



## Referenz

### NetApp Disaster Recovery

NetApp  
February 04, 2026

# Inhalt

- Referenz ..... 1
  - Erforderliche vCenter-Berechtigungen für NetApp Disaster Recovery ..... 1
  - Switch Console-Agenten bei Verwendung von NetApp Disaster Recovery ..... 4
    - Bevor Sie beginnen ..... 4
    - Schritte ..... 4
    - Weitere Informationen ..... 5
- Verwenden Sie NetApp Disaster Recovery mit Amazon EVS ..... 5
  - Einführung von NetApp Disaster Recovery mit Amazon Elastic VMware Service und Amazon FSx for NetApp ONTAP ..... 6
  - Lösungsübersicht für NetApp Disaster Recovery mit Amazon EVS und Amazon FSs für NetApp ONTAP ..... 6
  - Installieren Sie den NetApp Console -Agenten für NetApp Disaster Recovery ..... 8
  - Konfigurieren Sie NetApp Disaster Recovery für Amazon EVS ..... 8
  - Erstellen von Replikationsplänen für Amazon EVS ..... 21
  - Ausführen von Replikationsplanvorgängen mit NetApp Disaster Recovery ..... 34

# Referenz

## Erforderliche vCenter-Berechtigungen für NetApp Disaster Recovery

Damit NetApp Disaster Recovery seine Dienste ausführen kann, muss das vCenter-Konto über einen Mindestumfang an vCenter-Berechtigungen verfügen. Diese Berechtigungen umfassen das Registrieren und Deregistrieren von Datenspeichern, das Starten und Stoppen virtueller Maschinen (VMs) sowie das Rekonfigurieren von VMs.

Die folgende Tabelle listet alle Berechtigungen auf, die für Disaster Recovery zur Schnittstelle mit einem vCenter-Cluster erforderlich sind.

| Typ           | Berechtigungsname (vSphere client) | Berechtigungsname (API)     | Beschreibung  |
|---------------|------------------------------------|-----------------------------|---|
| Datenspeicher | Datastore.Config                   | Datenspeicher konfigurieren | Ermöglicht die Konfiguration eines Datastores.  |
|               | Datastore.Delete                   | Datenspeicher entfernen     | Ermöglicht das Entfernen eines Datenspeichers.  |
|               | Datastore.Rename                   | Datenspeicher umbenennen    | Ermöglicht das Umbenennen eines Datenspeichers.   |
| Ordner        | Ordner.Create                      | Ordner erstellen            | Ermöglicht das Erstellen eines neuen Ordners.   |
|               | Ordner.Delete                      | Ordner löschen              | Ermöglicht das Löschen eines Ordners. Erfordert Berechtigungen sowohl für das Objekt als auch für dessen übergeordnetes Objekt. |
|               | Ordner.Rename                      | Ordner umbenennen           | Ermöglicht das Ändern eines Ordnersnamens.  |
| Netzwerk      | Network.Assign                     | Netzwerk zuweisen           | Ermöglicht die Zuweisung eines Netzwerks zu einer VM.   |
|               | Network.Config                     | Konfigurieren               | Ermöglicht die Konfiguration eines Netzwerks.   |

| Typ                                   | Berechtigungsname (vSphere client)           | Berechtigungsname (API)              | Beschreibung   |
|---------------------------------------|--|--------------------------------------|--|
| Konfiguration der virtuellen Maschine | VirtualMachine.Config.AdvancedConfig         | Erweiterte Konfiguration             | Ermöglicht das Hinzufügen oder Ändern erweiterter Parameter in der Konfigurationsdatei der VM.   |
|                                       | VirtualMachine.Config.Settings               | Einstellungen ändern                 | Ermöglicht das Ändern allgemeiner VM-Einstellungen.  |
|                                       | VirtualMachine.Config.CPUCount               | CPU-Anzahl ändern                    | Ermöglicht das Ändern der Anzahl von virtuellen CPUs.  |
|                                       | VirtualMachine.Config.Memory                 | Speicher ändern                      | Ermöglicht das Ändern der der VM zugewiesenen Speichermenge.                                     |
|                                       | VirtualMachine.Config.Resource               | Ressource ändern                     | Ermöglicht das Ändern der Ressourcenkonfiguration von VM-Knoten in einem Ressourcenpool.         |
|                                       | VirtualMachine.Config.Rename                 | Umbenennen                           | Ermöglicht das Umbenennen einer VM oder das Ändern ihrer Notizen.                                |
|                                       | VirtualMachine.Config.EditDevice             | Geräteeinstellungen ändern           | Ermöglicht das Ändern der Eigenschaften eines bestehenden Geräts.                                |
|                                       | VirtualMachine.Config.ReloadFromPath         | Vom Pfad neu laden                   | Ermöglicht das Ändern eines VM-Konfigurationspfads unter Beibehaltung der Identität.             |
|                                       | VirtualMachine.Config.ResetGuestInfo         | Gastinformationen zurücksetzen       | Ermöglicht das Bearbeiten der Gastbetriebssysteminformationen für eine VM.                       |
| Virtueller Maschinen-Gast             | VirtualMachine.GuestOperations.ModifyAliases | Änderung des Gastbetrieb-Alias       | Ermöglicht das Ändern des Alias für die VM.  |
|                                       | VirtualMachine.GuestOperations.QueryAliases  | Gastoperationsaliasabfrage           | Ermöglicht das Abfragen des Alias einer VM.  |
|                                       | VirtualMachine.GuestOperations.Modify        | Änderungen an Gastoperationen        | Ermöglicht Änderungsvorgänge, einschließlich der Übertragung einer Datei auf die VM.             |
|                                       | VirtualMachine.GuestOperations.Execute       | Ausführung des Gastbetrieb-Programms | Ermöglicht das Ausführen einer Anwendung innerhalb der VM.                                       |
|                                       | VirtualMachine.GuestOperations.Query         | Gastbetrieb-Abfragen                 | Ermöglicht das Abfragen des Gastbetriebssystems. Operationen umfassen das Auflisten von Dateien. |

| Typ   | Berechtigungsname (vSphere client)          | Berechtigungsname (API)         | Beschreibung  |
|---|---|---------------------------------|---|
| Interaktion mit der virtuellen Maschine         | VirtualMachine.Interact.AnswerQuestion      | Frage beantworten               | Ermöglicht das Beheben von Problemen während VM-Zustandsübergängen oder Laufzeitfehlern.  |
|   | VirtualMachine.Interact.PowerOff            | Ausschalten                     | Ermöglicht das Ausschalten einer eingeschalteten VM.  |
|   | VirtualMachine.Interact.PowerOn             | Einschalten                     | Ermöglicht das Einschalten oder Fortsetzen einer VM.  |
|   | VirtualMachine.Interact.ToolsInstall        | VMware Tools installieren       | Ermöglicht das Einbinden/Aushängen des VMware Tools Installer.  |
|   | VirtualMachine.Inventory.CreateFromExisting | Aus bestehendem erstellen       | Ermöglicht das Klonen oder Bereitstellen einer VM aus einer Vorlage.  |
|   | VirtualMachine.Inventory.Create             | Neu erstellen                   | Ermöglicht das Erstellen einer VM und das Zuweisen von Ressourcen.  |
|   | VirtualMachine.Inventory.Register           | Anmeldung                       | Ermöglicht das Hinzufügen einer bestehenden VM zu einem Inventar.   |
|   | VirtualMachine.Inventory.Delete             | Entfernen                       | Ermöglicht das Löschen einer virtuellen Maschine und ihrer Dateien. Erfordert Berechtigungen sowohl für das Objekt als auch für dessen übergeordnetes Objekt. |
|   | VirtualMachine.Inventory.Unregister         | Registrierung aufheben          | Ermöglicht das Abmelden einer VM. Diese Berechtigung erfordert Berechtigungen sowohl für das Objekt als auch für dessen übergeordnetes Objekt.                |
| Bereitstellung virtueller Maschinen             | VirtualMachine.Provisioning.Clone           | Virtuelle Maschine klonen       | Ermöglicht das Klonen einer VM und das Zuweisen von Ressourcen.   |
|   | VirtualMachine.Provisioning.Customize       | Gast anpassen                   | Ermöglicht das Anpassen des Gastbetriebssystems der VM.   |
|   | VirtualMachine.Provisioning.ModifyCustSpecs | Anpassungsspezifikation ändern  | Ermöglicht das Erstellen, Ändern oder Löschen von Anpassungsspezifikationen.  |
|   | VirtualMachine.Provisioning.ReadCustSpecs   | Anpassungsspezifikationen lesen | Ermöglicht das Lesen einer Anpassungsspezifikation für eine VM.   |
| Konfiguration des virtuellen Maschinen-Dienstes | VirtualMachine.Namespace.Query              | Dienstkonfigurationen abfragen  | Ermöglicht das Abrufen einer Liste von VM-Services.   |
|   | VirtualMachine.Namespace.ReadContent        | Dienstkonfiguration lesen       | Ermöglicht das Abrufen der bestehenden VM service-Konfiguration.  |

| Typ                              | Berechtigungsname (vSphere client)    | Berechtigungsname (API)   | Beschreibung  |
|----------------------------------|---------------------------------------|---------------------------|---|
| Snapshot der virtuellen Maschine | VirtualMachine.State.CreateSnapshot   | Snapshot erstellen        | Ermöglicht das Erstellen eines Snapshots aus dem aktuellen Zustand der VM.            |
|                                  | VirtualMachine.State.RemoveSnapshot   | Snapshot entfernen        | Ermöglicht das Entfernen eines Snapshots.   |
|                                  | VirtualMachine.State.RenameSnapshot   | Snapshot umbenennen       | Ermöglicht das Umbenennen eines Snapshots oder das Aktualisieren seiner Beschreibung. |
|                                  | VirtualMachine.State.RevertToSnapshot | Auf Snapshot zurücksetzen | Ermöglicht das Zurücksetzen der VM auf den Zustand eines angegebenen Snapshots.       |

## Switch Console-Agenten bei Verwendung von NetApp Disaster Recovery

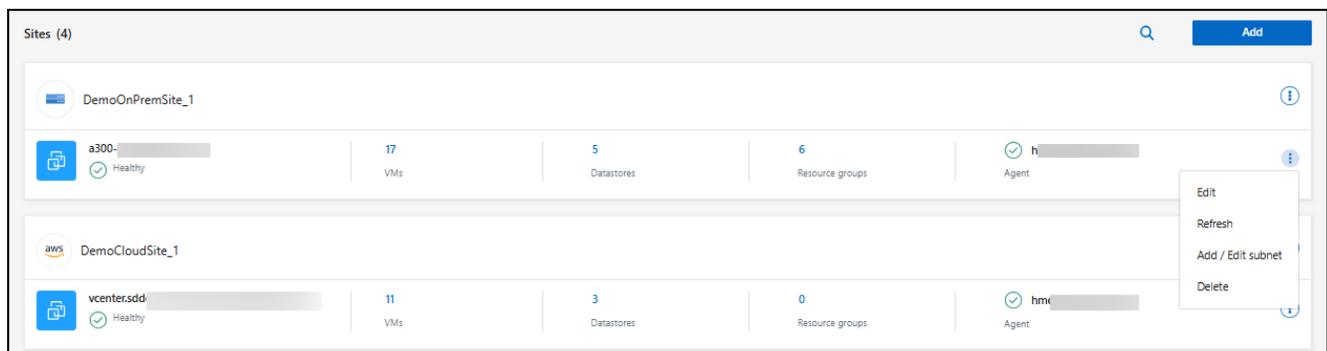
Die NetApp Console unterstützt die Verwendung mehrerer Console-Agenten in einer einzigen Arbeitsumgebung. Der Einsatz mehrerer Console-Agenten kann hilfreich sein, um den Zugriff auf Ressourcen aufrechtzuerhalten, während an einem anderen Console-Agenten Wartungsarbeiten durchgeführt werden oder wenn ein Console-Agent ausfällt. Da jeder Console-Agent über eine eindeutige Kennung verfügt, kann ein unsachgemäßer Wechsel der Console-Agenten die Verfügbarkeit von Ressourcen in einer Arbeitsumgebung beeinträchtigen.

### Bevor Sie beginnen

- Du musst haben [Fügen Sie mindestens zwei Console-Agenten für Ihre Arbeitsumgebung hinzu](#). Die
- Beide Console-Agenten müssen die gleichen ONTAP Cluster enthalten.

### Schritte

1. Im Bereich „Notfallwiederherstellung“ wählen Sie **Standorte** aus.
2. Sie müssen den Konsolenagenten sowohl für das Quell- als auch für das Ziel-vCenter ändern. Identifizieren Sie die vCenter-Server, die Sie ändern möchten. Wählen Sie im vCenter das Aktionsmenü und anschließend **Bearbeiten**.



3. Wählen Sie im Dropdown-Menü den gewünschten Konsolenagenten aus und geben Sie Ihren vCenter-Benutzernamen und Ihr Passwort erneut ein. Wählen Sie **Speichern**.

## Edit vCenter server

Enter connection details for the vCenter server that is accessible from the Console Agent.

|   |  |
|---|--|
| Site  | Console Agent  |
| <input type="text" value="DemoOnPremSite_1"/>                                   | <input type="text" value="hmcdrasconnector4"/>   |
| vCenter IP address  | <input type="text" value="ShivaOnPremConnDemo"/><br><input type="text" value="hmcdrasconnector4"/><br><input type="text" value="DRaaSTest"/> |
| vCenter user name   | vCenter password   |
| <input type="text"/>  | <input type="text"/>   |
| <input checked="" type="checkbox"/> Use self-signed certificates <span>?</span> |  |
| <input type="checkbox"/> Enable scheduled discovery                             |  |

Save

Cancel

4. Wiederholen Sie die Schritte 2 und 3 für jedes weitere vCenter, das Sie ändern möchten.
5. Aktualisieren Sie im vCenter, das Sie geändert haben, das vCenter, um den neuen Konsolenagenten zu erkennen. Wiederholen Sie diesen Schritt für jedes vCenter, das Sie geändert haben.
6. Navigieren Sie im Bereich „Notfallwiederherstellung“ zu **Replikationsplänen**.
7. Ermitteln Sie die Replikationspläne, die Sie zur Wiederaufnahme der Arbeitsabläufe verwenden möchten. Wählen Sie das Aktionsmenü aus ... Aktualisieren Sie anschließend die Ressourcen. Den Status der Aufträge können Sie unter **Auftragsüberwachung** einsehen.

## Weitere Informationen

- ["Erfahren Sie mehr über Konsolenagenten"](#)

## Verwenden Sie NetApp Disaster Recovery mit Amazon EVS

## **Einführung von NetApp Disaster Recovery mit Amazon Elastic VMware Service und Amazon FSx for NetApp ONTAP**

Kunden sind für Produktions-Rechenlasten zunehmend auf virtualisierte Infrastrukturen angewiesen, beispielsweise auf Basis von VMware vSphere. Da diese virtuellen Maschinen (VMs) für ihre Unternehmen immer wichtiger geworden sind, müssen Kunden diese VMs vor denselben Katastrophen schützen wie ihre physischen Rechenressourcen. Die derzeit angebotenen Disaster Recovery (DR)-Lösungen sind komplex, teuer und ressourcenintensiv. NetApp, der größte Speicheranbieter für virtualisierte Infrastrukturen, hat ein begründetes Interesse daran, sicherzustellen, dass die VMs seiner Kunden auf die gleiche Weise geschützt sind, wie wir auf ONTAP -Speicher gehostete Daten aller Art schützen. Um dieses Ziel zu erreichen, hat NetApp den NetApp Disaster Recovery Dienst entwickelt.

Eine der größten Herausforderungen bei jeder DR-Lösung besteht darin, die zusätzlichen Kosten für den Kauf, die Konfiguration und die Wartung zusätzlicher Rechen-, Netzwerk- und Speicherressourcen zu bewältigen, nur um eine DR-Replikations- und Wiederherstellungsinfrastruktur bereitzustellen. Eine beliebte Option zum Schutz kritischer virtueller Ressourcen vor Ort ist die Verwendung in der Cloud gehosteter virtueller Ressourcen als DR-Replikations- und Wiederherstellungsinfrastruktur. Amazon ist ein Beispiel für eine solche Lösung, die kostengünstige Ressourcen bereitstellen kann, die mit von NetApp ONTAP gehosteten VM-Infrastrukturen kompatibel sind.

Amazon hat seinen Amazon Elastic VMware Service (Amazon EVS) eingeführt, der VMware Cloud Foundation in Ihrer Virtual Private Cloud (VPC) ermöglicht. Amazon EVS bietet die Ausfallsicherheit und Leistung von AWS zusammen mit der vertrauten VMware-Software und -Tools, sodass Amazon EVS vCenters als Erweiterung Ihrer virtualisierten Infrastruktur vor Ort integriert werden können.

Obwohl Amazon EVS über integrierte Speicherressourcen verfügt, kann die Verwendung von nativem Speicher die Effektivität für Organisationen mit speicherintensiven Arbeitslasten verringern. In diesen Fällen kann die Kombination von Amazon EVS mit Amazon FSx for NetApp ONTAP -Speicher (Amazon FSxN) eine flexiblere Speicherlösung bieten. Wenn Sie NetApp ONTAP -Speicherlösungen vor Ort zum Hosten Ihrer VMware-Infrastruktur verwenden, erhalten Sie durch die Verwendung von Amazon EVS mit FSx für ONTAP außerdem erstklassige Dateninteroperabilitäts- und Schutzfunktionen zwischen Ihren lokalen und in der Cloud gehosteten Infrastrukturen.

Informationen zu Amazon FSx for NetApp ONTAP finden Sie unter "[Erste Schritte mit Amazon FSx for NetApp ONTAP](#)".

## **Lösungsübersicht für NetApp Disaster Recovery mit Amazon EVS und Amazon FSs für NetApp ONTAP**

NetApp Disaster Recovery ist ein Mehrwertdienst, der in der Software-as-a-Service-Umgebung der NetApp Console gehostet wird und auf der Kernarchitektur der NetApp Console basiert. Der DR-Dienst für den VMware-Schutz innerhalb der Konsole besteht aus mehreren Hauptkomponenten.

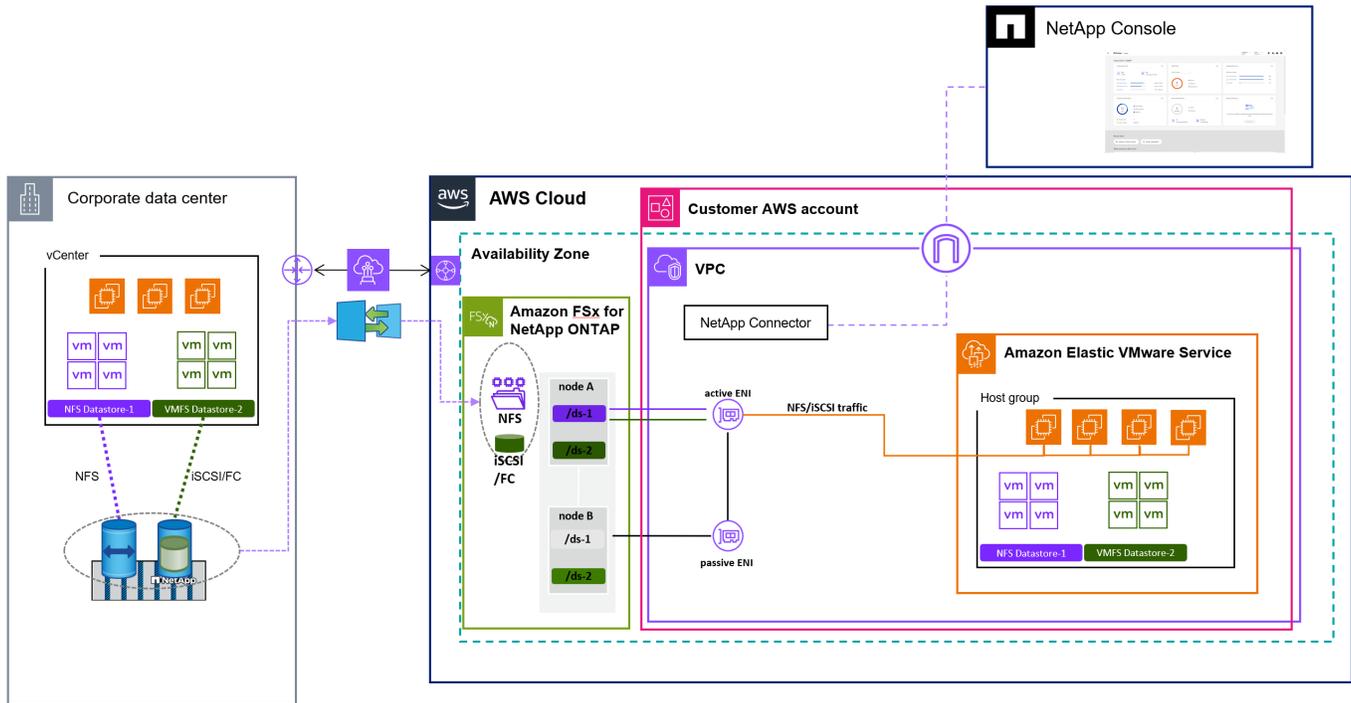
Eine vollständige Übersicht über die NetApp Disaster Recovery -Lösung finden Sie unter "[Erfahren Sie mehr über NetApp Disaster Recovery für VMware](#)".

Wenn Sie Ihre lokalen, von VMware gehosteten virtuellen Maschinen auf Amazon AWS schützen möchten, verwenden Sie den Dienst zum Sichern auf Amazon EVS mit Amazon FSx for NetApp ONTAP Speicher

gehostete Datenspeicher.

Die folgende Abbildung zeigt, wie der Dienst zum Schutz Ihrer VMs mit Amazon EVS funktioniert.

Übersicht über NetApp Disaster Recovery mit Amazon EVS und FSx für ONTAP



1. Amazon EVS wird in Ihrem Konto in einer einzigen Availability Zone (AZ)-Konfiguration und innerhalb Ihrer Virtual Private Cloud (VPC) bereitgestellt.
2. Ein FSx für ONTAP -Dateisystem wird in derselben AZ wie die Amazon EVS-Bereitstellung bereitgestellt. Das Dateisystem stellt entweder direkt über eine Elastic Network Interface (ENI), eine VPC-Peer-Verbindung oder ein AmazonTransit Gateway eine Verbindung zu Amazon EVS her.
3. Der NetApp Console Agent ist in Ihrer VPC installiert. Der NetApp Console Agent hostet mehrere Datenverwaltungsdienste (sogenannte Agenten), darunter den NetApp Disaster Recovery -Agenten, der die Notfallwiederherstellung der VMware-Infrastruktur sowohl in Ihren lokalen physischen Rechenzentren als auch auf Ihren von Amazon AWS gehosteten Ressourcen verwaltet.
4. Der NetApp Disaster Recovery -Agent kommuniziert sicher mit dem in der Cloud gehosteten Dienst der NetApp Console, um Aufgaben zu empfangen und diese Aufgaben an die entsprechenden lokalen und von AWS gehosteten vCenter- und ONTAP Speicherinstanzen zu verteilen.
5. Sie erstellen einen Replikationsplan mithilfe der in der Cloud gehosteten Benutzeroberflächenkonsole NetApp Console und geben dabei die zu schützenden VMs, die Häufigkeit des Schutzes dieser VMs und die Verfahren an, die zum Neustart dieser VMs im Falle eines Failovers vom lokalen Standort ausgeführt werden müssen.
6. Der Replikationsplan bestimmt, welche vCenter-Datenspeicher die geschützten VMs hosten und welche ONTAP -Volumes diese Datenspeicher hosten. Wenn auf dem FSx für ONTAP -Cluster noch keine Volumes vorhanden sind, werden diese von NetApp Disaster Recovery automatisch erstellt.
7. Für jedes identifizierte Quell- ONTAP -Volume wird eine SnapMirror -Beziehung zu jedem Ziel-FSx für das von ONTAP gehostete ONTAP -Volume erstellt und ein Replikationszeitplan wird basierend auf dem vom Benutzer bereitgestellten RPO im Replikationsplan erstellt.
8. Im Falle eines Ausfalls des primären Standorts leitet ein Administrator einen manuellen Failover-Prozess

innerhalb der NetApp Console ein und wählt ein Backup aus, das als Wiederherstellungspunkt verwendet werden soll.

9. Der NetApp Disaster Recovery -Agent aktiviert die von FSx für ONTAP gehosteten Datensicherungsvolumen.
10. Der Agent registriert jedes aktivierte FSx für ONTAP -Volume beim Amazon EVS vCenter, registriert jede geschützte VM beim Amazon EVS vCenter und startet jede gemäß den im Replikationsplan enthaltenen vordefinierten Regeln.

## Installieren Sie den NetApp Console -Agenten für NetApp Disaster Recovery

Ein NetApp Console-Agent ermöglicht es Ihnen, Ihre NetApp Console-Bereitstellungen mit Ihrer Infrastruktur zu verbinden, um Lösungen sicher über AWS, Azure, Google Cloud oder lokale Umgebungen hinweg zu orchestrieren. Der Console-Agent führt die Aktionen aus, die die NetApp Console zur Verwaltung Ihrer Dateninfrastruktur ausführen muss. Der Console-Agent fragt die NetApp Disaster Recovery Software-as-a-Service-Schicht kontinuierlich ab, um alle erforderlichen Aktionen auszuführen.

