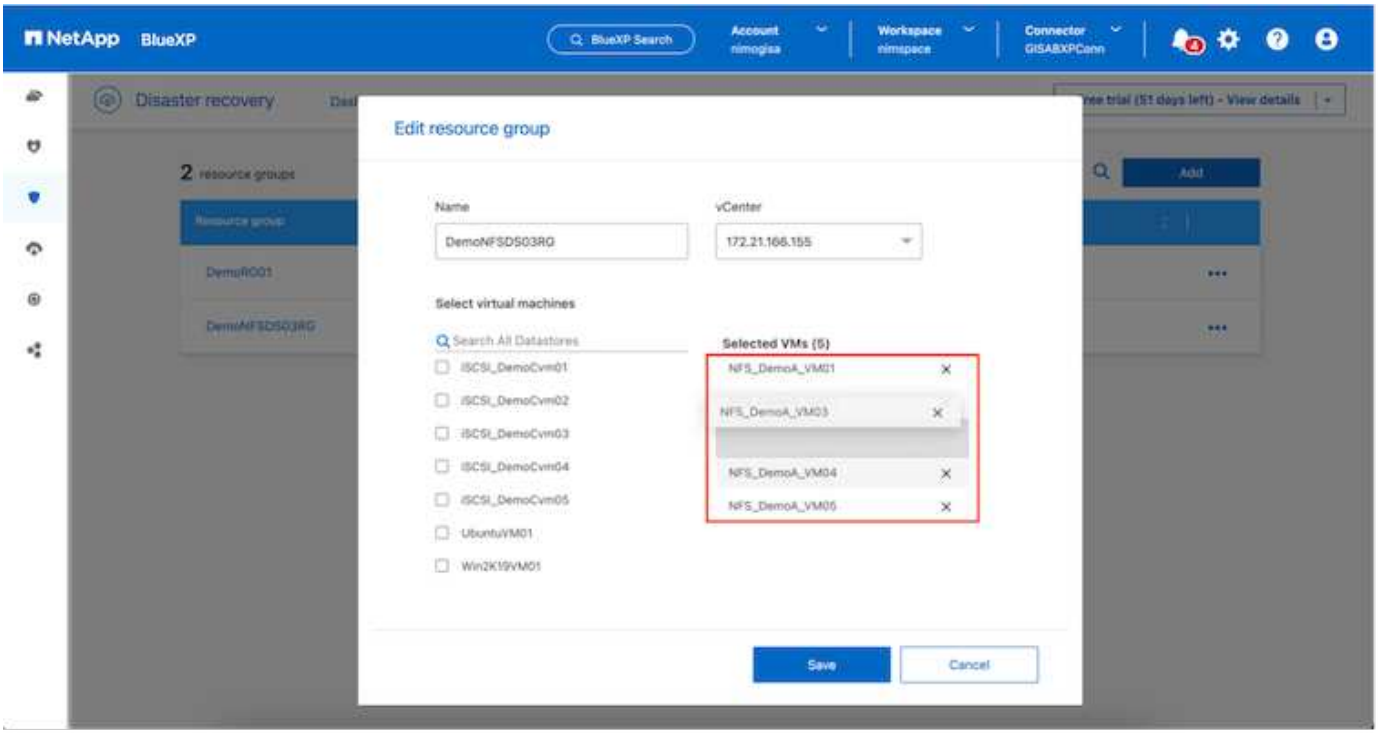




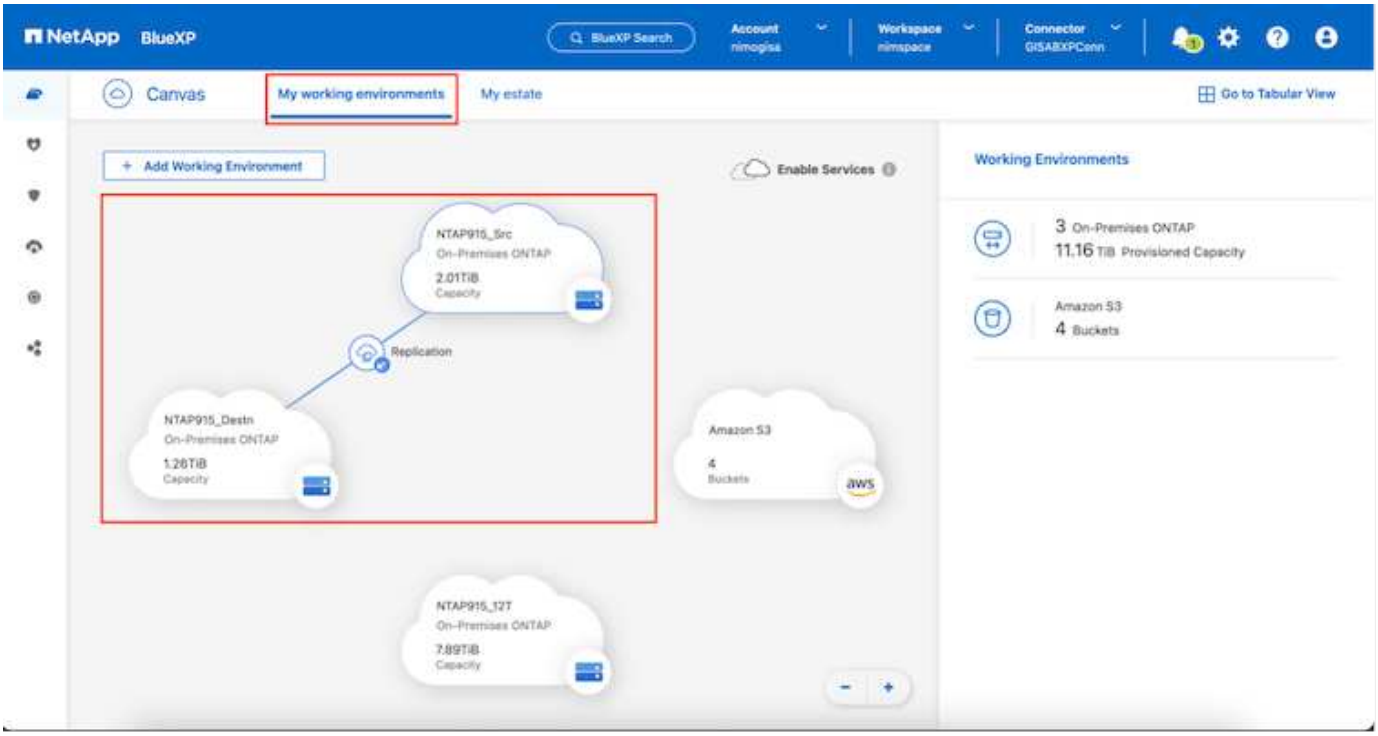
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

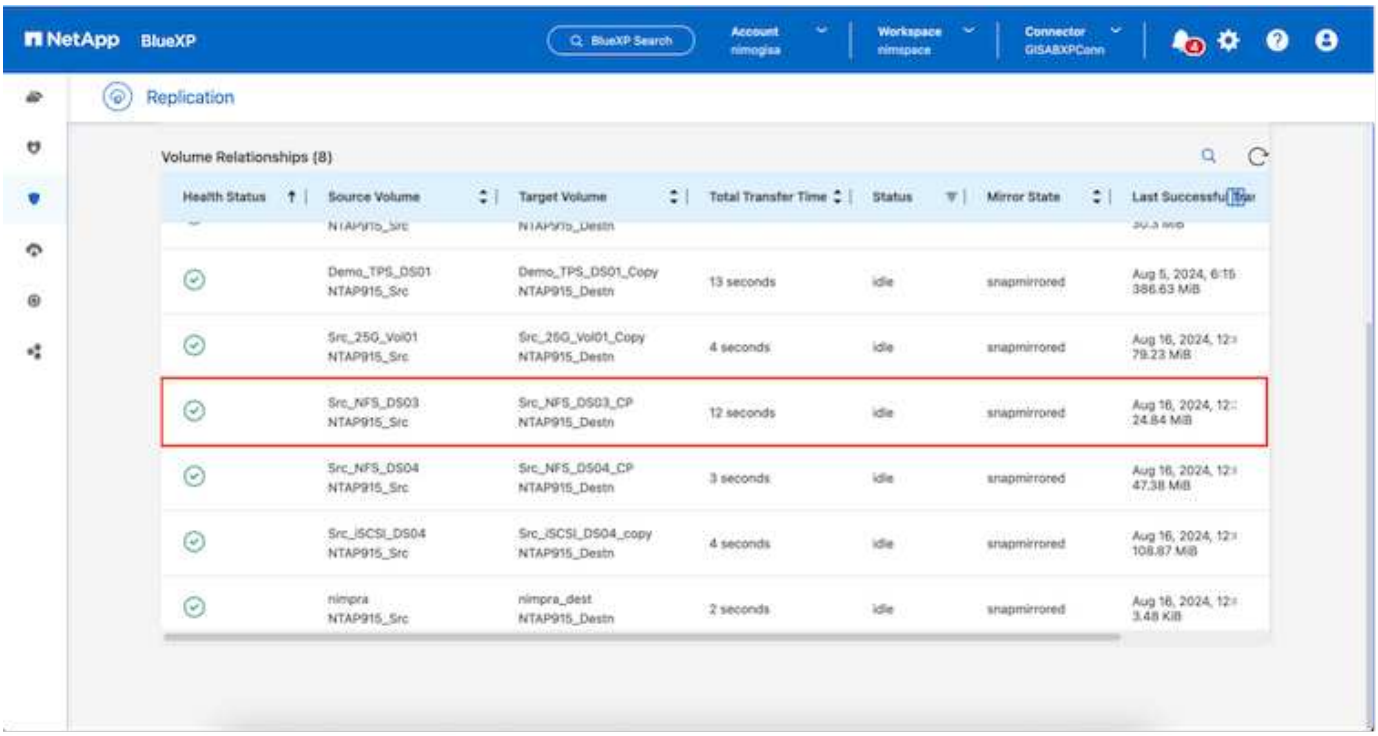
Die Boot-Reihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen

Drag-and-Drop-Mechanismus definiert oder geändert werden.



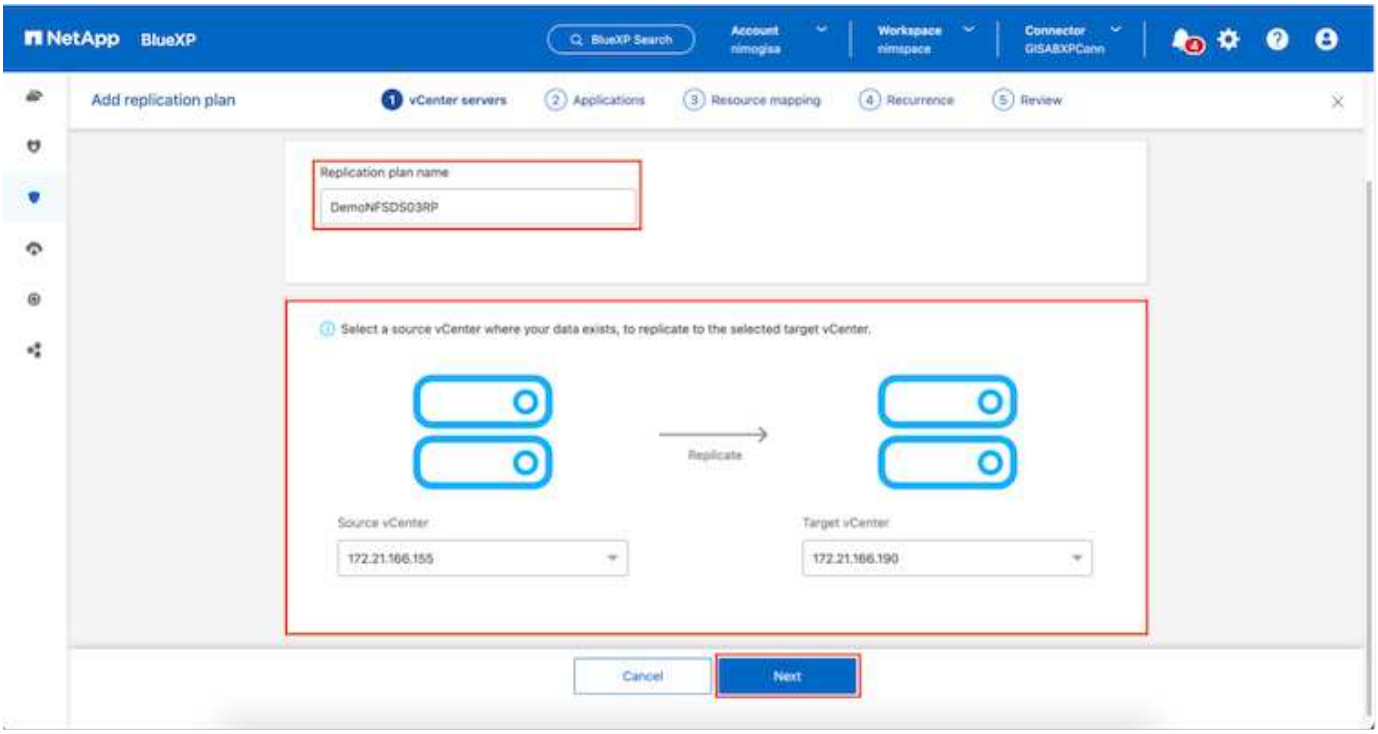
Nach der Erstellung der Ressourcengruppen erstellen Sie im nächsten Schritt einen Ausführungsentwurf oder einen Plan für die Wiederherstellung von virtuellen Maschinen und Anwendungen bei einem Notfall. Wie in den Voraussetzungen erwähnt, kann die SnapMirror-Replikation vorab konfiguriert werden, oder DRaaS kann sie mithilfe der RPO und der Aufbewahrungszahl konfigurieren, die während der Erstellung des Replikationsplans angegeben wurde.





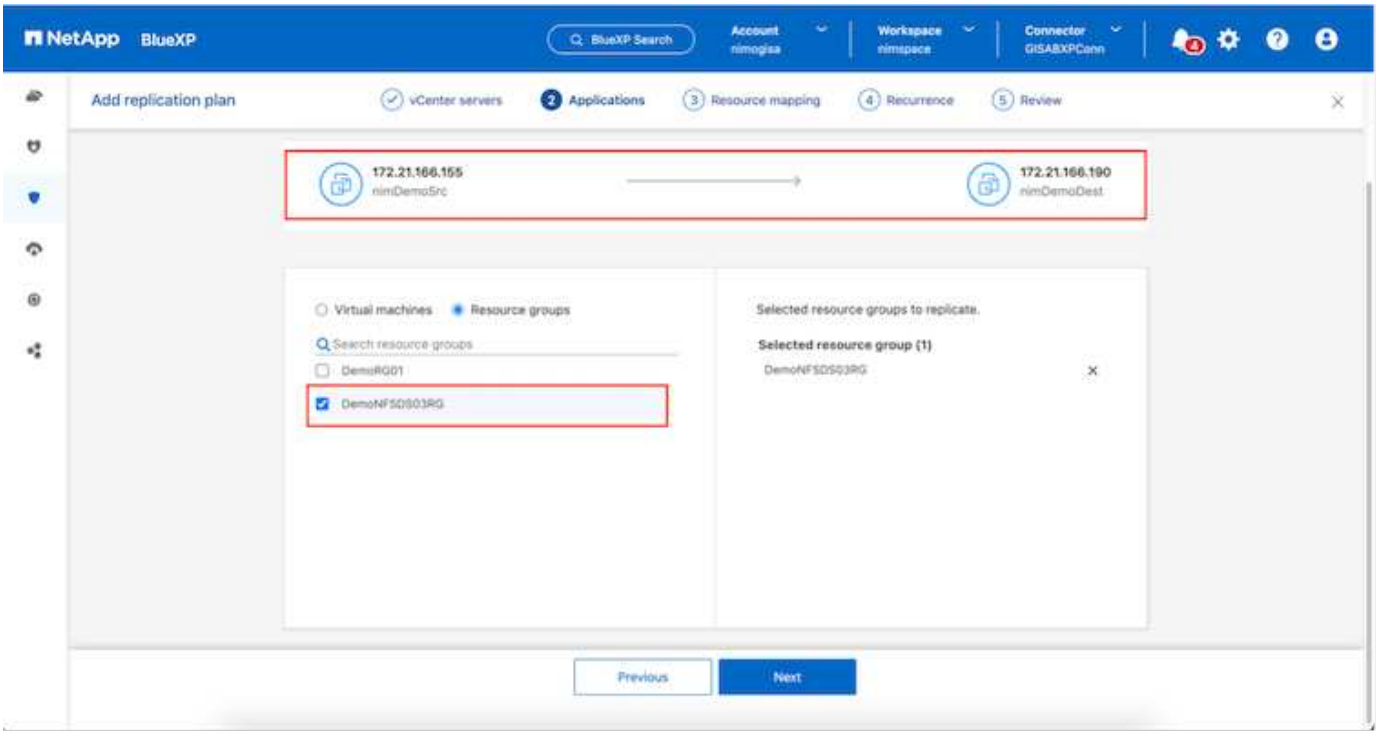
Konfigurieren Sie den Replizierungsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus dem Dropdown auswählen und die Ressourcengruppen auswählen, die in den Plan einbezogen werden sollen, sowie die Gruppierung der Art und Weise, wie Applikationen wiederhergestellt und eingeschaltet werden sollen, sowie die Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

Wählen Sie zunächst das Quell-vCenter aus und dann das Ziel-vCenter aus.



Im nächsten Schritt wählen Sie vorhandene Ressourcengruppen aus. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent, die erforderlichen virtuellen Maschinen zu gruppieren (im Grunde erstellen Sie

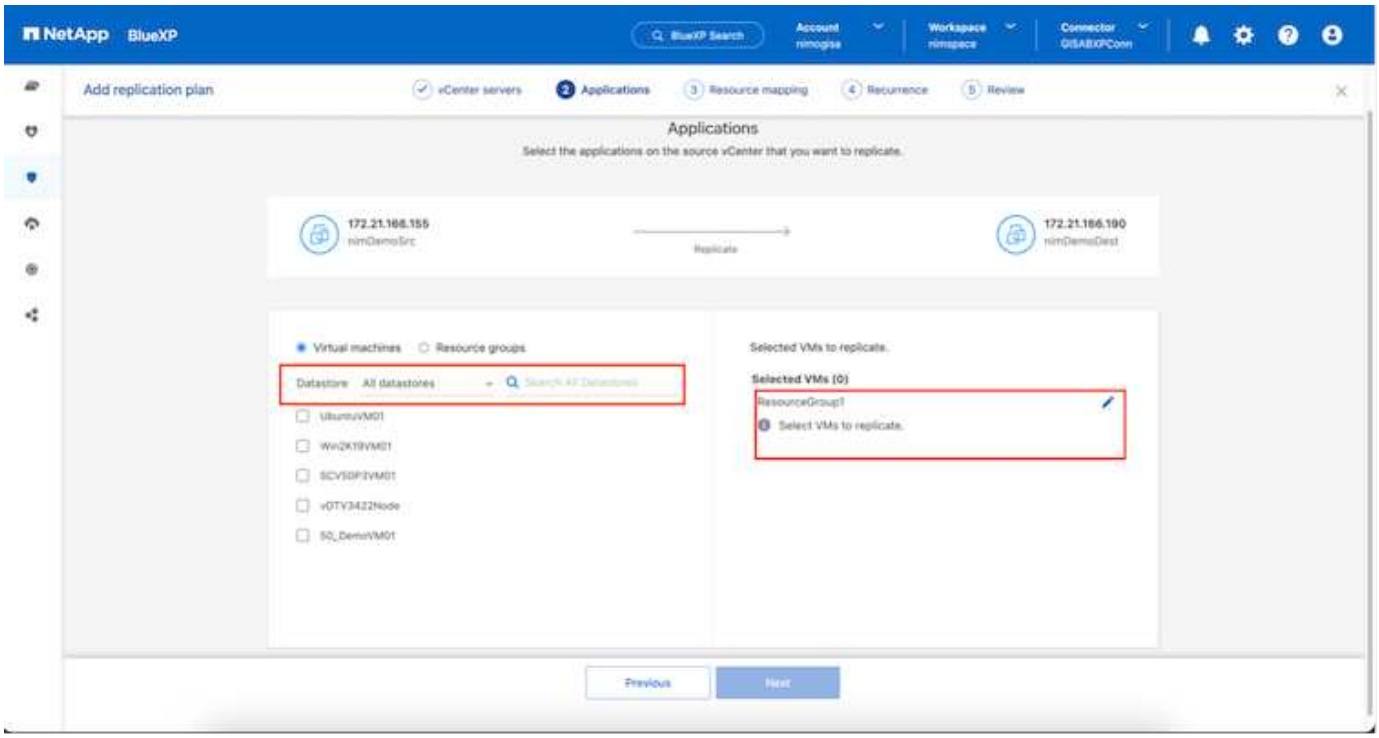
funktionale Ressourcengruppen) auf der Grundlage der Wiederherstellungsziele. Dies hilft auch dabei, die Reihenfolge der Wiederherstellung von virtuellen Maschinen der Anwendung festzulegen.



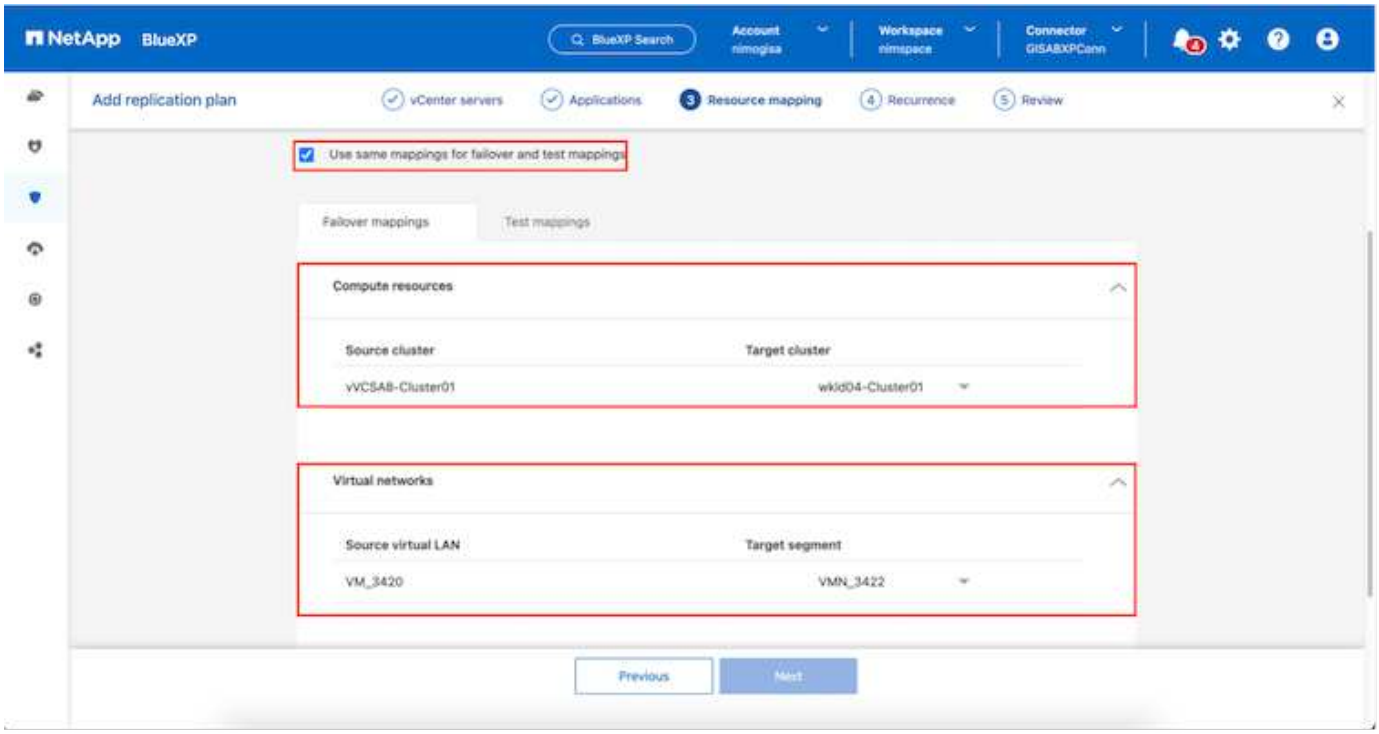
Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge mithilfe der Drag-and-Drop-Funktion. Damit kann die Reihenfolge, in der die VMs während des Recovery-Prozesses eingeschaltet werden, leicht geändert werden.

