Verwenden Sie NetApp Disaster Recovery

NetApp Disaster Recovery

NetApp
January 12, 2026

Inhalt

Verwenden Sie NetApp Disaster Recovery

Übersicht zur NetApp Disaster Recovery verwenden

Mit NetApp Disaster Recovery können Sie die folgenden Ziele erreichen:

- "Überprüfen Sie den Zustand Ihrer Notfallwiederherstellungspläne" .
- "vCenter-Sites hinzufügen" .
- "Erstellen Sie Ressourcengruppen, um VMs gemeinsam zu organisieren"
- "Erstellen Sie einen Notfallwiederherstellungsplan" .
- "Replizieren von VMware-Apps"auf Ihrem primären Standort zu einem Remote-Standort zur Notfallwiederherstellung in der Cloud mithilfe der SnapMirror -Replikation.
- "Migrieren von VMware-Apps"auf Ihrer primären Site zu einer anderen Site.
- "Testen des Failovers"ohne die ursprünglichen virtuellen Maschinen zu stören.
- Im Falle einer Katastrophe"Failover Ihrer primären Site" zu VMware Cloud auf AWS mit FSx für NetApp ONTAP.
- Nachdem die Katastrophe behoben ist,"Failback" vom Disaster-Recovery-Standort zum primären Standort.
- "Überwachen von Notfallwiederherstellungsvorgängen"auf der Seite „Jobüberwachung“.

Sehen Sie sich den Zustand Ihrer NetApp Disaster Recovery -Pläne auf dem Dashboard an

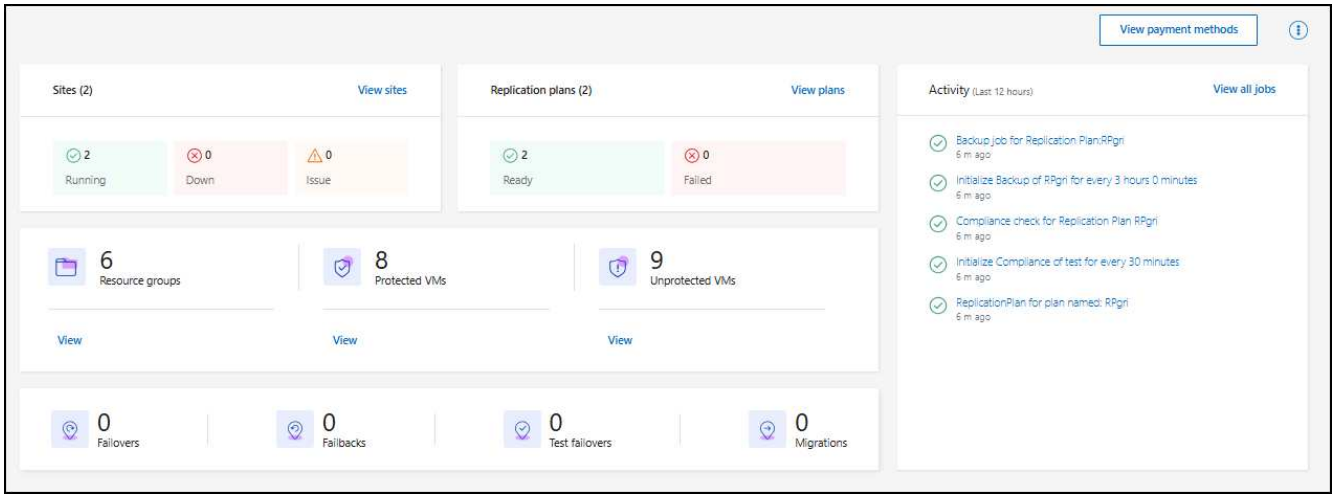
Mithilfe des NetApp Disaster Recovery Dashboards können Sie den Zustand Ihrer Disaster Recovery-Sites und Replikationspläne ermitteln. Sie können schnell feststellen, welche Websites und Pläne fehlerfrei, getrennt oder beeinträchtigt sind.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Anwendungsadministrator oder Disaster Recovery-Viewer-Rolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im NetApp Disaster Recovery Menü **Dashboard** aus.



4. Überprüfen Sie die folgenden Informationen auf dem Dashboard:
   - **Sites**: Zeigen Sie den Zustand Ihrer Sites an. Eine Site kann einen der folgenden Status haben:
     - **Läuft**: Das vCenter ist verbunden, fehlerfrei und läuft.
     - **Down**: Das vCenter ist nicht erreichbar oder hat Verbindungsprobleme.
     - **Problem**: Das vCenter ist nicht erreichbar oder hat Verbindungsprobleme.

       Um Sitedetails anzuzeigen, wählen Sie **Alle anzeigen** für einen Status oder **Sites anzeigen**, um sie alle anzuzeigen.
   - **Replikationspläne**: Zeigen Sie den Zustand Ihrer Pläne an. Ein Plan kann einen der folgenden Status haben:
     - **Bereit**
     - **Fehlgeschlagen**

       Um die Details des Replikationsplans zu überprüfen, wählen Sie **Alle anzeigen** für einen Status oder **Replikationspläne anzeigen**, um sie alle anzuzeigen.
   - **Ressourcengruppen**: Zeigen Sie den Zustand Ihrer Ressourcengruppen an. Eine Ressourcengruppe kann einen der folgenden Status haben:
   - **Geschützte VMs**: Die VMs sind Teil einer Ressourcengruppe.
   - **Ungeschützte VMs**: Die VMs sind nicht Teil einer Ressourcengruppe.