Für NetApp Disaster Recovery orchestrieren die ausgeführten Aktionen VMware vCenter-Cluster und ONTAP-Speicherinstanzen mithilfe nativer APIs für jeden jeweiligen Dienst, um Schutz für Produktions-VMs zu bieten, die an einem lokalen Standort ausgeführt werden. Obwohl der Console-Agent an jedem Ihrer Netzwerkstandorte installiert werden kann, wird empfohlen, den Console-Agent am Disaster-Recovery-Standort für NetApp Disaster Recovery zu installieren. Die Installation am DR-Standort stellt sicher, dass im Falle eines Ausfalls des primären Standorts die NetApp Console UI die Verbindung zum Console-Agent aufrechterhält und den Wiederherstellungsprozess innerhalb dieses DR-Standorts orchestrieren kann.

### Installation

- Um NetApp Disaster Recovery zu nutzen, installieren Sie den Console-Agenten im Standardmodus. Weitere Informationen zu den Typen der Console-Agenten-Installationen finden Sie unter ["Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console"](#).

Die konkreten Installationsschritte für den Konsolenagenten hängen von Ihrem Bereitstellungstyp ab. Siehe ["Erfahren Sie mehr über Konsolenagenten"](#) für weitere Informationen.



Die einfachste Methode zur Installation des Console-Agenten mit Amazon AWS ist die Verwendung des AWS Marketplace. Weitere Informationen zur Installation des Console-Agenten über den AWS Marketplace finden Sie unter ["Erstellen Sie einen Console-Agenten aus dem AWS Marketplace"](#).

## Konfigurieren Sie NetApp Disaster Recovery für Amazon EVS

### Übersicht: Konfigurieren von NetApp Disaster Recovery für Amazon EVS

Nachdem Sie den NetApp Console Agenten installiert haben, müssen Sie alle ONTAP -Speicher- und VMware vCenter-Ressourcen, die am Disaster Recovery-Prozess teilnehmen, mit NetApp Disaster Recovery integrieren.

- ["Voraussetzungen für Amazon EVS mit NetApp Disaster Recovery"](#)
- ["Fügen Sie ONTAP Speicher-Arrays zu NetApp Disaster Recovery hinzu"](#)

- ["Aktivieren Sie NetApp Disaster Recovery für Amazon EVS"](#)
- ["vCenter-Sites zu NetApp Disaster Recovery hinzufügen"](#)
- ["vCenter-Cluster zu NetApp Disaster Recovery hinzufügen"](#)

## Voraussetzungen für Amazon EVS mit NetApp Disaster Recovery

Stellen Sie sicher, dass Sie die Anforderungen für die Konfiguration von Amazon EVS mit NetApp Disaster Recovery überprüfen und erfüllen.

### Voraussetzungen

- Überprüfen Sie die ["Allgemeine Voraussetzungen für Disaster Recovery"](#).
- Erstellen Sie ein vCenter-Benutzerkonto mit den spezifischen VMware-Berechtigungen, die für NetApp Disaster Recovery erforderlich sind, um die erforderlichen Vorgänge auszuführen.



Es wird empfohlen, **nicht** das Standardkonto „administrator@vsphere.com“ als Administrator zu verwenden. Stattdessen sollten Sie ein NetApp Disaster Recovery-spezifisches Benutzerkonto auf allen vCenter Clustern erstellen, die am Disaster-Recovery-Prozess teilnehmen. Eine Liste der spezifischen erforderlichen Berechtigungen finden Sie unter ["Für NetApp Disaster Recovery erforderliche vCenter-Berechtigungen"](#).

- Stellen Sie sicher, dass alle vCenter Datenspeicher, die VMs hosten, die durch Disaster Recovery geschützt sind, sich auf NetApp ONTAP Speicherressourcen befinden.

Disaster Recovery unterstützt NFS und VMFS über iSCSI (und nicht FC) bei Verwendung von Amazon FSx auf NetApp ONTAP. Obwohl Disaster Recovery FC unterstützt, unterstützt Amazon FSx for NetApp ONTAP dies nicht.

- Stellen Sie sicher, dass Ihr Amazon EVS vCenter mit einem Amazon FSx for NetApp ONTAP Storage-Cluster verbunden ist.
- Stellen Sie sicher, dass VMware tools auf allen geschützten VMs installiert sind.
- Stellen Sie sicher, dass Ihr lokales Netzwerk über eine von Amazon zugelassene Verbindungsmethode mit Ihrem AWS VPC-Netzwerk verbunden ist. Es wird empfohlen, AWS Direct Connect, AWS Private Link oder eine AWS Site-to-Site VPN zu verwenden.
- Überprüfen und sicherstellen, dass die Anschluss- und Portanforderungen für EVS mit Disaster Recovery eingehalten werden:

| Quelle               | Ziel  | Port                   | Details                          |
|----------------------|---|------------------------|----------------------------------|
| Amazon FSxN          | On-Premises-ONTAP                               | TCP 11104, 11105, ICMP | SnapMirror                       |
| On-Premises-ONTAP    | Amazon FSxN                                     | TCP 11104, 11105, ICMP | SnapMirror                       |
| NetApp Console-Agent | On-Premises-ONTAP                               | TCP 443, nur ICMP      | API-Aufrufe                      |
| NetApp Console-Agent | Amazon FSxN                                     | TCP 441, nur ICMP      | API-Aufrufe                      |
| NetApp Console-Agent | vCenter (lokal, EVS),<br>ESXi-Host (lokal, EVS) | 443                    | API-Aufrufe,<br>Skriptausführung |

## Fügen Sie mit NetApp Disaster Recovery lokale Arrays zum NetApp Console für Amazon EVS hinzu

Bevor Sie NetApp Disaster Recovery verwenden, müssen Sie dem NetApp Console lokale und in der Cloud gehostete Speicherinstanzen hinzufügen.

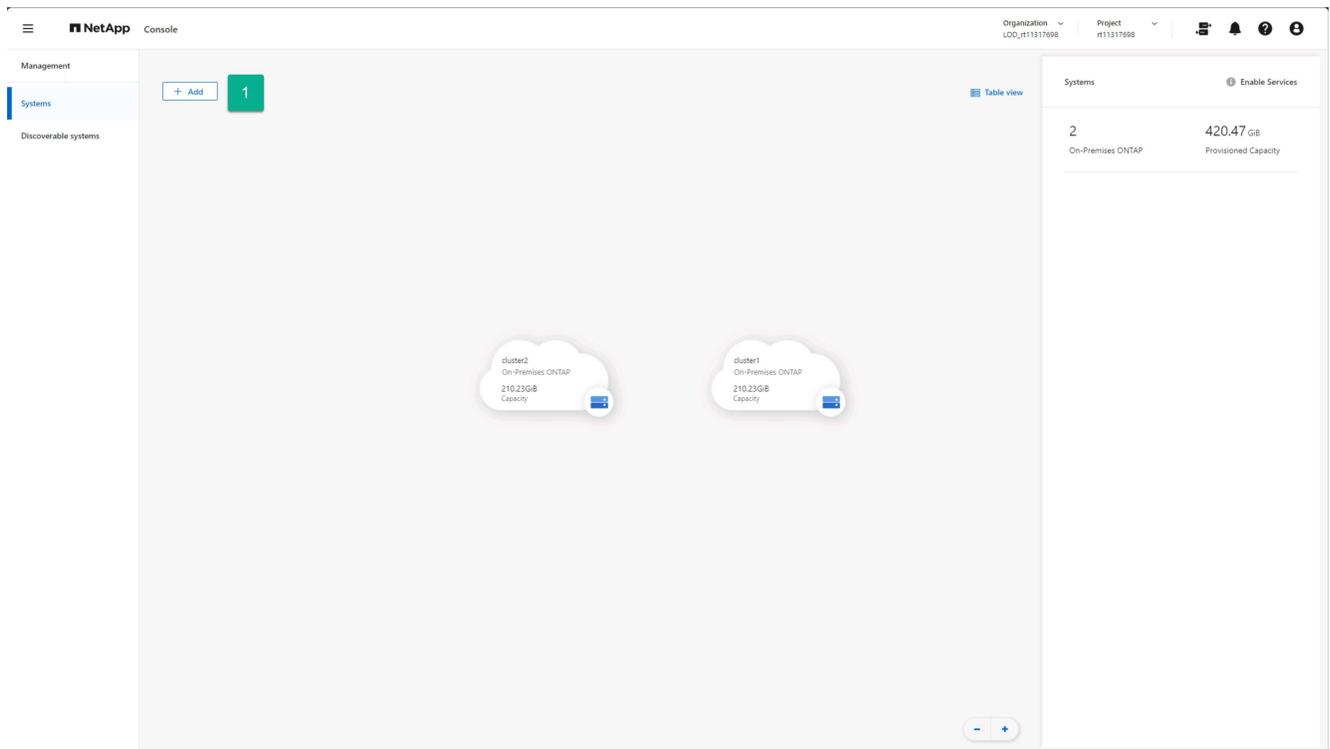
Sie müssen Folgendes tun:

- Fügen Sie Ihrem NetApp Console lokale Arrays hinzu.
- Fügen Sie Ihrem NetApp Console Amazon FSx for NetApp ONTAP (FSx für ONTAP )-Instanzen hinzu.

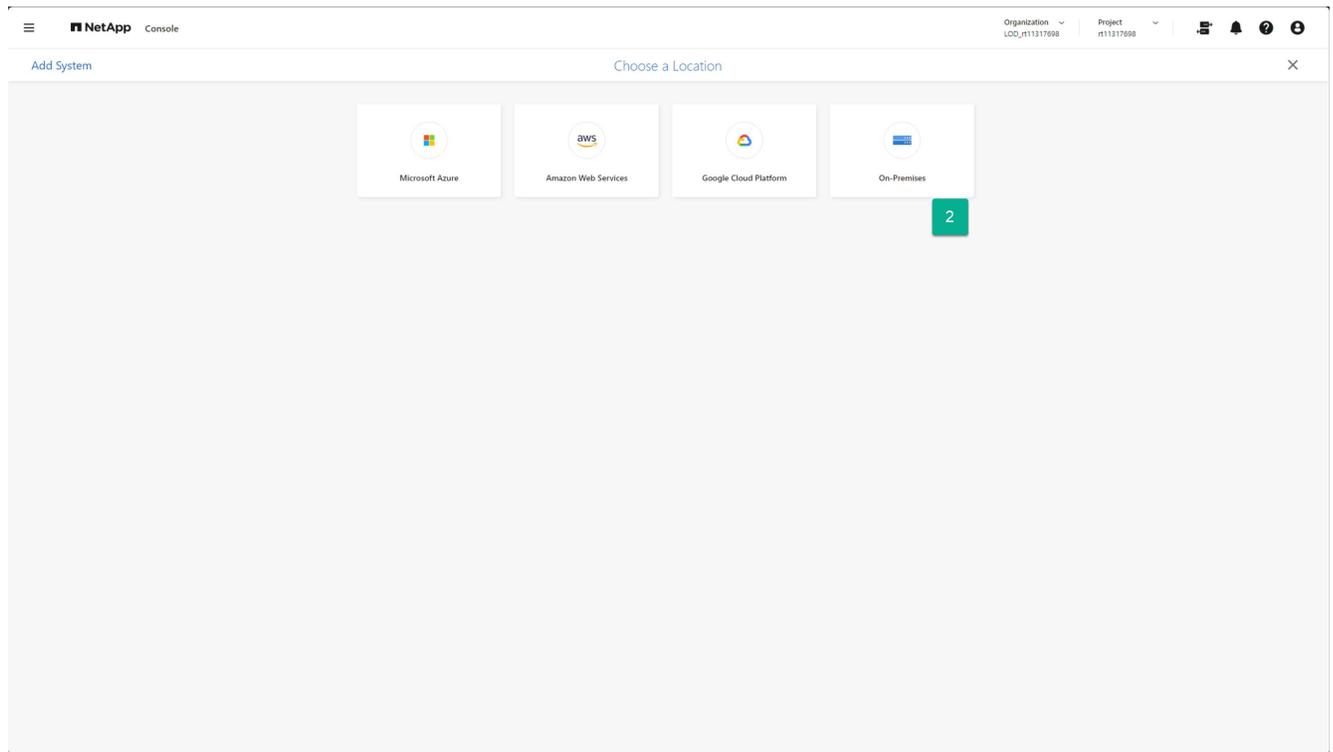
### Fügen Sie dem NetApp Console lokale Speicher-Arrays hinzu

Fügen Sie Ihrem NetApp Console lokale ONTAP Speicherressourcen hinzu.

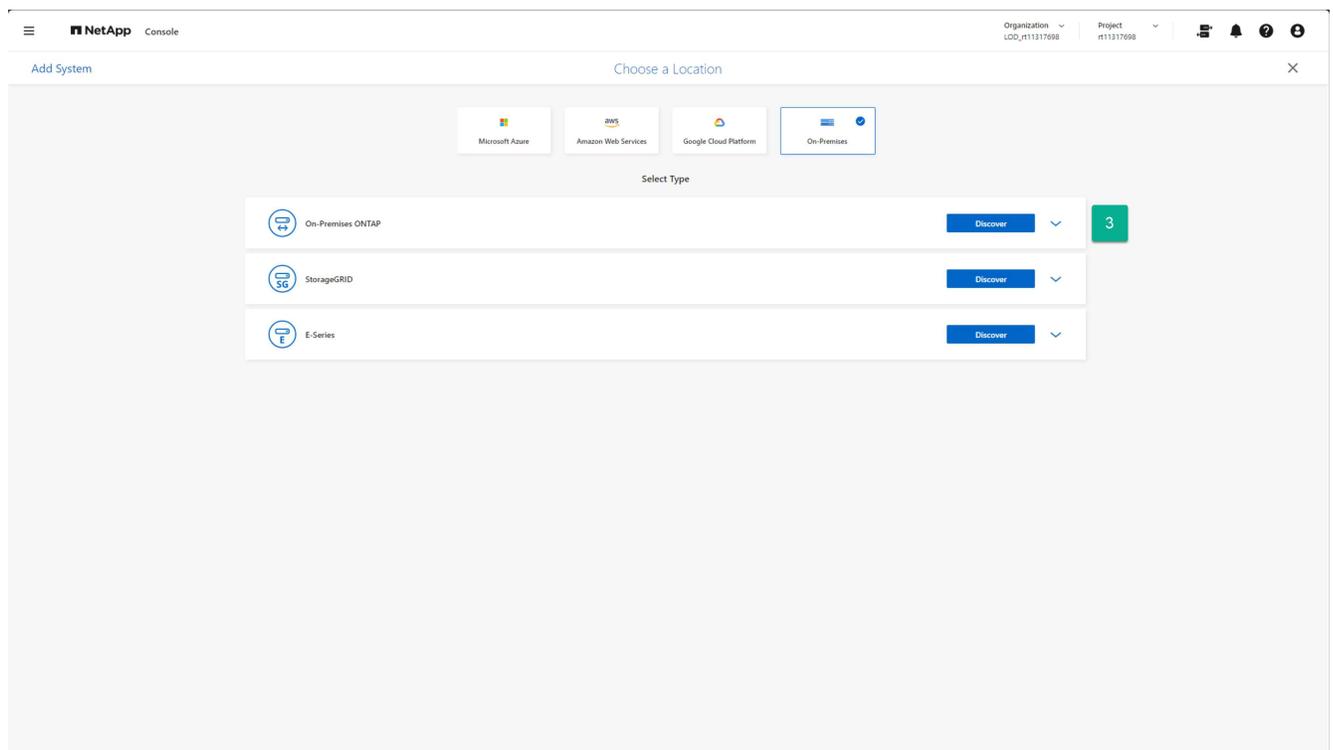
1. Wählen Sie auf der Seite „NetApp Console “ die Option „System hinzufügen“ aus.



2. Wählen Sie auf der Seite „System hinzufügen“ die Karte **On-Premises** aus.



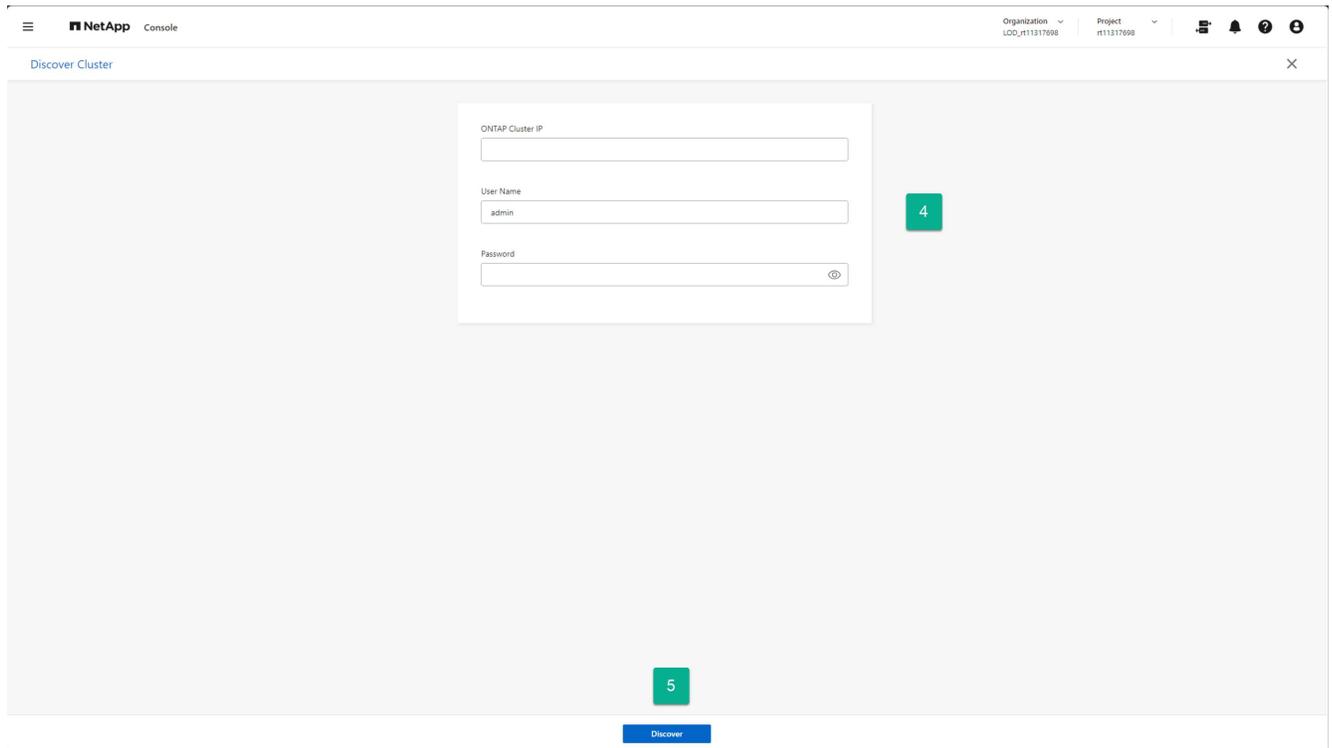
3. Wählen Sie **Erkennen** auf der On-Premises ONTAP Karte.



4. Geben Sie auf der Seite „Cluster ermitteln“ die folgenden Informationen ein:

- Die IP-Adresse des ONTAP -Array-Cluster-Management-Ports
- Der Administrator-Benutzername
- Das Administratorkennwort

5. Wählen Sie unten auf der Seite **Entdecken** aus.

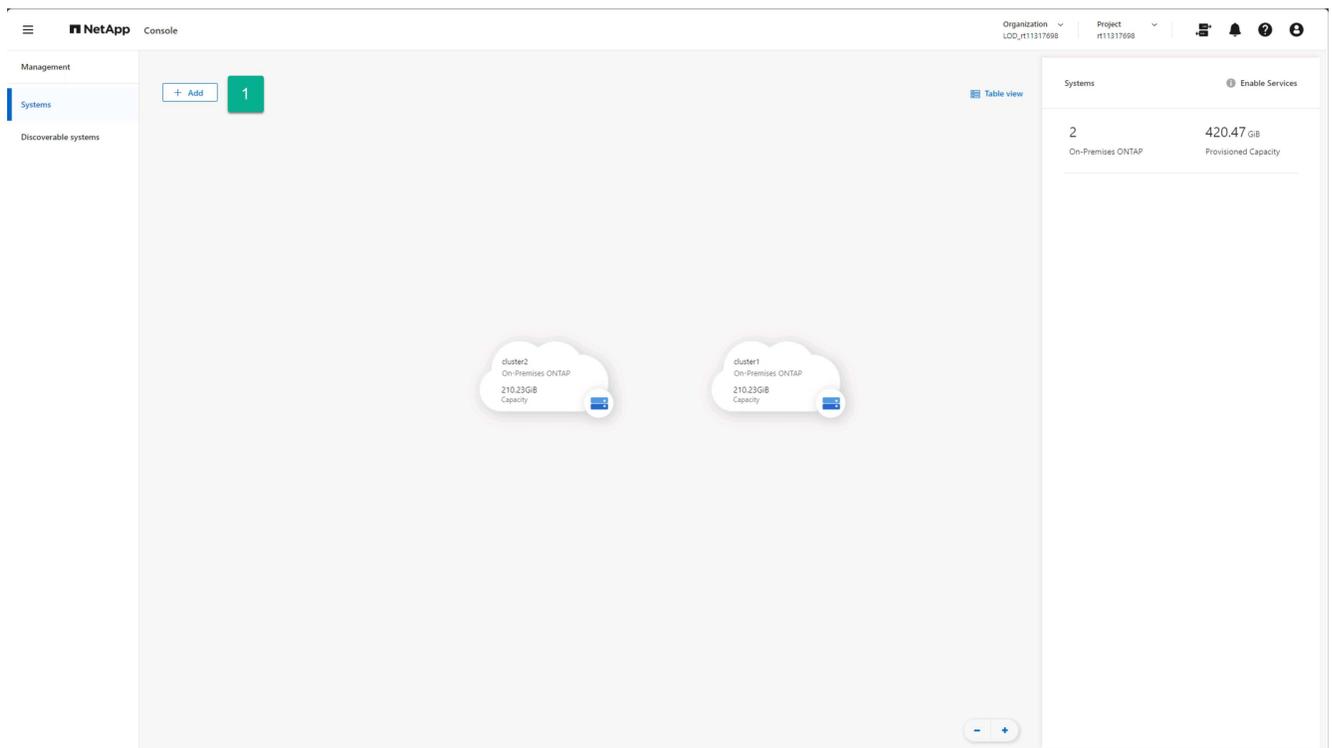


6. Wiederholen Sie die Schritte 1–5 für jedes ONTAP Array, das vCenter-Datenspeicher hosten soll.

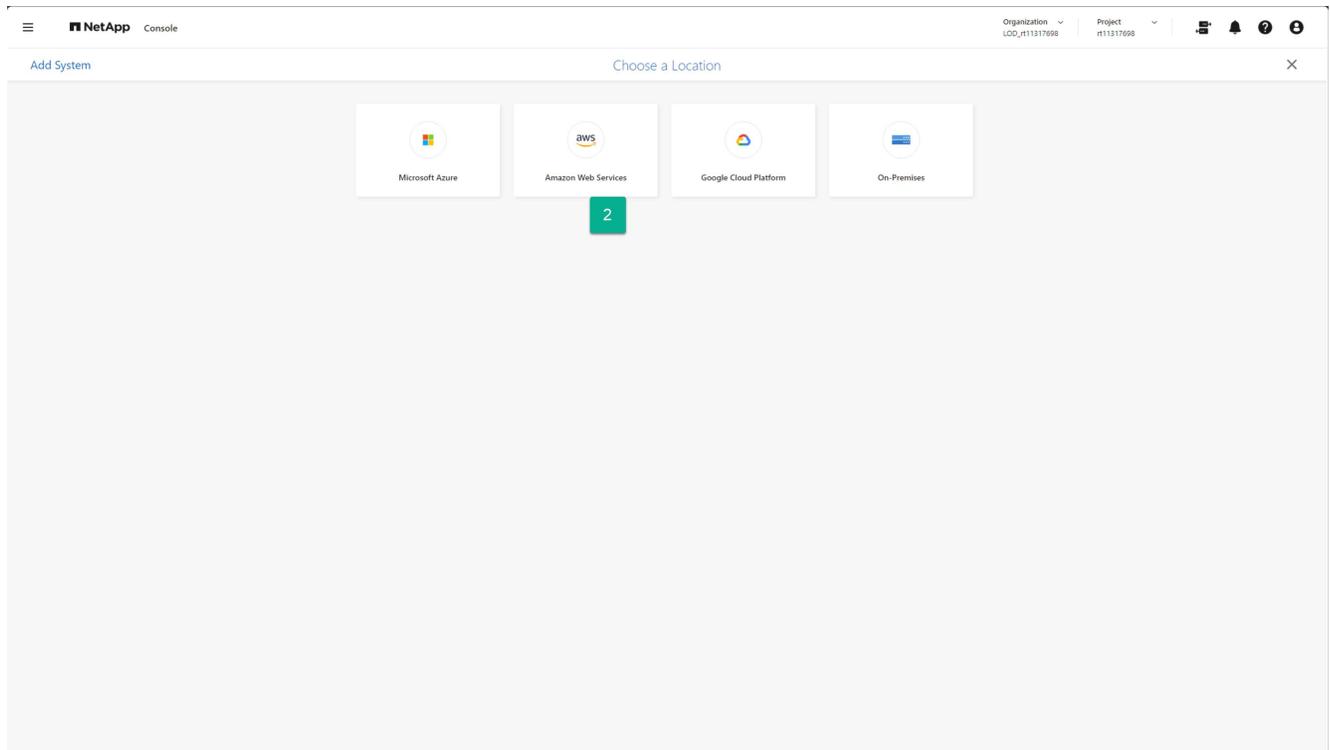
**Fügen Sie Amazon FSx for NetApp ONTAP Speicherinstanzen zum NetApp Console hinzu**

Fügen Sie als Nächstes Ihrem NetApp Console Amazon FSx for NetApp ONTAP -Speicherressourcen hinzu.