Jede virtuelle Maschine in einer Ressourcengruppe wird in der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

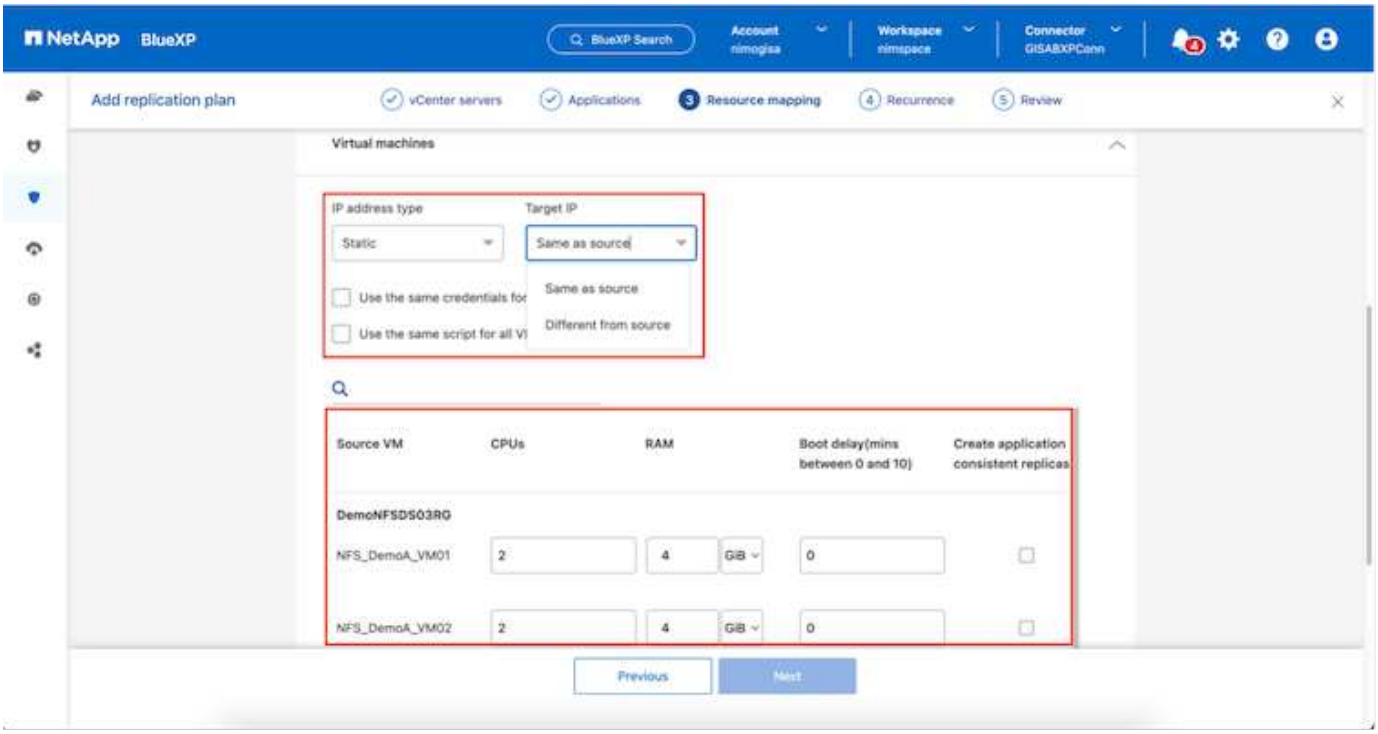
Der Screenshot unten zeigt die Option zum Filtern virtueller Maschinen oder spezieller Datastores nach Unternehmensanforderungen, wenn Ressourcengruppen nicht vorab erstellt werden.



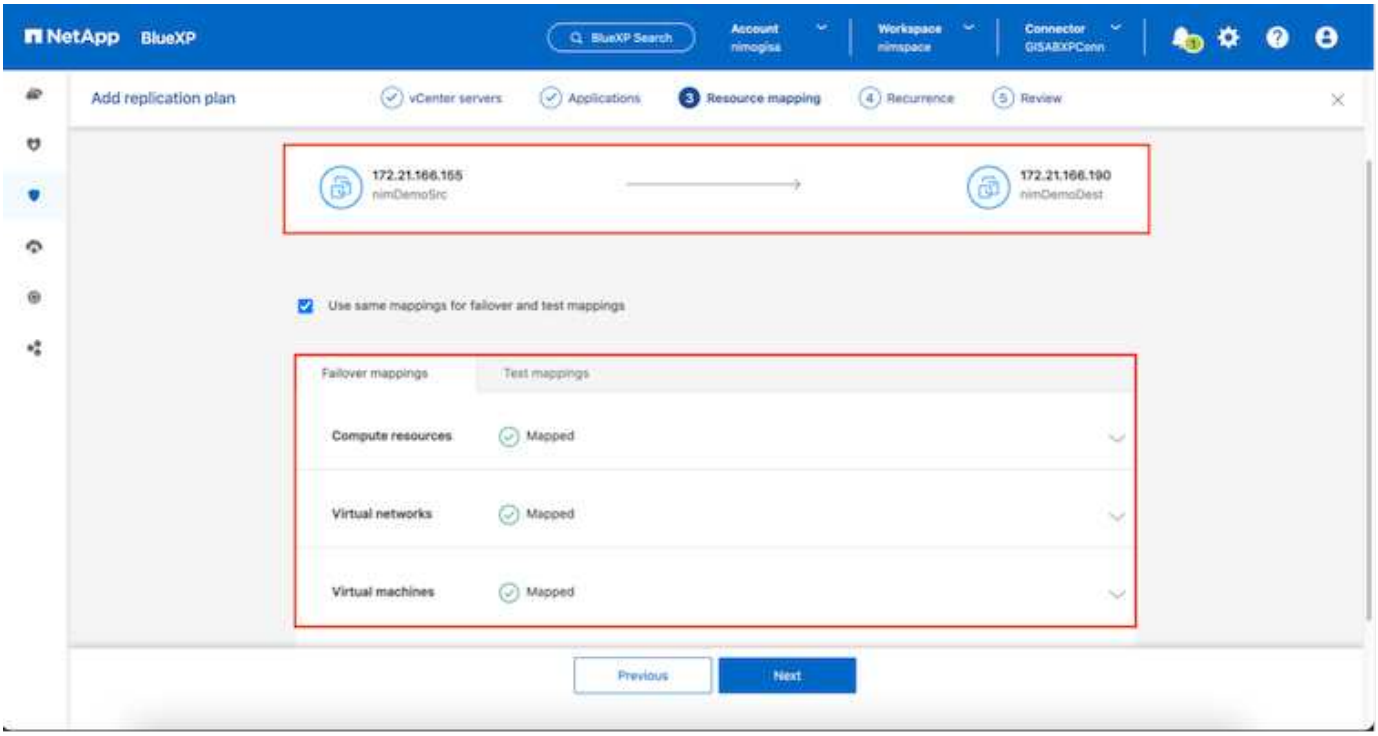
Sobald die Ressourcengruppen ausgewählt sind, erstellen Sie die Failover-Zuordnungen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen, virtuelle Netzwerke. IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Applikationskonsistenz usw. Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".



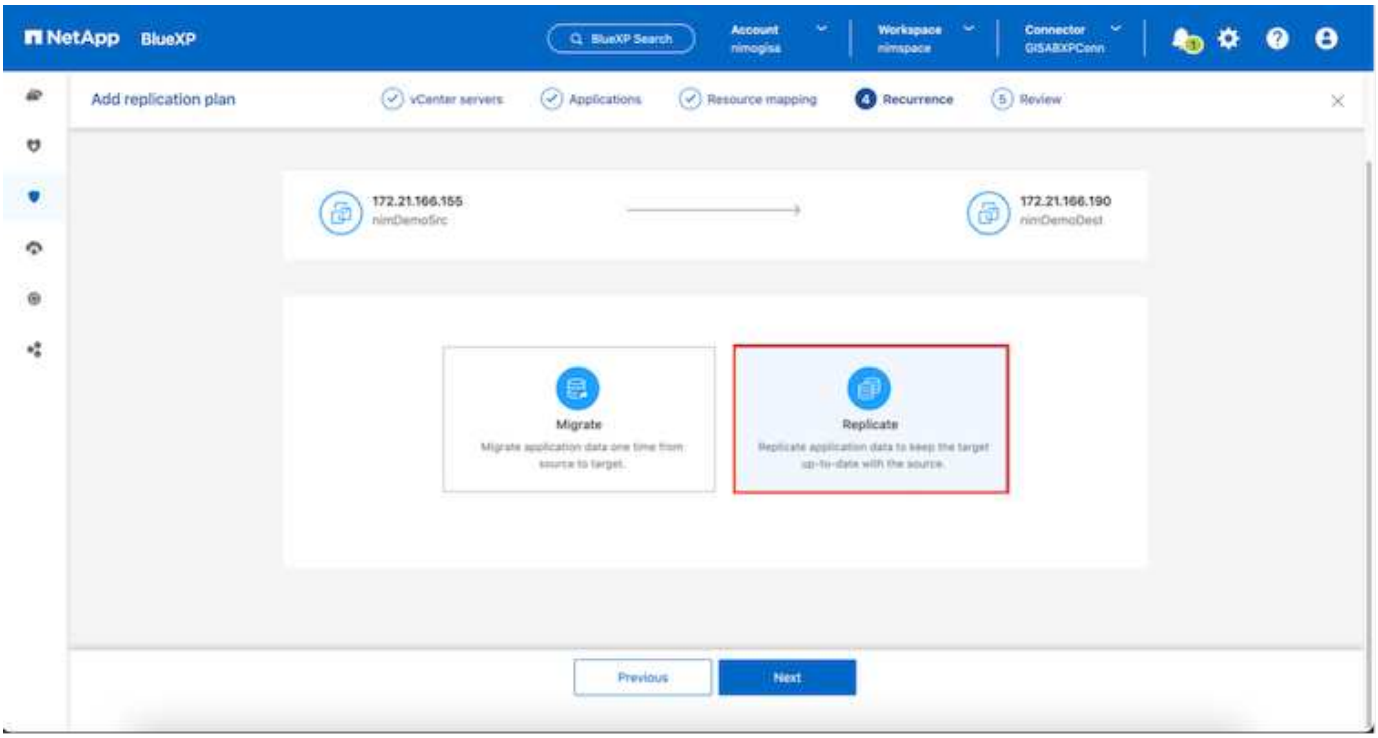
Standardmäßig werden für Test- und Failover-Vorgänge dieselben Zuordnungsparameter verwendet. Um unterschiedliche Zuordnungen für die Testumgebung festzulegen, aktivieren Sie die Option Testzuordnung, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:



Klicken Sie nach Abschluss der Ressourcenzuordnung auf Weiter.

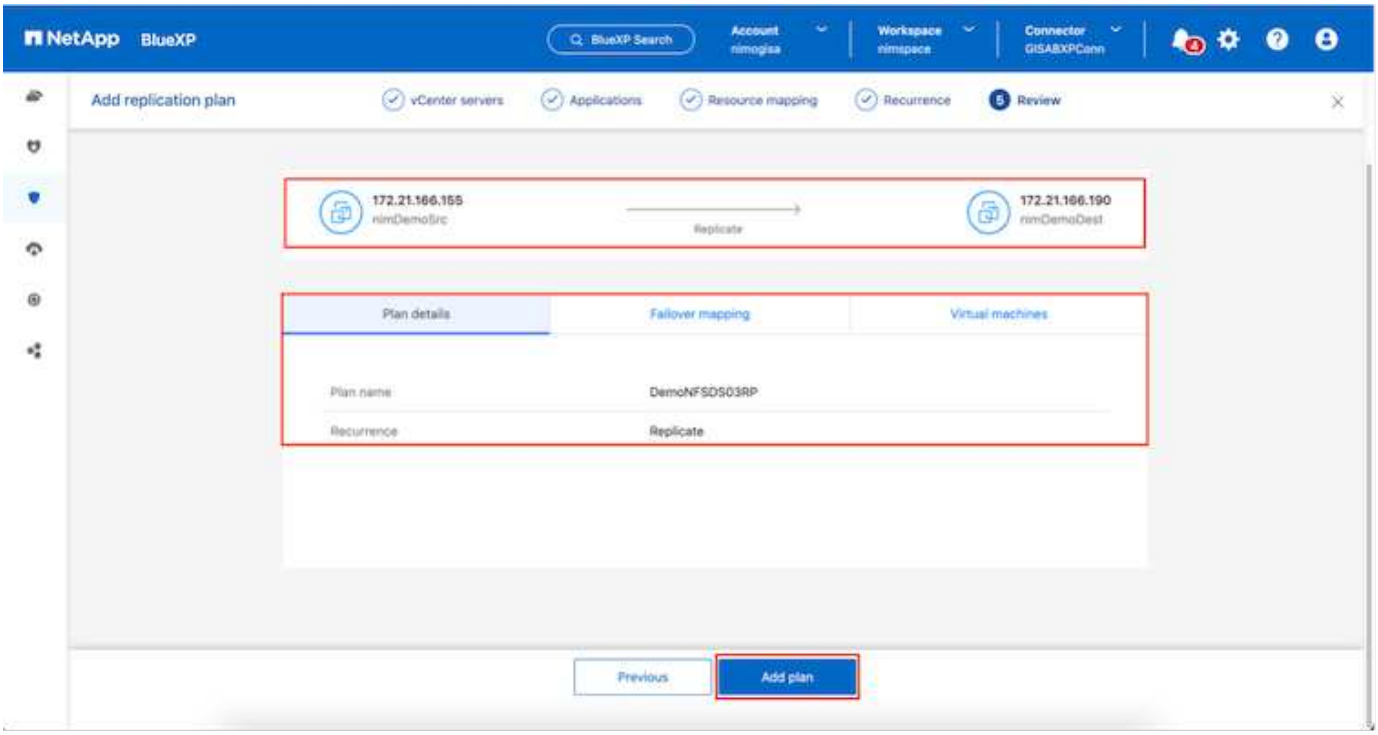


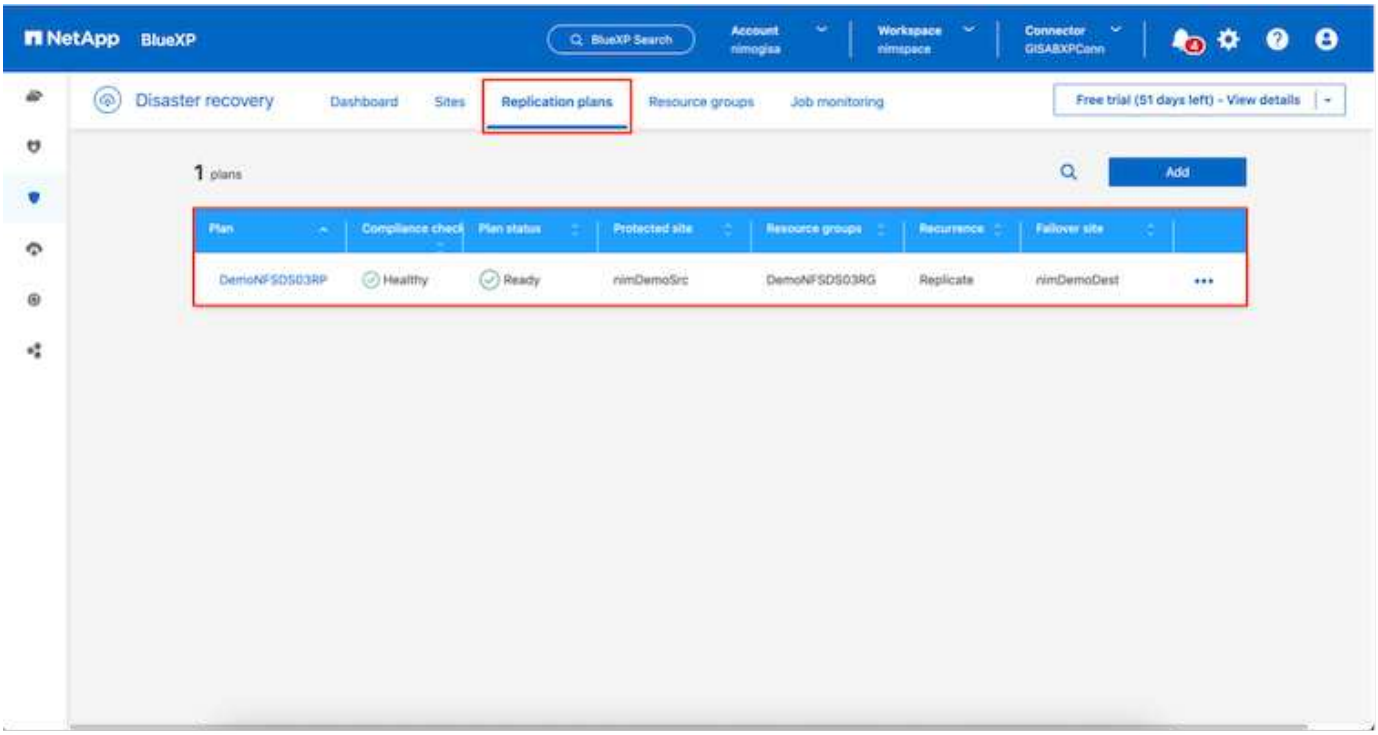
Wählen Sie den Wiederholungstyp aus. In einfachen Worten: Wählen Sie Migrate (einmalige Migration mit Failover) oder die Option wiederkehrende kontinuierliche Replikation aus. In dieser Übersicht ist die Option „Replikat“ ausgewählt.



Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf **Plan hinzufügen**.

VMs von verschiedenen Volumes und SVMs können in einem Replizierungsplan enthalten sein. Abhängig von der VM-Platzierung (ob auf demselben Volume oder separaten Volumes innerhalb derselben SVM, separaten Volumes auf unterschiedlichen SVMs) erstellt das Disaster Recovery von BlueXP einen Snapshot einer Konsistenzgruppe.



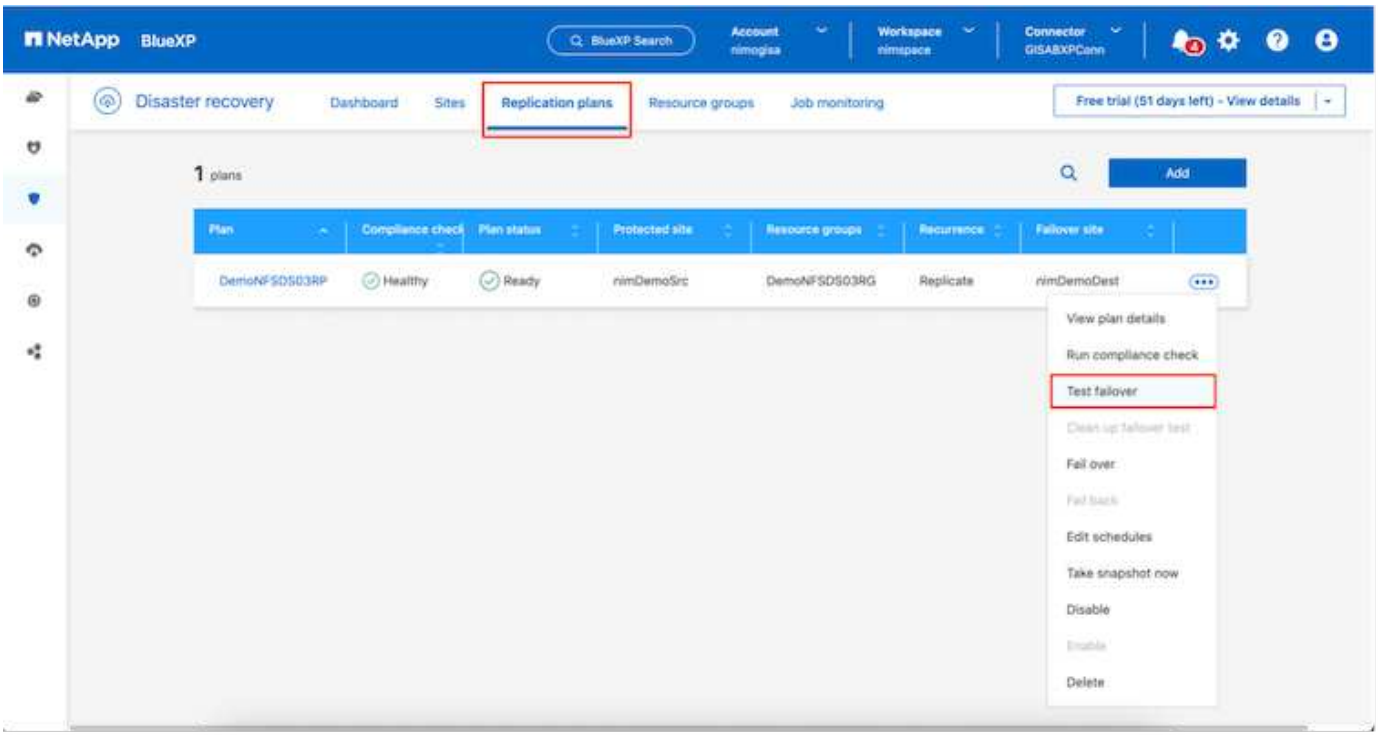


BlueXP DRaaS besteht aus den folgenden Workflows:

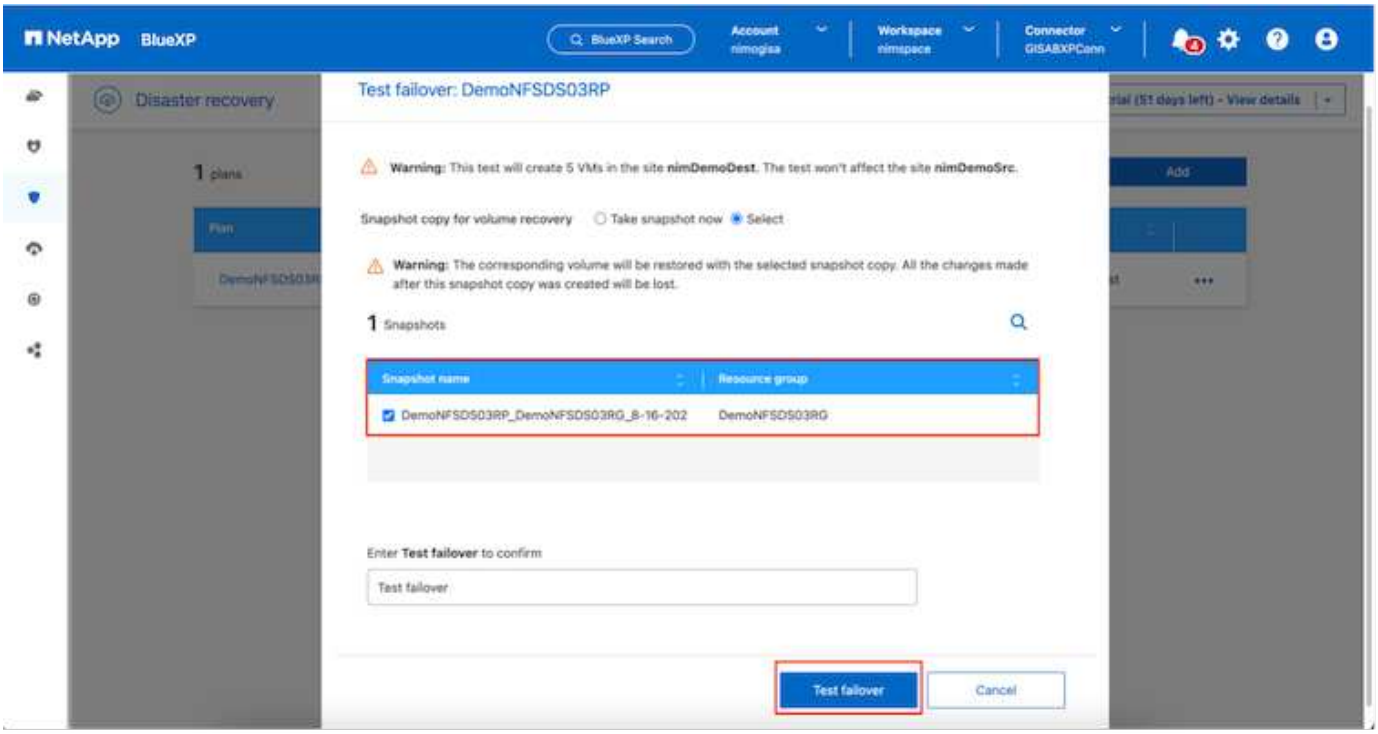
- Testen von Failover (einschließlich regelmäßiger, automatisierter Simulationen)
- Failover-Test bereinigen
- Failover
- Failback

Testen Sie den Failover

Test-Failover in BlueXP DRaaS ist ein operatives Verfahren, mit dem VMware Administratoren ihre Recovery-Pläne vollständig validieren können, ohne ihre Produktionsumgebungen zu unterbrechen.