     Um die Details zu überprüfen, wählen Sie jeweils den Link **Anzeigen** darunter aus.
   - Die Anzahl der Failovers, Test-Failover und Migrationen. Wenn Sie beispielsweise zwei Pläne erstellt und zu den Zielen migriert haben, wird als Migrationsanzahl „2“ angezeigt.
5. Überprüfen Sie alle Vorgänge im Aktivitätsbereich. Um alle Vorgänge im Job Monitor anzuzeigen, wählen Sie **Alle Jobs anzeigen**.

Hinzufügen von vCentern zu einer Site in NetApp Disaster Recovery

Bevor Sie einen Notfallwiederherstellungsplan erstellen können, müssen Sie einem Standort einen primären vCenter-Server und in der NetApp Console einen vCenter-

Zielstandort für die Notfallwiederherstellung hinzufügen.

Stellen Sie sicher, dass sowohl das Quell- als auch das Ziel-vCenter denselben NetApp Console verwenden.

Nachdem vCenter hinzugefügt wurden, führt NetApp Disaster Recovery eine umfassende Erkennung der vCenter-Umgebungen durch, einschließlich vCenter-Cluster, ESXi-Hosts, Datenspeicher, Speicherbedarf, Details zu virtuellen Maschinen, SnapMirror Replikaten und Netzwerken virtueller Maschinen.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator oder Notfallwiederherstellungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Über diese Aufgabe

Wenn Sie in früheren Versionen vCenter hinzugefügt haben und den Erkennungszeitplan anpassen möchten, müssen Sie die vCenter-Server-Site bearbeiten und den Zeitplan festlegen.

NetApp Disaster Recovery führt alle 24 Stunden eine Erkennung durch. Nachdem Sie eine Site eingerichtet haben, können Sie das vCenter später bearbeiten, um den Erkennungszeitplan an Ihre Anforderungen anzupassen. Wenn Sie beispielsweise über eine große Anzahl VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 23 Stunden und 59 Minuten ausgeführt wird. Wenn Sie nur eine kleine Anzahl von VMs haben, können Sie den Erkennungszeitplan so einstellen, dass er alle 12 Stunden ausgeführt wird. Das Mindestintervall beträgt 30 Minuten und das Höchstintervall 24 Stunden.

Sie sollten zunächst einige manuelle Ermittlungen durchführen, um die aktuellsten Informationen zu Ihrer Umgebung zu erhalten. Danach können Sie den Zeitplan so einstellen, dass er automatisch ausgeführt wird.

Wenn Sie über vCenter aus früheren Versionen verfügen und den Zeitpunkt der Erkennung ändern möchten, bearbeiten Sie die vCenter-Server-Site und legen Sie den Zeitplan fest.

Neu hinzugefügte oder gelöschte VMs werden bei der nächsten geplanten Erkennung oder während einer sofortigen manuellen Erkennung erkannt.

VMs können nur geschützt werden, wenn sich der Replikationsplan in einem der folgenden Zustände befindet:

- Bereit
- Failback durchgeführt
- Test-Failover festgeschrieben

vCenter-Cluster an einem Standort Jeder Standort enthält ein oder mehrere vCenter. Diese vCenter verwenden einen oder mehrere ONTAP Speichercluster zum Hosten von NFS- oder VMFS-Datenspeichern.

Ein vCenter-Cluster kann sich nur an einem Standort befinden. Sie benötigen die folgenden Informationen, um einer Site einen vCenter-Cluster hinzuzufügen:

- Die vCenter-Verwaltungs-IP-Adresse oder der FQDN
- Anmeldeinformationen für ein vCenter-Konto mit den erforderlichen Berechtigungen zum Ausführen von Vorgängen. Sehen"erforderliche vCenter-Berechtigungen" für weitere Informationen.

- Für Cloud-gehostete VMware-Sites die erforderlichen Cloud-Zugriffsschlüssel
- Ein Sicherheitszertifikat für den Zugriff auf Ihr vCenter.

> Der Dienst unterstützt selbstsignierte Sicherheitszertifikate oder Zertifikate einer zentralen Zertifizierungsstelle (CA).