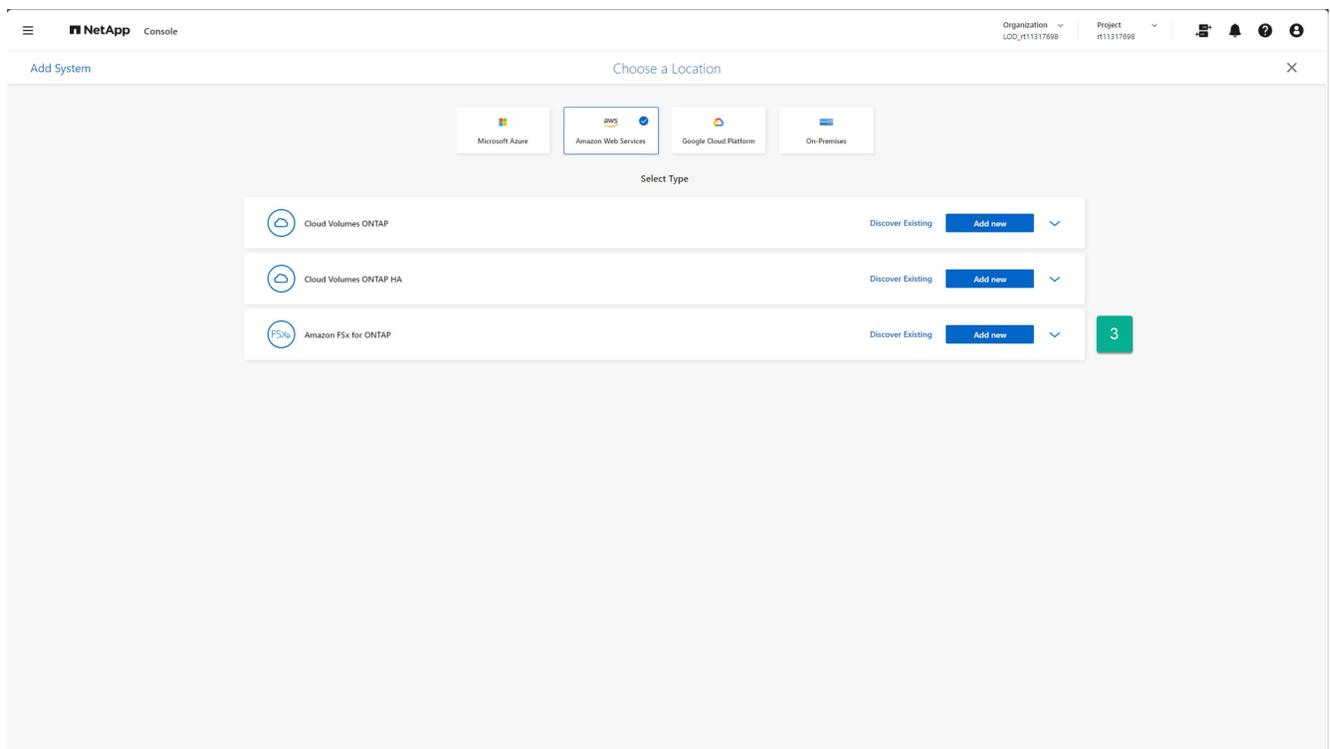
1. Wählen Sie auf der Seite „NetApp Console “ die Option „System hinzufügen“ aus.



2. Wählen Sie auf der Seite „System hinzufügen“ die Karte **Amazon Web Services** aus.



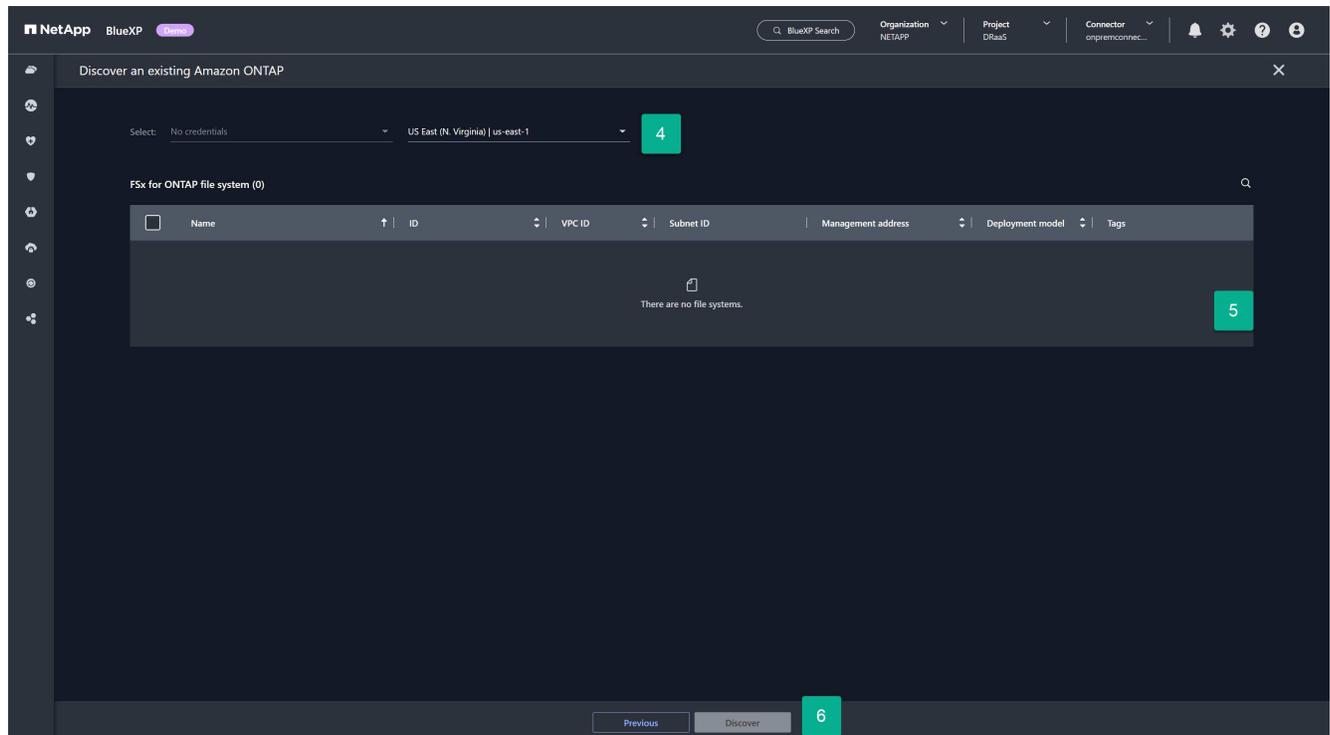
3. Wählen Sie den Link **Vorhandenes entdecken** auf der Amazon FSx for ONTAP -Karte.



4. Wählen Sie die Anmeldeinformationen und die AWS-Region aus, in der die FSx for ONTAP Instanz gehostet wird.

5. Wählen Sie ein oder mehrere FSx for ONTAP -Dateisysteme aus, die hinzugefügt werden sollen.

6. Wählen Sie unten auf der Seite **Entdecken** aus.



7. Wiederholen Sie die Schritte 1–6 für jede FSx for ONTAP -Instanz, die vCenter-Datenspeicher hosten wird.

### Fügen Sie Ihrem NetApp Console für Amazon EVS den NetApp Disaster Recovery -Dienst hinzu

NetApp Disaster Recovery ist ein lizenziertes Produktangebot, das vor der Verwendung erworben werden muss. Es gibt verschiedene Arten von Lizenzen und verschiedene Möglichkeiten, Lizenzen zu erwerben. Eine Lizenz berechtigt Sie zum Schutz einer bestimmten Datenmenge für einen bestimmten Zeitraum.

Weitere Informationen zu NetApp Disaster Recovery Lizenzen finden Sie unter ["Einrichten der Lizenzierung für NetApp Disaster Recovery"](#) .

### Lizenztypen

Es gibt zwei primäre Lizenztypen:

- NetApp bietet eine **"30-Tage-Testlizenz"** mit dem Sie NetApp Disaster Recovery unter Verwendung Ihrer ONTAP und VMware-Ressourcen evaluieren können. Diese Lizenz ermöglicht eine 30-tägige Nutzung einer unbegrenzten Menge an geschützter Kapazität.
- Erwerben Sie eine Produktionslizenz, wenn Sie DR-Schutz über den 30-tägigen Testzeitraum hinaus wünschen. Diese Lizenz kann über die Marktplätze aller Cloud-Partner von NetApp erworben werden. Für diesen Leitfaden empfehlen wir jedoch, dass Sie Ihre Marktplatzlizenz für NetApp Disaster Recovery über den Amazon AWS Marketplace erwerben. Weitere Informationen zum Erwerb einer Lizenz über den Amazon Marketplace finden Sie unter ["Abonnieren Sie über AWS Marketplace"](#) .

### Bemessen Sie Ihren Kapazitätsbedarf für die Notfallwiederherstellung

Bevor Sie Ihre Lizenz erwerben, sollten Sie wissen, wie viel ONTAP Speicherkapazität Sie schützen müssen. Einer der Vorteile der Verwendung von NetApp ONTAP Speicher ist die hohe Effizienz, mit der NetApp Ihre

Daten speichert. Alle in einem ONTAP Volume gespeicherten Daten – beispielsweise VMware-Datenspeicher, die VMs hosten – werden auf hocheffiziente Weise gespeichert. ONTAP verwendet beim Schreiben von Daten in den physischen Speicher standardmäßig drei Arten der Speichereffizienz: Komprimierung, Deduplizierung und Komprimierung. Das Nettoergebnis ist eine Speichereffizienz zwischen 1,5:1 und 4:1, abhängig von den gespeicherten Datentypen. Tatsächlich bietet NetApp eine "**Speichereffizienzgarantie**" für bestimmte Arbeitslasten.

Dies kann für Sie von Vorteil sein, da NetApp Disaster Recovery die Kapazität für Lizenzierungszwecke berechnet, nachdem alle ONTAP Speichereffizienzen angewendet wurden. Nehmen wir beispielsweise an, Sie haben in vCenter einen 100 Terabyte (TiB) großen NFS-Datenspeicher bereitgestellt, um 100 VMs zu hosten, die Sie mithilfe des Dienstes schützen möchten. Nehmen wir außerdem an, dass beim Schreiben der Daten auf das ONTAP Volume automatisch angewendete Techniken zur Speichereffizienz dazu führen, dass diese VMs nur 33 TiB verbrauchen (Speichereffizienz 3:1). NetApp Disaster Recovery muss nur für 33 TiB lizenziert werden, nicht für 100 TiB. Dies kann im Vergleich zu anderen DR-Lösungen einen sehr großen Vorteil hinsichtlich der Gesamtbetriebskosten Ihrer DR-Lösung bedeuten.

### Schritte

1. Um zu ermitteln, wie viele Daten auf jedem Volume verbraucht werden, auf dem sich ein zu schützender VMware-Datenspeicher befindet, ermitteln Sie den Kapazitätsverbrauch auf der Festplatte, indem Sie für jedes Volume den ONTAP CLI-Befehl ausführen: `volume show-space -volume < volume name > -vserver < SVM name > .`