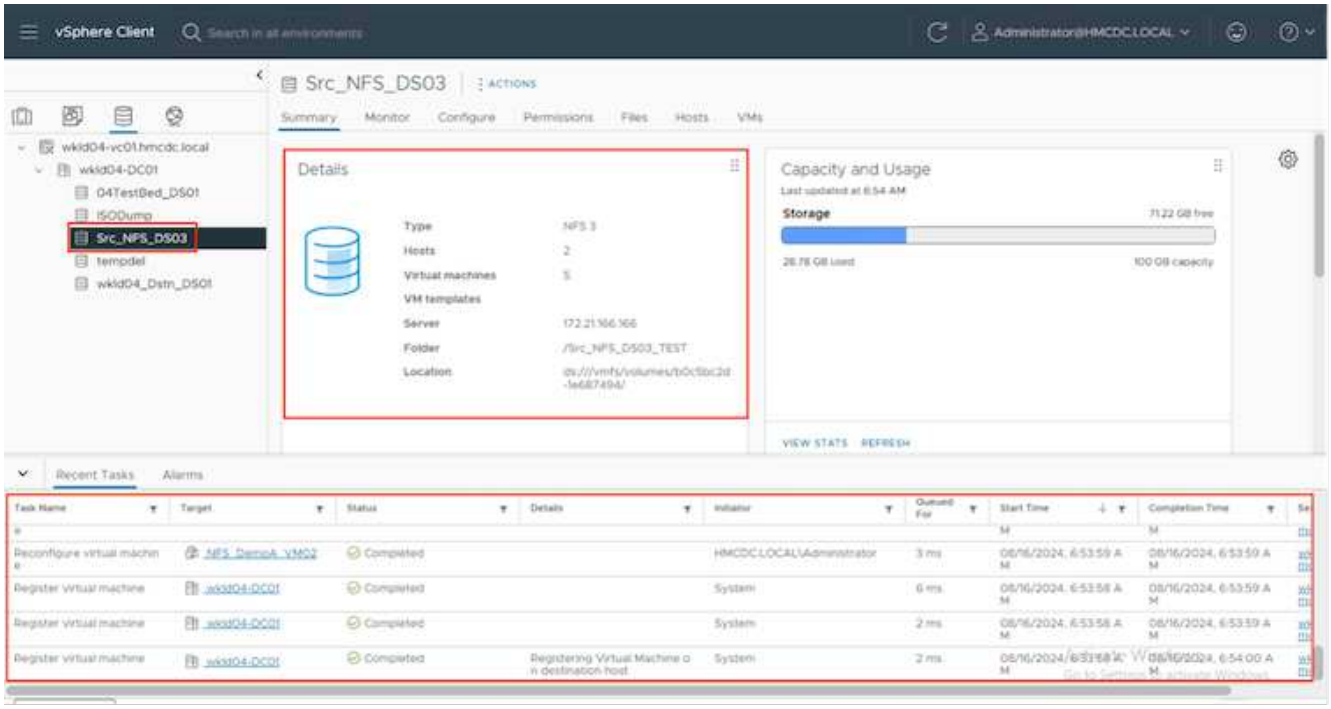
BlueXP DRaaS umfasst die Möglichkeit, den Snapshot als optionale Funktion im Test-Failover-Vorgang auszuwählen. Mit dieser Funktion kann der VMware Administrator überprüfen, ob alle kürzlich in der Umgebung vorgenommenen Änderungen am Zielstandort repliziert und somit während des Tests vorhanden sind. Zu diesen Änderungen gehören auch Patches für das VM-Gastbetriebssystem



Wenn der VMware-Administrator einen Test-Failover ausführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

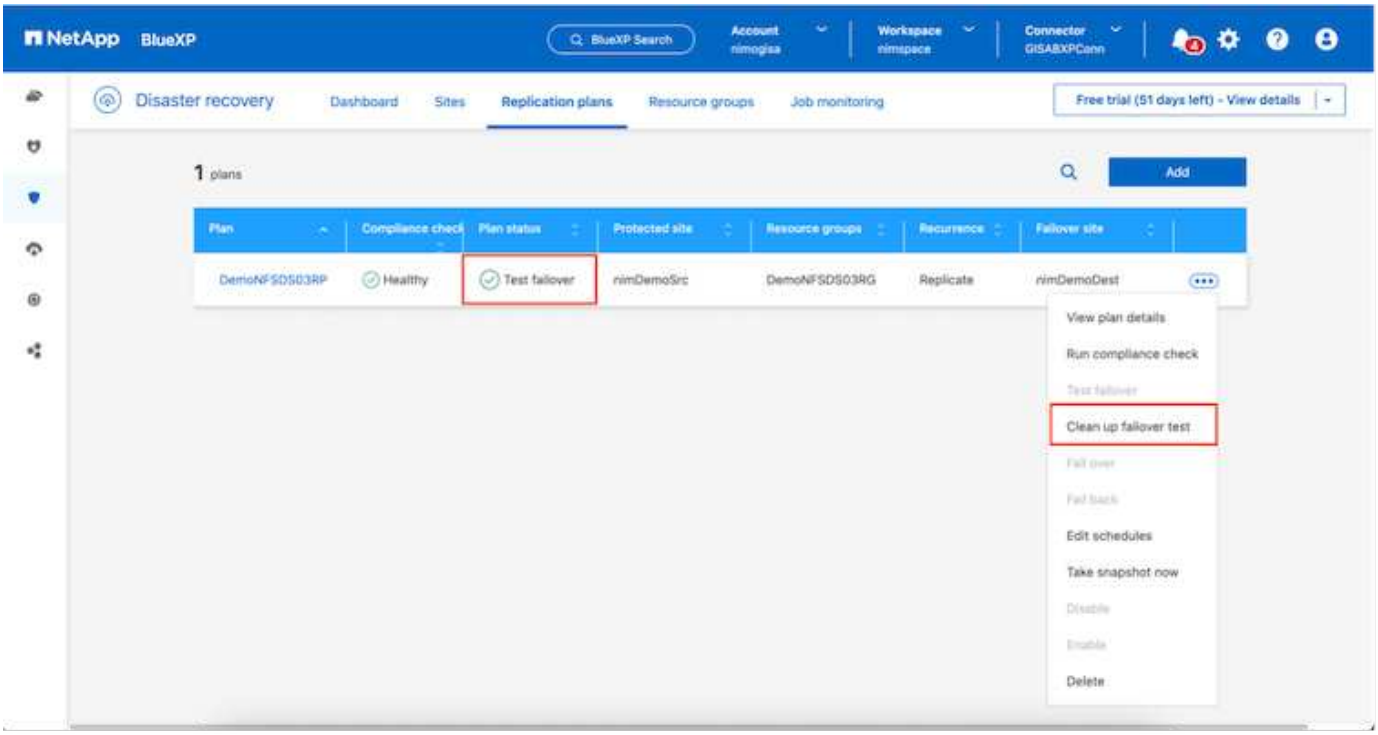
- Auslösung von SnapMirror-Beziehungen zur Aktualisierung des Speichers am Zielstandort auf kürzlich am Produktionsstandort vorgenommene Änderungen

- Erstellen von NetApp FlexClone Volumes der FlexVol Volumes auf dem DR-Storage-Array.
- Verbinden der NFS-Datastores in den FlexClone-Volumes mit den ESXi-Hosts am DR-Standort.
- Verbinden der VM-Netzwerkadapter mit dem während der Zuordnung angegebenen Testnetzwerk.
- Neukonfigurieren der Netzwerkeinstellungen des VM-Gastbetriebssystems, wie für das Netzwerk am DR-Standort definiert.
- Ausführen von benutzerdefinierten Befehlen, die im Replizierungsplan gespeichert wurden.
- Einschalten der VMs in der im Replizierungsplan definierten Reihenfolge



Bereinigen Sie den Failover-Testvorgang

Der Bereinigungstest für das Failover findet statt, nachdem der Test des Replikationsplans abgeschlossen wurde, und der VMware-Administrator reagiert auf die Bereinigungsaufforderung.



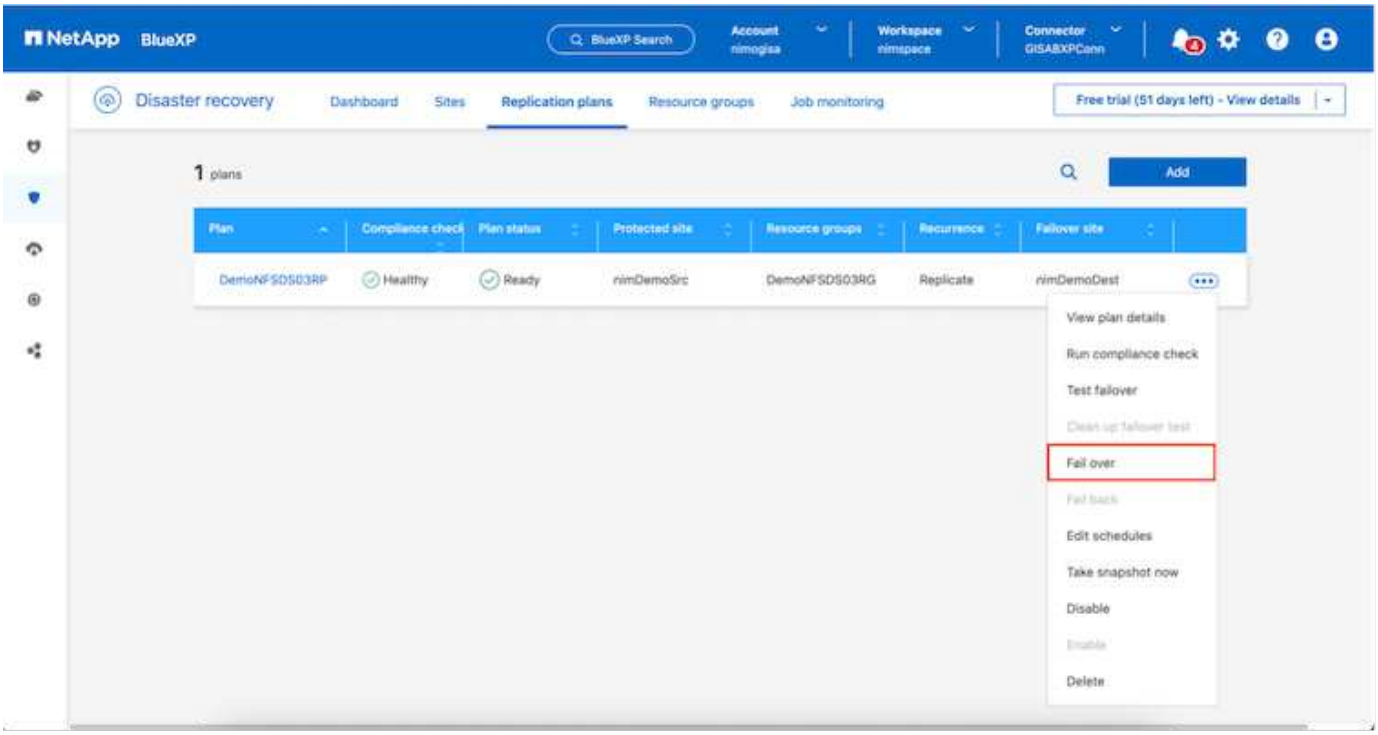
Durch diese Aktion werden die virtuellen Maschinen (VMs) und der Status des Replikationsplans auf den Bereitschaftszustand zurückgesetzt.

Wenn der VMware-Administrator einen Recovery-Vorgang durchführt, führt BlueXP DRaaS den folgenden Prozess aus:

1. Er schaltet jede wiederhergestellte VM in der FlexClone-Kopie, die für Tests verwendet wurde, ab.
2. Es löscht das FlexClone Volume, das verwendet wurde, um die wiederhergestellten VMs während des Tests darzustellen.

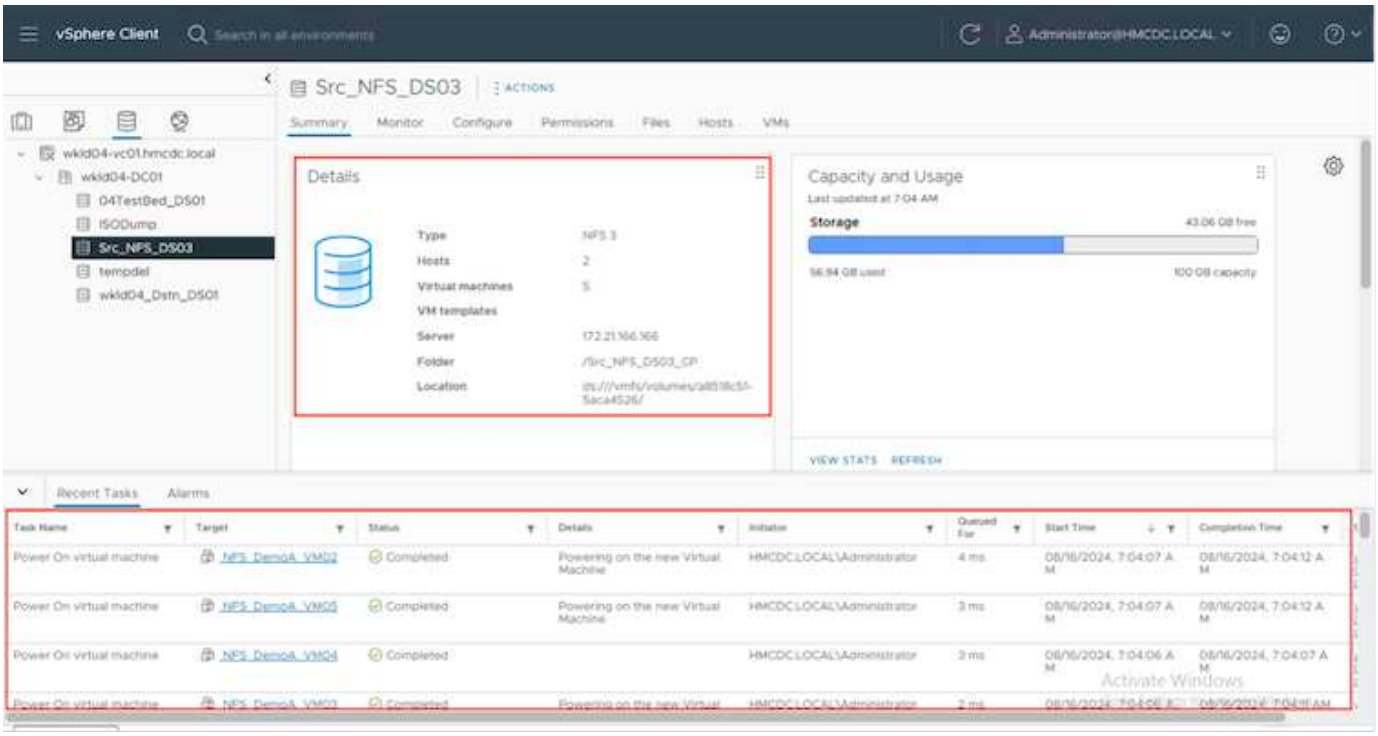
Geplante Migration und Failover

BlueXP DRaaS bietet zwei Methoden zur Durchführung eines echten Failover: Geplante Migration und Failover. Die erste Methode, die geplante Migration, umfasst die Synchronisierung von VM Shutdown und Storage-Replizierung in den Prozess, um die VMs wiederherzustellen oder effektiv zum Zielstandort zu verschieben. Für die geplante Migration ist der Zugriff auf den Quellstandort erforderlich. Die zweite Methode, Failover, ist ein geplantes/ungeplantes Failover, bei dem die VMs vom letzten Storage-Replizierungsintervall, das abgeschlossen werden konnte, am Zielstandort wiederhergestellt werden. Abhängig von dem RPO, der in die Lösung integriert wurde, kann im DR-Szenario ein gewisser Datenverlust erwartet werden.



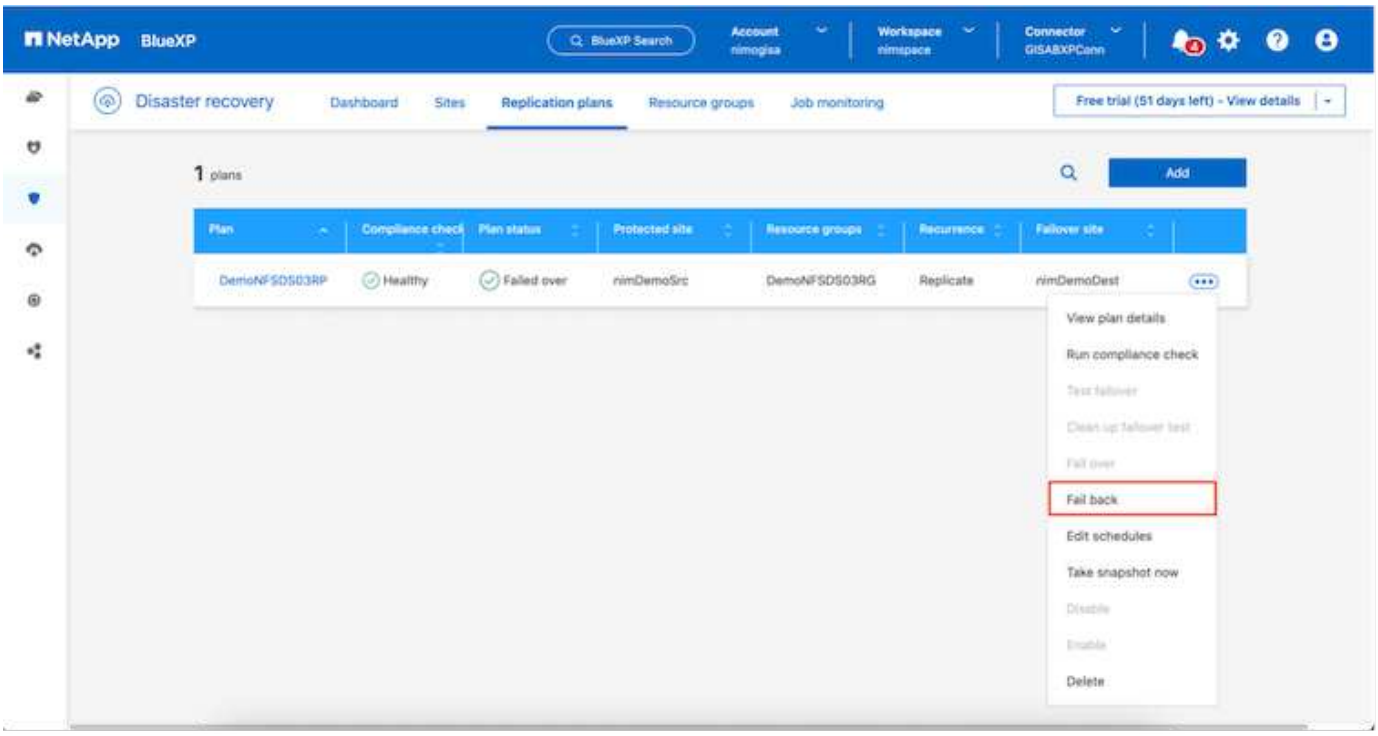
Wenn der VMware-Administrator einen Failover durchführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

- Trennung und Failover der NetApp SnapMirror Beziehungen
- Verbinden Sie die replizierten NFS-Datastores mit den ESXi-Hosts am DR-Standort.
- Verbinden Sie die VM-Netzwerkadapter mit dem entsprechenden Netzwerk des Zielstandorts.
- Konfigurieren Sie die Netzwerkeinstellungen des VM-Gastbetriebssystems wie für das Netzwerk am Zielstandort definiert neu.
- Führen Sie alle benutzerdefinierten Befehle (falls vorhanden) aus, die im Replizierungsplan gespeichert wurden.
- Schalten Sie die VMs in der im Replizierungsplan definierten Reihenfolge ein.



Failback

Ein Failback ist ein optionales Verfahren, das die ursprüngliche Konfiguration der Quell- und Zielstandorte nach einer Wiederherstellung wiederherstellt.



VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie Services am ursprünglichen Quellstandort wiederherstellen möchten.