Schritte

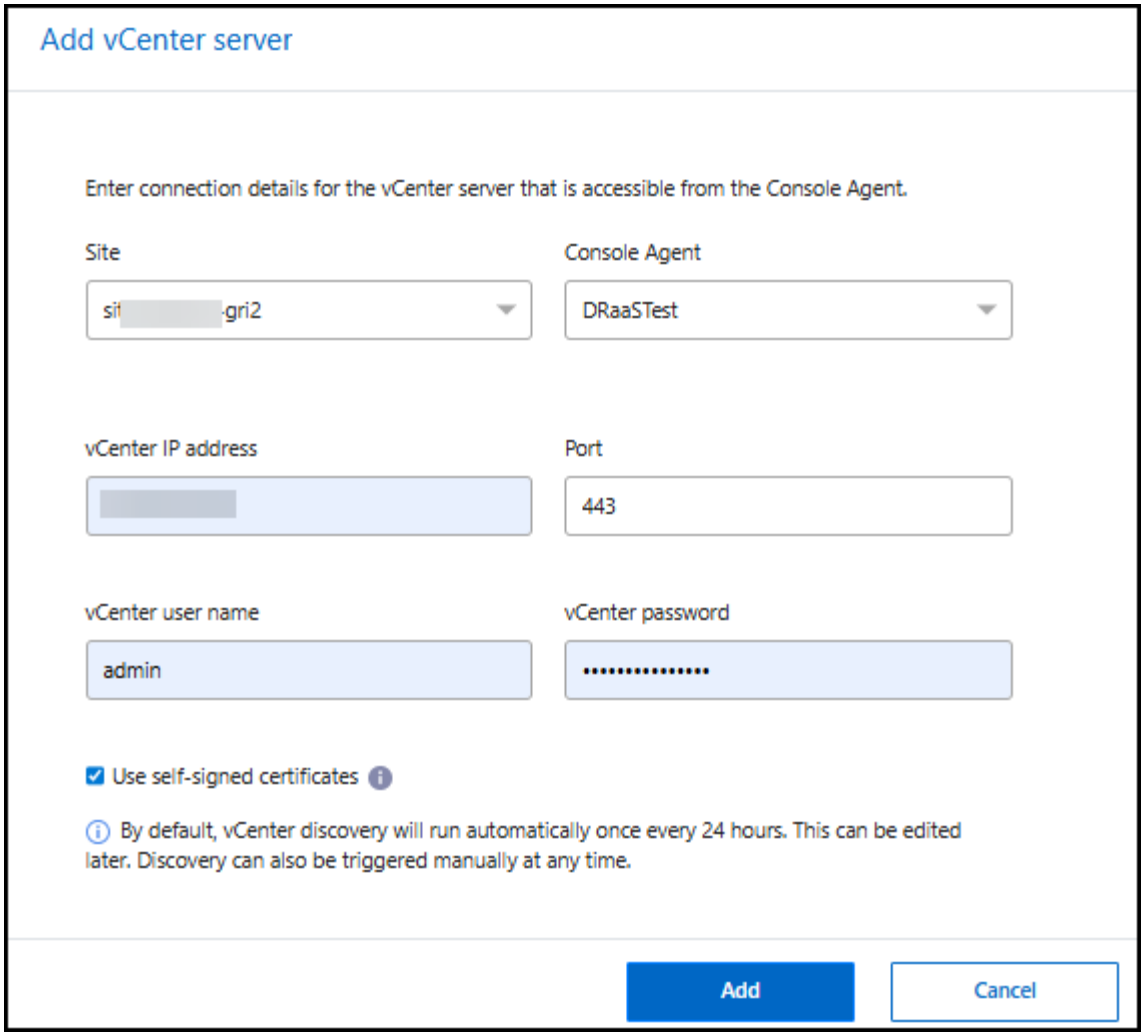
1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.

   Wenn Sie NetApp Disaster Recovery zum ersten Mal verwenden, müssen Sie vCenter-Informationen hinzufügen. Wenn Sie bereits vCenter-Informationen hinzugefügt haben, wird Ihnen das Dashboard angezeigt.

   > Je nach Art der Site, die Sie hinzufügen, werden unterschiedliche Felder angezeigt.

3. Wenn bereits einige vCenter-Sites vorhanden sind und Sie weitere hinzufügen möchten, wählen Sie im Menü **Sites** und dann **Hinzufügen** aus.
4. Wählen Sie auf der Seite „Sites“ die Site aus und wählen Sie **vCenter hinzufügen**.
5. **Quelle**: Wählen Sie **vCenter-Server ermitteln**, um Informationen zur vCenter-Quellsite einzugeben.

   > Um weitere vCenter-Sites hinzuzufügen, wählen Sie **Sites** und anschließend **Hinzufügen**.



- Wählen Sie einen Standort und anschließend den NetApp Console Agenten aus und geben Sie die vCenter-Anmeldeinformationen an.
- **Nur für lokale Installationen:** Um selbstsignierte Zertifikate für das Quell-vCenter zu akzeptieren, aktivieren Sie das Kontrollkästchen.

> Selbstsignierte Zertifikate sind nicht so sicher wie andere Zertifikate. Wenn Ihr vCenter **NICHT** mit Zertifikaten einer Zertifizierungsstelle (CA) konfiguriert ist, sollten Sie dieses Kontrollkästchen aktivieren. Andernfalls funktioniert die Verbindung zum vCenter nicht.

6. Wählen Sie **Hinzufügen**.

   Als Nächstes fügen Sie ein Ziel-vCenter hinzu.

7. Fügen Sie erneut eine Site für das Ziel-vCenter hinzu.
8. Wählen Sie erneut **vCenter hinzufügen** und fügen Sie die Ziel-vCenter-Informationen hinzu.
9. **Ziel**:

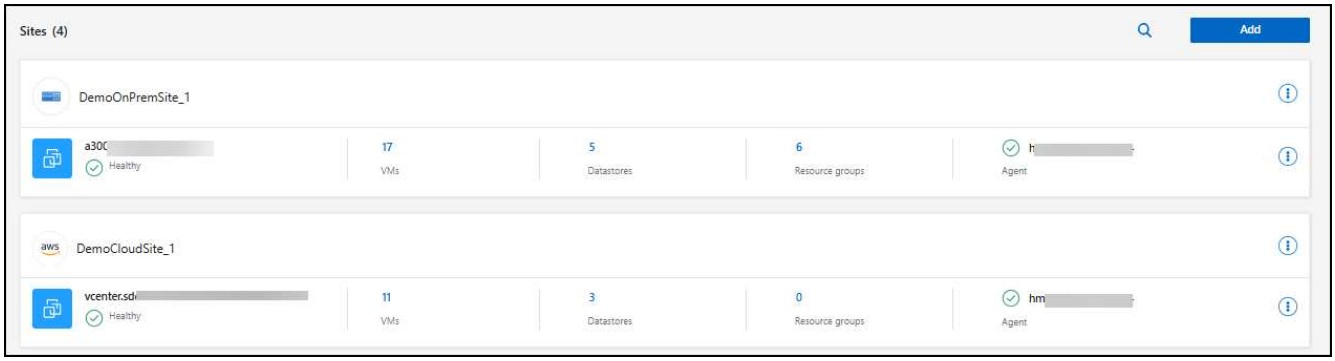
   a. Wählen Sie die Zielsite und den Standort aus. Wenn das Ziel die Cloud ist, wählen Sie **AWS**.