Beispiel:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                               Used           Used%
-----
User Data                             163.4MB        3%
Filesystem Metadata                   172KB          0%
Inodes                                2.93MB         0%
Snapshot Reserve                       292.9MB        5%
Total Metadata                         185KB          0%
Total Used                             459.4MB        8%
Total Physical Used                    166.4MB        3%
```

2. Notieren Sie den Wert **Total Physical Used** für jedes Volume. Dies ist die Datenmenge, die NetApp Disaster Recovery schützen muss. Anhand dieses Werts bestimmen Sie, wie viel Kapazität Sie lizenzieren müssen.

### Hinzufügen von Sites in NetApp Disaster Recovery für Amazon EVS

Bevor Sie Ihre VM-Infrastruktur schützen können, müssen Sie ermitteln, welche VMware vCenter-Cluster die zu schützenden VMs hosten und wo sich diese vCenter befinden. Der erste Schritt besteht darin, eine Site zu erstellen, die die Quell- und Ziel-Rechenzentren darstellt. Eine Site ist eine Fehlerdomäne oder eine Wiederherstellungsdomäne.

Sie müssen Folgendes erstellen:

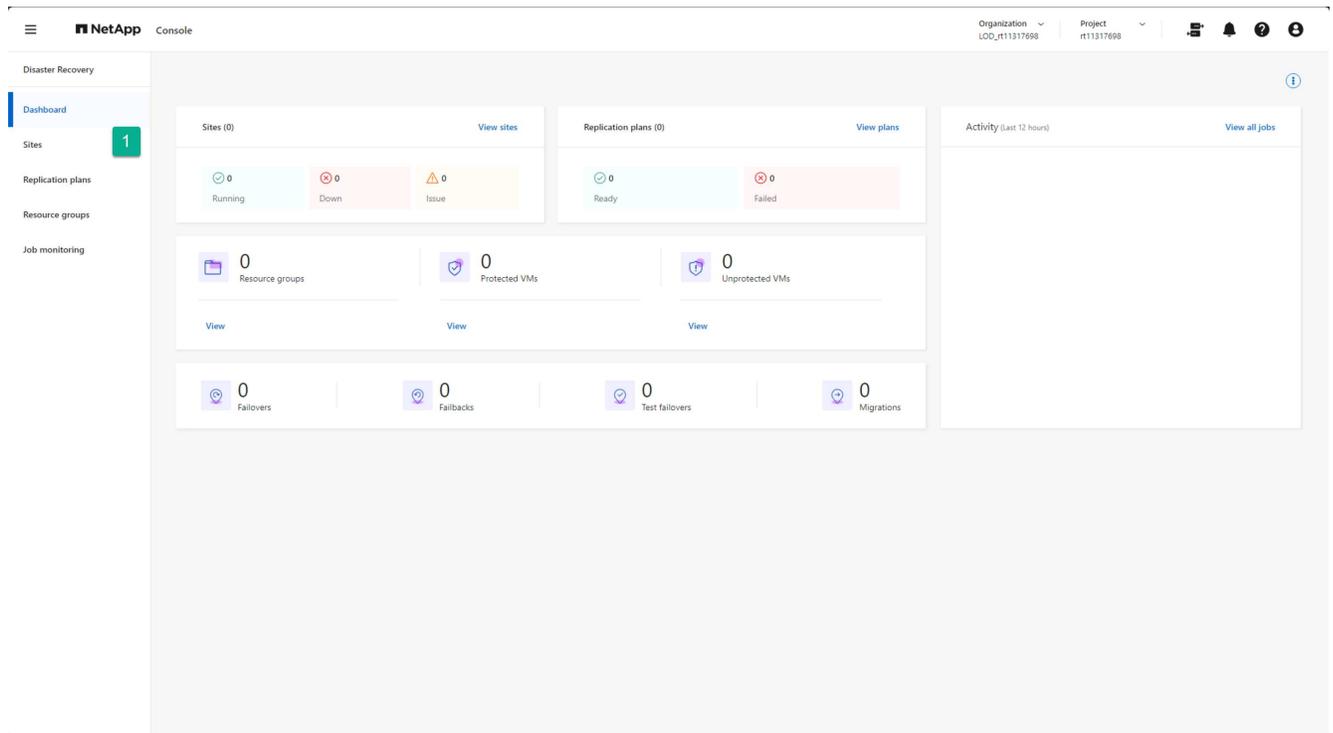
- Eine Site zur Darstellung jedes Produktionsrechenzentrums, in dem sich Ihre Produktions-vCenter-Cluster befinden
- Eine Site für Ihr Amazon EVS/ Amazon FSx for NetApp ONTAP Cloud-Rechenzentrum

### Erstellen lokaler Websites

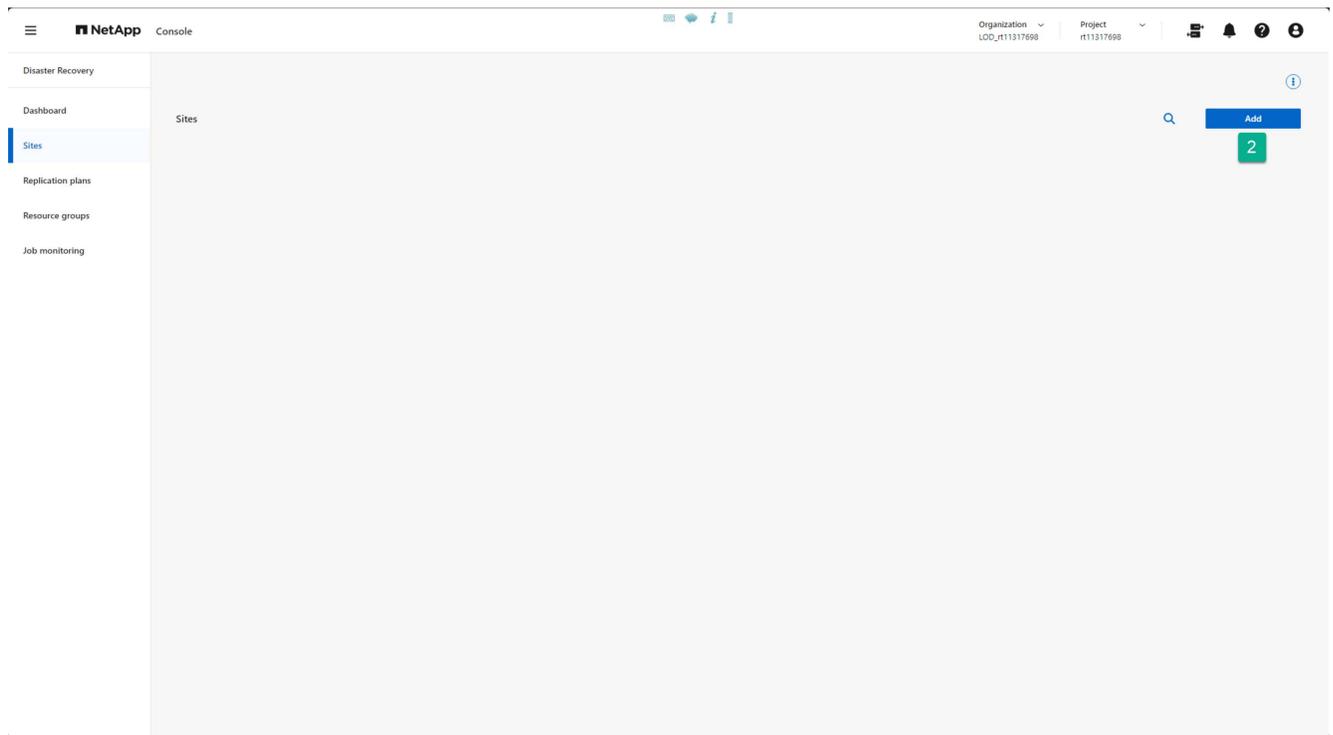
Erstellen Sie eine vCenter-Produktionssite.

### Schritte

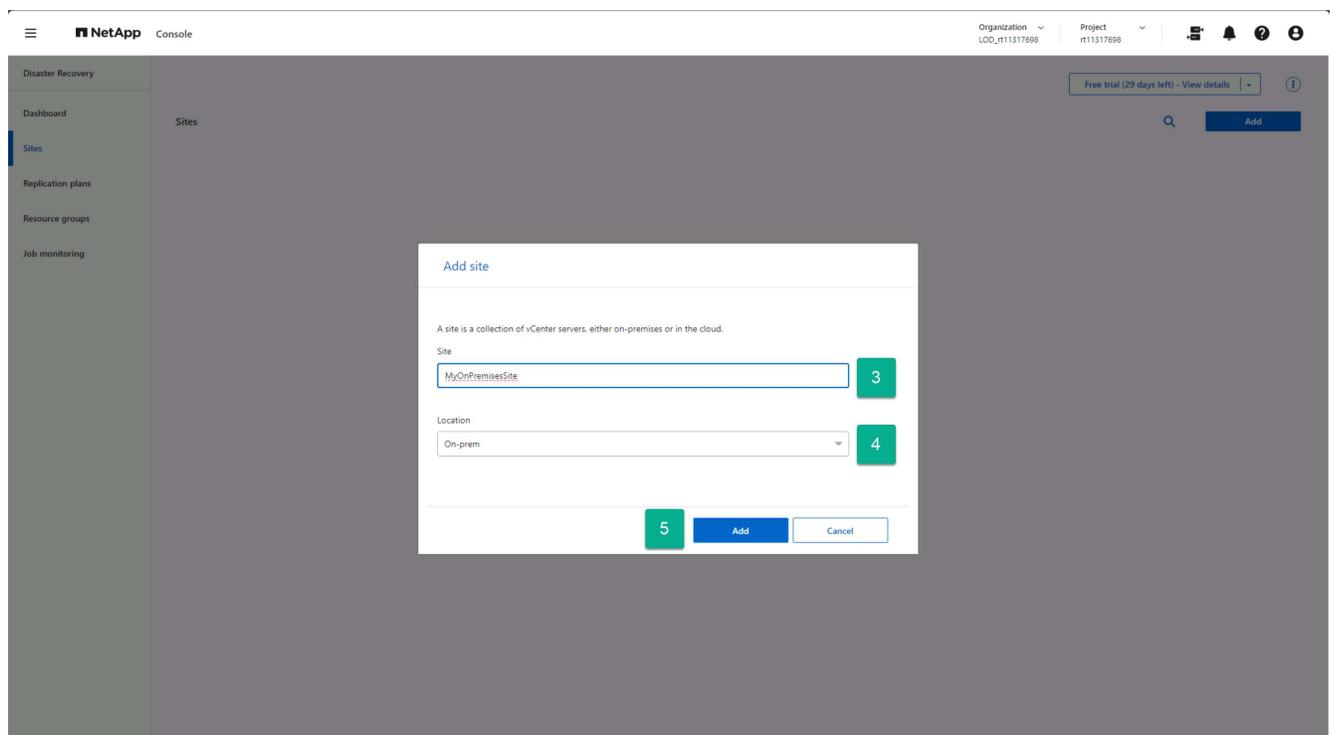
1. Wählen Sie in der linken Navigationsleiste der NetApp Console **Schutz > Notfallwiederherstellung**.
2. Wählen Sie auf einer beliebigen Seite in NetApp Disaster Recovery die Option **Sites** aus.



3. Wählen Sie unter der Option „Sites“ die Option „Hinzufügen“ aus.



4. Geben Sie im Dialogfeld „Site hinzufügen“ einen Sitenamen ein.
5. Wählen Sie als Standort „On-Prem“ aus.
6. Wählen Sie **Hinzufügen**.

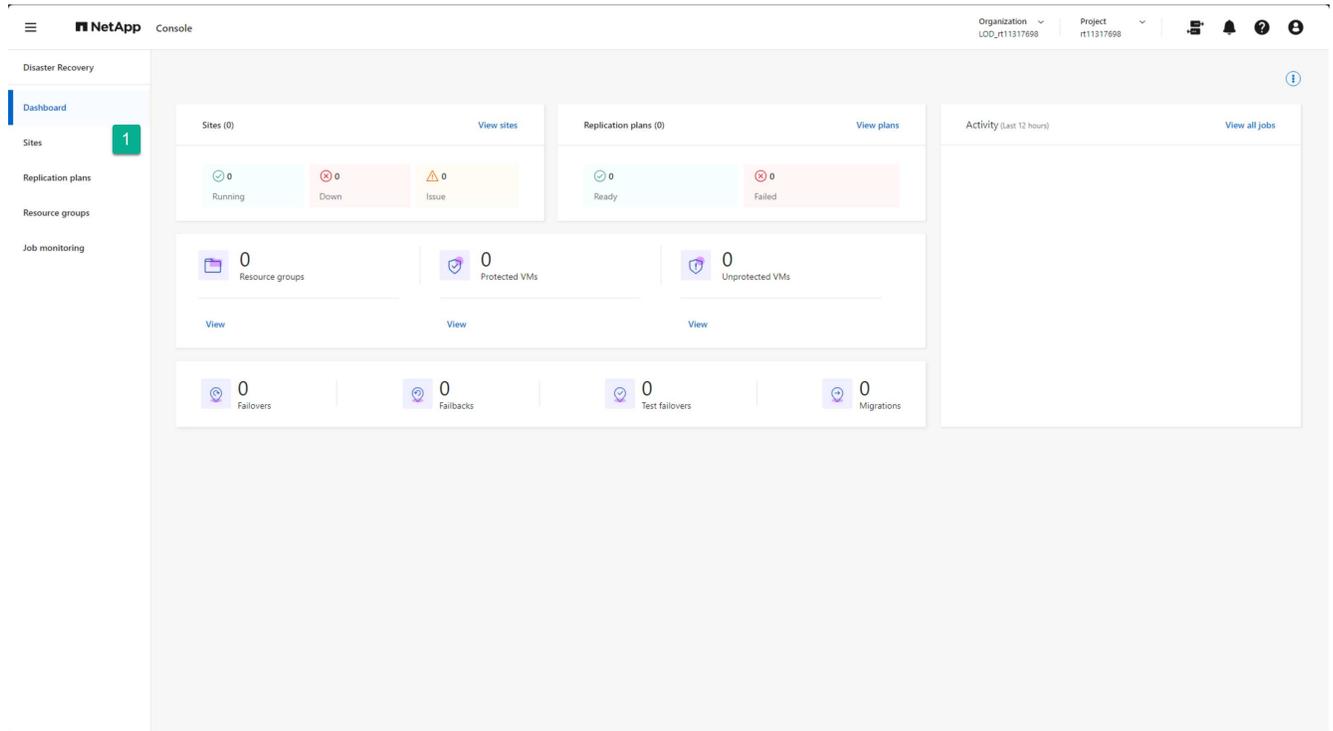


Wenn Sie über andere vCenter-Produktionssites verfügen, können Sie diese mit denselben Schritten hinzufügen.

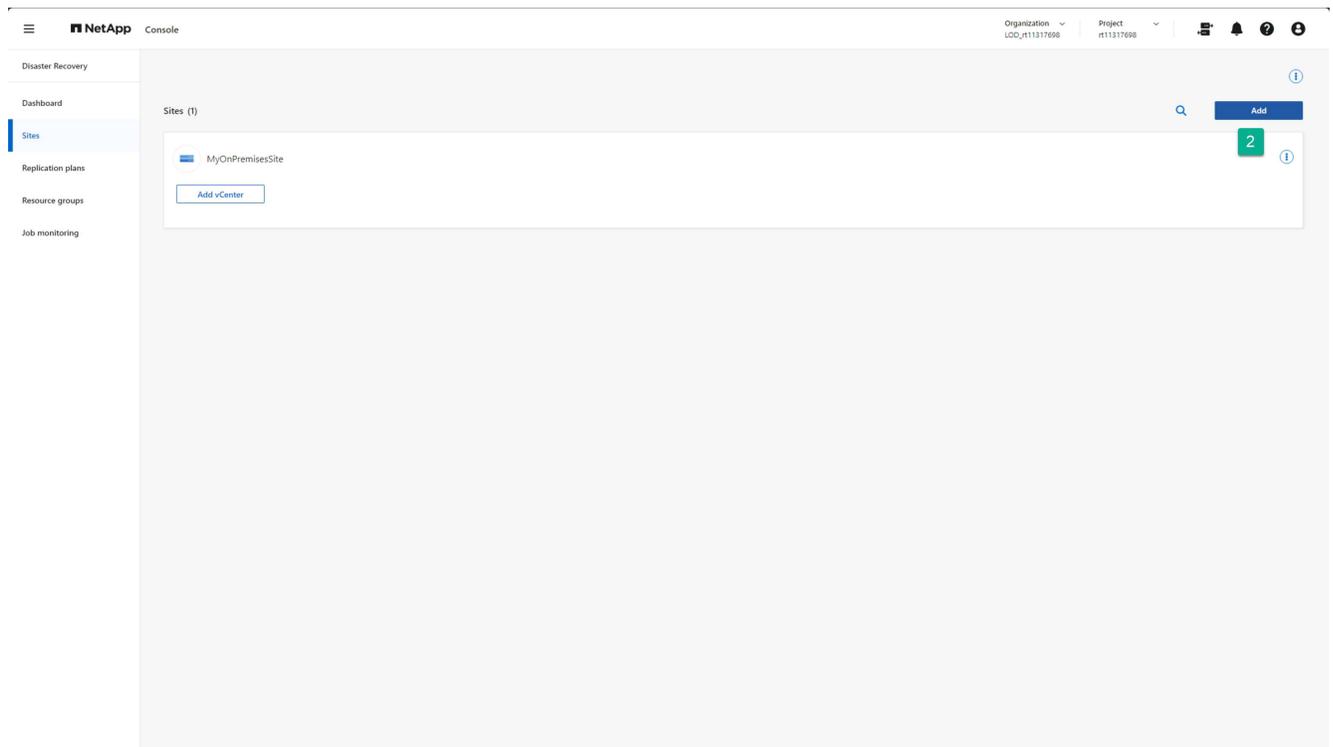
## Erstellen Sie Amazon Cloud-Sites

Erstellen Sie eine DR-Site für Amazon EVS mit Amazon FSx for NetApp ONTAP -Speicher.

1. Wählen Sie auf einer beliebigen Seite in NetApp Disaster Recovery die Option **Sites** aus.



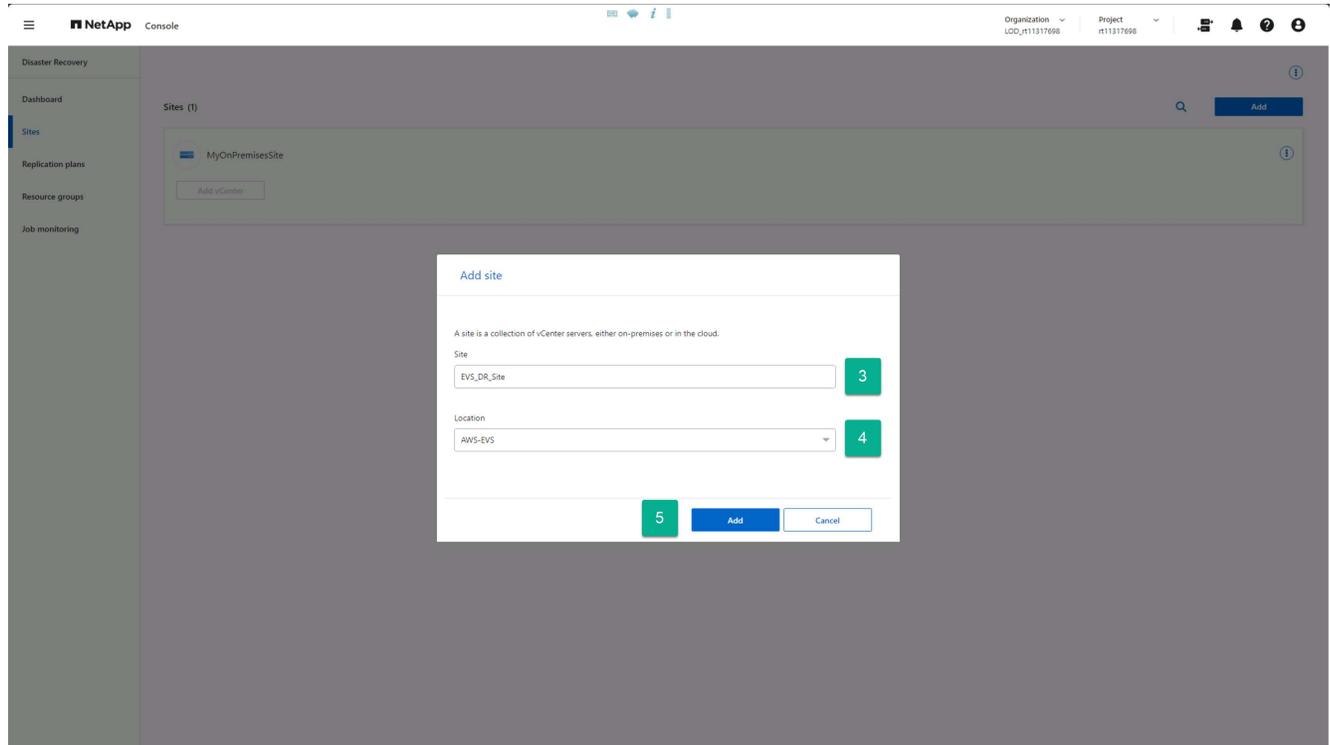
2. Wählen Sie unter der Option „Sites“ die Option „Hinzufügen“ aus.



3. Geben Sie im Dialogfeld „Site hinzufügen“ einen Sitenamen ein.

4. Wählen Sie „AWS-EVS“ als Standort aus.

5. Wählen Sie **Hinzufügen**.



## Ergebnis

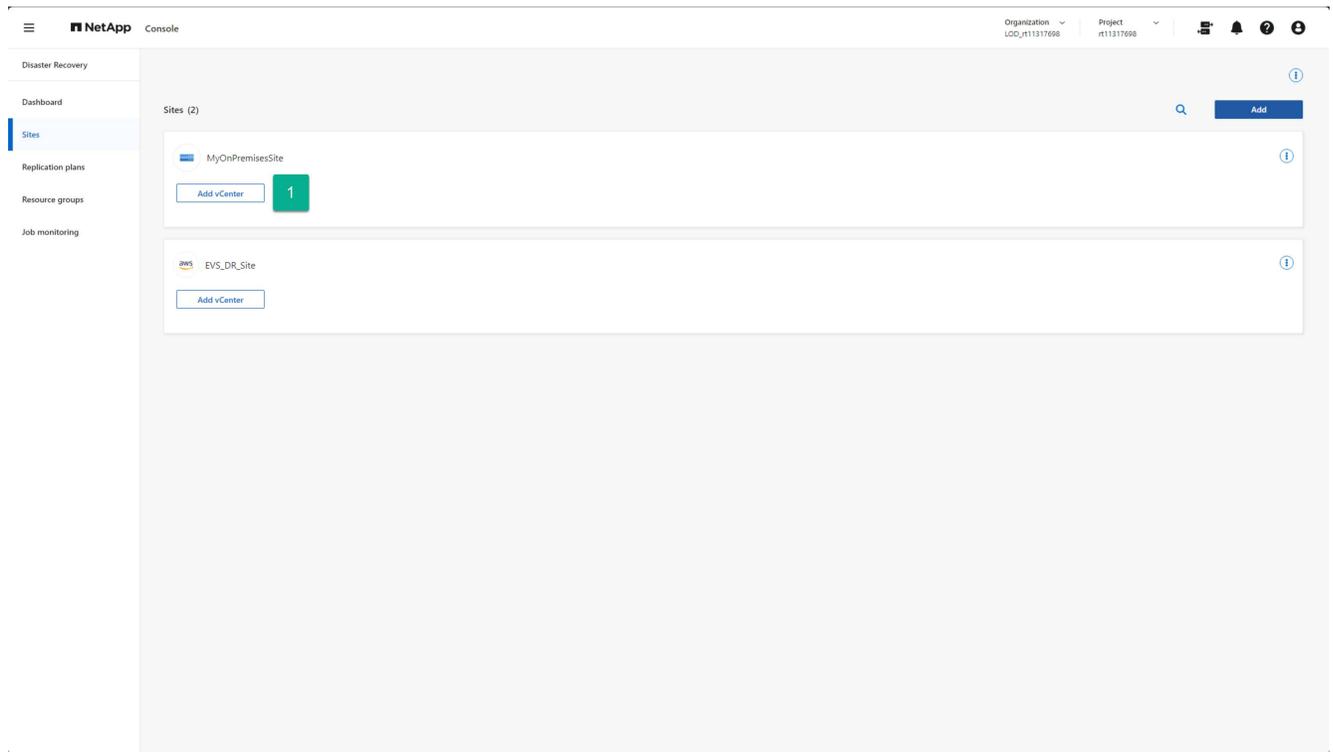
Sie haben jetzt einen Produktionsstandort (Quellstandort) und einen DR-Standort (Zielstandort) erstellt.

## Hinzufügen von lokalen und Amazon EVS vCenter-Clustern in NetApp Disaster Recovery

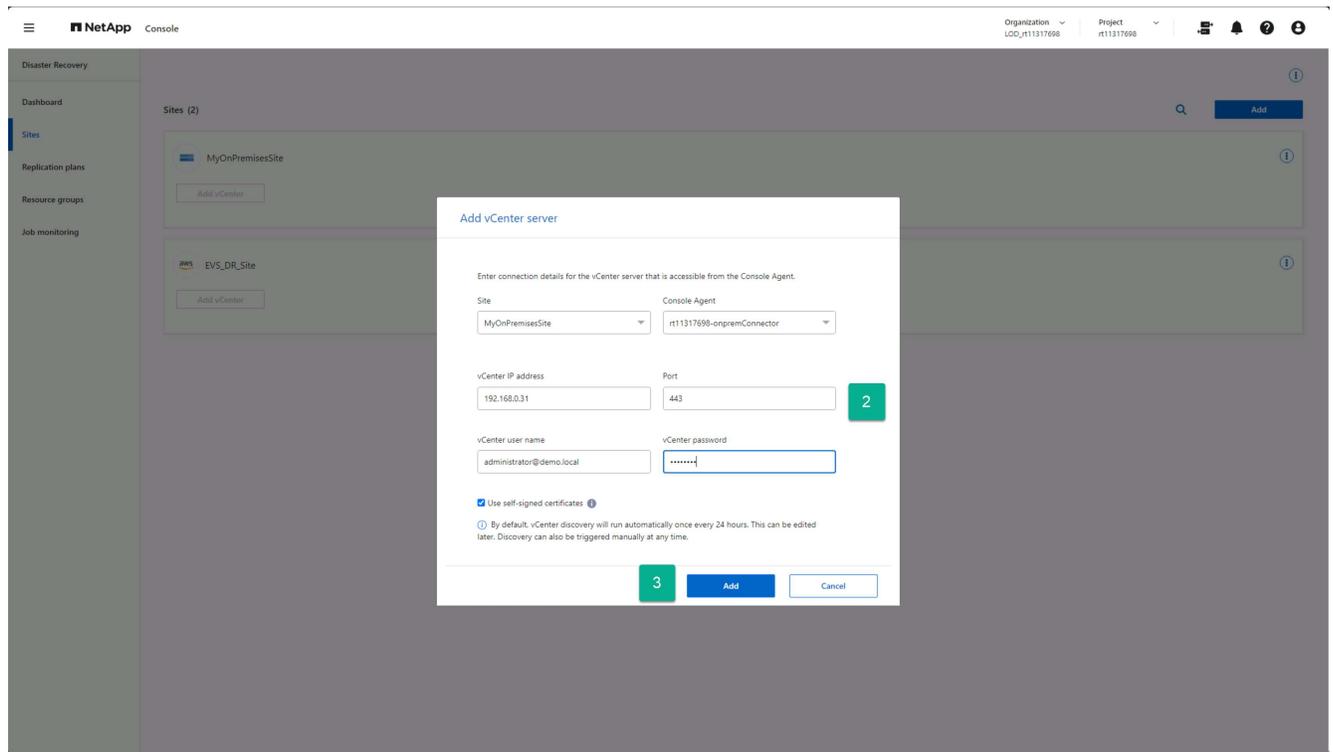
Nachdem Sie die Sites erstellt haben, fügen Sie nun Ihre vCenter-Cluster zu jeder Site in NetApp Disaster Recovery hinzu. Beim Erstellen der einzelnen Sites haben wir die einzelnen Site-Typen angegeben. Dadurch wird NetApp Disaster Recovery mitgeteilt, welche Art von Zugriff für die in jedem Site-Typ gehosteten vCenter erforderlich ist. Einer der Vorteile von Amazon EVS besteht darin, dass es keinen wirklichen Unterschied zwischen einem Amazon EVS vCenter und einem lokalen vCenter gibt. Beide erfordern dieselben Verbindungs- und Authentifizierungsinformationen.

### Schritte zum Hinzufügen eines vCenters zu jeder Site

1. Wählen Sie unter der Option **Sites** für die gewünschte Site die Option **vCenter hinzufügen** aus.



2. Wählen Sie im Dialogfeld „vCenter-Server hinzufügen“ die folgenden Informationen aus bzw. geben Sie sie ein:
  - a. Der NetApp Console , der in Ihrem AWS VPC gehostet wird.
  - b. Die IP-Adresse oder der FQDN für das hinzuzufügende vCenter.
  - c. Falls abweichend, ändern Sie den Portwert in den TCP-Port, der von Ihrem vCenter-Cluster-Manager verwendet wird.
  - d. Der vCenter-Benutzername für das zuvor erstellte Konto, der von NetApp Disaster Recovery zum Verwalten des vCenter verwendet wird.
  - e. Das vCenter-Passwort für den angegebenen Benutzernamen.
  - f. Wenn Ihr Unternehmen eine externe Zertifizierungsstelle (CA) oder den vCenter Endpoint Certificate Store verwendet, um Zugriff auf Ihre vCenter zu erhalten, deaktivieren Sie das Kontrollkästchen **Selbstsignierte Zertifikate verwenden**. Andernfalls lassen Sie das Kontrollkästchen aktiviert.
3. Wählen Sie **Hinzufügen**.



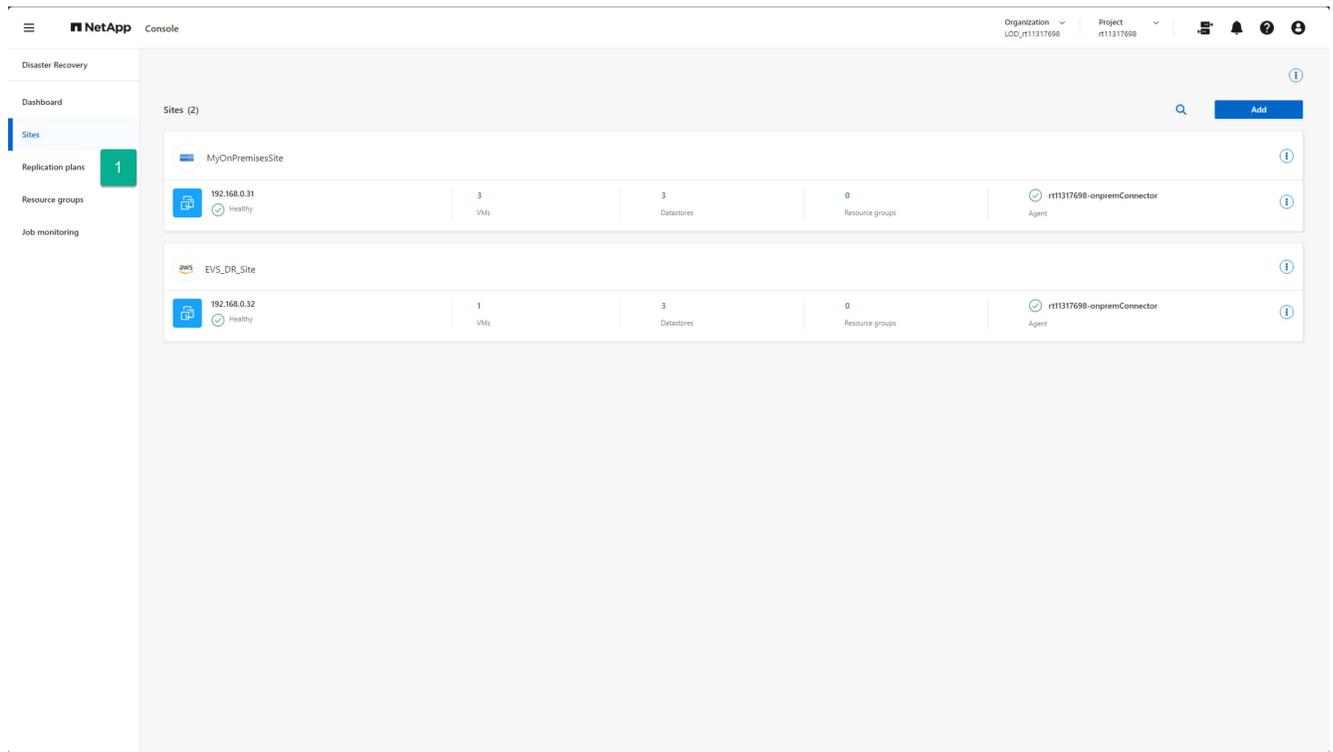
## Erstellen von Replikationsplänen für Amazon EVS

### Erstellen von Replikationsplänen in der NetApp Disaster Recovery Übersicht

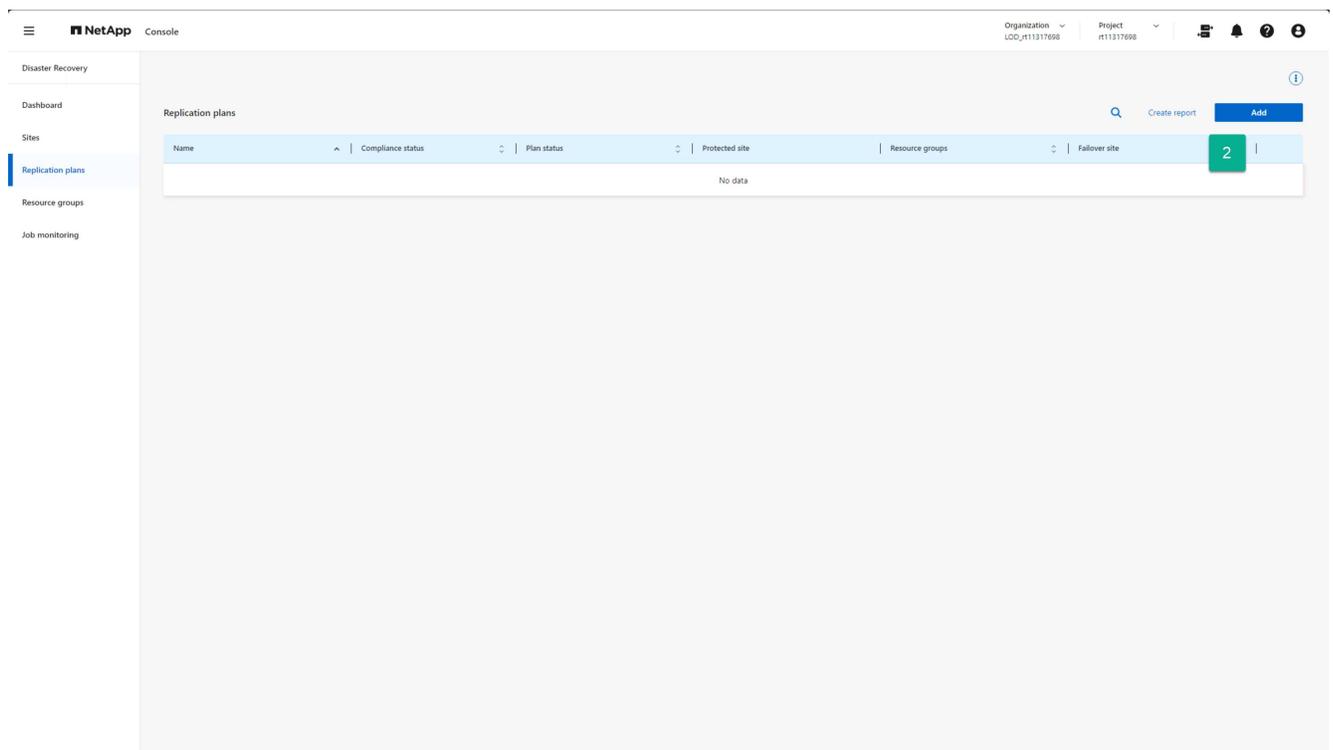
Nachdem Sie vCenter zum Schutz auf der lokalen Site haben und eine Amazon EVS-Site für die Verwendung von Amazon FSx for NetApp ONTAP konfiguriert haben, die Sie als DR-Ziel verwenden können, können Sie einen Replikationsplan (RP) erstellen, um alle auf dem vCenter-Cluster innerhalb Ihrer lokalen Site gehosteten VM-Gruppen zu schützen.

#### So starten Sie den Prozess zur Erstellung des Replikationsplans:

1. Wählen Sie auf einem beliebigen NetApp Disaster Recovery Bildschirm die Option **Replikationspläne** aus.



2. Wählen Sie auf der Seite „Replikationspläne“ die Option **Hinzufügen** aus.



Dadurch wird der Assistent „Replikationsplan erstellen“ geöffnet.

Weiter mit "Assistent zum Erstellen eines Replikationsplans – Schritt 1" .

## Erstellen eines Replikationsplans: Schritt 1 – Auswählen von vCentern in NetApp Disaster Recovery

Geben Sie zunächst mithilfe von NetApp Disaster Recovery einen Replikationsplannamen an und wählen Sie die Quell- und Ziel-vCenter für die Replikation aus.

1. Geben Sie einen eindeutigen Namen für den Replikationsplan ein.

Für Replikationsplannamen sind nur alphanumerische Zeichen und Unterstriche (\_) zulässig.

2. Wählen Sie einen Quell-vCenter-Cluster aus.
3. Wählen Sie einen vCenter-Zielcluster aus.
4. Wählen Sie **Weiter**.

Weiter mit "[Assistent zum Erstellen eines Replikationsplans – Schritt 2](#)".

## Erstellen eines Replikationsplans: Schritt 2 – Auswählen von VM-Ressourcen in NetApp Disaster Recovery

Wählen Sie die virtuellen Maschinen aus, die mit NetApp Disaster Recovery geschützt werden sollen.

Es gibt mehrere Möglichkeiten, VMs zum Schutz auszuwählen:

- **Einzelne VMs auswählen:** Durch Klicken auf die Schaltfläche **Virtuelle Maschinen** können Sie einzelne VMs zum Schutz auswählen. Wenn Sie eine VM auswählen, fügt der Dienst sie einer Standardressourcengruppe auf der rechten Seite des Bildschirms hinzu.
- **Zuvor erstellte Ressourcengruppen auswählen:** Sie können im Voraus benutzerdefinierte Ressourcengruppen erstellen, indem Sie die Option „Ressourcengruppe“ im NetApp Disaster Recovery

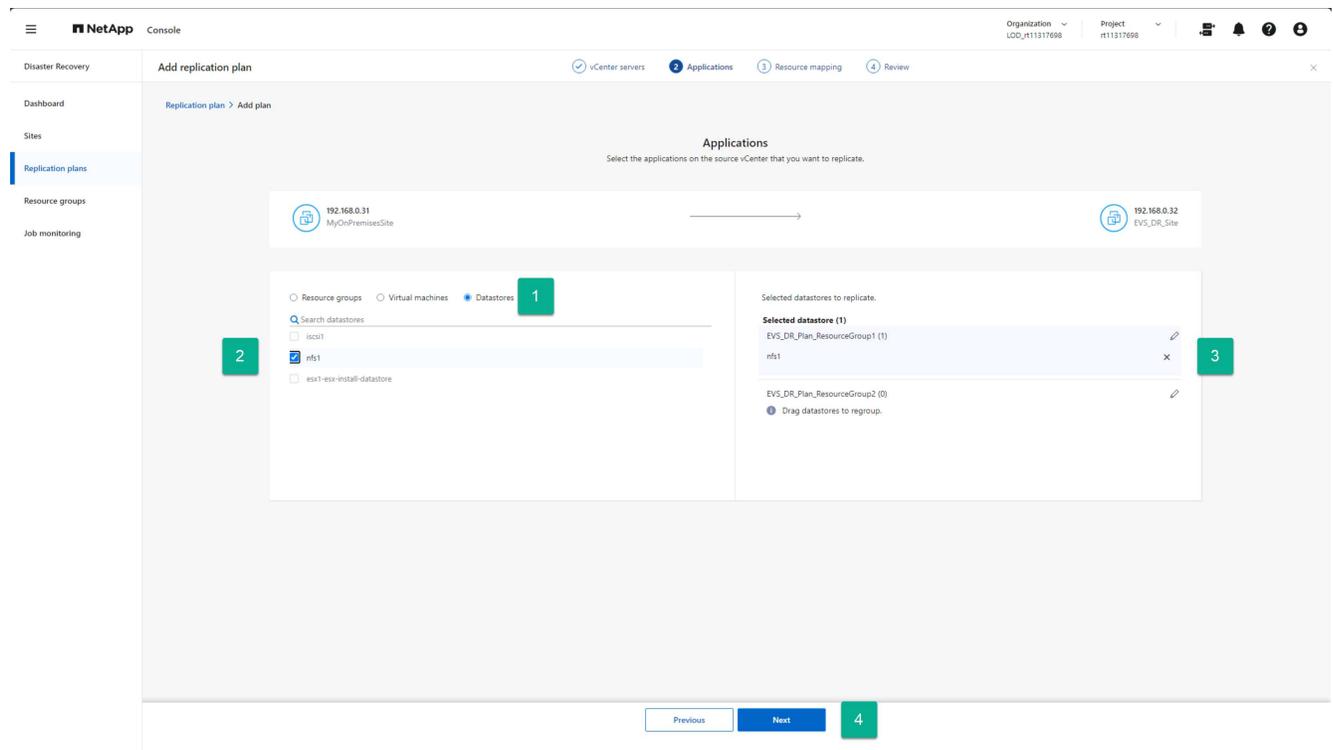
Menü verwenden. Dies ist keine Voraussetzung, da Sie die beiden anderen Methoden verwenden können, um im Rahmen des Replikationsplanprozesses eine Ressourcengruppe zu erstellen. Weitere Informationen finden Sie unter ["Erstellen eines Replikationsplans"](#) .