HINWEIS: BlueXP DRaaS repliziert (resynchronisiert) alle Änderungen zurück auf die ursprüngliche virtuelle Quellmaschine, bevor die Replikationsrichtung umkehrt. Dieser Prozess beginnt mit einer Beziehung, die das

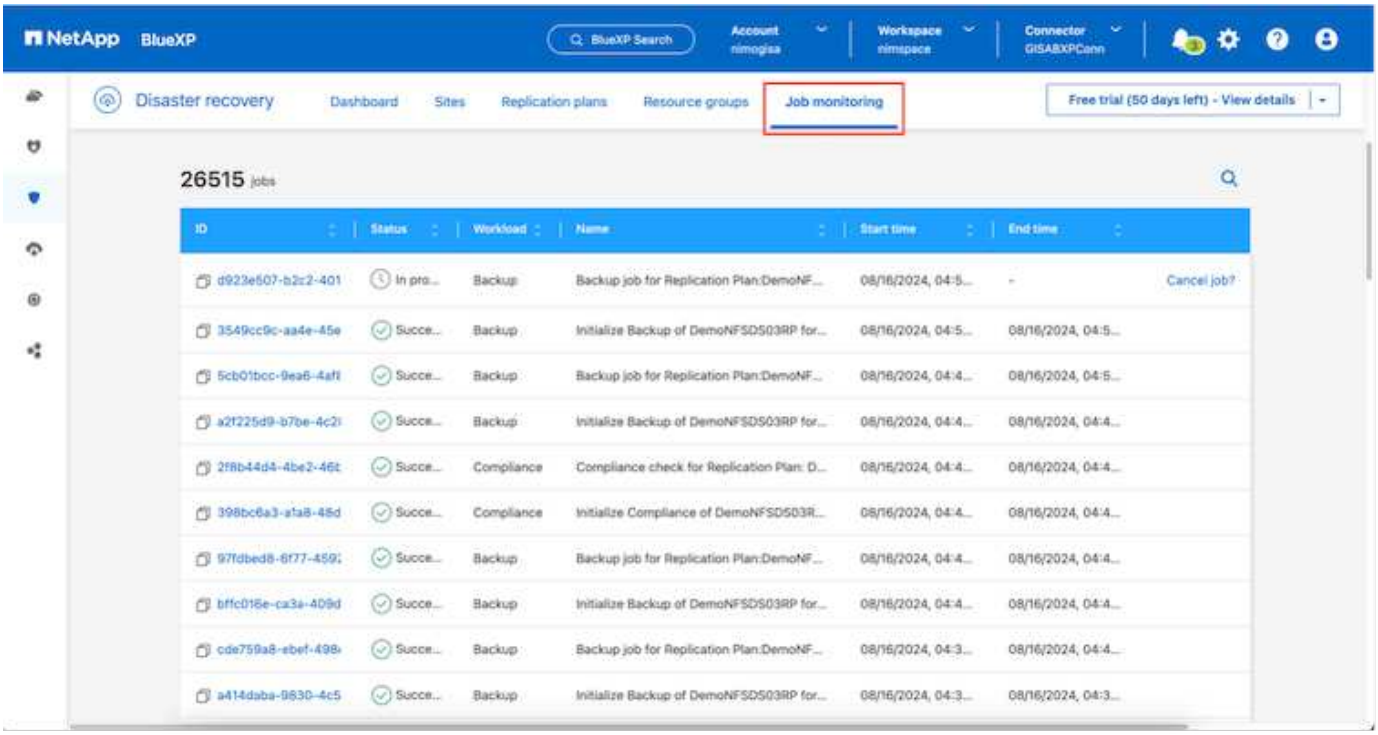
Failover zu einem Ziel abgeschlossen hat, und umfasst die folgenden Schritte:

- Das aus- und Abschalten der virtuellen Maschinen und Volumes am Zielstandort wird aufgehoben.
- Break die SnapMirror Beziehung auf der ursprünglichen Quelle ist gebrochen, um sie zu lesen/schreiben.
- Synchronisieren Sie die SnapMirror-Beziehung erneut, um die Replikation umzukehren.
- Mounten Sie das Volume auf der Quelle, schalten Sie die virtuellen Quellmaschinen ein und registrieren Sie sie.

Weitere Informationen über den Zugriff auf und die Konfiguration von BlueXP -DRaaS finden Sie im "Erfahren Sie mehr über BlueXP Disaster Recovery für VMware".

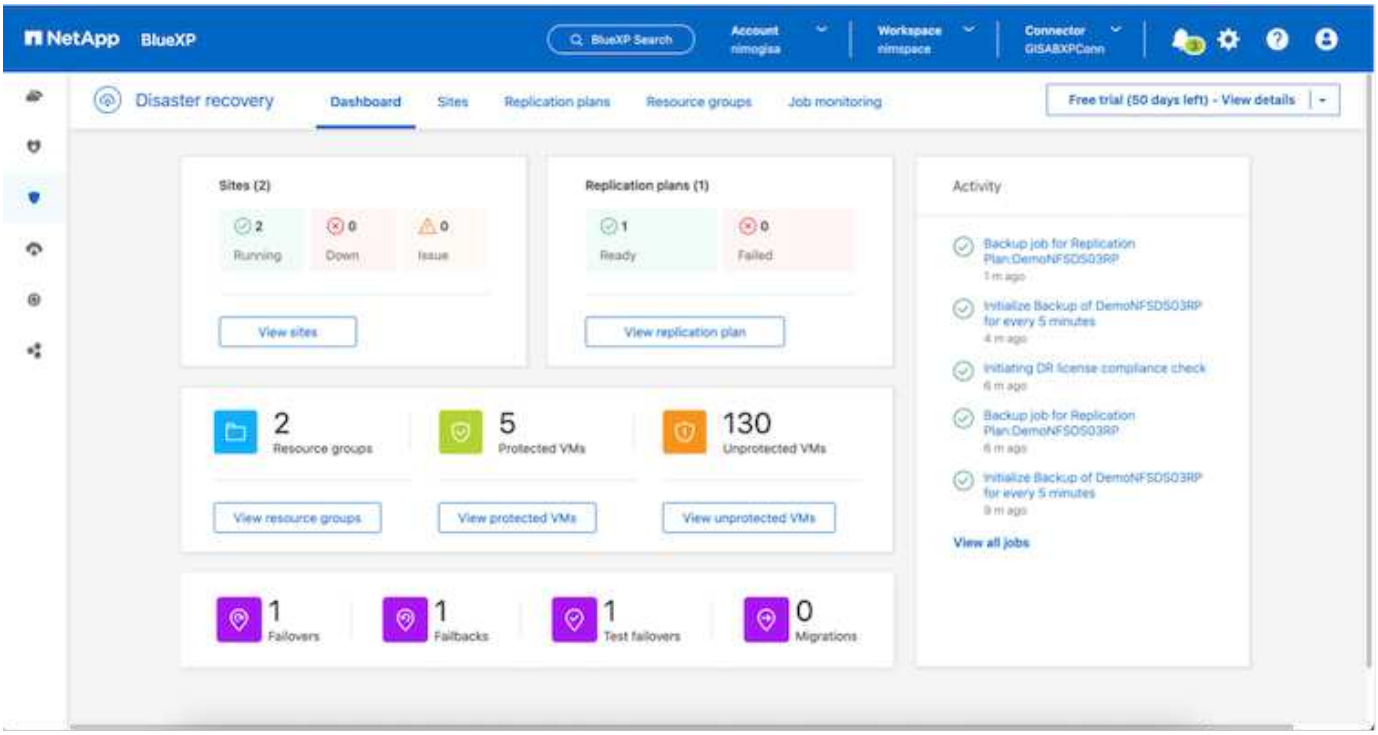
Monitoring und Dashboard

Über BlueXP oder die ONTAP-CLI können Sie den Replikationsstatus für die entsprechenden Datenspeicher-Volumes überwachen und den Status eines Failover oder Test-Failovers über die Jobüberwachung nachverfolgen.



Wenn ein Job derzeit in Bearbeitung ist oder in der Warteschlange steht und Sie ihn anhalten möchten, gibt es eine Option, um ihn abzubrechen.

Bewerten Sie mit dem BlueXP Dashboard für Disaster Recovery mühelos den Status von Disaster-Recovery-Standorten und Replizierungsplänen. So können Administratoren schnell gesunde, nicht verbundene oder beeinträchtigte Standorte und Pläne identifizieren.



Auf diese Weise erhalten Sie eine leistungsstarke Lösung, die einen individuellen Disaster-Recovery-Plan umsetzt. Failover lässt sich als geplanter Failover oder Failover mit einem Mausklick durchführen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung des DR-Standorts getroffen wird.

Um mehr über diesen Prozess zu erfahren, folgen Sie dem ausführlichen Walkthrough-Video oder verwenden Sie die "Lösungssimulator".

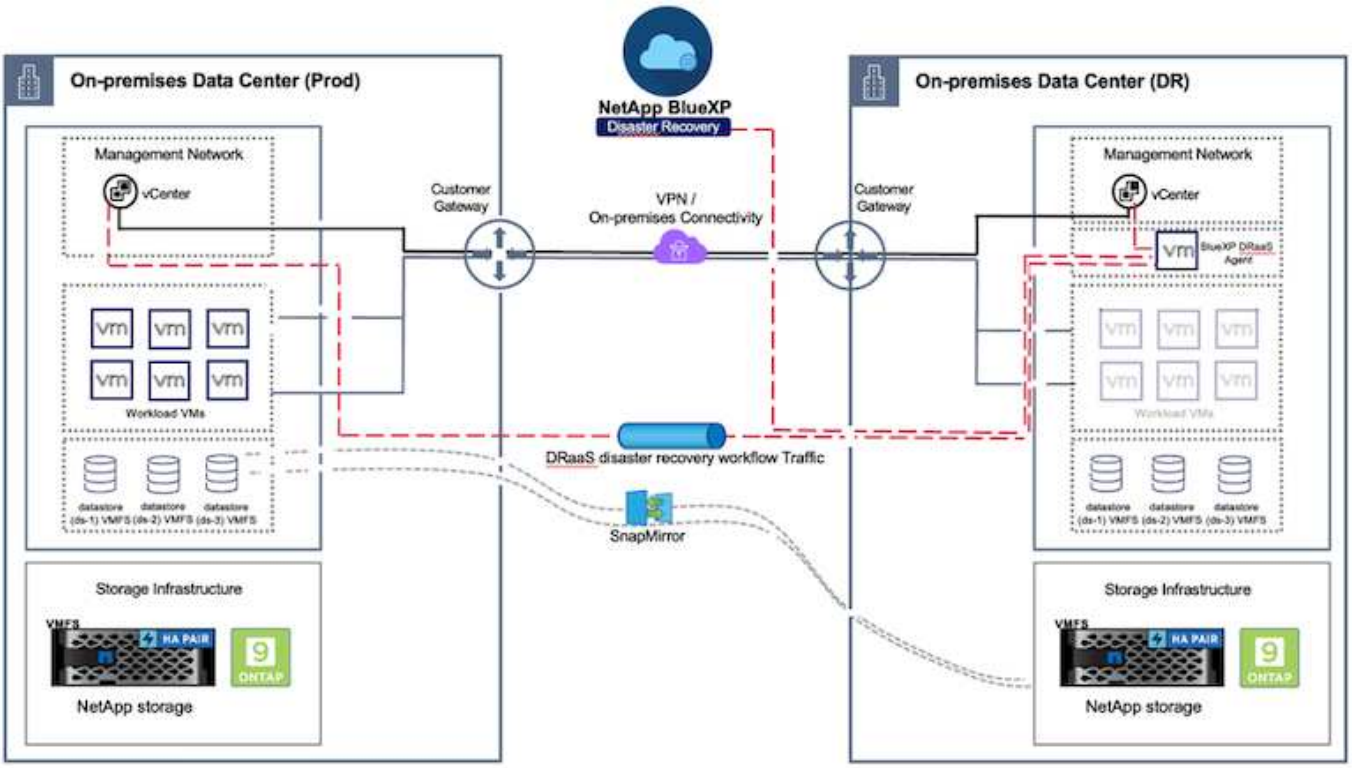
DR, die BlueXP DRaaS für VMFS-Datastores verwendet

Disaster Recovery mit Replizierung auf Blockebene vom Produktionsstandort zum Disaster-Recovery-Standort ist eine ausfallsichere und kostengünstige Möglichkeit, um Workloads vor Standortausfällen und Datenbeschädigung, z. B. Ransomware-Angriffen, zu schützen. Durch die NetApp SnapMirror-Replizierung können VMware Workloads, die lokale ONTAP Systeme mit VMFS Datastore ausführen, auf ein anderes ONTAP Storage-System in einem festgelegten Recovery-Datacenter repliziert werden, in dem sich VMware befindet

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zur Einrichtung von Disaster Recovery für lokale VMware VMs an einem anderen designierten Standort beschrieben. Als Teil dieser Einrichtung, das BlueXP Konto, BlueXP Connector, die ONTAP-Arrays in BlueXP Workspace hinzugefügt, die erforderlich sind, um die Kommunikation von VMware vCenter zum ONTAP Storage zu ermöglichen. Darüber hinaus wird in diesem Dokument beschrieben, wie die Replikation zwischen Standorten konfiguriert und ein Recovery-Plan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Standort-Failover und zum Failback, wenn der primäre Standort wiederhergestellt und online gekauft wird.

Mithilfe des BlueXP Disaster Recovery Service, der in die NetApp BlueXP Konsole integriert ist, können Kunden ihre lokalen VMware vCenter zusammen mit ONTAP Storage erkennen, Ressourcengruppen erstellen, einen Disaster Recovery-Plan erstellen, ihn Ressourcengruppen zuordnen und Failover und Failback testen oder ausführen. SnapMirror bietet Block-Replizierung auf Storage-Ebene, sodass die beiden Standorte mit inkrementellen Änderungen aktualisiert werden können, was zu einem RPO von bis zu 5 Minuten führt.

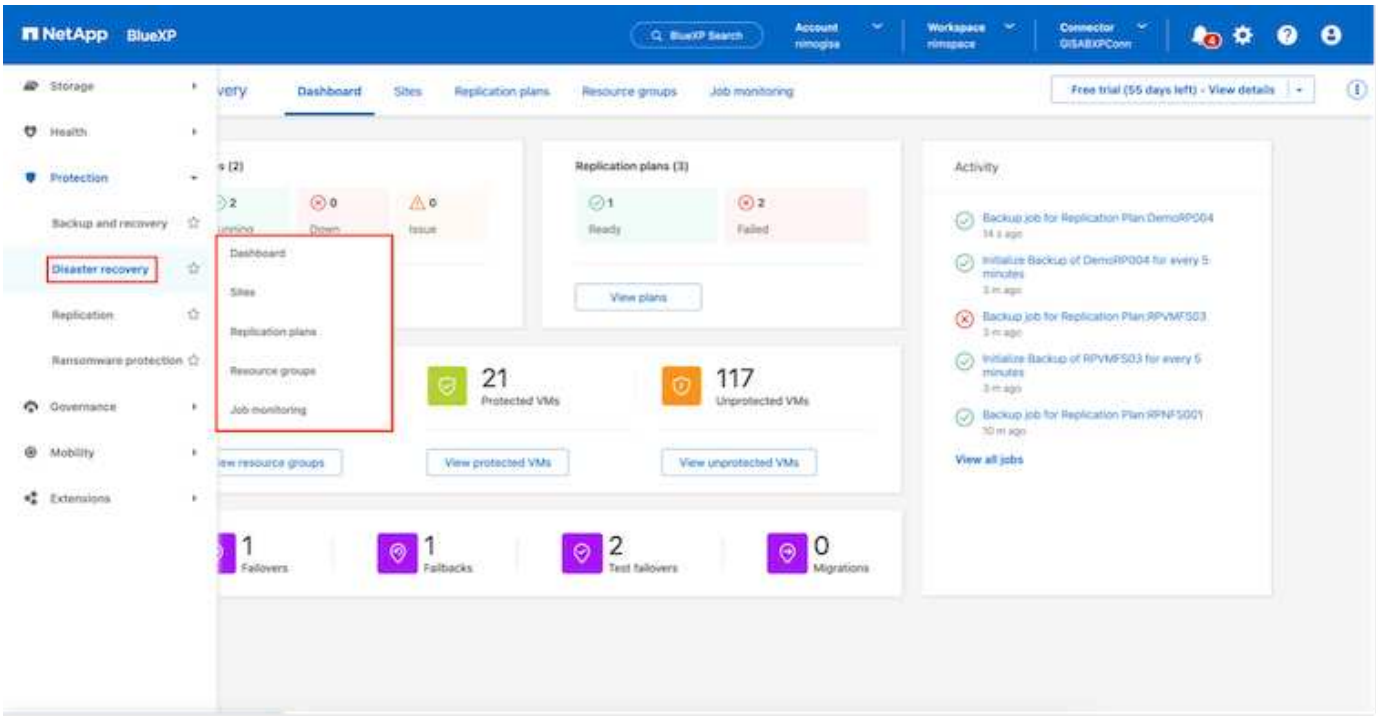
Außerdem ist es möglich, DR-Verfahren als regelmäßiges Drill-Verfahren zu simulieren, ohne Auswirkungen auf die Produktion und replizierte Datenspeicher zu haben oder zusätzliche Storage-Kosten entstehen. Bei BlueXP Disaster Recovery wird mithilfe der FlexClone Technologie von ONTAP eine platzsparende Kopie des VMFS Datastore vom letzten replizierten Snapshot am DR-Standort erstellt. Nach Abschluss des DR-Tests können Kunden die Testumgebung wieder löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Wenn (geplant oder ungeplant) das eigentliche Failover mit nur wenigen Klicks ausgeführt werden muss, orchestriert der BlueXP Disaster Recovery Service alle Schritte, die zum automatischen Einrichten der geschützten Virtual Machines am designierten Disaster Recovery-Standort erforderlich sind. Der Service umkehrt auch die SnapMirror-Beziehung zum primären Standort und repliziert bei Bedarf alle Änderungen für einen Failback-Vorgang von sekundär zu primär. All dies kann mit einem Bruchteil der Kosten im Vergleich zu anderen bekannten Alternativen erreicht werden.



Erste Schritte

Um die BlueXP Disaster Recovery zu starten, verwenden Sie die BlueXP Konsole und greifen Sie dann auf den Service zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste des BlueXP die Option Schutz > Notfallwiederherstellung.
3. Das BlueXP Disaster Recovery Dashboard wird angezeigt.

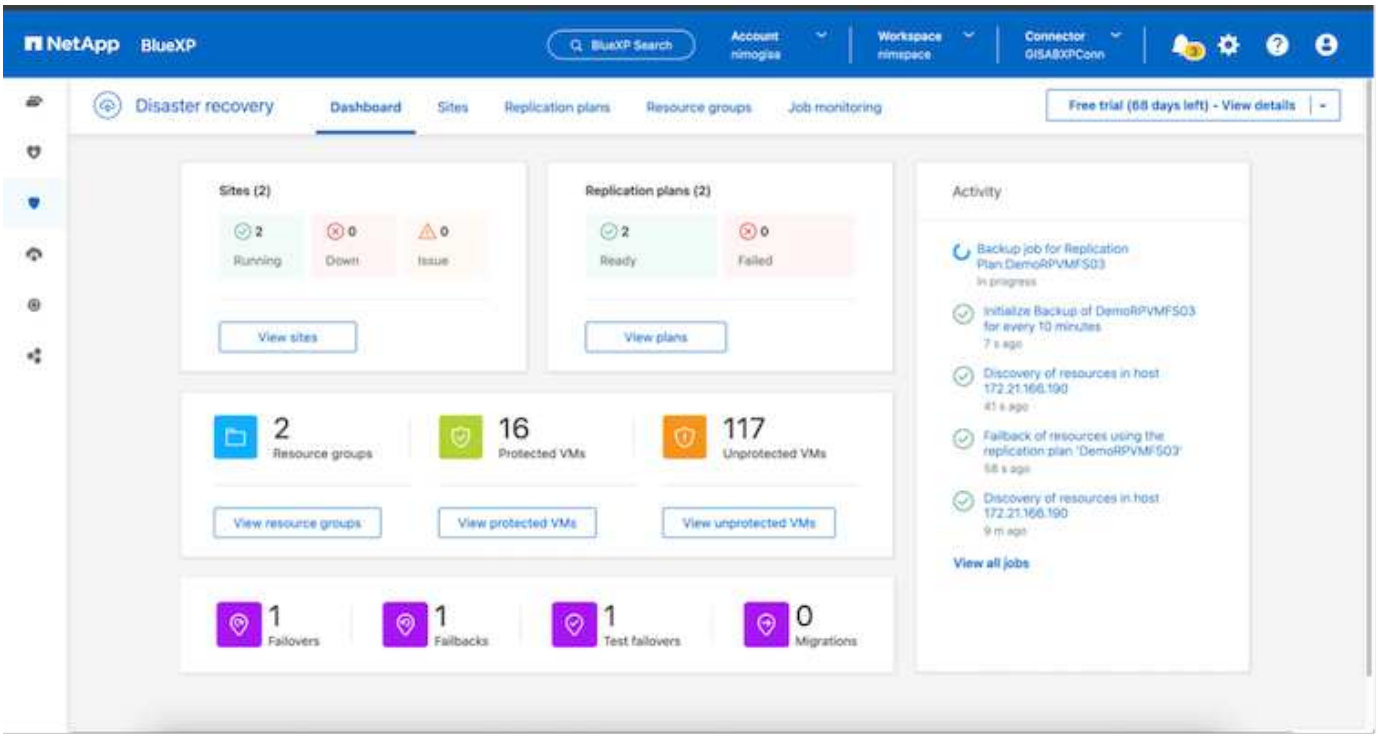


Stellen Sie vor der Konfiguration des Disaster Recovery-Plans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der BlueXP -Anschluss ist in NetApp BlueXP eingerichtet. Der Connector sollte in AWS VPC implementiert werden.
- Die BlueXP Connector-Instanz ist mit dem Quell- und Ziel-vCenter sowie mit den Storage-Systemen verbunden.
- Lokale NetApp Storage-Systeme, die VMFS-Datastores für VMware hosten, werden in BlueXP hinzugefügt.
- Bei der Verwendung von DNS-Namen sollte die DNS-Auflösung vorhanden sein. Verwenden Sie andernfalls IP-Adressen für vCenter.
- Die SnapMirror-Replikation ist für die festgelegten VMFS-basierten Datastore Volumes konfiguriert.

Sobald die Verbindung zwischen dem Quell- und dem Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Diese dauert etwa 3 bis 5 Minuten.

NetApp empfiehlt die Implementierung des BlueXP Connectors am Disaster Recovery-Standort oder an einem dritten Standort, damit der BlueXP Connector über das Netzwerk mit den Quell- und Zielressourcen kommunizieren kann, wenn es zu echten Ausfällen oder Naturkatastrophen kommt.

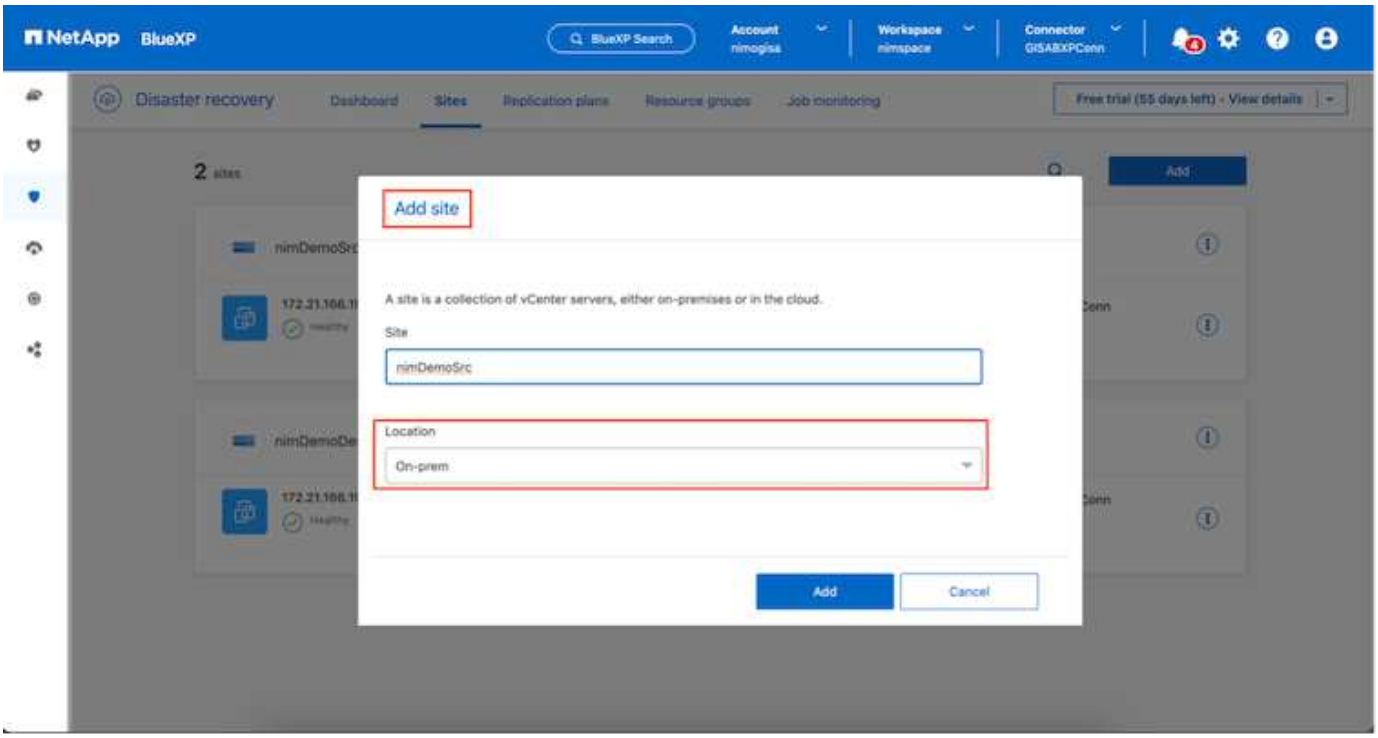


Die Unterstützung von lokalen zu lokalen VMFS-Datastores wird in einer Vorschau auf Technologie ausgeführt, während dieses Dokument verfasst wird. Die Funktion wird sowohl bei FC- als auch bei ISCSI-protokollbasierten VMFS-Datenspeichern unterstützt.