      - (Gilt nur für Cloud-Sites) **API-Token**: Geben Sie das API-Token ein, um den Dienstzugriff für Ihre Organisation zu autorisieren. Erstellen Sie das API-Token, indem Sie bestimmte Organisations- und Servicerollen angeben.

- (Gilt nur für Cloud-Sites) **Lange Organisations-ID**: Geben Sie die eindeutige ID für die Organisation ein. Sie können diese ID ermitteln, indem Sie im Abschnitt „Konto“ der NetApp Console auf den Benutzernamen klicken.

b. Wählen Sie **Hinzufügen**.

Die Quell- und Ziel-vCenter werden in der Siteliste angezeigt.



10. Um den Fortschritt des Vorgangs anzuzeigen, wählen Sie im Menü **Jobüberwachung** aus.

Subnetzzuordnung für eine vCenter-Site hinzufügen

Sie können IP-Adressen bei Failover-Vorgängen mithilfe der Subnetzzuordnung verwalten, wodurch Sie für jedes vCenter Subnetze hinzufügen können. Dabei definieren Sie das IPv4-CIDR, das Standard-Gateway und das DNS für jedes virtuelle Netzwerk.

Beim Failover verwendet NetApp Disaster Recovery das CIDR des zugeordneten Netzwerks, um jeder vNIC eine neue IP-Adresse zuzuweisen.

Beispiel:

- NetzwerkA = 10.1.1.0/24
- NetzwerkB = 192.168.1.0/24

VM1 verfügt über eine vNIC (10.1.1.50), die mit NetworkA verbunden ist. In den Replikationsplaneinstellungen wird NetworkA NetworkB zugeordnet.

Beim Failover ersetzt NetApp Disaster Recovery den Netzwerkteil der ursprünglichen IP-Adresse (10.1.1) und behält die Hostadresse (.50) der ursprünglichen IP-Adresse (10.1.1.50) bei. Für VM1 prüft NetApp Disaster Recovery die CIDR-Einstellungen für NetworkB und verwendet den NetworkB-Netzwerkteil 192.168.1, während der Hostteil (.50) beibehalten wird, um die neue IP-Adresse für VM1 zu erstellen. Die neue IP wird 192.168.1.50.

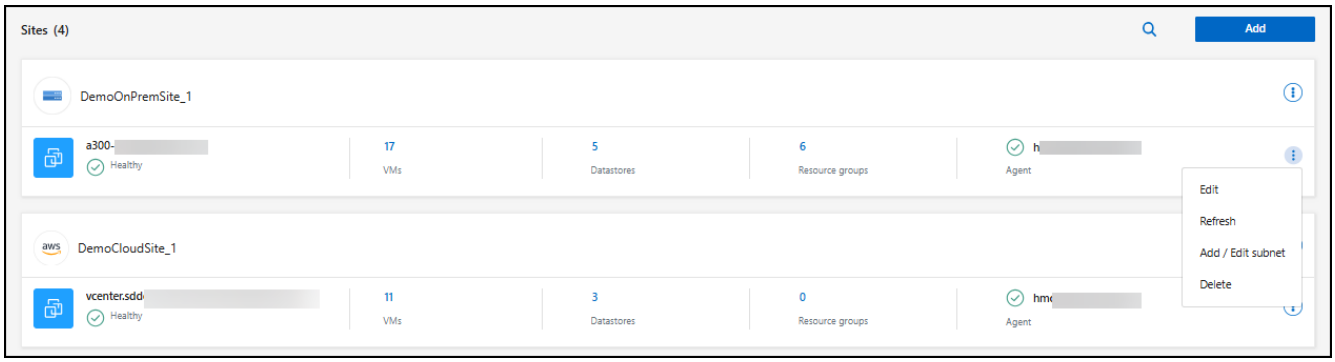
Zusammenfassend lässt sich sagen, dass die Hostadresse gleich bleibt, während die Netzwerkadresse durch die in der Site-Subnetzzuordnung konfigurierte Adresse ersetzt wird. Auf diese Weise können Sie die Neuzuweisung von IP-Adressen bei einem Failover einfacher verwalten, insbesondere wenn Sie Hunderte von Netzwerken und Tausende von VMs verwalten müssen.