- **Gesamte vCenter-Datenspeicher auswählen:** Wenn Sie mit diesem Replikationsplan viele VMs schützen müssen, ist die Auswahl einzelner VMs möglicherweise nicht so effizient. Da NetApp Disaster Recovery zum Schutz der VMs die volumebasierte SnapMirror -Replikation verwendet, werden alle auf einem Datenspeicher befindlichen VMs als Teil des Volumens repliziert. In den meisten Fällen sollten Sie alle im Datenspeicher befindlichen VMs durch NetApp Disaster Recovery schützen und neu starten. Verwenden Sie diese Option, um den Dienst anzuweisen, alle auf einem ausgewählten Datenspeicher gehosteten VMs zur Liste der geschützten VMs hinzuzufügen.

Für diese geführte Anleitung wählen wir den gesamten vCenter-Datenspeicher aus.

### Schritte zum Zugriff auf diese Seite

1. Fahren Sie auf der Seite **Replikationsplan** mit dem Abschnitt **Anwendungen** fort.
2. Überprüfen Sie die Informationen auf der Seite **Anwendungen**, die geöffnet wird.



### Schritte zum Auswählen des Datenspeichers bzw. der Datenspeicher:

1. Wählen Sie **Datenspeicher** aus.
2. Aktivieren Sie die Kontrollkästchen neben jedem Datenspeicher, den Sie schützen möchten.
3. (Optional) Benennen Sie die Ressourcengruppe in einen geeigneten Namen um, indem Sie das Stiftsymbol neben dem Namen der Ressourcengruppe auswählen.
4. Wählen Sie **Weiter**.

Weiter mit ["Assistent zum Erstellen eines Replikationsplans – Schritt 3"](#) .

## Erstellen eines Replikationsplans: Schritt 3 – Zuordnen von Ressourcen in NetApp Disaster Recovery

Nachdem Sie eine Liste der VMs erstellt haben, die Sie mit NetApp Disaster Recovery schützen möchten, geben Sie die Failover-Zuordnung und die VM-Konfigurationsinformationen an, die während eines Failovers verwendet werden sollen.

Sie müssen vier primäre Arten von Informationen zuordnen:

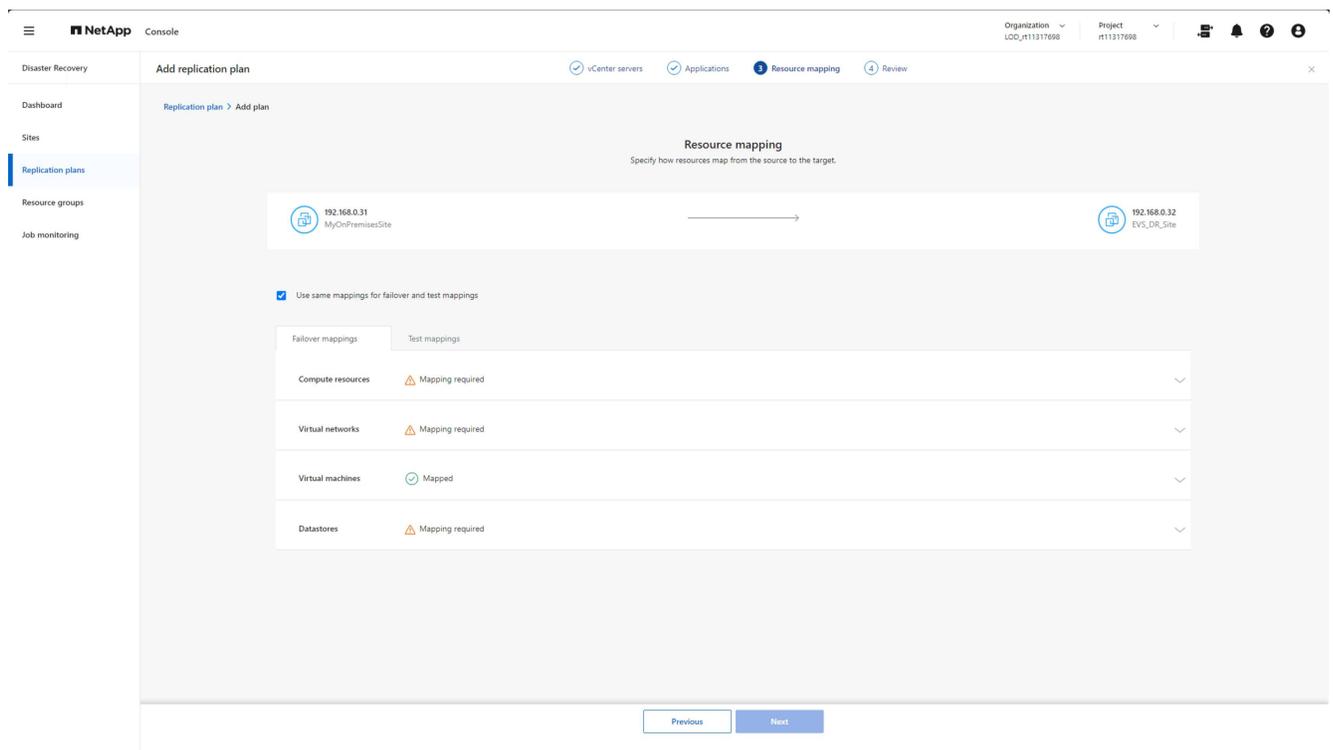
- Rechenressourcen
- Virtuelle Netzwerke
- VM-Neukonfiguration
- Datenspeicherzuordnung

Jede VM benötigt die ersten drei Arten von Informationen. Für jeden Datenspeicher, der zu schützende VMs hostet, ist eine Datenspeicherzuordnung erforderlich.

- Die Abschnitte mit dem Vorsichtssymbol (  ) erfordern die Angabe von Zuordnungsinformationen.
- Der mit dem Häkchensymbol (  ) wurden zugeordnet oder verfügen über Standardzuordnungen. Überprüfen Sie sie, um sicherzustellen, dass die aktuelle Konfiguration Ihren Anforderungen entspricht.

### Schritte zum Zugriff auf diese Seite

1. Fahren Sie auf der Seite **Replikationsplan** mit dem Abschnitt **Ressourcenzuordnung** fort.
2. Überprüfen Sie die Informationen auf der Seite **Ressourcenzuordnung**, die geöffnet wird.



The screenshot displays the 'Resource mapping' configuration page in the NetApp Disaster Recovery console. It shows a mapping from the source site '192.168.0.31 MyOnPremisesSite' to the target site '192.168.0.32 EVS\_DR\_Site'. A checkbox labeled 'Use same mappings for failover and test mappings' is checked. Below this, a table lists resource categories and their mapping status:

| Category          | Status           |
|-------------------|------------------|
| Compute resources | Mapping required |
| Virtual networks  | Mapping required |
| Virtual machines  | Mapped           |
| Datastores        | Mapping required |

At the bottom of the page, there are 'Previous' and 'Next' navigation buttons.

3. Um die einzelnen Kategorien der erforderlichen Zuordnungen zu öffnen, wählen Sie den Abwärtspfeil (v)

neben dem Abschnitt aus.

## Zuordnung von Rechenressourcen

Da ein Standort mehrere virtuelle Rechenzentren und mehrere vCenter-Cluster hosten kann, müssen Sie ermitteln, auf welchem vCenter-Cluster die VMs im Falle eines Failovers wiederhergestellt werden sollen.

### Schritte zum Zuordnen von Computeressourcen

1. Wählen Sie das virtuelle Rechenzentrum aus der Liste der Rechenzentren am DR-Standort aus.
2. Wählen Sie aus der Liste der Cluster im ausgewählten virtuellen Rechenzentrum den Cluster aus, der die Datenspeicher und VMs hosten soll.
3. (Optional) Wählen Sie einen Zielhost im Zielcluster aus.

Dieser Schritt ist nicht erforderlich, da NetApp Disaster Recovery den ersten Host auswählt, der dem Cluster in vCenter hinzugefügt wird. An diesem Punkt werden die VMs entweder weiterhin auf diesem ESXi-Host ausgeführt oder VMware DRS verschiebt die VM je nach Bedarf basierend auf den konfigurierten DRS-Regeln auf einen anderen ESXi-Host.

4. (Optional) Geben Sie den Namen eines vCenter-Ordners der obersten Ebene an, in dem die VM-Registrierungen abgelegt werden sollen.

Dies dient Ihren organisatorischen Anforderungen und ist nicht erforderlich.

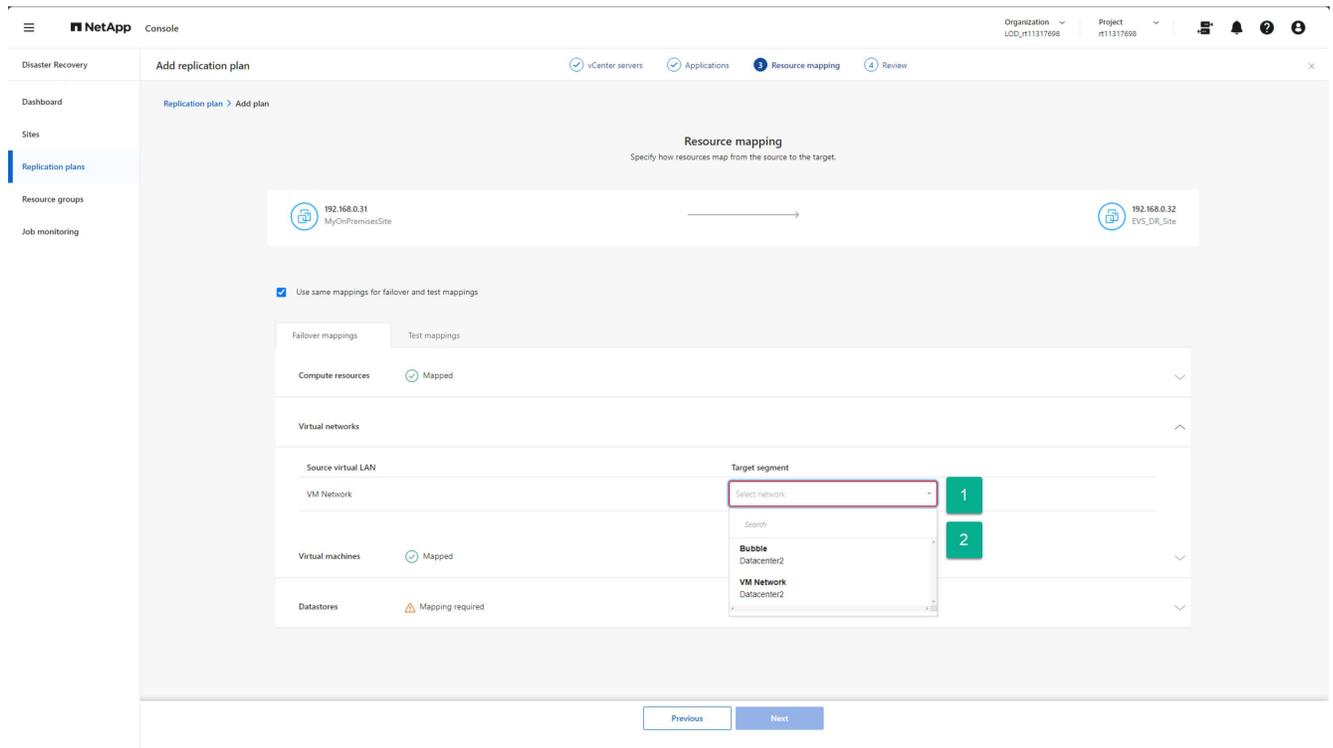
The screenshot displays the 'Resource mapping' configuration page in the NetApp console. It shows the process of mapping resources from a source site (192.168.0.31 MyOnPremisesSite) to a target site (192.168.0.32 EVS\_DR\_Site). The 'Compute resources mapping' section includes dropdowns for 'Target datacenter' (Datacenter2), 'Target cluster' (Cluster2), 'Target host (optional)', and 'Target VM folder (optional)'. The 'Virtual networks' section indicates that mapping is required, while 'Virtual machines' are already mapped. The 'Datastores' section also indicates that mapping is required. The page includes a 'Previous' button and a 'Next' button at the bottom.

## Zuordnen virtueller Netzwerkressourcen

Jede VM kann über eine oder mehrere virtuelle Netzwerkkarten verfügen, die mit virtuellen Netzwerken innerhalb der vCenter-Netzwerkinfrastruktur verbunden sind. Um sicherzustellen, dass jede VM beim Neustart am DR-Standort ordnungsgemäß mit den gewünschten Netzwerken verbunden ist, ermitteln Sie, mit welchen virtuellen Netzwerken am DR-Standort diese VMs verbunden werden sollen. Ordnen Sie dazu jedes virtuelle Netzwerk am lokalen Standort einem zugehörigen Netzwerk am DR-Standort zu.

## Wählen Sie aus, welches virtuelle Zielnetzwerk den einzelnen virtuellen Quellnetzwerken zugeordnet werden soll

1. Wählen Sie das Zielsegment aus der Dropdown-Liste aus.
2. Wiederholen Sie den vorherigen Schritt für jedes aufgeführte virtuelle Quellnetzwerk.



## Definieren Sie Optionen für die VM-Neukonfiguration während des Failovers

Für jede VM sind möglicherweise Änderungen erforderlich, damit sie auf der DR-vCenter-Site ordnungsgemäß funktioniert. Im Bereich „Virtuelle Maschinen“ können Sie die notwendigen Änderungen vornehmen.

Standardmäßig verwendet NetApp Disaster Recovery für jede VM dieselben Einstellungen wie am lokalen Quellstandort. Dies setzt voraus, dass VMs dieselbe IP-Adresse, virtuelle CPU und virtuelle DRAM-Konfiguration verwenden.

## Netzwerkneukonfiguration

Unterstützte IP-Adresstypen sind statisch und DHCP. Für statische IP-Adressen stehen Ihnen die folgenden Ziel-IP-Einstellungen zur Verfügung:

- **Gleich wie Quelle:** Wie der Name schon sagt, verwendet der Dienst auf der Ziel-VM dieselbe IP-Adresse, die auf der VM am Quellstandort verwendet wurde. Dazu müssen Sie die im vorherigen Schritt zugeordneten virtuellen Netzwerke für dieselben Subnetzeinstellungen konfigurieren.
- **Unterscheidet sich von der Quelle:** Der Dienst stellt für jede VM eine Reihe von IP-Adressfeldern bereit, die für das entsprechende Subnetz konfiguriert werden müssen, das im virtuellen Zielnetzwerk verwendet wird, das Sie im vorherigen Abschnitt zugeordnet haben. Für jede VM müssen Sie eine IP-Adresse, eine Subnetzmaske, DNS und Standard-Gateway-Werte angeben. Verwenden Sie optional für alle VMs die gleichen Subnetzmasken-, DNS- und Gateway-Einstellungen, um den Prozess zu vereinfachen, wenn alle VMs an dasselbe Subnetz angeschlossen sind.
- **Subnetzuordnung:** Diese Option konfiguriert die IP-Adresse jeder VM basierend auf der CIDR-Konfiguration des virtuellen Zielnetzwerks neu. Um diese Funktion zu verwenden, stellen Sie sicher, dass