BlueXP Disaster Recovery-Konfiguration

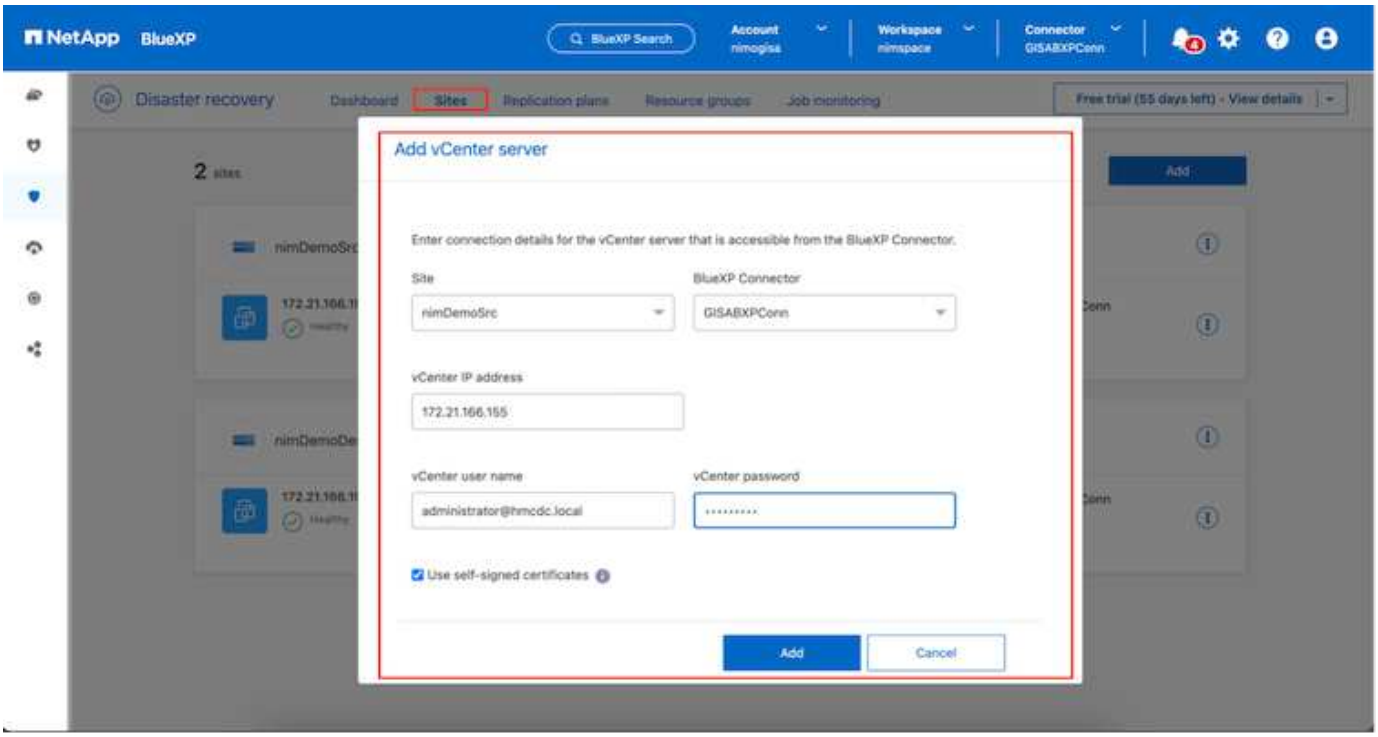
Der erste Schritt zur Vorbereitung auf Disaster Recovery besteht darin, die lokalen vCenter und Storage-Ressourcen zu erkennen und zu BlueXP Disaster Recovery hinzuzufügen.

Stellen Sie sicher, dass die ONTAP-Speichersysteme der Arbeitsumgebung innerhalb des Arbeitsbereichs hinzugefügt werden. Öffnen Sie die BlueXP -Konsole, und wählen Sie aus der linken Navigation **Schutz > Notfallwiederherstellung** aus. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü, Wählen Sie **Standorte > Hinzufügen > vCenter hinzufügen**.

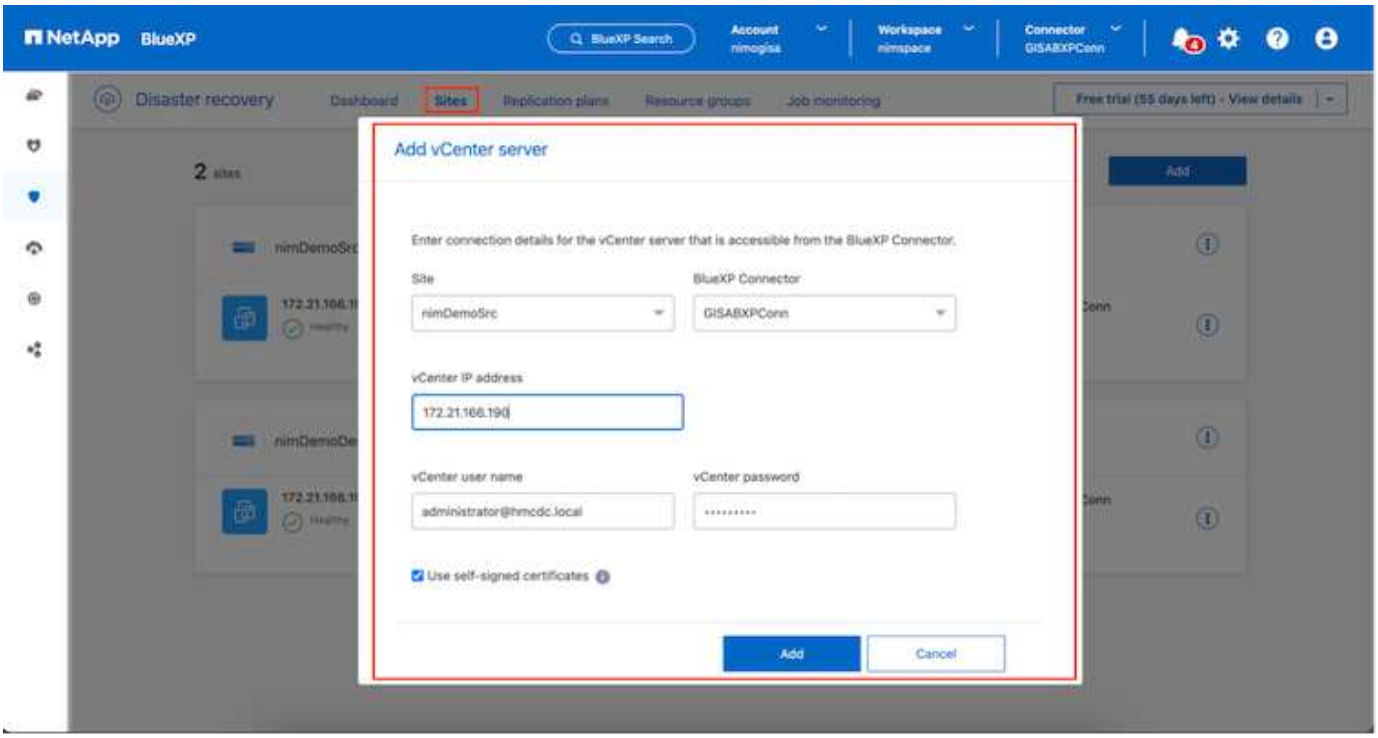


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle**. VCenter vor Ort.



- **Ziel**. VMC SDDC vCenter:



Sobald die vCenters hinzugefügt wurden, wird eine automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort

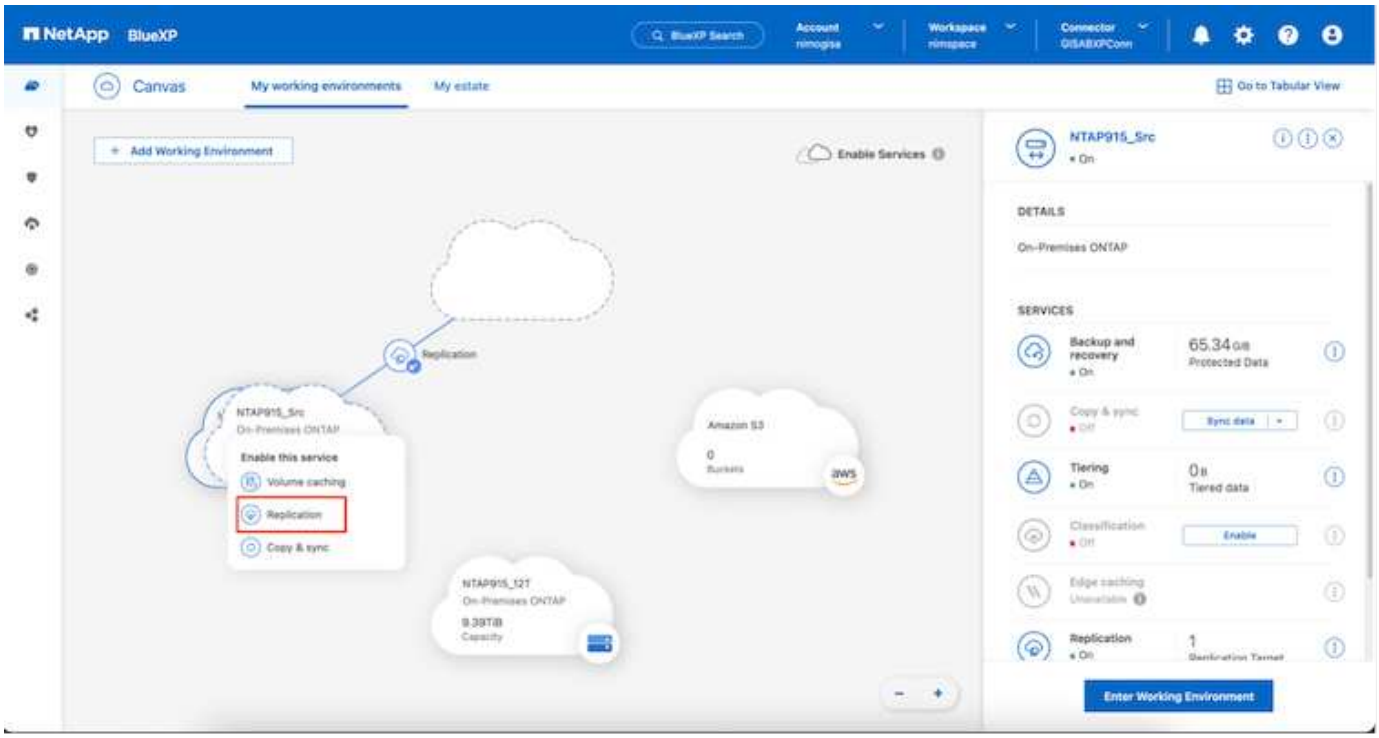
SnapMirror nutzt ONTAP Snapshots, um die Übertragung von Daten von einem Ort zum anderen zu verwalten. Zunächst wird eine vollständige Kopie, die auf einem Snapshot des Quell-Volume basiert, zum Ziel kopiert, um eine Basissynchronisierung durchzuführen. Wenn an der Quelle Datenänderungen auftreten, wird ein neuer Snapshot erstellt und mit dem Basis-Snapshot verglichen. Die gefundenen Blöcke werden dann auf das Zielsystem repliziert. Der neuere Snapshot wird dabei zur aktuellen Basislinie oder zum neuesten gemeinsamen Snapshot. Dadurch kann der Prozess wiederholt und inkrementelle Updates an das Ziel gesendet werden.

Wenn eine SnapMirror Beziehung hergestellt wurde, befindet sich das Ziel-Volume in einem schreibgeschützten Online-Zustand und ist somit noch zugänglich. SnapMirror arbeitet mit physischen Storage-Blöcken und nicht auf File- oder logischer Ebene. Das heißt, das Ziel-Volume ist ein identisches Replikat der Quelle, einschließlich Snapshots, Volume-Einstellungen usw. Wenn das Quell-Volume ONTAP-Funktionen zur Speicherplatzeffizienz wie Datenkomprimierung und Datendeduplizierung verwendet, so behält das replizierte Volume diese Optimierungen bei.

Wenn die SnapMirror Beziehung unterbrochen wird, wird das Ziel-Volume beschreibbar gemacht und normalerweise für einen Failover verwendet, wenn SnapMirror zur Synchronisierung von Daten mit einer DR-Umgebung verwendet wird. SnapMirror ist ausreichend ausgereift, damit die am Failover-Standort geänderten Daten effizient zurück zum primären System resynchronisiert werden können, falls sie später wieder online sind, und dann die ursprüngliche SnapMirror Beziehung wiederhergestellt werden kann.

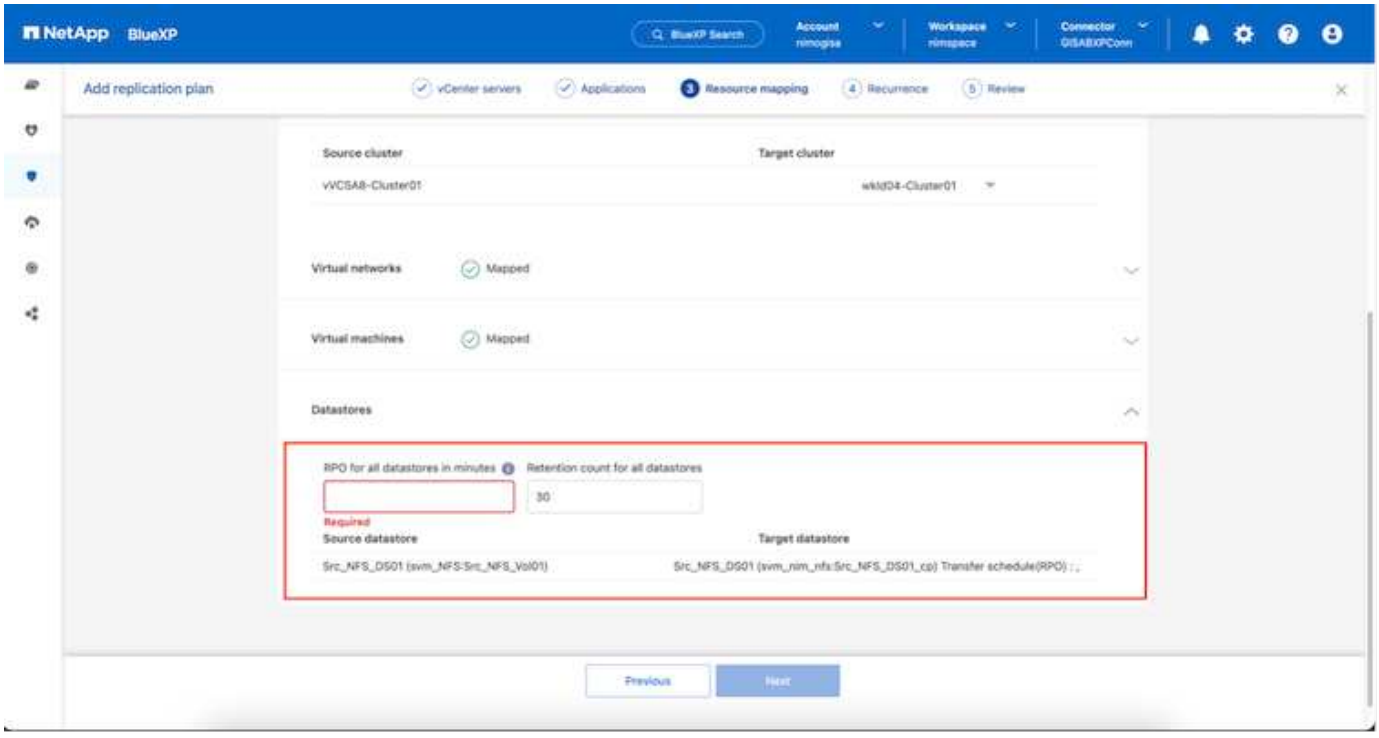
Wie Sie es für VMware Disaster Recovery einrichten

Der Prozess zur Erstellung der SnapMirror-Replizierung bleibt für jede Applikation unverändert. Der Prozess kann manuell oder automatisiert werden. Am einfachsten lässt sich BlueXP zur Konfiguration der SnapMirror Replizierung nutzen, indem das ONTAP Quell-System der Umgebung einfach per Drag & Drop auf das Ziel gezogen wird, um den Assistenten zu starten, der den Rest des Prozesses durchläuft.



Auch BlueXP DRaaS kann dasselbe automatisieren, wenn die folgenden beiden Kriterien erfüllt sind:

- Quell- und Ziel-Cluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.

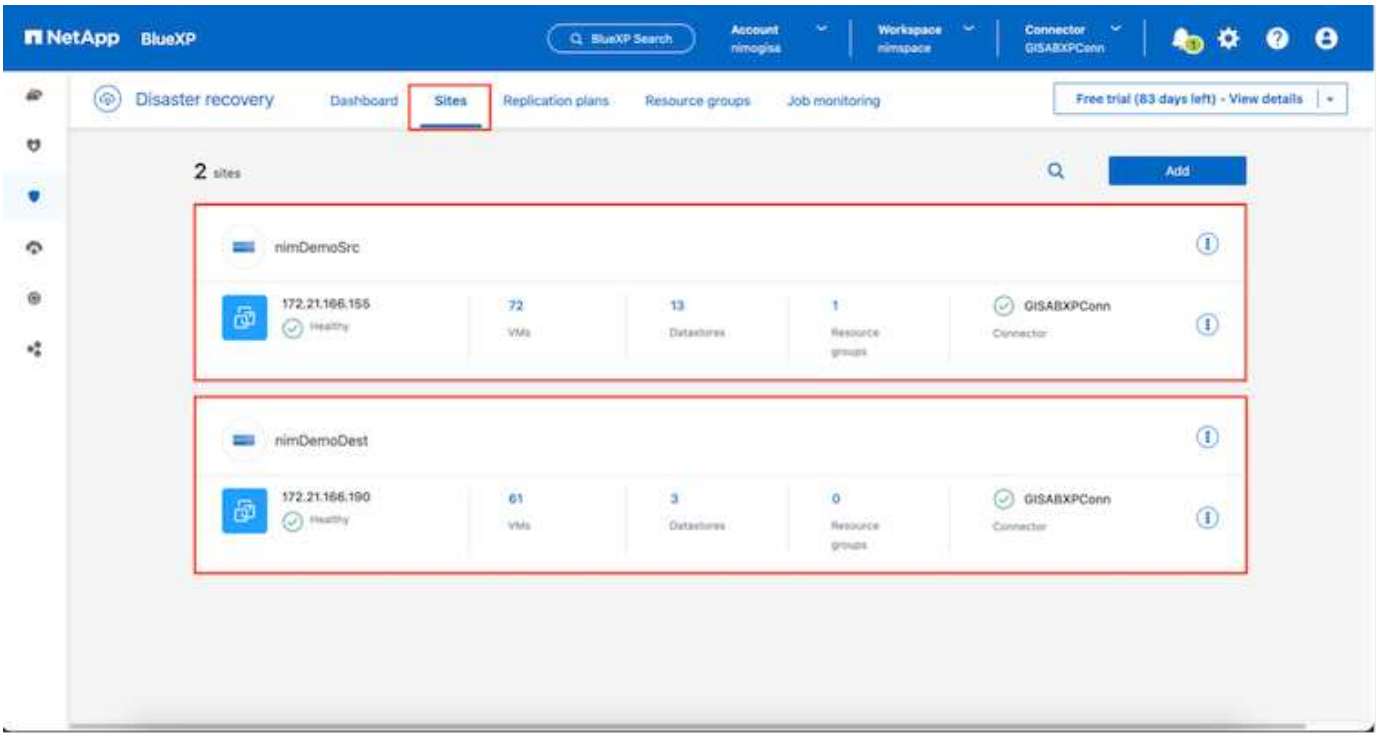


Wenn die SnapMirror-Beziehung bereits über CLI für das Volume konfiguriert ist, nimmt BlueXP DRaaS die Beziehung auf und fährt mit den restlichen Workflow-Operationen fort.

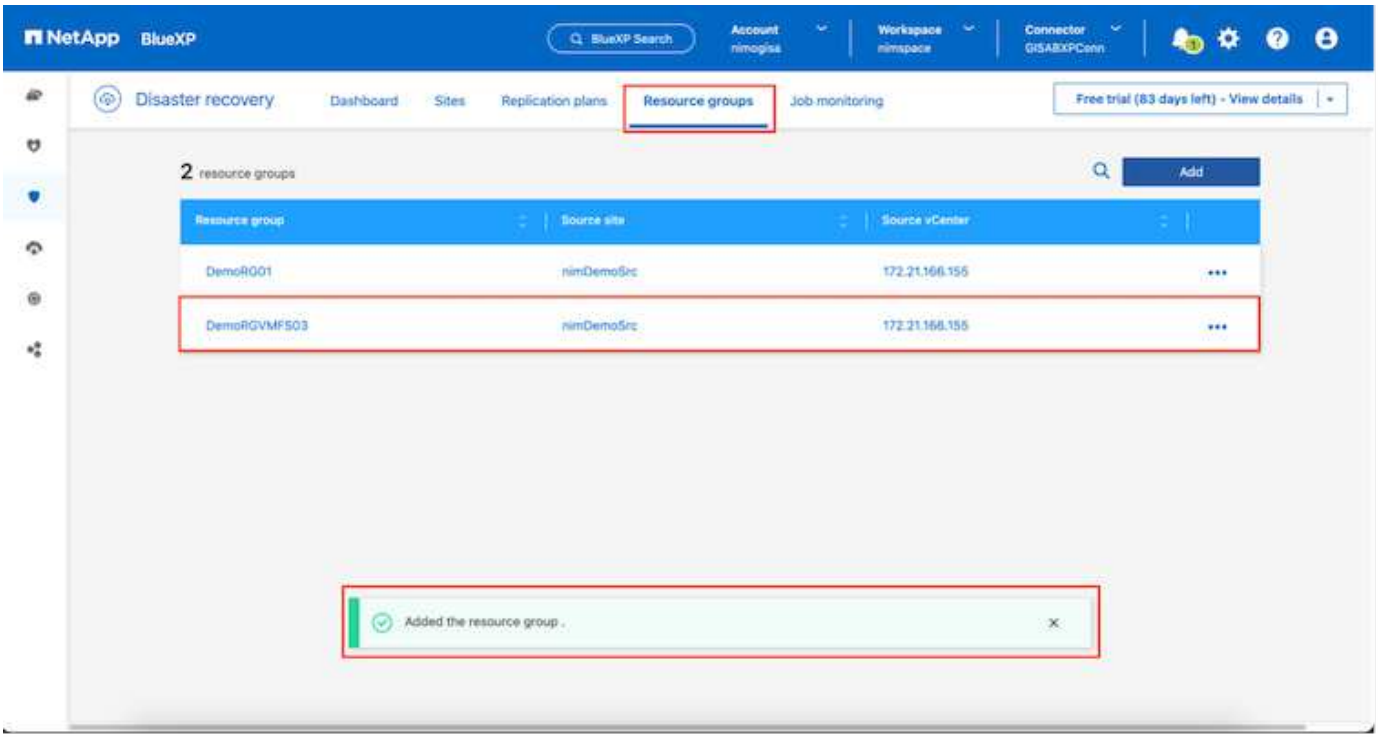
Abgesehen von den oben genannten Ansätzen kann die SnapMirror Replikation auch über ONTAP CLI oder System Manager erstellt werden. Unabhängig vom Ansatz zur Datensynchronisierung mit SnapMirror orchestriert BlueXP DRaaS den Workflow für nahtlose und effiziente Disaster-Recovery-Vorgänge.