Die Verwendung der Subnetzzuordnung ist ein optionaler zweistufiger Prozess:

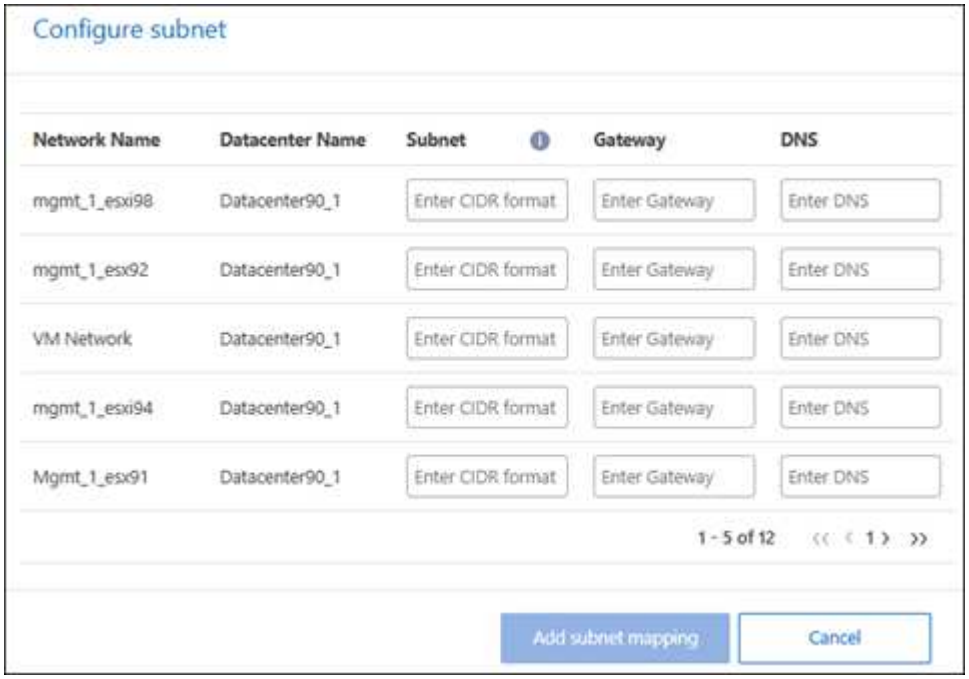
- Fügen Sie zunächst die Subnetzzuordnung für jeden vCenter-Standort hinzu.
- Geben Sie zweitens im Replikationsplan auf der Registerkarte „Virtuelle Maschinen“ und im Feld „Ziel-IP“ an, dass Sie die Subnetzzuordnung verwenden möchten.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Sites** aus.
2. Von den Aktionen Symbol rechts und wählen Sie **Subnetz hinzufügen**.



Die Seite „Subnetz konfigurieren“ wird angezeigt:



3. Geben Sie auf der Seite „Subnetz konfigurieren“ die folgenden Informationen ein:
   a. Subnetz: Geben Sie den IPv4-CIDR für das Subnetz bis zu /32 ein.

> Die CIDR-Notation ist eine Methode zum Angeben von IP-Adressen und ihren Netzwerkmasken. Die /24 bezeichnet die Netzmaske. Die Nummer besteht aus einer IP-Adresse, wobei die Zahl nach dem „/“ angibt, wie viele Bits der IP-Adresse das Netzwerk bezeichnen. Beispiel: 192.168.0.50/24, die IP-Adresse ist 192.168.0.50 und die Gesamtzahl der Bits in der Netzwerkadresse beträgt 24. 192.168.0.50 255.255.255.0 wird zu 192.168.0.0/24.

   b. Gateway: Geben Sie das Standard-Gateway für das Subnetz ein.
   c. DNS: Geben Sie den DNS für das Subnetz ein.

4. Wählen Sie **Subnetzzuordnung hinzufügen**.

Auswählen der Subnetzzuordnung für einen Replikationsplan

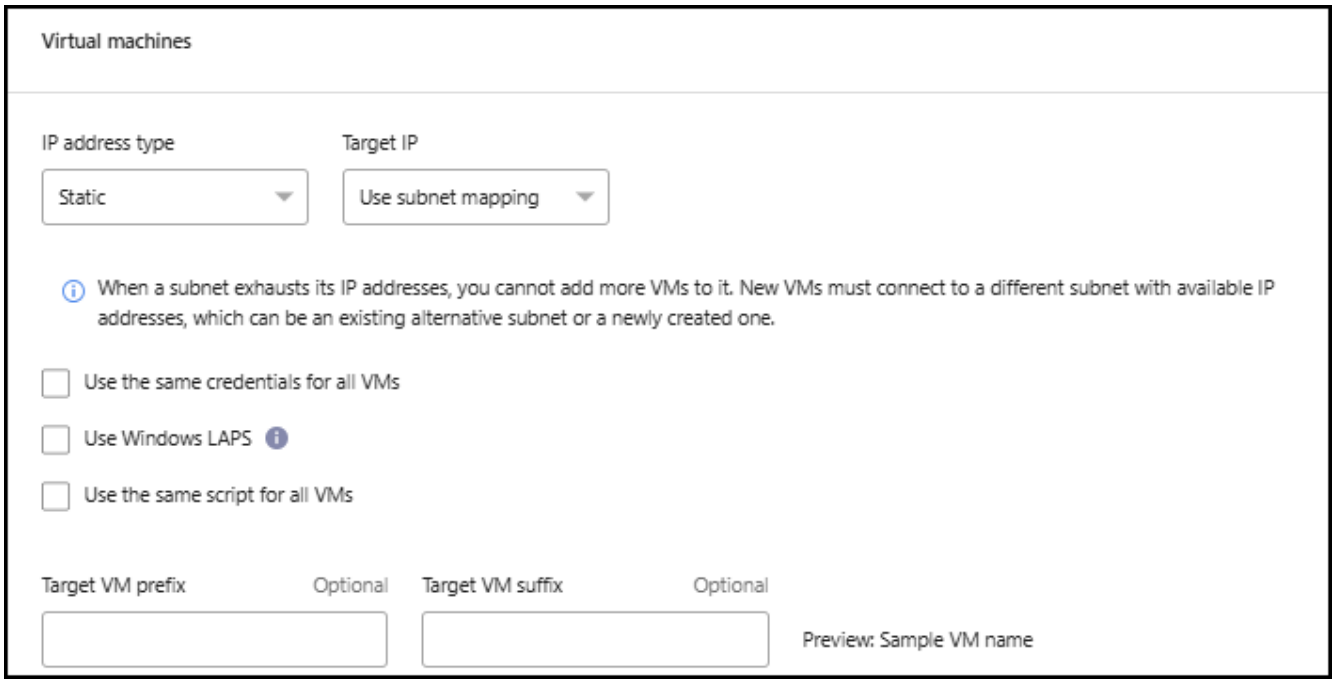
Wenn Sie einen Replikationsplan erstellen, können Sie die Subnetzzuordnung für den Replikationsplan auswählen.