die virtuellen Netzwerke jedes vCenters über eine definierte CIDR-Einstellung innerhalb des Dienstes verfügen, wie in den vCenter-Informationen auf der Sites-Seite geändert.

Nachdem Sie Subnetze konfiguriert haben, verwendet die Subnetzzuordnung dieselbe Einheitenkomponente der IP-Adresse für die Quell- und Ziel-VM-Konfiguration, ersetzt jedoch die Subnetzkomponente der IP-Adresse basierend auf den bereitgestellten CIDR-Informationen. Diese Funktion erfordert außerdem, dass sowohl das virtuelle Quell- als auch das virtuelle Zielnetzwerk dieselbe IP-Adressklasse haben (die /xx Komponente des CIDR). Dadurch wird sichergestellt, dass am Zielstandort genügend IP-Adressen verfügbar sind, um alle geschützten VMs zu hosten.

Bei diesem EVS-Setup gehen wir davon aus, dass die Quell- und Ziel-IP-Konfigurationen identisch sind und keine zusätzliche Neukonfiguration erforderlich ist.

### Nehmen Sie Änderungen an der Neukonfiguration der Netzwerkeinstellungen vor

1. Wählen Sie den IP-Adresstyp aus, der für VMs verwendet werden soll, bei denen ein Failover durchgeführt wurde.
2. (Optional) Stellen Sie ein VM-Umbenennungsschema für neu gestartete VMs bereit, indem Sie einen optionalen Präfix- und Suffixwert angeben.

The screenshot shows the 'Add replication plan' configuration page in the NetApp console. The 'Virtual machines' section is expanded, showing the following configuration:

- IP address type:** Static (highlighted with a red box and '1')
- Target IP:** Same as source
- Use the same credentials for all VMs
- Use the same script for all VMs
- Target VM prefix:** (Optional, empty field)
- Target VM suffix:** (Optional, empty field)
- Preview: Sample VM name:** (empty field)

| Source VM | Operating system | CPU | RAM   | Boot order | Boot delay (mins between 0 and 10) | Create application consistent replicas | Scripts | Credentials  |
|-----------|------------------|-----|-------|------------|------------------------------------|--|---------|--------------|
| Linux1    | Linux            | 1   | 2 GiB | 1          | 0                                  | <input type="checkbox"/>               | None    | Not required |
| Linux4    | Linux            | 1   | 2 GiB | 3          | 5                                  | <input type="checkbox"/>               | None    | Not required |
| Linux3    | Linux            | 1   | 2 GiB | 2          | 5                                  | <input type="checkbox"/>               | None    | Not required |

### Neukonfiguration der VM-Rechenressourcen

Es gibt mehrere Optionen zum Neukonfigurieren der VM-Rechenressourcen. NetApp Disaster Recovery unterstützt das Ändern der Anzahl virtueller CPUs, der Menge an virtuellem DRAM und des VM-Namens.

### Geben Sie alle VM-Konfigurationsänderungen an

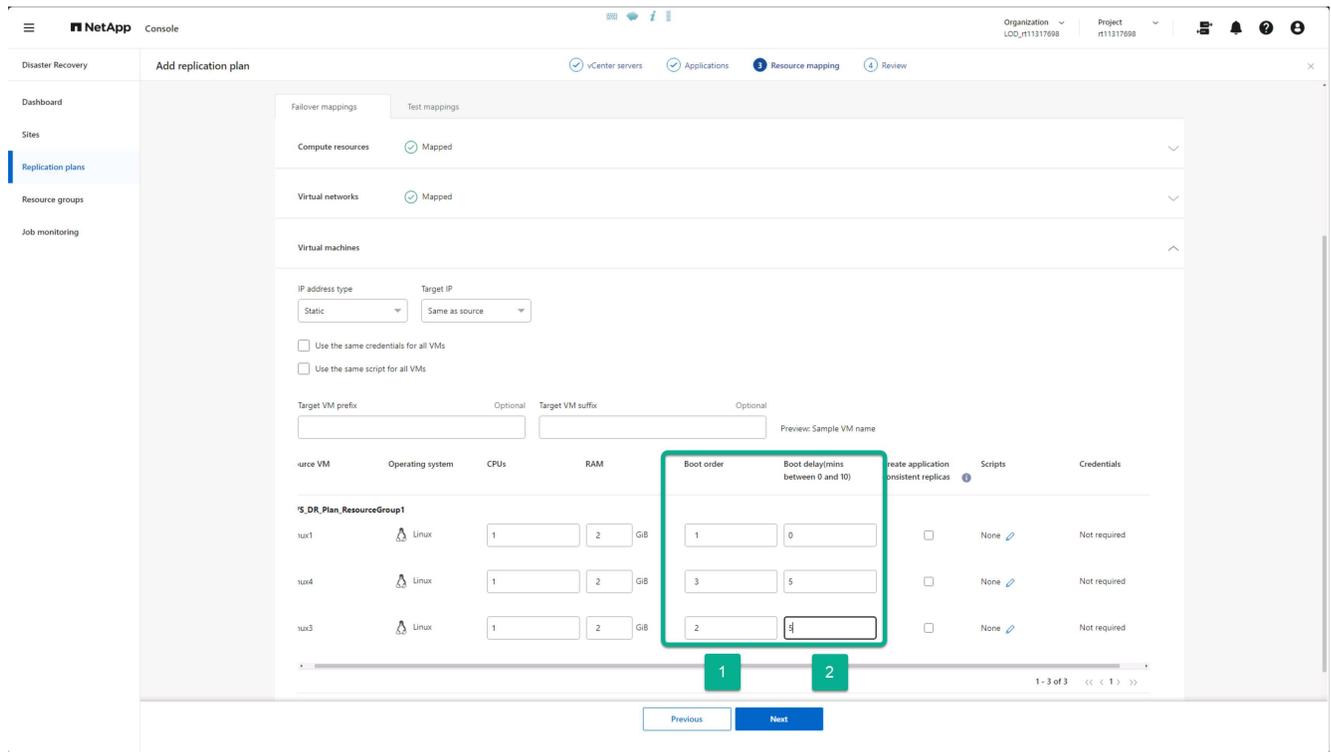
1. (Optional) Ändern Sie die Anzahl der virtuellen CPUs, die jede VM verwenden soll. Dies kann erforderlich sein, wenn Ihre DR-vCenter-Cluster-Hosts nicht über so viele CPU-Kerne verfügen wie der Quell-vCenter-Cluster.
2. (Optional) Ändern Sie die Menge an virtuellem DRAM, die jede VM verwenden soll. Dies kann erforderlich sein, wenn Ihre DR-vCenter-Cluster-Hosts nicht über so viel physischen DRAM verfügen wie die Quell-

## Bootreihenfolge

NetApp Disaster Recovery unterstützt einen geordneten Neustart von VMs basierend auf einem Bootreihenfolgefeld. Das Feld „Startreihenfolge“ gibt an, wie die VMs in jeder Ressourcengruppe starten. Die VMs mit dem gleichen Wert im Feld „Bootreihenfolge“ werden parallel gestartet.

### Ändern Sie die Einstellungen für die Startreihenfolge

1. (Optional) Ändern Sie die Reihenfolge, in der Ihre VMs neu gestartet werden sollen. Dieses Feld nimmt einen beliebigen numerischen Wert an. NetApp Disaster Recovery versucht, VMs mit demselben numerischen Wert parallel neu zu starten.
2. (Optional) Geben Sie eine Verzögerung an, die zwischen den einzelnen VM-Neustarts verwendet werden soll. Die Zeit wird eingefügt, nachdem der Neustart dieser VM abgeschlossen ist und vor der/den VM(s) mit der nächsthöheren Startreihenfolgenummer. Diese Zahl ist in Minuten angegeben.



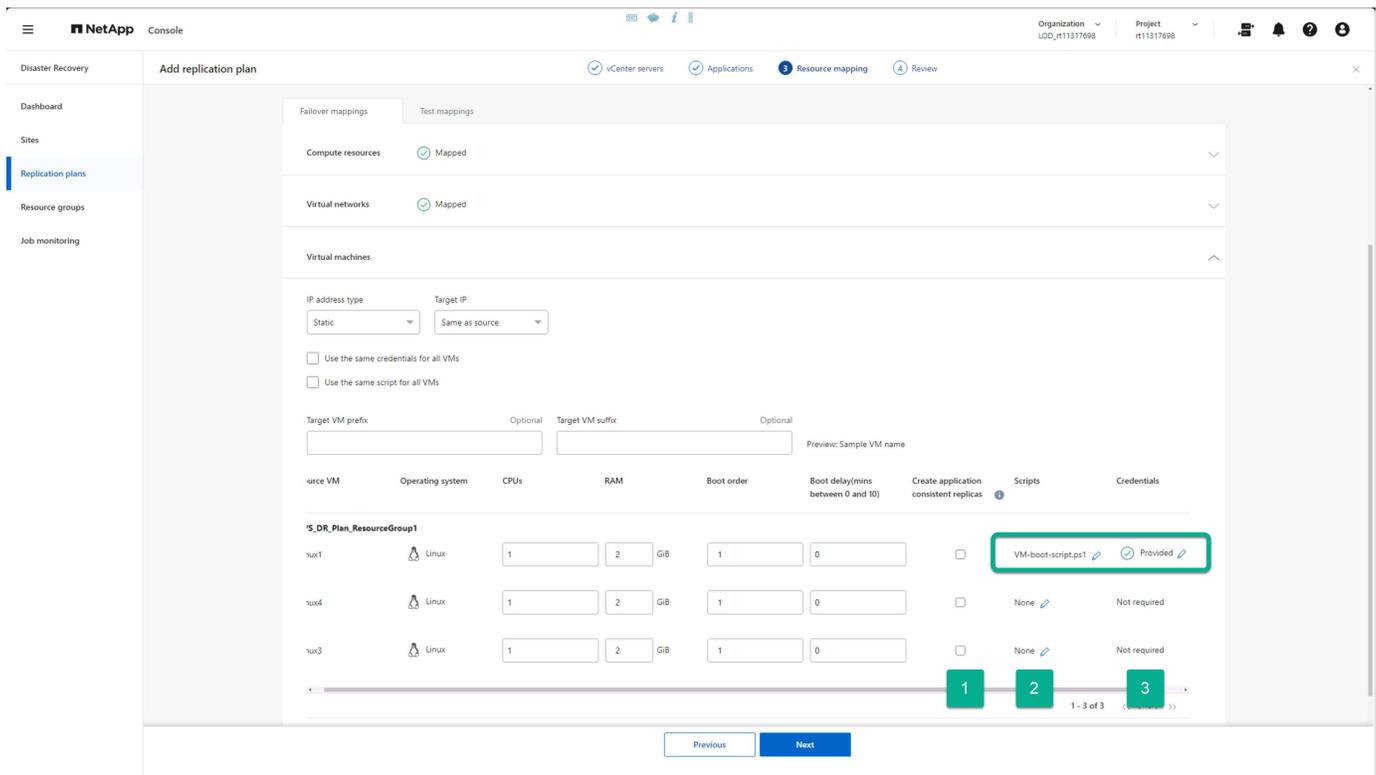
## Benutzerdefinierte Gastbetriebssystemvorgänge

NetApp Disaster Recovery unterstützt die Durchführung einiger Gastbetriebssystemvorgänge für jede VM:

- NetApp Disaster Recovery kann anwendungskonsistente Backups von VMs für VMs erstellen, auf denen Oracle-Datenbanken und Microsoft SQL Server-Datenbanken ausgeführt werden.
- NetApp Disaster Recovery kann für jede VM benutzerdefinierte, für das Gastbetriebssystem geeignete Skripte ausführen. Zum Ausführen solcher Skripte sind für das Gastbetriebssystem akzeptable Benutzeranmeldeinformationen mit ausreichenden Berechtigungen zum Ausführen der im Skript aufgeführten Vorgänge erforderlich.

### Ändern Sie die benutzerdefinierten Gastbetriebssystemvorgänge jeder VM

1. (Optional) Aktivieren Sie das Kontrollkästchen **Anwendungskonsistente Replikate erstellen**, wenn die VM eine Oracle- oder SQL Server-Datenbank hostet.
2. (Optional) Um im Rahmen des Startvorgangs benutzerdefinierte Aktionen innerhalb des Gastbetriebssystems auszuführen, laden Sie ein Skript für alle VMs hoch. Um ein einzelnes Skript in allen VMs auszuführen, aktivieren Sie das Kontrollkästchen und füllen Sie die Felder aus.
3. Für bestimmte Konfigurationsänderungen sind Benutzeranmeldeinformationen mit entsprechenden Berechtigungen zum Ausführen der Vorgänge erforderlich. Geben Sie in den folgenden Fällen Anmeldeinformationen an:
  - Innerhalb der VM wird vom Gastbetriebssystem ein Skript ausgeführt.
  - Es muss ein anwendungskonsistenter Snapshot durchgeführt werden.



## Kartendatenspeicher

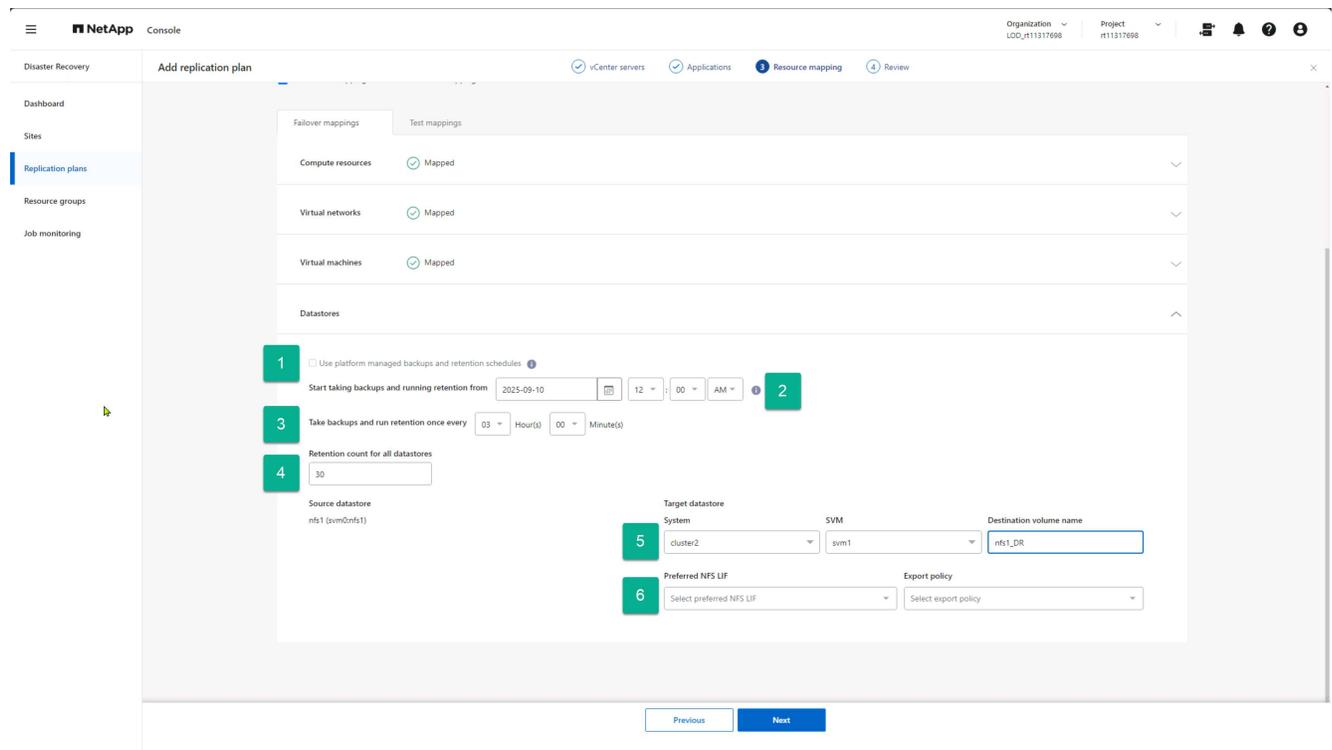
Der letzte Schritt beim Erstellen eines Replikationsplans besteht darin, festzulegen, wie ONTAP die Datenspeicher schützen soll. Diese Einstellungen definieren das Recovery Point Objective (RPO) der Replikationspläne, wie viele Backups aufbewahrt werden sollen und wohin die ONTAP -Volumes jedes vCenter-Datstores repliziert werden sollen.

Standardmäßig verwaltet NetApp Disaster Recovery seinen eigenen Snapshot-Replikationszeitplan. Optional können Sie jedoch angeben, dass Sie den vorhandenen SnapMirror -Replikationsrichtlinienzeitplan zum Schutz des Datenspeichers verwenden möchten.

Darüber hinaus können Sie optional anpassen, welche Daten-LIFs (logische Schnittstellen) und Exportrichtlinien verwendet werden sollen. Wenn Sie diese Einstellungen nicht angeben, verwendet NetApp Disaster Recovery alle Daten-LIFs, die mit dem entsprechenden Protokoll (NFS, iSCSI oder FC) verknüpft sind, und verwendet die Standardexportrichtlinie für NFS-Volumes.

### So konfigurieren Sie die Datenspeicherzuordnung (Volume)

1. (Optional) Entscheiden Sie, ob Sie einen vorhandenen ONTAP SnapMirror Replikationszeitplan verwenden oder den Schutz Ihrer VMs von NetApp Disaster Recovery verwalten lassen möchten (Standard).
2. Geben Sie einen Startpunkt an, ab dem der Dienst mit der Erstellung von Sicherungen beginnen soll.
3. Geben Sie an, wie oft der Dienst eine Sicherung durchführen und diese auf das DR-Ziel-Cluster Amazon FSx for NetApp ONTAP replizieren soll.
4. Geben Sie an, wie viele historische Sicherungen aufbewahrt werden sollen. Der Dienst verwaltet die gleiche Anzahl von Backups auf dem Quell- und Zielspeichercluster.