Welche Vorteile bietet BlueXP Disaster Recovery für Sie?

Nachdem die Quell- und Zielstandorte hinzugefügt wurden, führt die BlueXP Disaster Recovery automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. BlueXP Disaster Recovery erkennt auch automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt diese aus.

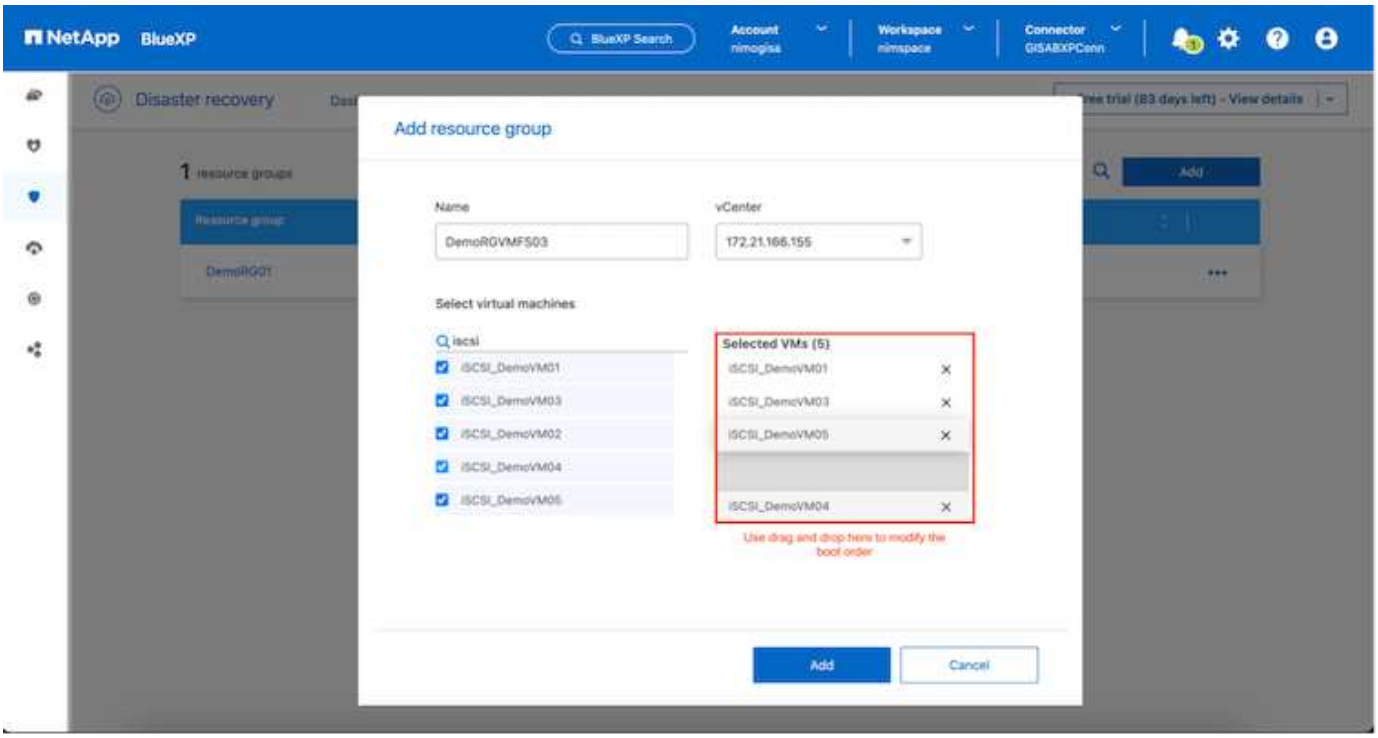


Nach dem Hinzufügen der Standorte können VMs zu Ressourcengruppen zusammengefasst werden. Mit den BlueXP Disaster Recovery-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logischen Gruppen gruppieren, die ihre Boot-Aufträge und Boot-Verzögerungen enthalten, die bei der Recovery ausgeführt werden können. Um Ressourcengruppen zu erstellen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.



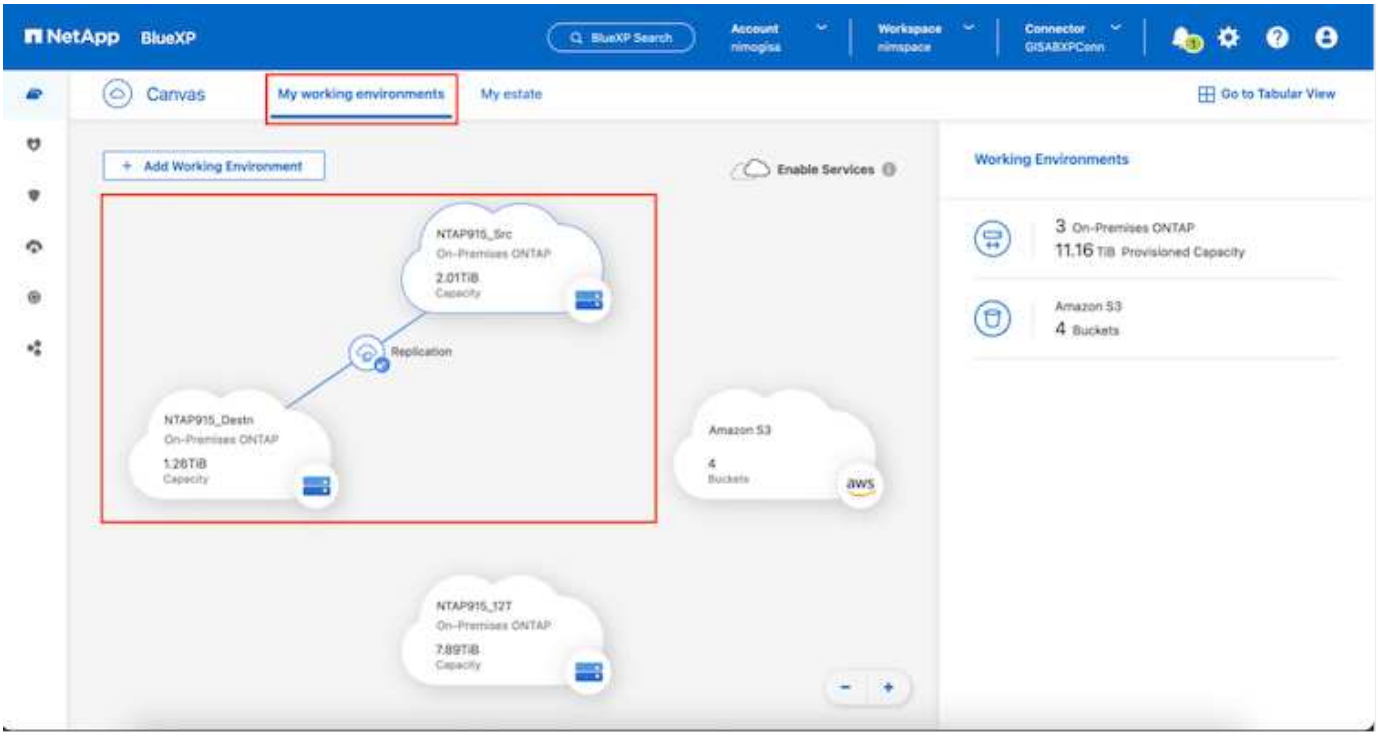
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

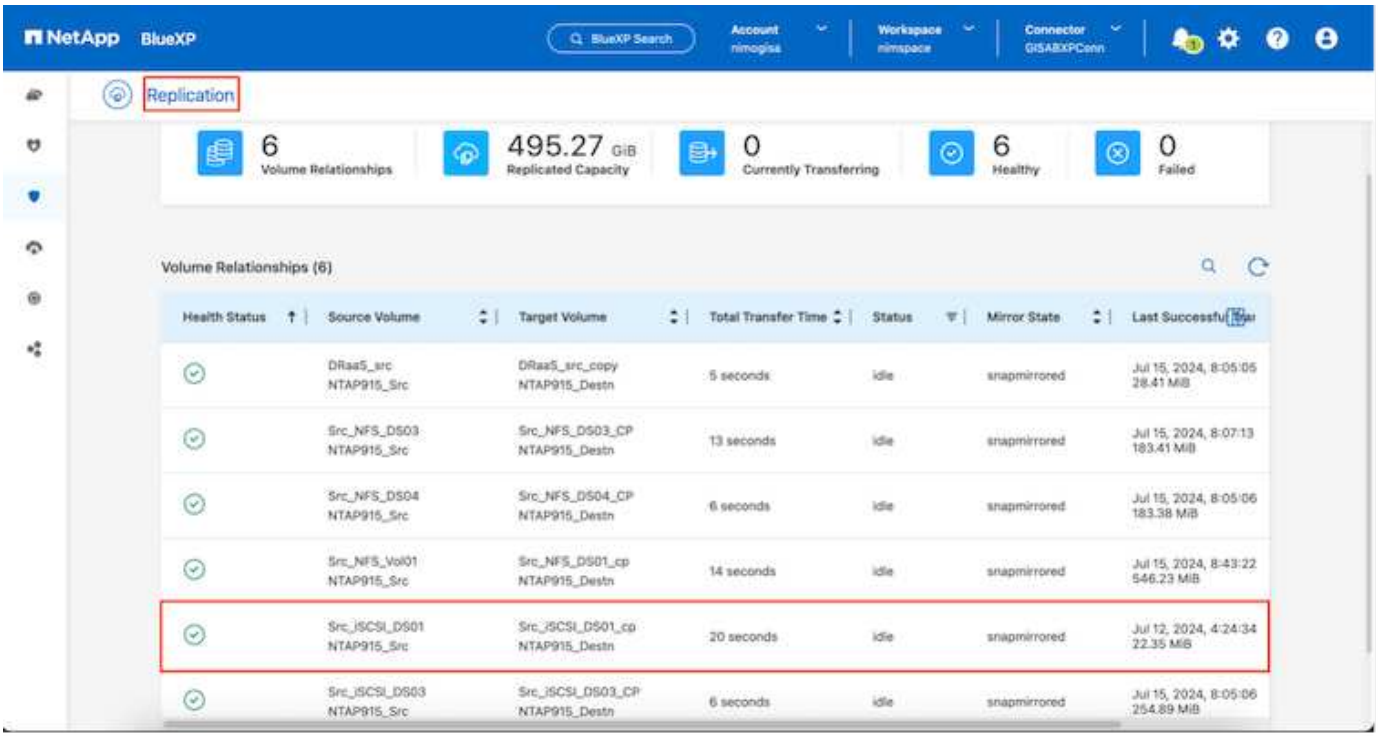
Die Boot-Reihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen Drag-and-Drop-Mechanismus definiert oder geändert werden.



Nach der Erstellung der Ressourcengruppen erstellen Sie im nächsten Schritt einen Ausführungsentwurf oder einen Plan für die Wiederherstellung von virtuellen Maschinen und Anwendungen bei einem Notfall. Wie in den Voraussetzungen erwähnt, kann die SnapMirror-Replikation vorab konfiguriert werden, oder DRaaS kann sie mithilfe der RPO und der Aufbewahrungszahl konfigurieren, die während der Erstellung des Replikationsplans

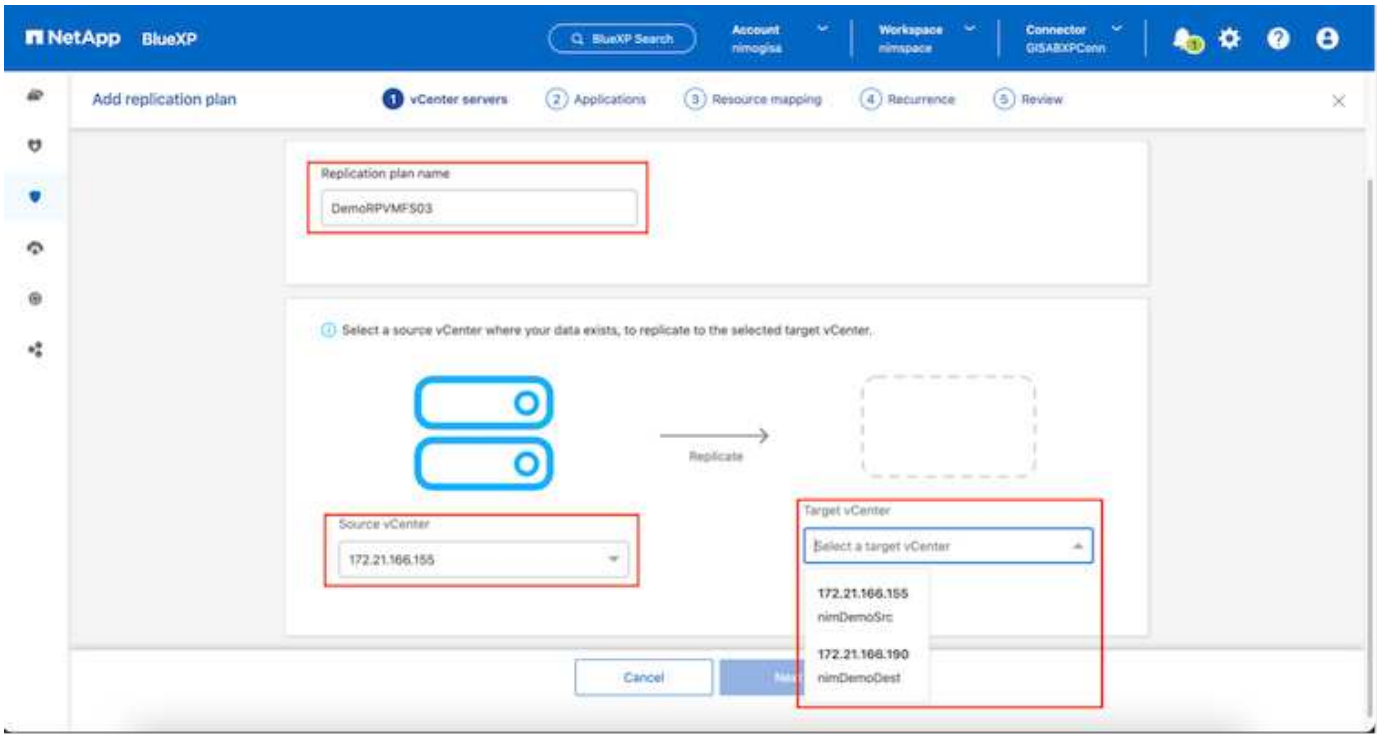
angegeben wurde.



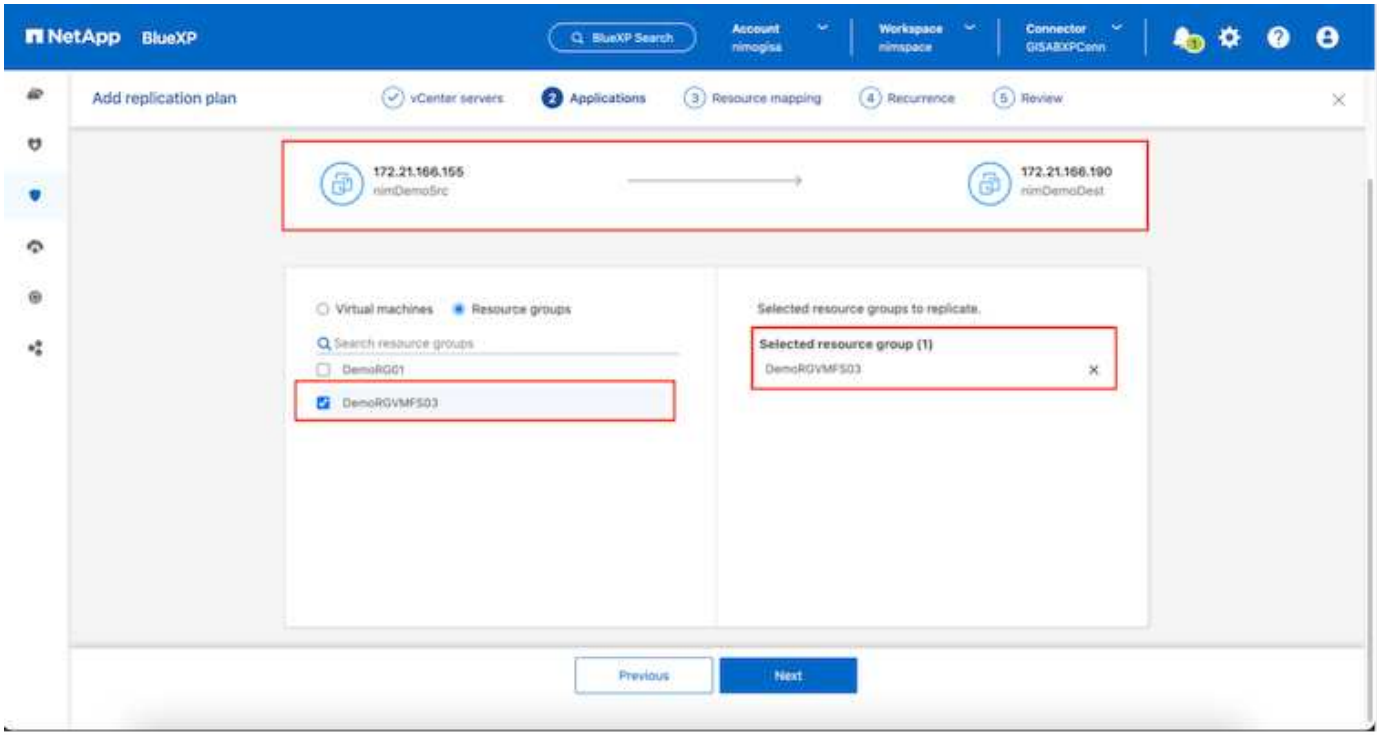


Konfigurieren Sie den Replizierungsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus dem Dropdown auswählen und die Ressourcengruppen auswählen, die in den Plan einbezogen werden sollen, sowie die Gruppierung der Art und Weise, wie Applikationen wiederhergestellt und eingeschaltet werden sollen, sowie die Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

Wählen Sie zunächst das Quell-vCenter aus und dann das Ziel-vCenter aus.



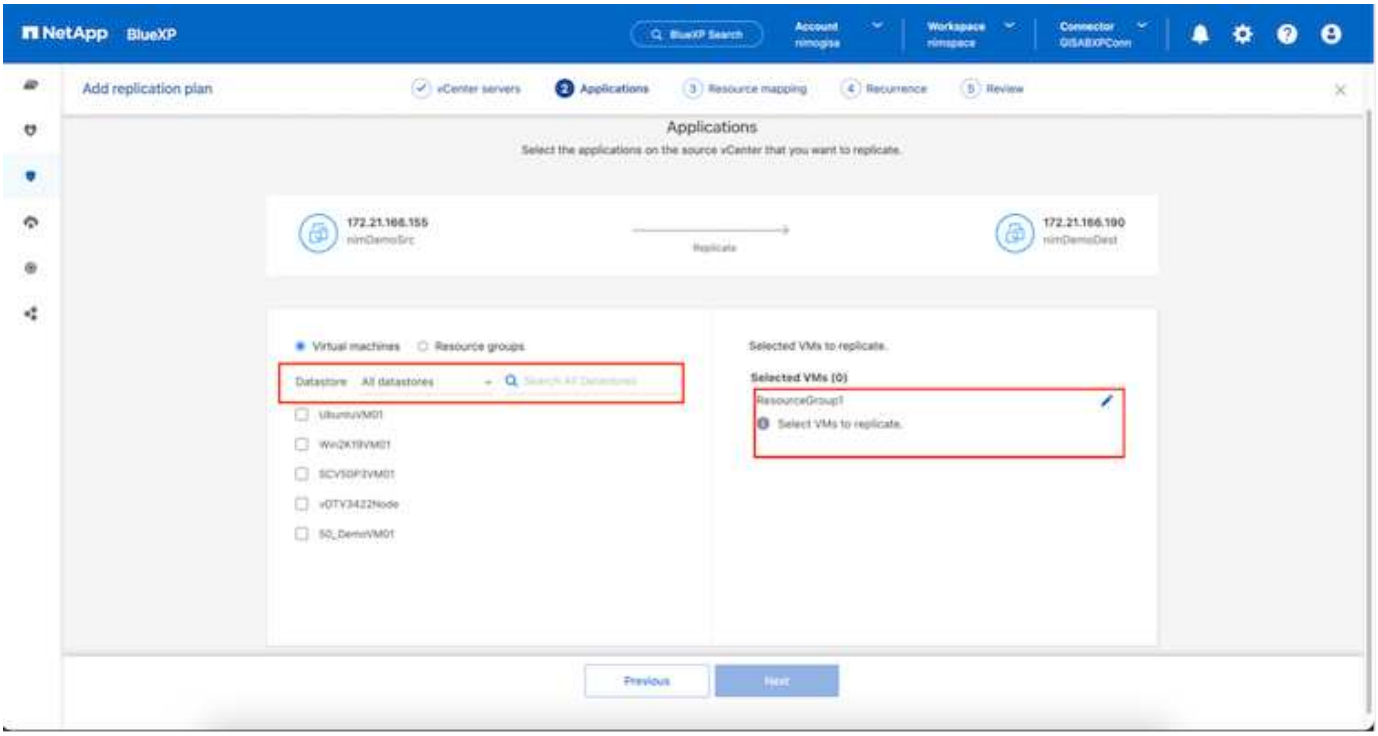
Im nächsten Schritt wählen Sie vorhandene Ressourcengruppen aus. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent, die erforderlichen virtuellen Maschinen zu gruppieren (im Grunde erstellen Sie funktionale Ressourcengruppen) auf der Grundlage der Wiederherstellungsziele. Dies hilft auch dabei, die Reihenfolge der Wiederherstellung von virtuellen Maschinen der Anwendung festzulegen.