Die Verwendung der Subnetzzuordnung ist ein optionaler zweistufiger Prozess:

- Fügen Sie zunächst die Subnetzzuordnung für jeden vCenter-Standort hinzu.
- Geben Sie zweitens im Replikationsplan an, dass Sie die Subnetzzuordnung verwenden möchten.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.
2. Wählen Sie **Hinzufügen**, um einen Replikationsplan hinzuzufügen.
3. Füllen Sie die Felder wie gewohnt aus, indem Sie die vCenter-Server hinzufügen, die Ressourcengruppen oder Anwendungen auswählen und die Zuordnungen vervollständigen.
4. Wählen Sie auf der Seite Replikationsplan > Ressourcenzuordnung den Abschnitt **Virtuelle Maschinen** aus.



5. Wählen Sie im Feld **Ziel-IP** aus der Dropdown-Liste **Subnetzzuordnung verwenden** aus.

> Wenn zwei VMs vorhanden sind (beispielsweise eine mit Linux und die andere mit Windows), werden Anmeldeinformationen nur für Windows benötigt.

6. Fahren Sie mit der Erstellung des Replikationsplans fort.

Bearbeiten Sie die vCenter-Server-Site und passen Sie den Erkennungszeitplan an

Sie können die vCenter-Server-Site bearbeiten, um den Erkennungszeitplan anzupassen. Wenn Sie beispielsweise über eine große Anzahl von VMs verfügen, können Sie den Erkennungszeitplan so einstellen,

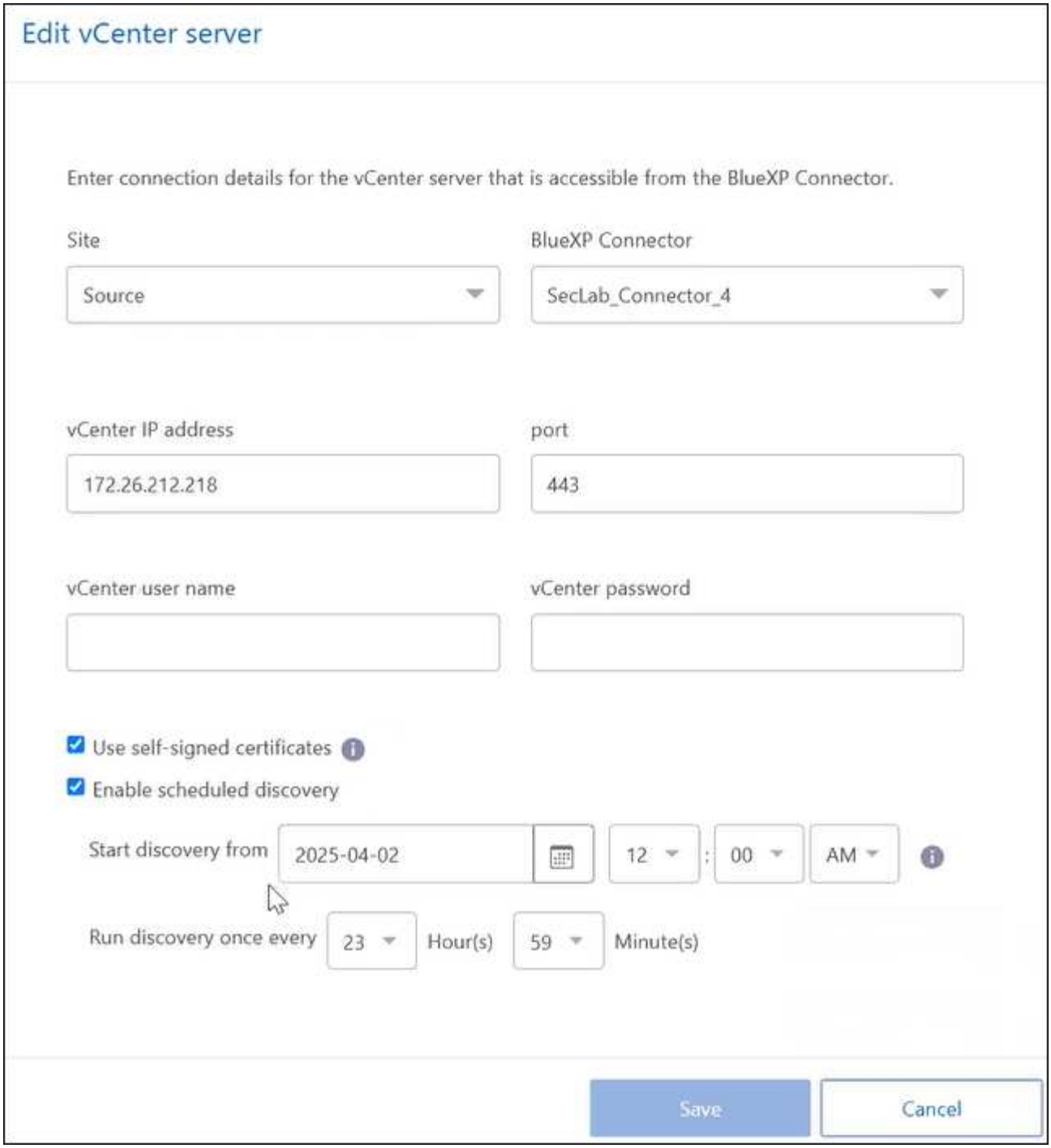
dass er alle 23 Stunden und 59 Minuten ausgeführt wird. Wenn Sie nur eine kleine Anzahl von VMs haben, können Sie den Erkennungszeitplan so einstellen, dass er alle 12 Stunden ausgeführt wird.