5. (Optional) Wählen Sie für jedes Volume eine logische Standardschnittstelle (Daten-LIFs) aus. Wenn keine ausgewählt ist, werden alle Daten-LIFs im Ziel-SVM konfiguriert, die das Volume-Zugriffsprotokoll unterstützen.
6. (Optional) Wählen Sie eine Exportrichtlinie für alle NFS-Volumes aus. Wenn nicht ausgewählt, wird die



Weiter mit "Assistent zum Erstellen eines Replikationsplans, Schritt 4".

## Erstellen eines Replikationsplans: Schritt 4 – Überprüfen der Einstellungen in NetApp Disaster Recovery

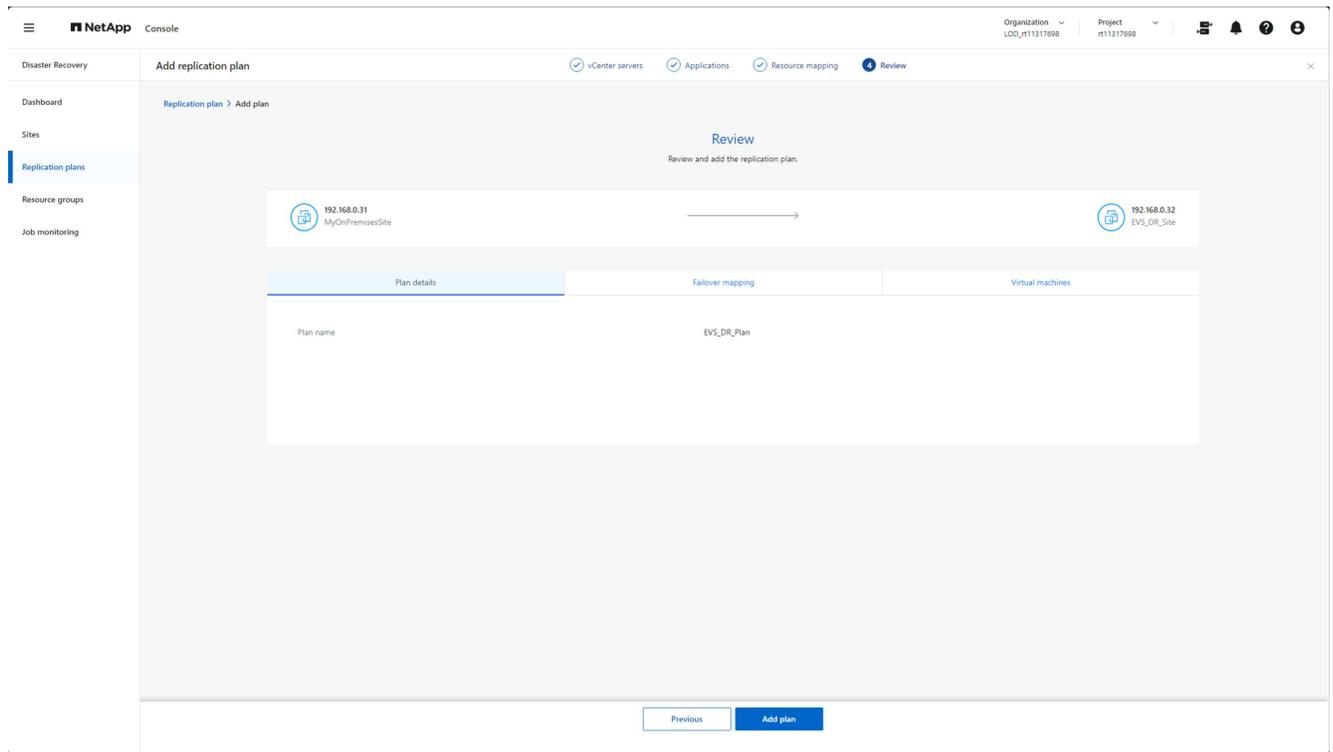
Nachdem Sie die Replikationsplaninformationen in NetApp Disaster Recovery hinzugefügt haben, überprüfen Sie, ob die eingegebenen Informationen richtig sind.

### Schritte

1. Wählen Sie **Speichern**, um Ihre Einstellungen zu überprüfen, bevor Sie den Replikationsplan aktivieren.

Sie können jede Registerkarte auswählen, um die Einstellungen zu überprüfen und auf jeder Registerkarte Änderungen vorzunehmen, indem Sie das Stiftsymbol auswählen.

Überprüfung der  
Replikationsplaneinstellungen



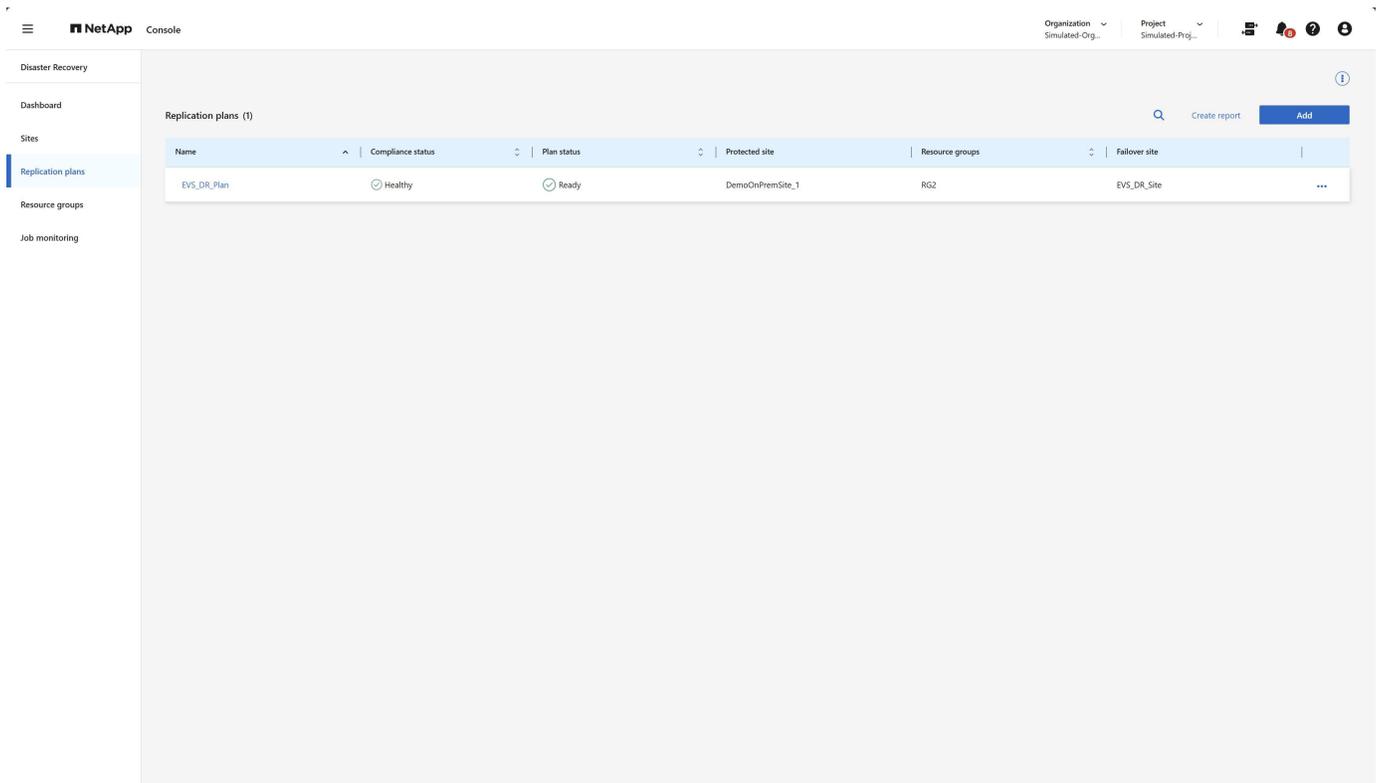
2. Wenn Sie sicher sind, dass alle Einstellungen korrekt sind, wählen Sie unten auf dem Bildschirm **Plan hinzufügen** aus.

Weiter mit "[Überprüfen des Replikationsplans](#)".

### Überprüfen Sie, ob in NetApp Disaster Recovery alles funktioniert

Nachdem Sie den Replikationsplan in NetApp Disaster Recovery hinzugefügt haben, kehren Sie zur Seite „Replikationspläne“ zurück, auf der Sie Ihre Replikationspläne und deren Status anzeigen können. Sie sollten überprüfen, ob sich der Replikationsplan im Zustand **Healthy** befindet. Wenn dies nicht der Fall ist, sollten Sie den Status des Replikationsplans überprüfen und alle Probleme beheben, bevor Sie fortfahren.

Abbildung: Seite „Replikationspläne“



NetApp Disaster Recovery führt eine Reihe von Tests durch, um sicherzustellen, dass alle Komponenten (ONTAP Cluster, vCenter-Cluster und VMs) zugänglich sind und sich im richtigen Zustand befinden, damit der Dienst die VMs schützen kann. Dies wird als Compliance-Prüfung bezeichnet und regelmäßig durchgeführt.

Auf der Seite „Replikationspläne“ können Sie die folgenden Informationen sehen:

- Status der letzten Compliance-Prüfung
- Der Replikationsstatus des Replikationsplans
- Der Name der geschützten (Quell-)Site
- Die Liste der durch den Replikationsplan geschützten Ressourcengruppen
- Der Name der Failover-Site (Zielsite)

## Ausführen von Replikationsplanvorgängen mit NetApp Disaster Recovery

Verwenden Sie NetApp Disaster Recovery mit Amazon EVS und Amazon FSx for NetApp ONTAP, um die folgenden Vorgänge auszuführen: Failover, Test-Failover, Ressourcen aktualisieren, migrieren, jetzt einen Snapshot erstellen, Replikationsplan deaktivieren/aktivieren, alte Snapshots bereinigen, Snapshots abgleichen, Replikationsplan löschen und Zeitpläne bearbeiten.

### Failover

Der wichtigste Vorgang, den Sie möglicherweise durchführen müssen, ist der, von dem Sie hoffen, dass er nie eintritt: das Failover zum DR-(Ziel-)Rechenzentrum im Falle eines katastrophalen Fehlers am Produktionsstandort vor Ort.

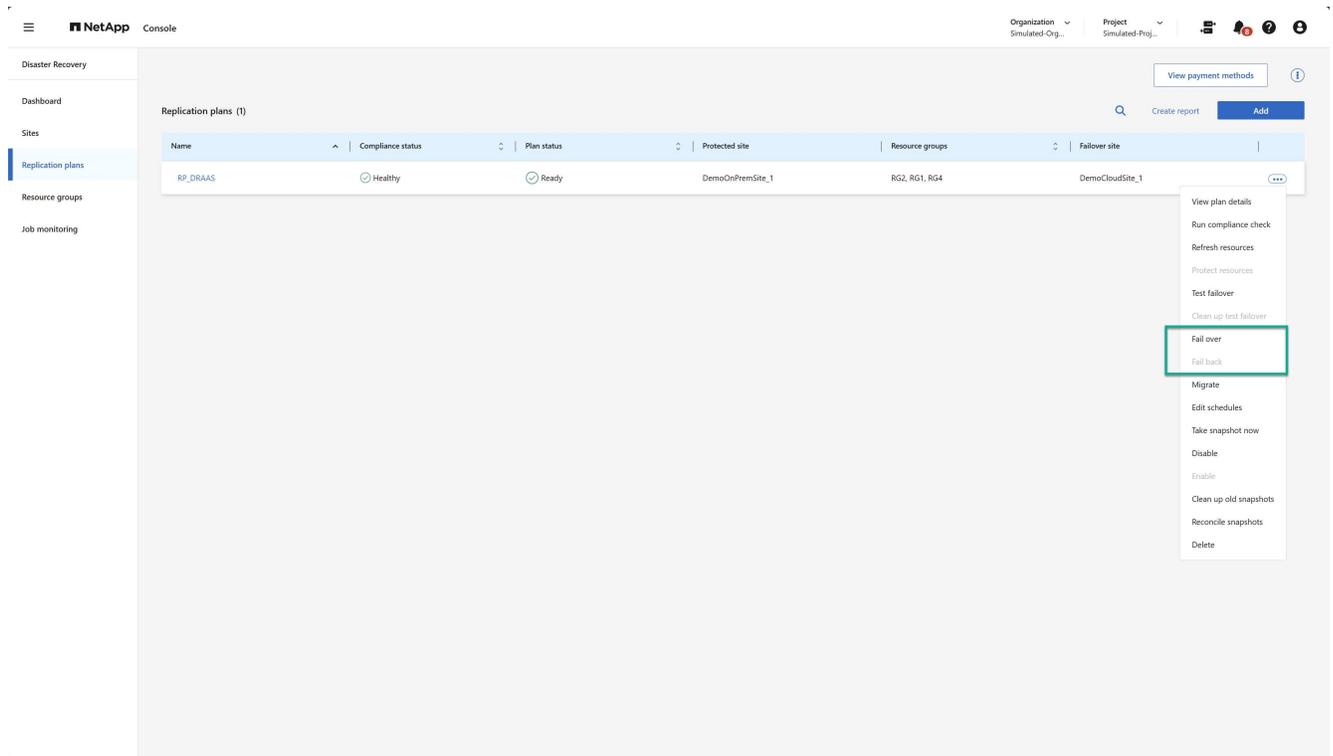
Failover ist ein manuell initiiertes Prozess.

## Schritte zum Zugriff auf den Failover-Vorgang

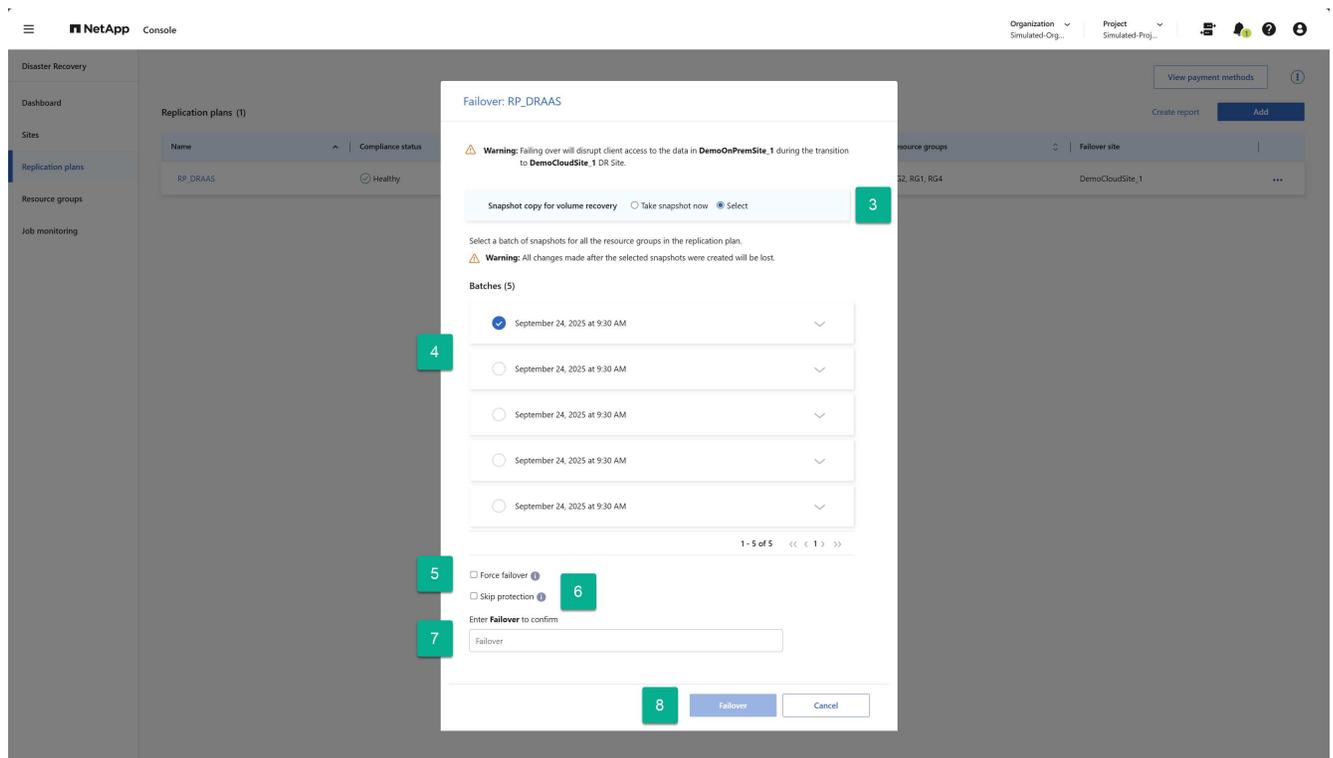
1. Wählen Sie in der linken Navigationsleiste der NetApp Console **Schutz > Notfallwiederherstellung**.
2. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.

## Schritte zum Durchführen eines Failovers

1. Wählen Sie auf der Seite Replikationspläne die Option Aktionen des Replikationsplans aus. **...**
2. Wählen Sie **Failover**.



3. Wenn auf die Produktionssite (geschützte Site) nicht zugegriffen werden kann, wählen Sie einen zuvor erstellten Snapshot als Wiederherstellungsimage aus. Wählen Sie dazu **Auswählen**.
4. Wählen Sie das Backup aus, das für die Wiederherstellung verwendet werden soll.
5. (Optional) Wählen Sie aus, ob NetApp Disaster Recovery den Failover-Prozess unabhängig vom Status des Replikationsplans erzwingen soll. Dies sollte nur als letztes Mittel erfolgen.
6. (Optional) Wählen Sie aus, ob NetApp Disaster Recovery nach der Wiederherstellung des Produktionsstandorts automatisch eine umgekehrte Schutzbeziehung erstellen soll.
7. Geben Sie das Wort „Failover“ ein, um zu bestätigen, dass Sie fortfahren möchten.
8. Wählen Sie **Failover**.



## Testen des Failovers

Ein Test-Failover ähnelt einem Failover, weist jedoch zwei Unterschiede auf.

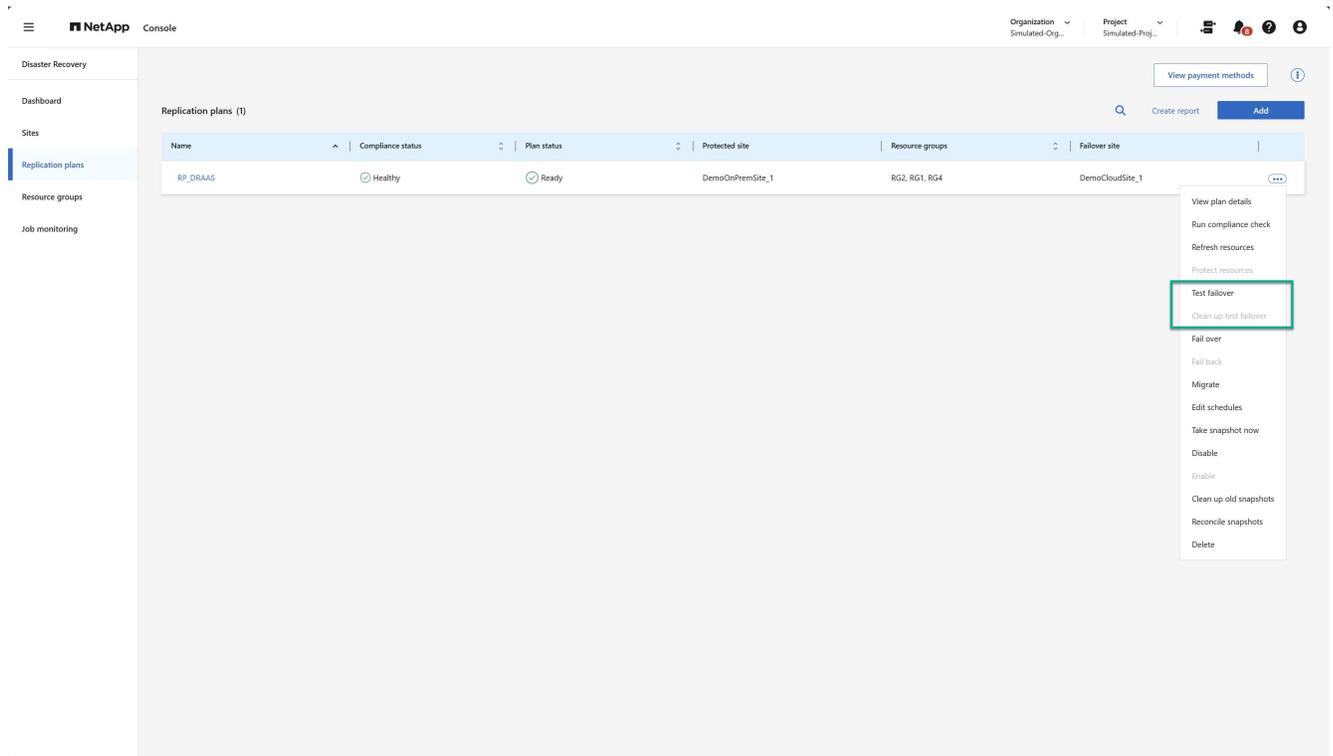
- Die Produktionssite ist weiterhin aktiv und alle VMs funktionieren weiterhin wie erwartet.
- Der NetApp Disaster Recovery Schutz der Produktions-VMs wird fortgesetzt.

Dies wird durch die Verwendung nativer ONTAP FlexClone -Volumes am Zielstandort erreicht. Weitere Informationen zum Testfailover finden Sie unter "[Failover von Anwendungen auf einen Remote-Standort | NetApp Dokumentation](#)".

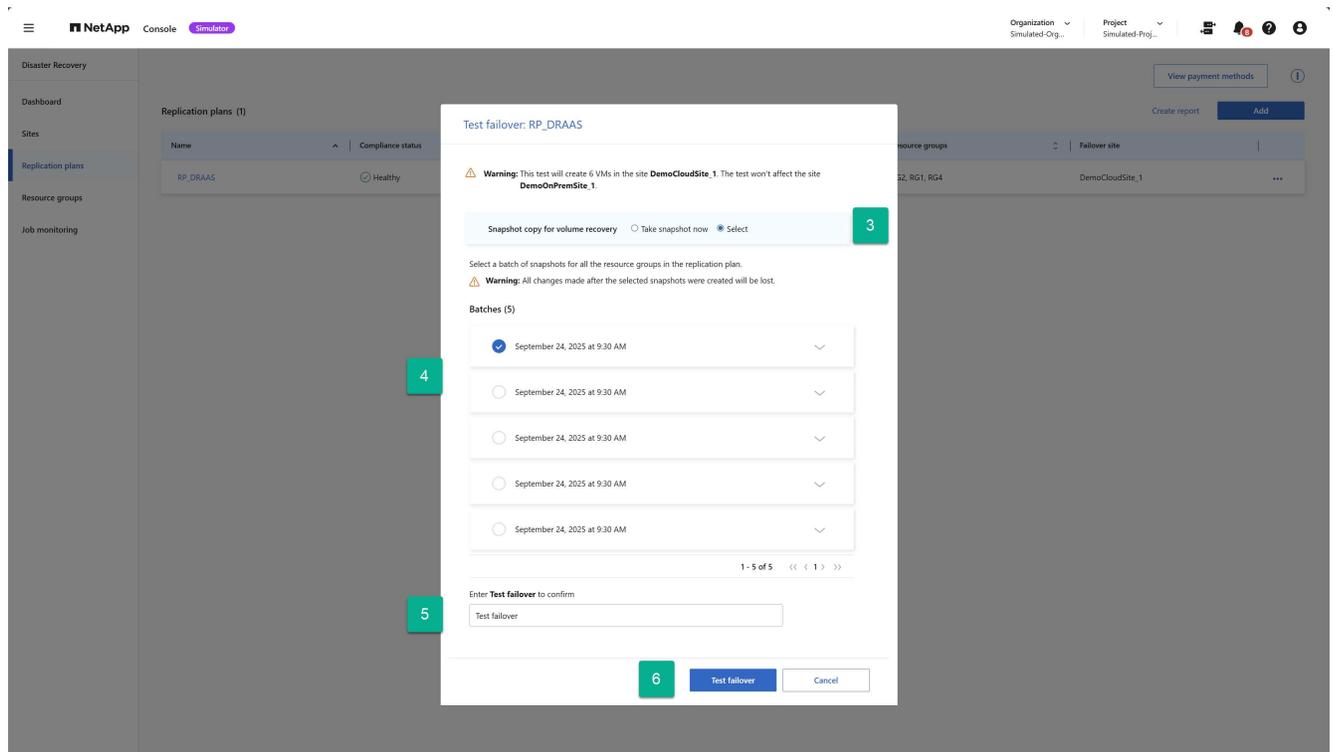
Die Schritte zum Ausführen eines Test-Failovers sind mit denen zum Ausführen eines echten Failovers identisch, mit der Ausnahme, dass Sie den Vorgang „Test-Failover“ im Kontextmenü des Replikationsplans verwenden.

### Schritte

1. Wählen Sie die Option Aktionen des Replikationsplans **...**.
2. Wählen Sie im Menü **Failover testen**.



3. Entscheiden Sie, ob Sie den neuesten Stand der Produktionsumgebung abrufen möchten (Jetzt Snapshot erstellen) oder ein zuvor erstelltes Backup des Replikationsplans verwenden möchten (Auswählen).
4. Wenn Sie ein zuvor erstelltes Backup ausgewählt haben, wählen Sie das Backup aus, das für die Wiederherstellung verwendet werden soll.
5. Geben Sie das Wort „Test-Failover“ ein, um zu bestätigen, dass Sie fortfahren möchten.
6. Wählen Sie **Failover testen**.

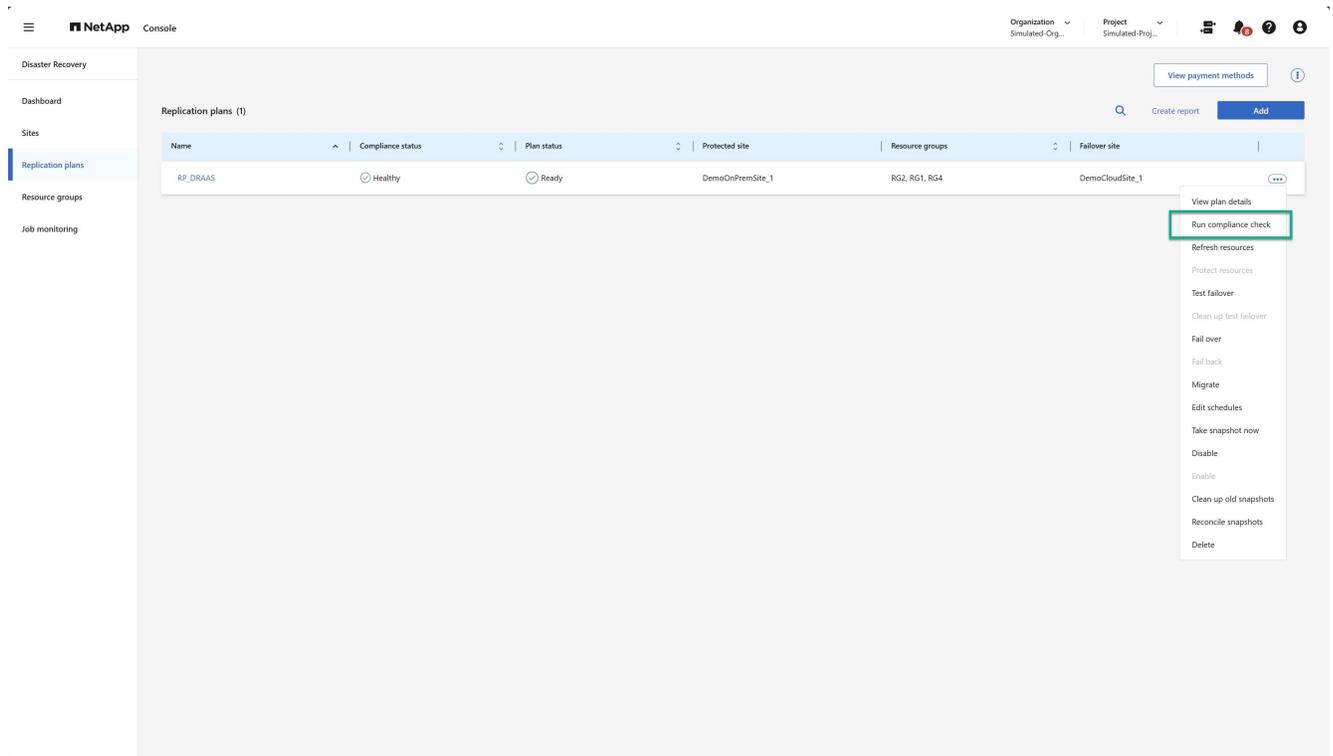


## Führen Sie eine Konformitätsprüfung durch

Konformitätsprüfungen werden standardmäßig alle drei Stunden durchgeführt. Sie können jederzeit manuell eine Konformitätsprüfung durchführen.

### Schritte

1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Konformitätsprüfung ausführen“ aus:



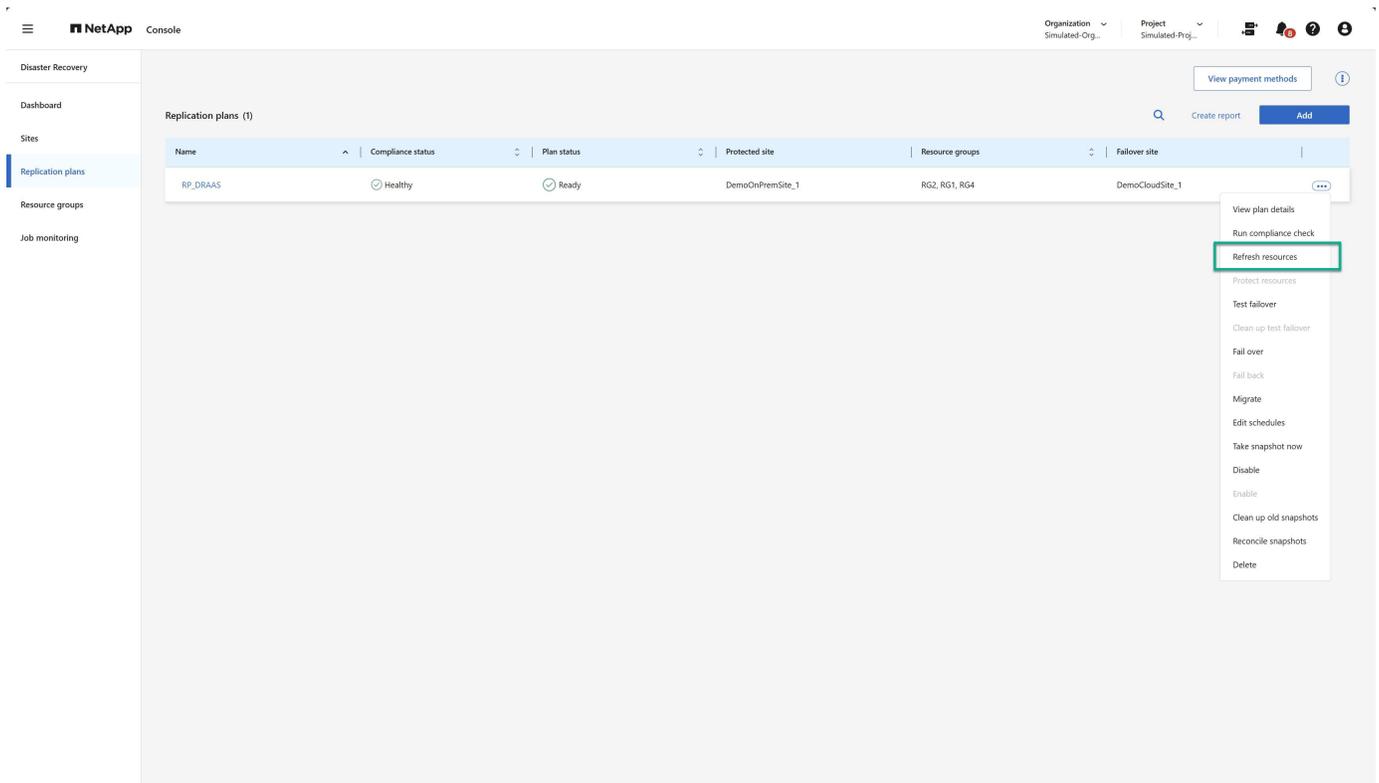
3. Um zu ändern, wie oft NetApp Disaster Recovery automatisch Konformitätsprüfungen durchführt, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Zeitpläne bearbeiten“ aus.

## Ressourcen aktualisieren

Jedes Mal, wenn Sie Änderungen an Ihrer virtuellen Infrastruktur vornehmen – beispielsweise VMs hinzufügen oder löschen, Datenspeicher hinzufügen oder löschen oder VMs zwischen Datenspeichern verschieben – müssen Sie eine Aktualisierung der betroffenen vCenter-Cluster im NetApp Disaster Recovery Dienst durchführen. Der Dienst führt dies standardmäßig alle 24 Stunden automatisch durch, eine manuelle Aktualisierung stellt jedoch sicher, dass die neuesten Informationen zur virtuellen Infrastruktur verfügbar sind und für den DR-Schutz berücksichtigt werden.

Es gibt zwei Fälle, in denen eine Aktualisierung erforderlich ist:

- vCenter-Aktualisierung: Führen Sie eine vCenter-Aktualisierung durch, wenn VMs zu einem vCenter-Cluster hinzugefügt, daraus gelöscht oder aus diesem verschoben werden:
- Aktualisierung des Replikationsplans: Führen Sie jedes Mal eine Aktualisierung des Replikationsplans durch, wenn eine VM zwischen Datenspeichern im selben Quell-vCenter-Cluster verschoben wird.