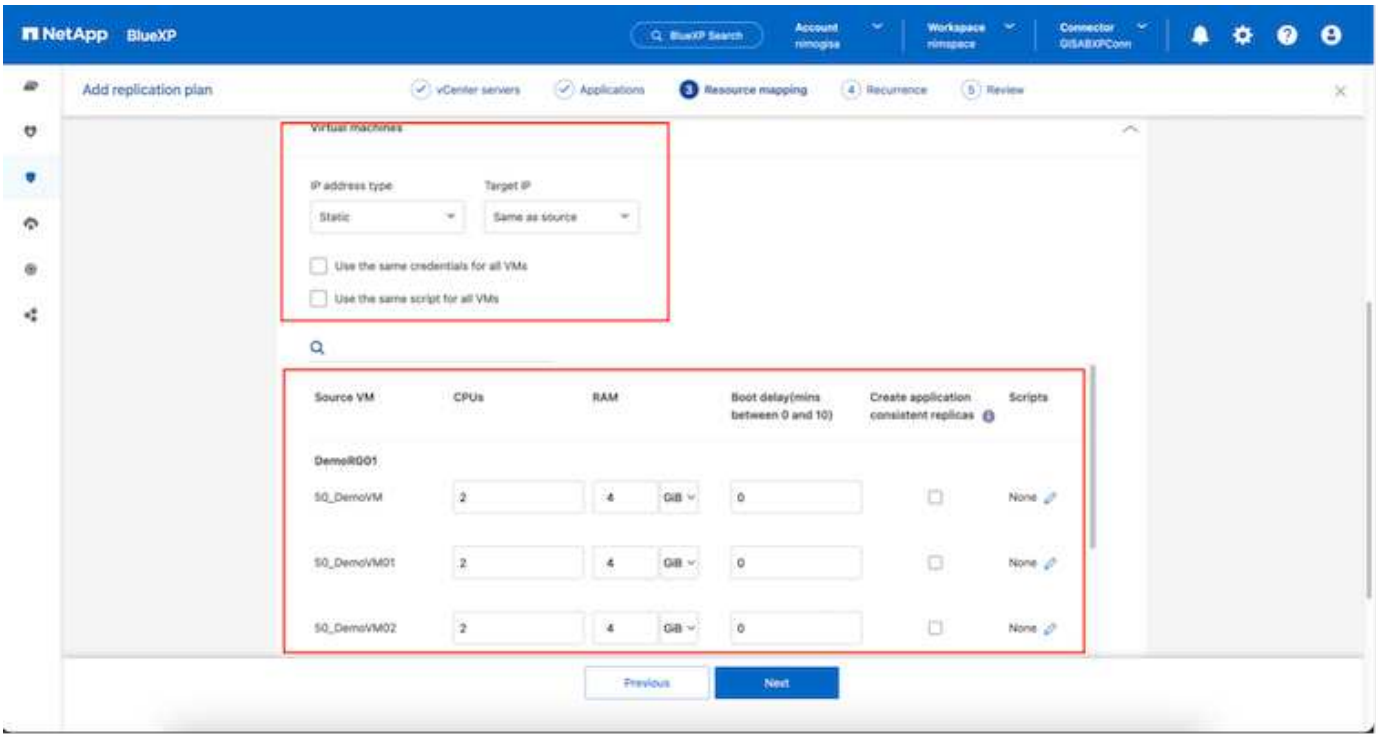
Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge mithilfe der Drag-and-Drop-Funktion. Damit kann die Reihenfolge, in der die VMs während des Recovery-Prozesses eingeschaltet werden, leicht geändert werden.

Jede virtuelle Maschine in einer Ressourcengruppe wird in der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

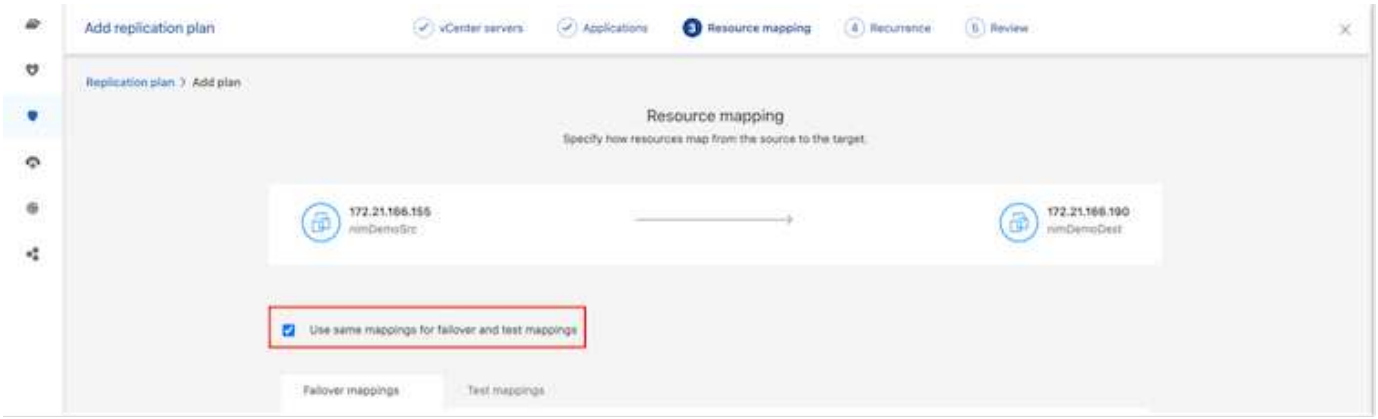
Der Screenshot unten zeigt die Option zum Filtern virtueller Maschinen oder spezieller Datastores nach Unternehmensanforderungen, wenn Ressourcengruppen nicht vorab erstellt werden.



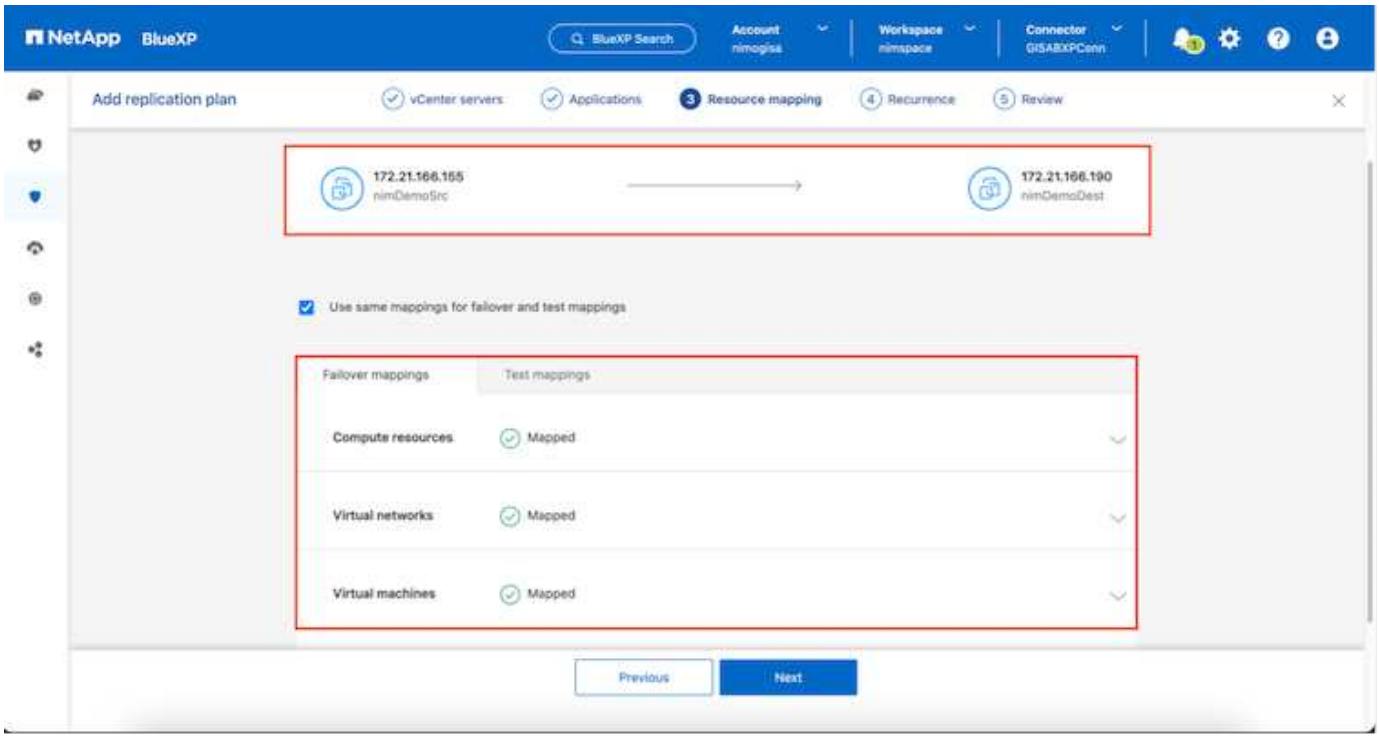
Sobald die Ressourcengruppen ausgewählt sind, erstellen Sie die Failover-Zuordnungen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen, virtuelle Netzwerke. IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Applikationskonsistenz usw. Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".



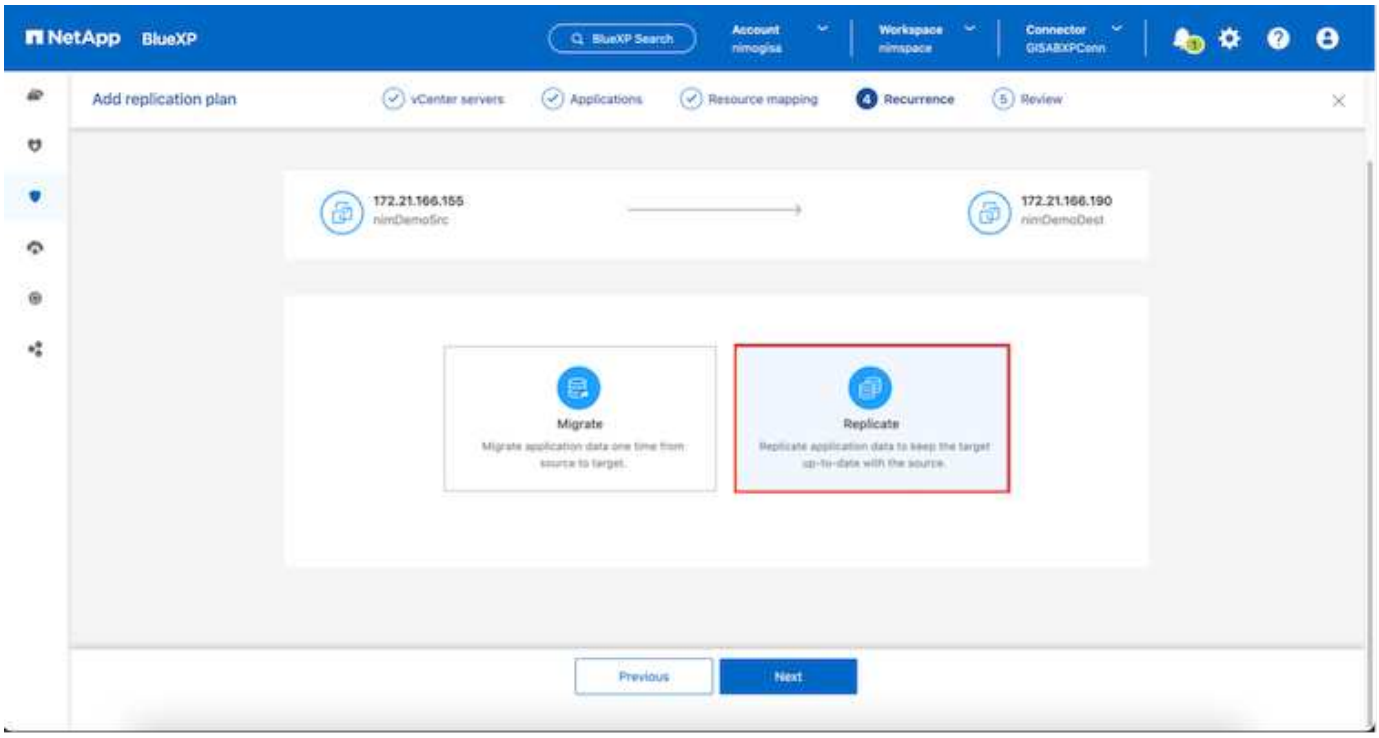
Standardmäßig werden für Test- und Failover-Vorgänge dieselben Zuordnungsparameter verwendet. Um unterschiedliche Zuordnungen für die Testumgebung anzuwenden, aktivieren Sie die Option Testzuordnung, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:



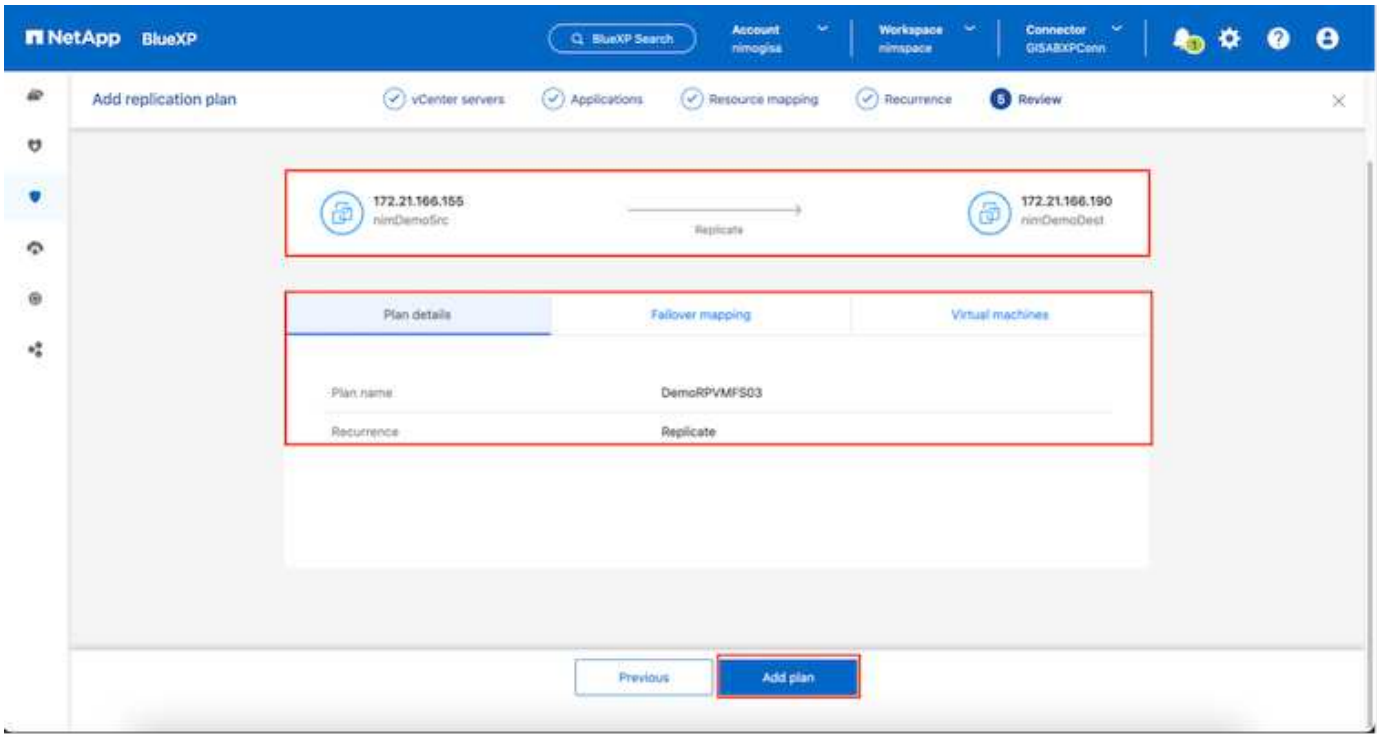
Klicken Sie nach Abschluss der Ressourcenzuordnung auf Weiter.

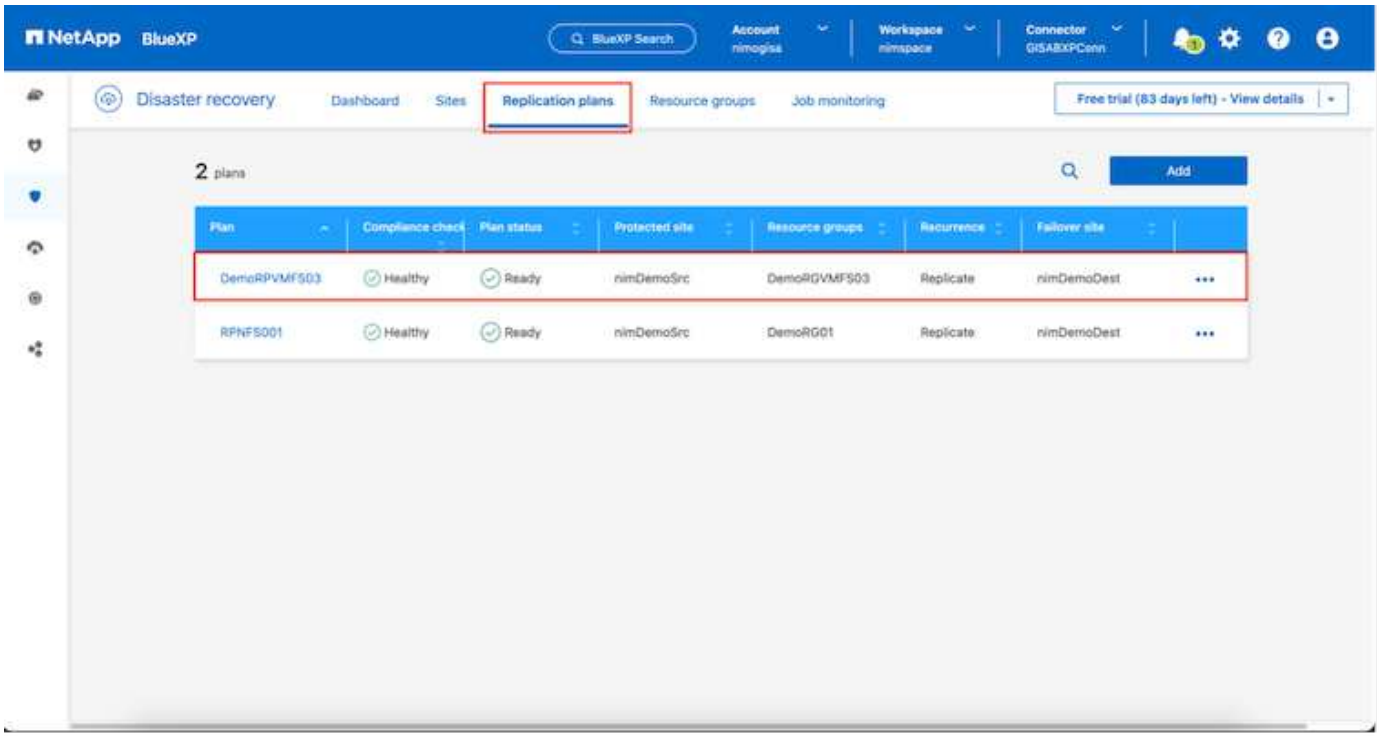


Wählen Sie den Wiederholungstyp aus. In einfachen Worten: Wählen Sie Migrate (einmalige Migration mit Failover) oder die Option wiederkehrende kontinuierliche Replikation aus. In dieser Übersicht ist die Option „Replikat“ ausgewählt.

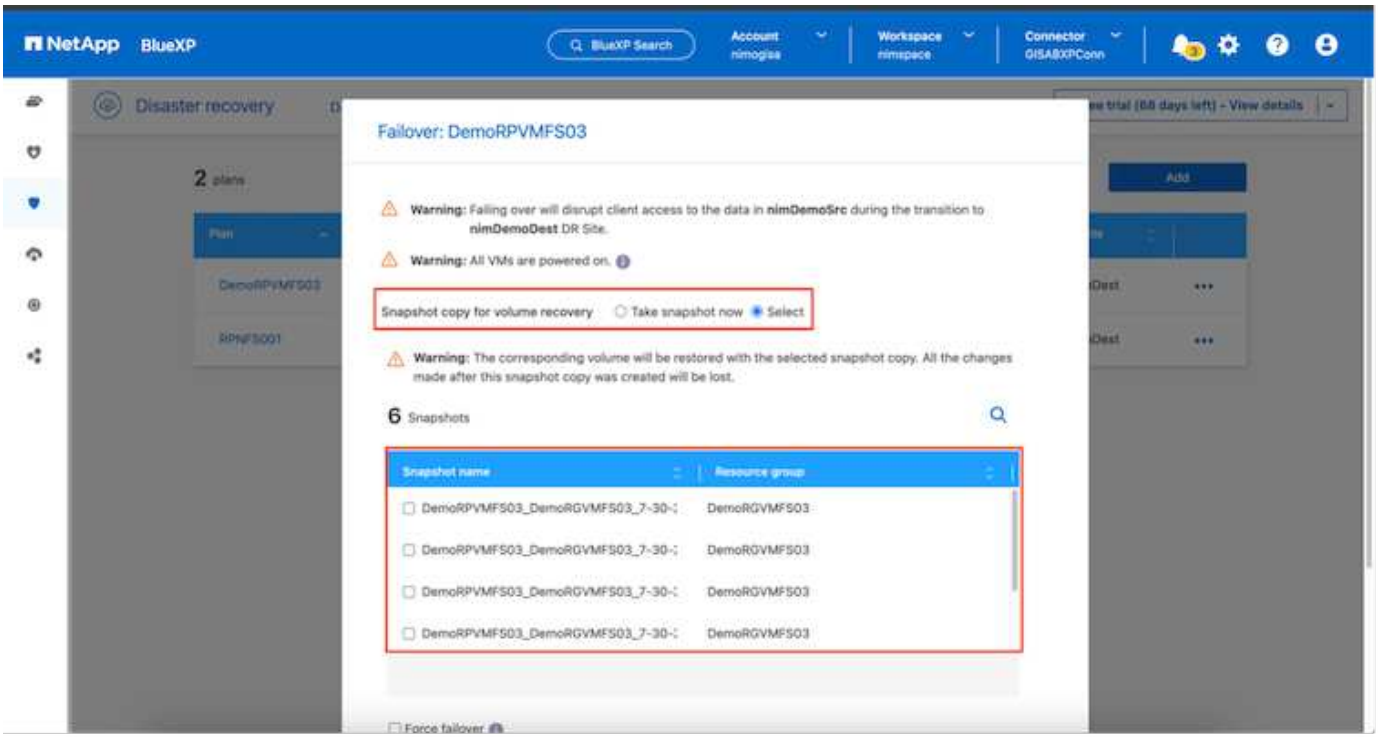


Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie auf Plan hinzufügen.

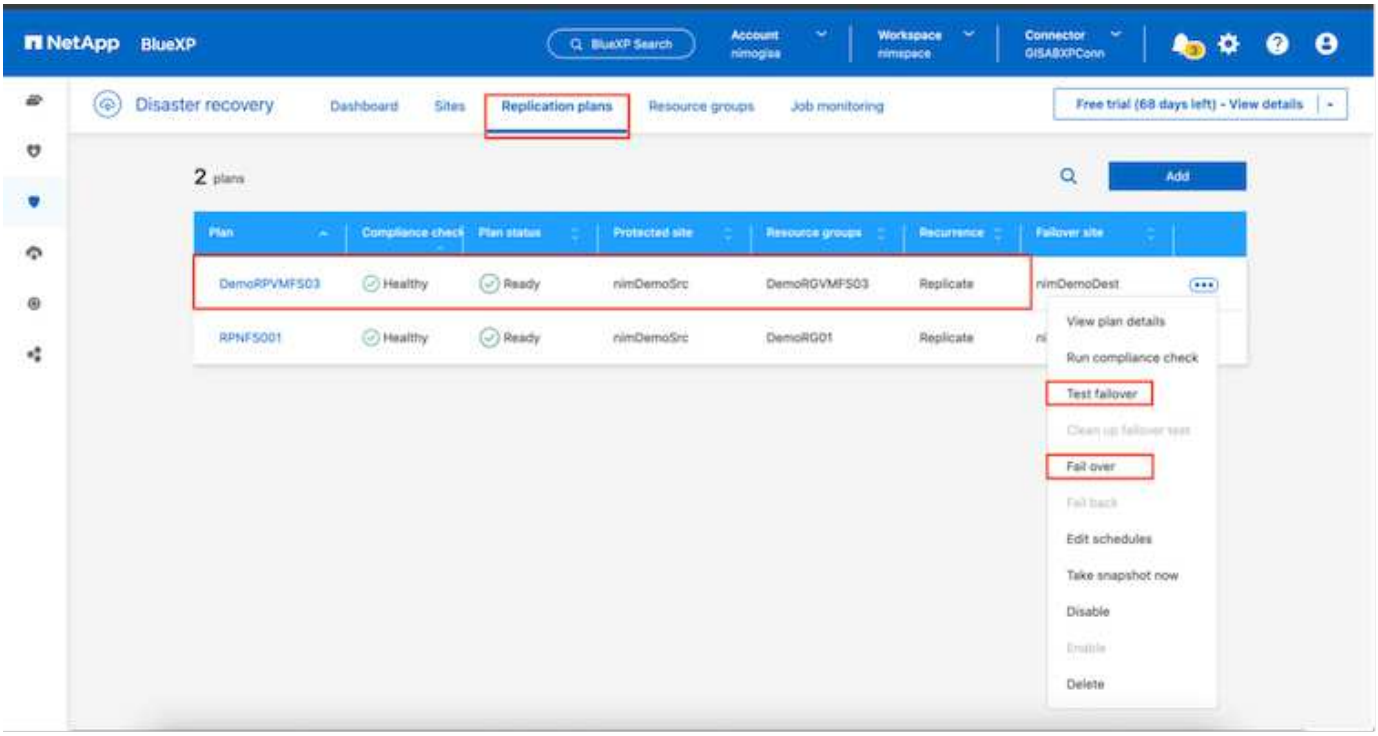




Sobald der Replizierungsplan erstellt wurde, kann ein Failover entsprechend den Anforderungen durchgeführt werden. Wählen Sie dazu die Failover-Option, die Test-Failover-Option oder die Option „Migrieren“. Die BlueXP Disaster Recovery gewährleistet, dass der Replizierungsprozess alle 30 Minuten planmäßig ausgeführt wird. Während der Optionen für Failover und Test-Failover können Sie die neueste SnapMirror Snapshot Kopie verwenden oder eine bestimmte Snapshot Kopie aus einer zeitpunktgenauen Snapshot Kopie auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann sehr hilfreich sein, wenn es ein Korruptionsereignis wie Ransomware gibt, wo die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. BlueXP Disaster Recovery zeigt alle verfügbaren Recovery-Punkte an.