Wenn Sie über vCenter aus früheren Versionen verfügen und den Zeitpunkt der Erkennung ändern möchten, bearbeiten Sie die vCenter-Server-Site und legen Sie den Zeitplan fest.

Wenn Sie die Erkennung nicht planen möchten, können Sie die Option zur geplanten Erkennung deaktivieren und die Erkennung jederzeit manuell aktualisieren.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Sites** aus.
2. Wählen Sie die Site aus, die Sie bearbeiten möchten.
3. Wählen Sie die Aktionen  Symbol rechts und wählen Sie **Bearbeiten**.
4. Bearbeiten Sie auf der Seite „vCenter-Server bearbeiten“ die Felder nach Bedarf.
5. Um den Erkennungszeitplan anzupassen, aktivieren Sie das Kontrollkästchen **Geplante Erkennung aktivieren** und wählen Sie das gewünschte Datum und Zeitintervall aus.



6. Wählen Sie **Speichern**.

Erkennung manuell aktualisieren

Sie können die Erkennung jederzeit manuell aktualisieren. Dies ist nützlich, wenn Sie VMs hinzugefügt oder entfernt haben und die Informationen in NetApp Disaster Recovery aktualisieren möchten.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Sites** aus.
2. Wählen Sie die Site aus, die Sie aktualisieren möchten.
3.

Wählen Sie die Aktionen  Symbol rechts und wählen Sie **Aktualisieren**.

Erstellen Sie eine Ressourcengruppe, um VMs gemeinsam in NetApp Disaster Recovery zu organisieren

Nachdem Sie vCenter-Sites hinzugefügt haben, können Sie Ressourcengruppen erstellen, um VMs nach VM oder Datenspeicher als einzelne Einheit zu schützen. Mithilfe von Ressourcengruppen können Sie eine Reihe abhängiger VMs in logischen Gruppen organisieren, die Ihren Anforderungen entsprechen. Sie können beispielsweise VMs gruppieren, die einer Anwendung zugeordnet sind, oder Sie können Anwendungen gruppieren, die ähnliche Ebenen haben. Ein weiteres Beispiel: Gruppen könnten verzögerte Startaufträge enthalten, die bei der Wiederherstellung ausgeführt werden können.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Notfallwiederherstellungsanwendungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Über diese Aufgabe

Sie können VMs selbst oder VMs in Datenspeichern gruppieren.

Sie können Ressourcengruppen mit den folgenden Methoden erstellen:

- Über die Option „Ressourcengruppen“
- Während Sie einen Notfallwiederherstellungs- oder *Replikationsplan* erstellen. Wenn Sie über viele VMs verfügen, die von einem vCenter-Quellcluster gehostet werden, ist es möglicherweise einfacher für Sie, die Ressourcengruppen zu erstellen, während Sie den Replikationsplan erstellen. Anweisungen zum Erstellen von Ressourcengruppen beim Erstellen eines Replikationsplans finden Sie unter"Erstellen eines Replikationsplans" .

Jede Ressourcengruppe kann eine oder mehrere VMs oder Datenspeicher enthalten. Die VMs werden basierend auf der Reihenfolge eingeschaltet, in der Sie sie in den Replikationsplan aufnehmen. Sie können die Reihenfolge ändern, indem Sie die VMs oder Datenspeicher in der Ressourcengruppenliste nach oben oder unten ziehen.

Informationen zu Ressourcengruppen

Mithilfe von Ressourcengruppen können Sie VMs oder Datenspeicher zu einer einzigen Einheit zusammenfassen.

Beispielsweise könnte eine Point-of-Sale-Anwendung mehrere VMs für Datenbanken, Geschäftslogik und Storefronts verwenden. Sie können alle diese VMs mit einer Ressourcengruppe verwalten. Richten Sie Ressourcengruppen ein, um Replikationsplanregeln für die VM-Startreihenfolge, Netzwerkverbindung und Wiederherstellung aller für die Anwendung benötigten VMs anzuwenden.

Wie funktioniert es?

NetApp Disaster Recovery schützt VMs durch Replikation der zugrunde liegenden ONTAP Volumes und LUNs,

die die VMs in der Ressourcengruppe hosten. Dazu fragt das System vCenter nach dem Namen jedes Datenspeichers ab, der VMs in einer Ressourcengruppe hostet. NetApp Disaster Recovery identifiziert dann das Quell ONTAP -Volume oder die LUN, auf der dieser Datenspeicher gehostet wird. Der gesamte Schutz wird auf ONTAP Volume-Ebene mithilfe der SnapMirror -Replikation durchgeführt.