## Wandern

NetApp Disaster Recovery wird zwar in erster Linie für Notfallwiederherstellungsfälle verwendet, kann aber auch einmalige Verschiebungen einer Reihe von VMs vom Quellstandort zum Zielstandort ermöglichen. Dies könnte für ein konzertiertes Migrationsprojekt in die Cloud oder zur Katastrophenvermeidung genutzt werden – etwa bei schlechtem Wetter, politischen Unruhen oder anderen potenziellen vorübergehenden Katastrophenereignissen.

1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Um die VMs in einem Replikationsplan in den Amazon EVS-Zielcluster zu verschieben, wählen Sie im Aktionsmenü des Replikationsplans die Option **Migrieren** aus:

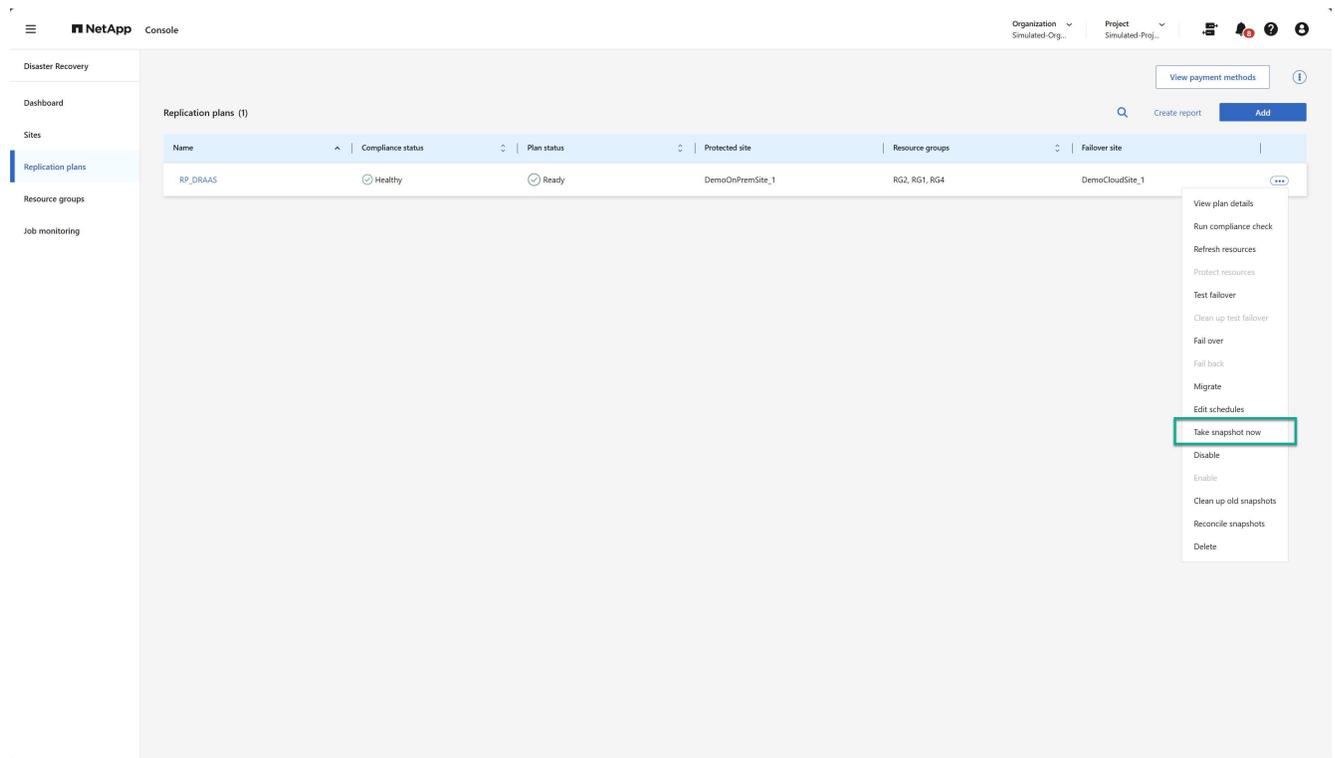
The screenshot shows the NetApp console interface. On the left, there is a navigation menu with options: Disaster Recovery, Dashboard, Sites, Application plans (selected), Resource groups, and Job monitoring. The main area displays a table titled 'Replication plans (1)'. The table has columns for Name, Compliance status, Plan status, Protected site, Resource groups, and Fallover site. The row for 'RP\_DRAAS' shows a 'Healthy' compliance status and a 'Ready' plan status. A context menu is open over the 'RP\_DRAAS' row, listing various actions such as 'View plan details', 'Run compliance check', 'Refresh resources', 'Protect resources', 'Test failover', 'Clean up test failover', 'Fall over', 'Fall back', 'Migrate' (highlighted with a red box), 'Edit schedules', 'Take snapshot now', 'Disable', 'Enable', 'Clean up old snapshots', 'Reconcile snapshots', and 'Delete'.

3. Geben Sie Informationen in das Dialogfeld „Migrieren“ ein.

## Jetzt Schnappschuss machen

Sie können jederzeit sofort einen Snapshot des Replikationsplans erstellen. Dieser Snapshot ist in den Überlegungen zur NetApp Disaster Recovery enthalten, die durch die Snapshot-Aufbewahrungsanzahl des Replikationsplans festgelegt werden.

1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Um sofort einen Snapshot der Ressourcen des Replikationsplans zu erstellen, wählen Sie im Aktionsmenü des Replikationsplans die Option **Jetzt Snapshot erstellen** aus:

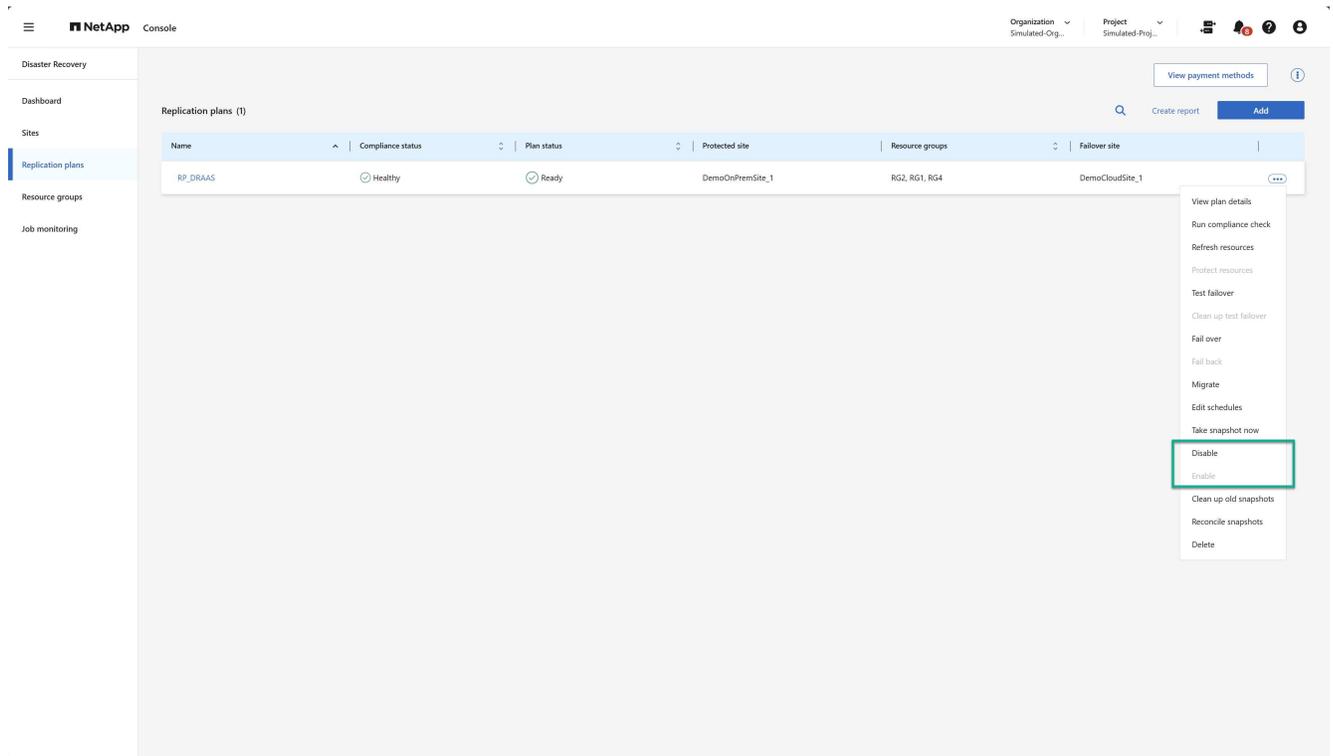


## Replikationsplan deaktivieren oder aktivieren

Möglicherweise müssen Sie den Replikationsplan vorübergehend anhalten, um Vorgänge oder Wartungsarbeiten durchzuführen, die sich auf den Replikationsprozess auswirken könnten. Der Dienst bietet eine Methode zum Stoppen und Starten der Replikation.

1. Um die Replikation vorübergehend zu stoppen, wählen Sie im Aktionsmenü des Replikationsplans die Option **Deaktivieren**.
2. Um die Replikation neu zu starten, wählen Sie im Aktionsmenü des Replikationsplans die Option **Aktivieren**.

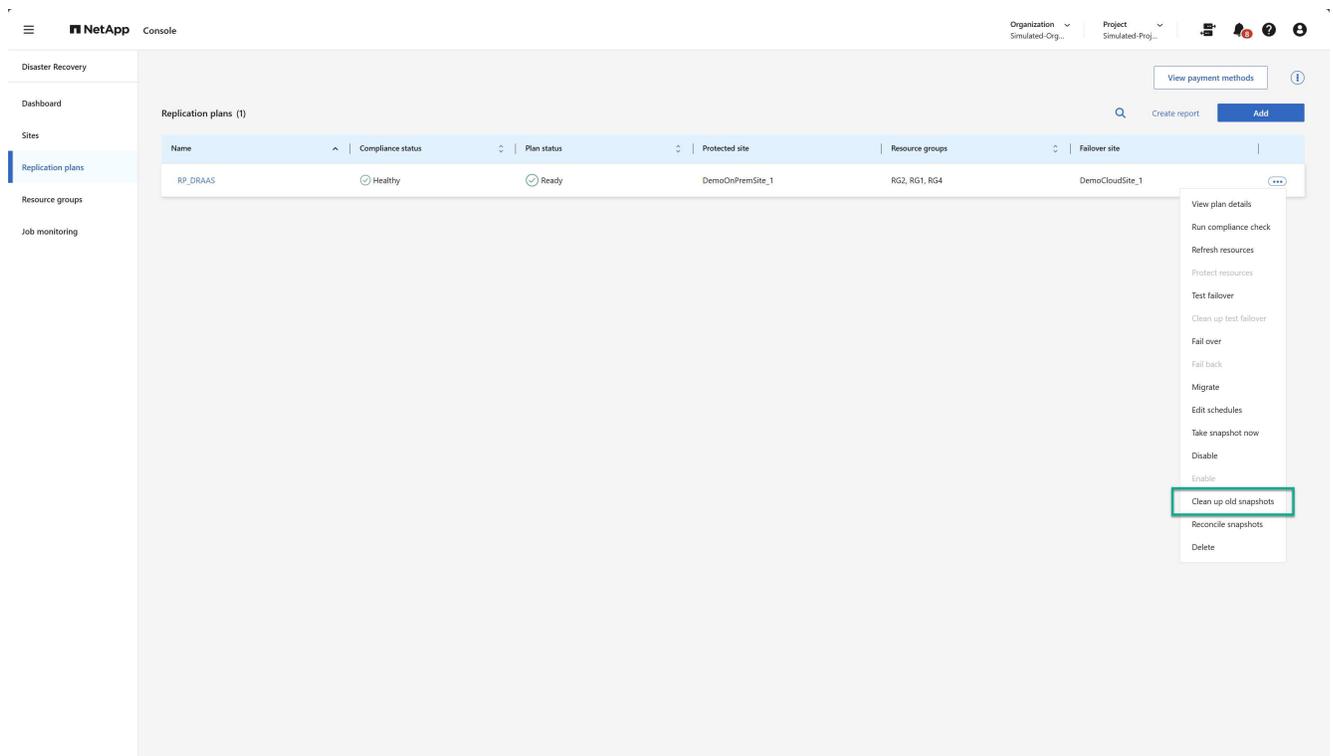
Wenn der Replikationsplan aktiv ist, ist der Befehl **Aktivieren** ausgegraut. Wenn der Replikationsplan deaktiviert ist, ist der Befehl **Deaktivieren** ausgegraut.



## Bereinigen Sie alte Snapshots

Möglicherweise möchten Sie ältere Snapshots bereinigen, die auf den Quell- und Zielsites aufbewahrt wurden. Dies kann passieren, wenn die Snapshot-Aufbewahrungsanzahl des Replikationsplans geändert wird.

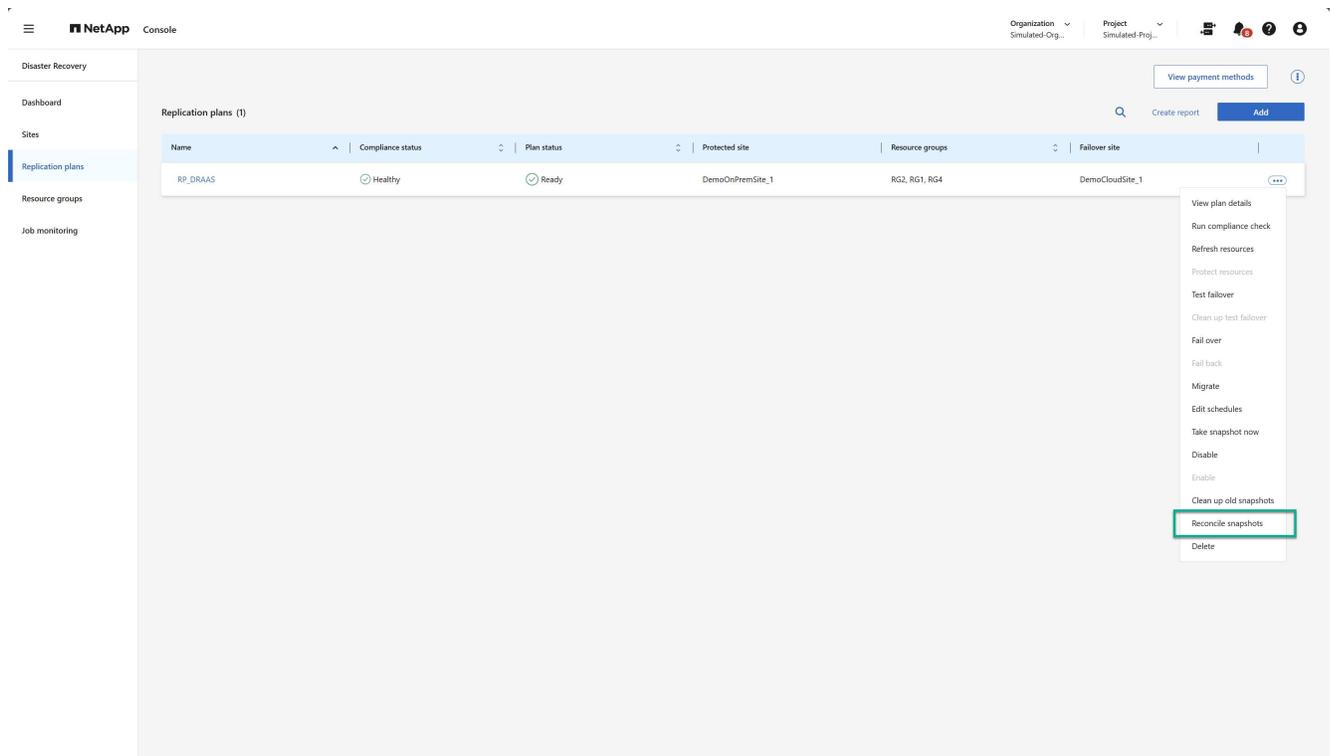
1. Wählen Sie die Option \*Aktionen\* neben dem Replikationsplan.
2. Um diese älteren Snapshots manuell zu entfernen, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Alte Snapshots bereinigen“ aus.



## Snapshots abgleichen

Da der Dienst ONTAP -Volume-Snapshots orchestriert, kann ein ONTAP Speicheradministrator Snapshots direkt mithilfe von ONTAP System Manager, der ONTAP CLI oder den ONTAP REST APIs löschen, ohne dass der Dienst davon Kenntnis hat. Der Dienst löscht automatisch alle 24 Stunden alle Snapshots auf der Quelle, die sich nicht auf dem Zielcluster befinden. Sie können dies jedoch auf Anfrage durchführen. Mit dieser Funktion können Sie sicherstellen, dass die Snapshots auf allen Sites konsistent sind.

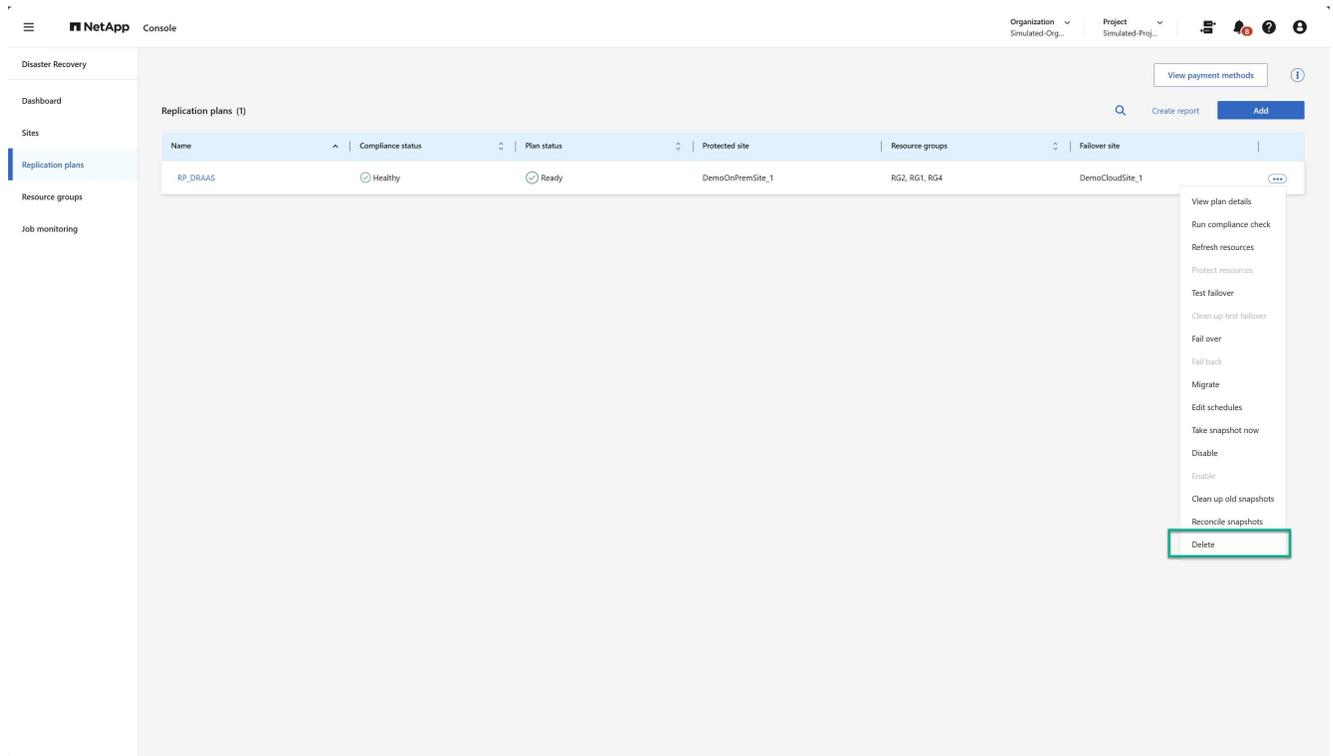
1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Um Snapshots aus dem Quellcluster zu löschen, die im Zielcluster nicht vorhanden sind, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Snapshots abgleichen“ aus.



## Replikationsplan löschen

Wenn der Replikationsplan nicht mehr benötigt wird, können Sie ihn löschen.

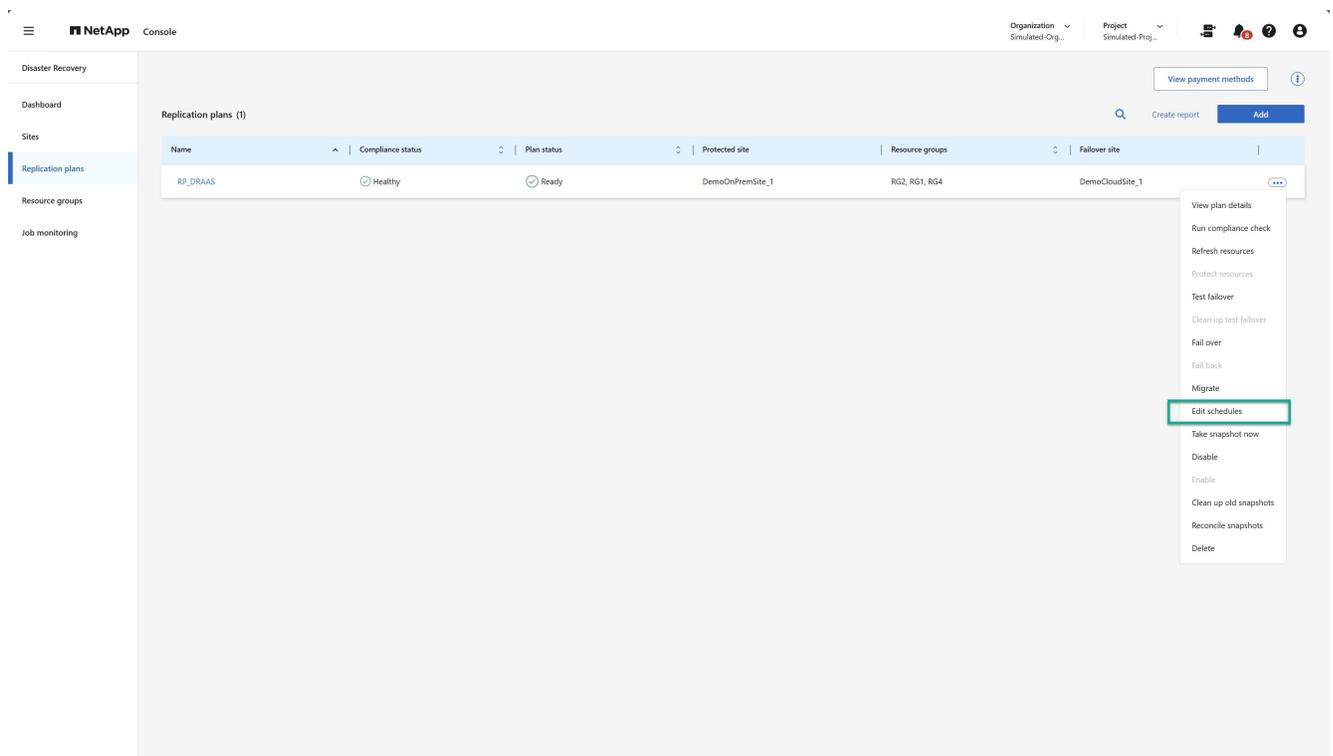
1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Um den Replikationsplan zu löschen, wählen Sie **Löschen** aus dem Kontextmenü des Replikationsplans.



## Zeitpläne bearbeiten

Zwei Vorgänge werden automatisch und regelmäßig durchgeführt: Test-Failover und Konformitätsprüfungen.

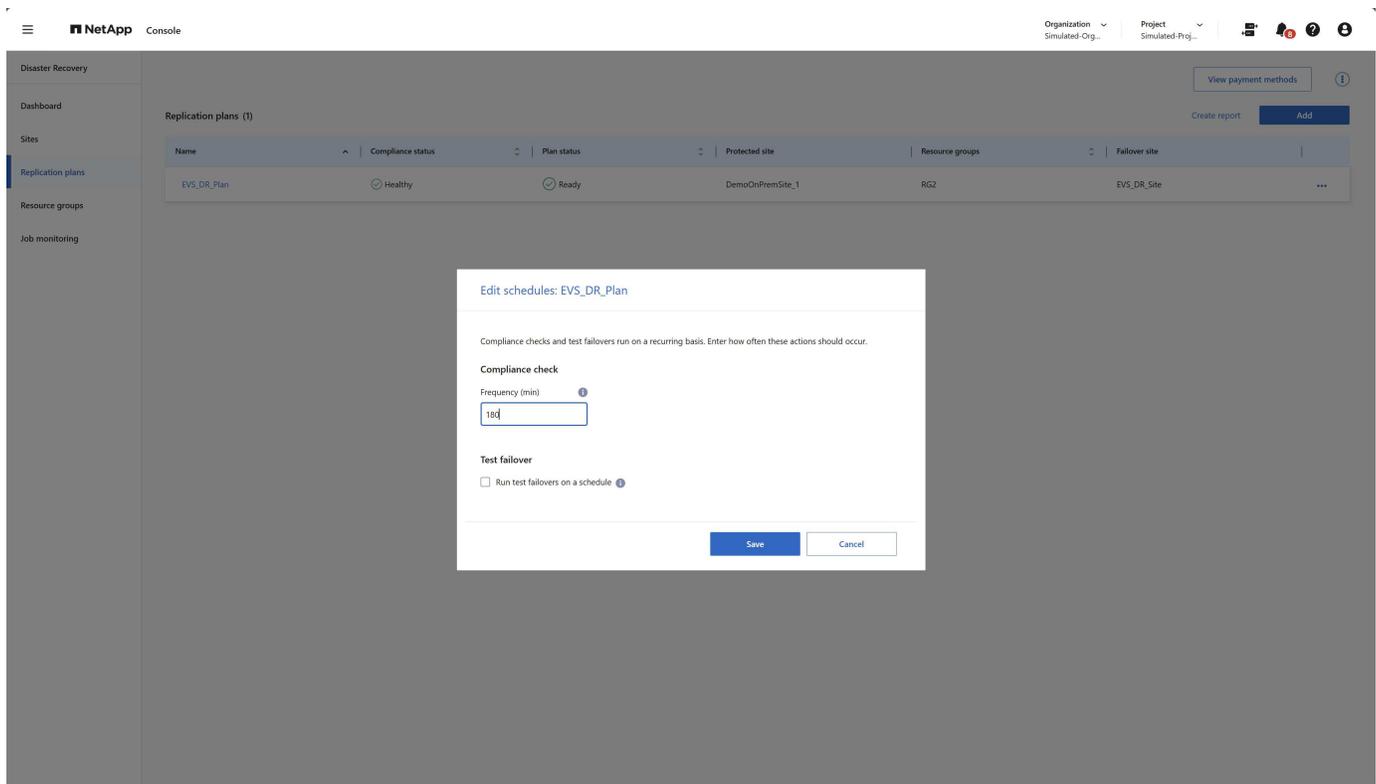
1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Um diese Zeitpläne für einen dieser beiden Vorgänge zu ändern, wählen Sie **Zeitpläne bearbeiten** für den Replikationsplan aus.



## Intervall für die Konformitätsprüfung ändern

Standardmäßig werden alle drei Stunden Konformitätsprüfungen durchgeführt. Sie können dies auf ein beliebiges Intervall zwischen 30 Minuten und 24 Stunden ändern.

Um dieses Intervall zu ändern, ändern Sie das Feld „Häufigkeit“ im Dialogfeld „Zeitpläne bearbeiten“:



The screenshot shows the NetApp console interface. On the left, there is a navigation menu with options like 'Dashboard', 'Sites', 'Replication plans', 'Resource groups', and 'Job monitoring'. The main area displays a table of replication plans. One plan, 'EVS\_DR\_Plan', is selected, and a dialog box titled 'Edit schedules: EVS\_DR\_Plan' is open. The dialog contains a 'Compliance check' section with a 'Frequency (min)' input field set to '180'. Below it is a 'Test failover' section with a checkbox labeled 'Run test failovers on a schedule' which is currently unchecked. 'Save' and 'Cancel' buttons are at the bottom of the dialog.

## Planen Sie automatisierte Test-Failover

Test-Failover werden standardmäßig manuell ausgeführt. Sie können automatische Test-Failover planen, um sicherzustellen, dass Ihre Replikationspläne wie erwartet funktionieren. Weitere Informationen zum Test-Failover-Prozess finden Sie unter ["Testen des Failover-Prozesses"](#).

### Schritte zum Planen von Test-Failovern

1. Wählen Sie die Option \*Aktionen\*  neben dem Replikationsplan.
2. Wählen Sie **Failover ausführen**.
3. Aktivieren Sie das Kontrollkästchen **Test-Failover nach Zeitplan ausführen**.
4. (Optional) Aktivieren Sie **On-Demand-Snapshot für geplantes Test-Failover verwenden**.
5. Wählen Sie im Dropdown-Menü „Wiederholen“ einen Intervalltyp aus.
6. Wählen Sie aus, wann das Test-Failover durchgeführt werden soll
  - a. Wöchentlich: Wählen Sie den Wochentag
  - b. Monatlich: Wählen Sie den Tag des Monats
7. Wählen Sie die Tageszeit für die Ausführung des Test-Failovers
8. Wählen Sie das Startdatum.
9. Entscheiden Sie, ob der Dienst die Testumgebung automatisch bereinigen soll und wie lange die Testumgebung ausgeführt werden soll, bevor der Bereinigungsprozess beginnt.

## 10. Wählen Sie Speichern.

The screenshot shows the NetApp console interface. The main window displays the 'Edit schedules: EVS\_DR\_Plan' dialog box. The dialog box contains the following fields and options:

- Compliance check:**
  - Frequency (min): 180
- Test failover:**
  - Run test failovers on a schedule (3)
  - Use on-demand snapshot for scheduled test failover (4)
- Repeat:** Weekly (5)
- Day of the week:** Saturday (6)
- Hour:** 01 (7)
- Minute:** 00
- AM/PM:** AM
- Start date:** 2025-09-23 (8)
- Automatically cleanup 10 minutes after test failover (9)

At the bottom of the dialog box, there are two buttons: 'Save' (10) and 'Cancel'.

## Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.