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

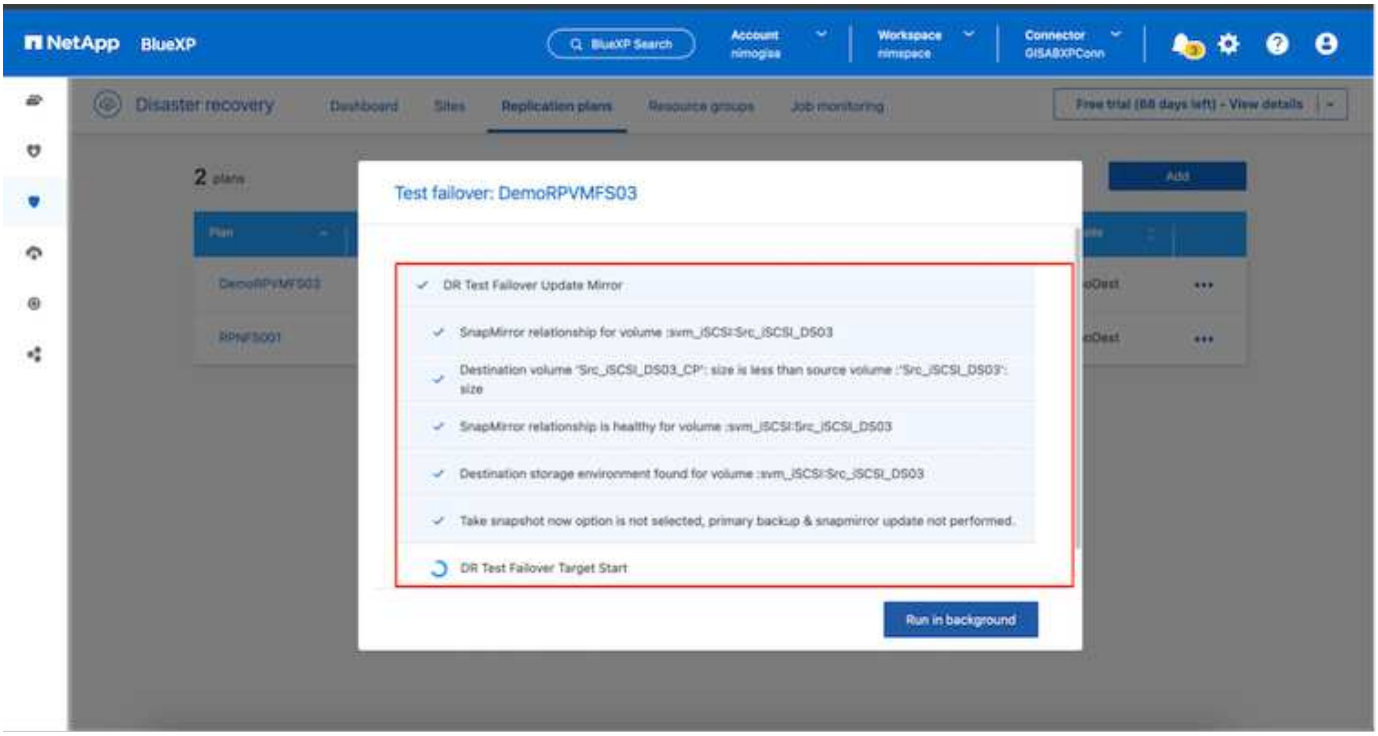


Was geschieht während eines Failover oder eines Test-Failovers?

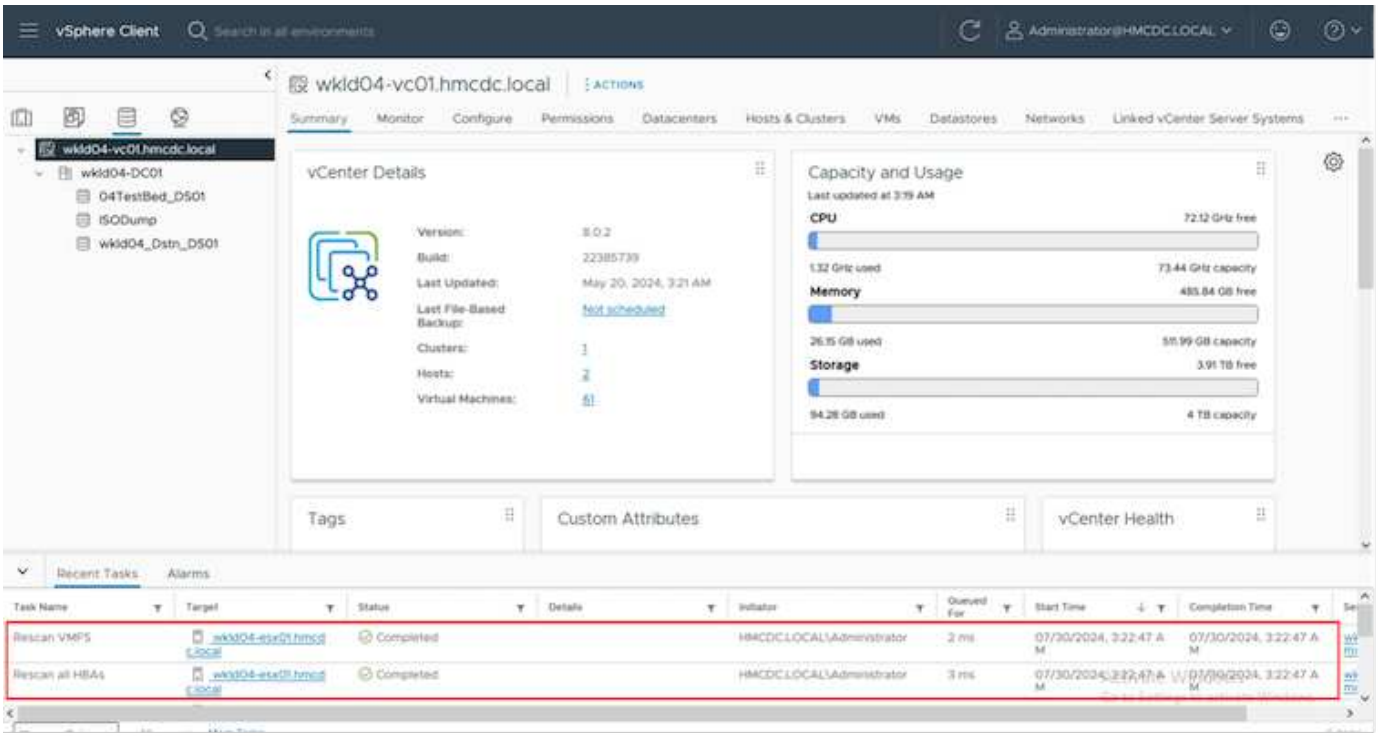
Während eines Test-Failover-Vorgangs erstellt die Disaster Recovery von BlueXP ein FlexClone Volume auf dem ONTAP Zielsystem. Dabei wird die neueste Snapshot Kopie oder ein ausgewählter Snapshot des Ziel-Volume verwendet.

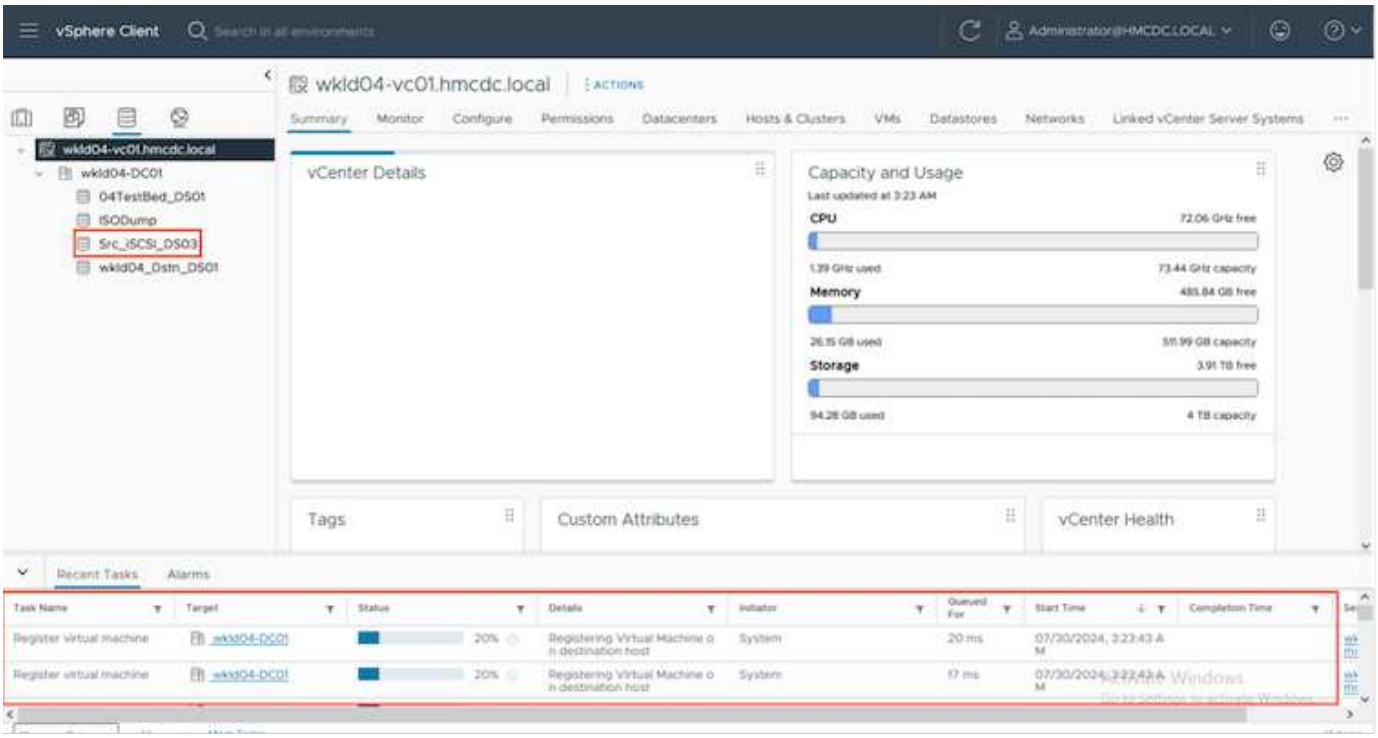
Ein Test-Failover-Vorgang erstellt ein geklontes Volume auf dem ONTAP Zielsystem.

Das Ausführen einer Testwiederherstellung hat keine Auswirkungen auf die SnapMirror-Replikation.



Während des Prozesses ordnet die Disaster Recovery von BlueXP das ursprüngliche Ziel-Volume nicht zu. Stattdessen wird ein neues FlexClone-Volume aus dem ausgewählten Snapshot erstellt und ein temporärer Datastore, der das FlexClone-Volume sichert, den ESXi Hosts zugeordnet.

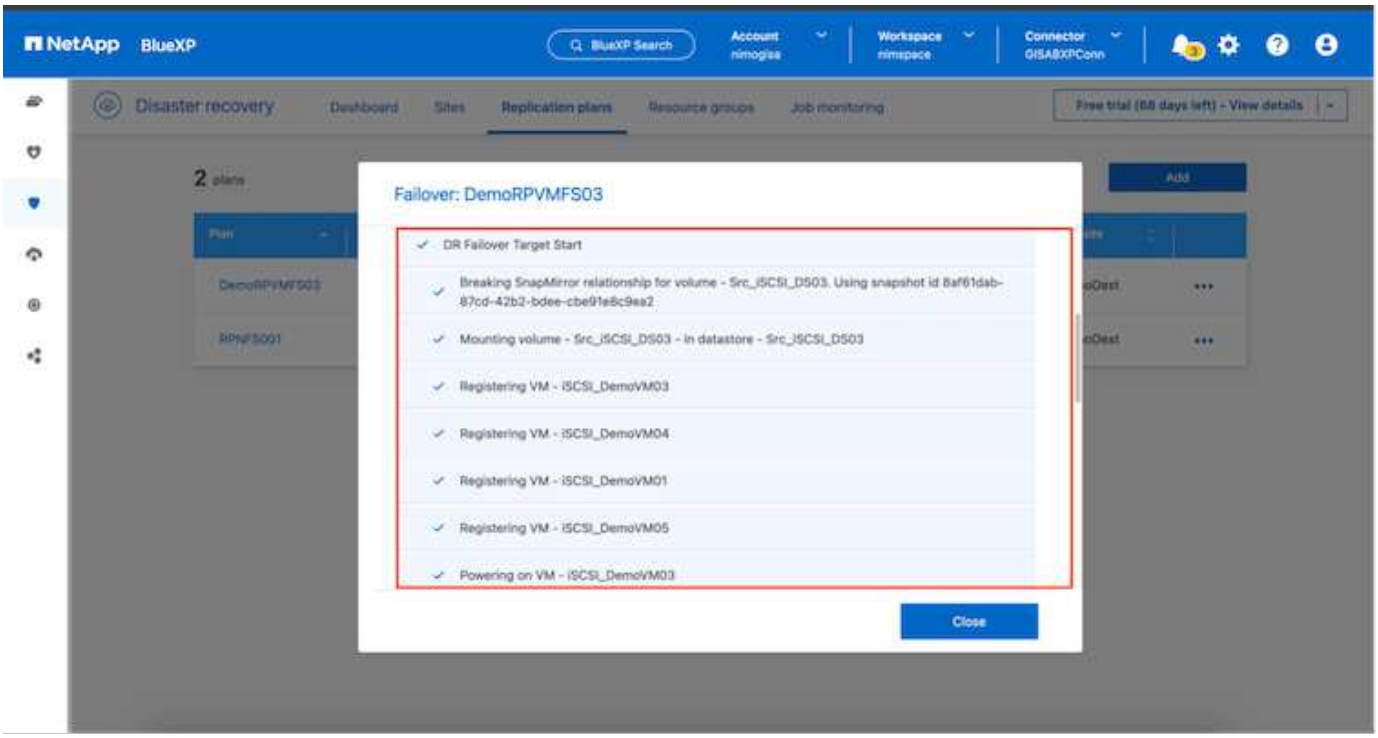




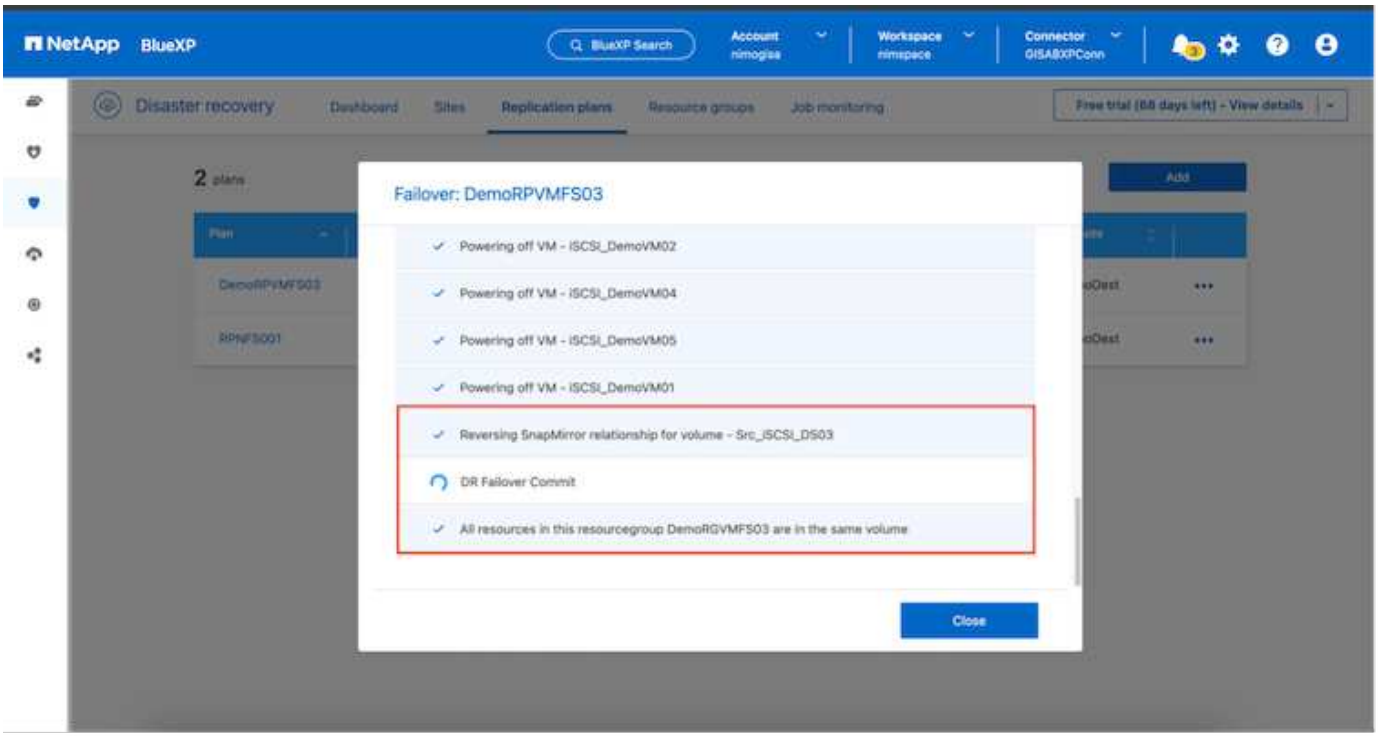
Nach Abschluss des Test-Failovers kann der Bereinigungsvorgang mit * „Clean up Failover Test“* ausgelöst werden. Während dieses Vorgangs zerstört die BlueXP Disaster Recovery das FlexClone Volume, das bei diesem Vorgang verwendet wurde.

Wenn ein echter Notfall eintritt, führt BlueXP Disaster Recovery folgende Schritte durch:

1. Bricht die SnapMirror-Beziehung zwischen den Standorten.
2. Bindet das VMFS-Datastore Volume nach der Neusignatur für die sofortige Verwendung ein.
3. Registrieren Sie die VMs
4. Schalten Sie die VMs ein



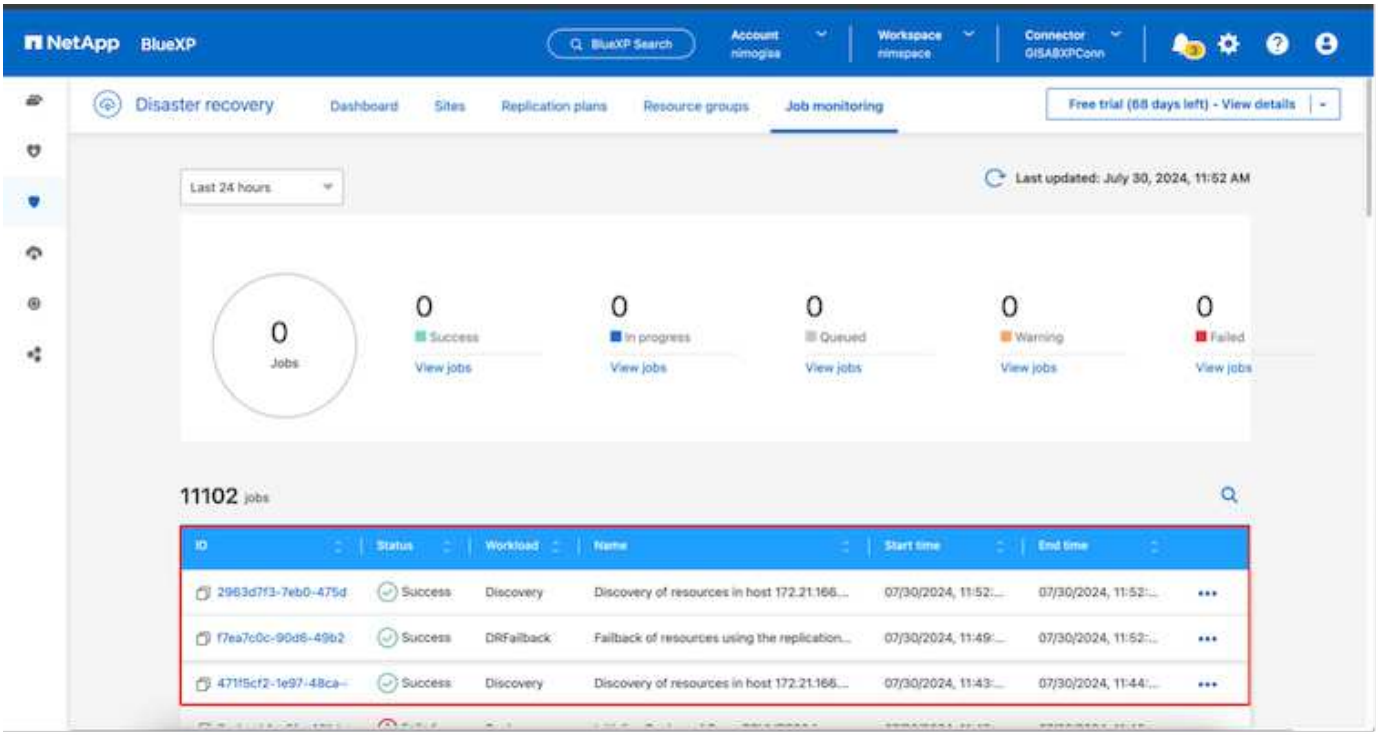
Sobald der primäre Standort in Betrieb ist, ermöglicht das BlueXP Disaster Recovery die umgekehrte Resynchronisierung für SnapMirror und ermöglicht Failback, das auch hier mit nur einem Mausklick durchgeführt werden kann.



Wenn die Option „Migration“ gewählt wird, wird dies als geplantes Failover-Ereignis angesehen. In diesem Fall wird ein zusätzlicher Schritt ausgelöst, der das Herunterfahren der virtuellen Maschinen am Quellstandort umfasst. Die restlichen Schritte bleiben dem Failover-Ereignis gleich.

Über BlueXP oder die ONTAP-CLI können Sie den Replikationsstatus für die entsprechenden Datenspeicher-Volumes überwachen und den Status eines Failover oder Test-Failovers über die Jobüberwachung

nachverfolgen.



Auf diese Weise erhalten Sie eine leistungsstarke Lösung, die einen individuellen Disaster-Recovery-Plan umsetzt. Failover lässt sich als geplanter Failover oder Failover mit einem Mausklick durchführen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung des DR-Standorts getroffen wird.

Um mehr über diesen Prozess zu erfahren, folgen Sie dem ausführlichen Walkthrough-Video oder verwenden Sie die "Lösungssimulator".

Copyright-Informationen

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

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

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