Wenn VMs in der Ressourcengruppe auf verschiedenen Datenspeichern gehostet werden, verwendet NetApp Disaster Recovery eine der folgenden Methoden, um einen datenkonsistenten Snapshot der ONTAP Volumes oder LUNs zu erstellen.

Relativer Standort von FlexVol -Volumes	**Snapshot-Replikationsprozess**
Mehrere Datenspeicher – FlexVol -Volumes im **gleichen SVM**	• ONTAP -Konsistenzgruppe erstellt • Snapshots der Konsistenzgruppe erstellt • Volume-bezogene SnapMirror -Replikation durchgeführt
Mehrere Datenspeicher – FlexVol -Volumes in **mehreren SVMs**	• ONTAP -API: `cg_start` . Stellt alle Volumes still, damit Snapshots erstellt werden können, und initiiert volumebezogene Snapshots aller Ressourcengruppen-Volumes. • ONTAP -API: `cg_end` . Setzt die E/A auf allen Volumes fort und aktiviert die Volume-bezogene SnapMirror Replikation, nachdem Snapshots erstellt wurden.

Berücksichtigen Sie beim Erstellen von Ressourcengruppen die folgenden Punkte:

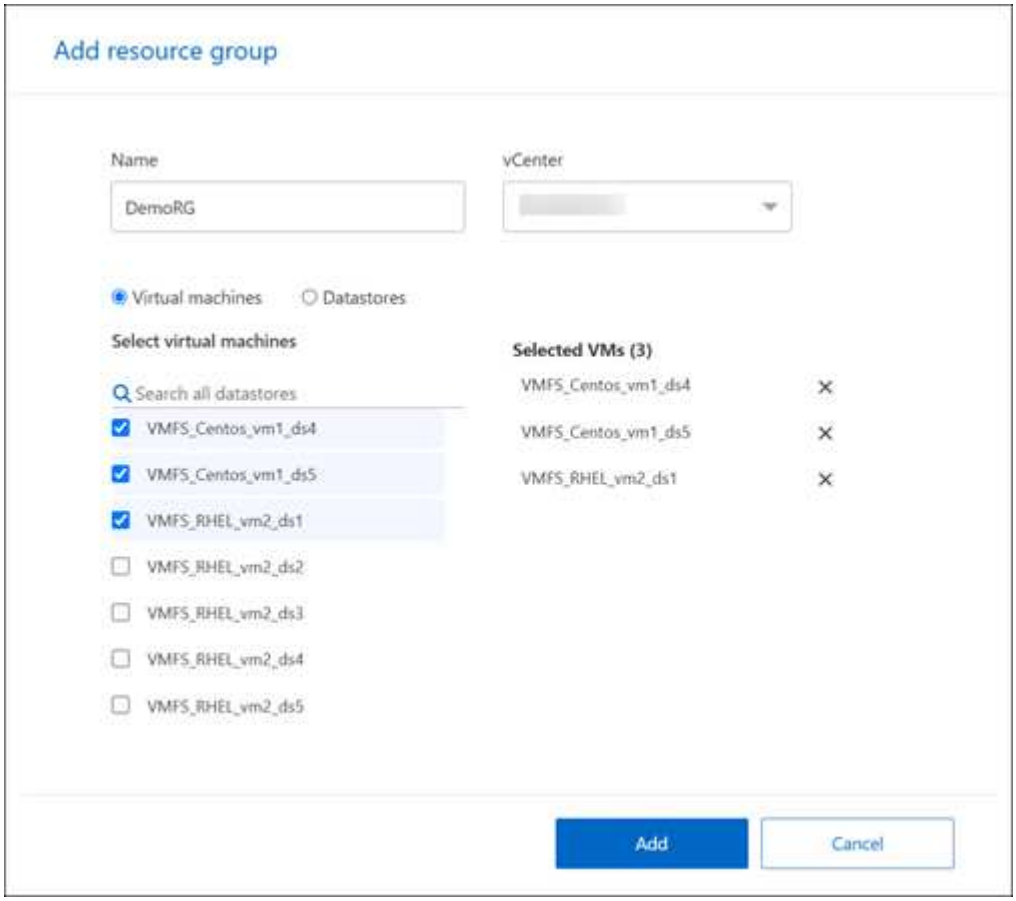
- Bevor Sie Datenspeicher zu Ressourcengruppen hinzufügen, starten Sie zunächst eine manuelle oder geplante Erkennung der VMs. Dadurch wird sichergestellt, dass die VMs erkannt und in der Ressourcengruppe aufgelistet werden. Wenn Sie keine manuelle Erkennung starten, werden die VMs möglicherweise nicht in der Ressourcengruppe aufgeführt.
- Stellen Sie sicher, dass sich mindestens eine VM im Datenspeicher befindet. Wenn sich im Datenspeicher keine VMs befinden, erkennt Disaster Recovery den Datenspeicher nicht.
- Ein einzelner Datenspeicher sollte keine VMs hosten, die durch mehr als einen Replikationsplan geschützt sind.
- Hosten Sie geschützte und ungeschützte VMs nicht auf demselben Datenspeicher. Wenn geschützte und ungeschützte VMs auf demselben Datenspeicher gehostet werden, können die folgenden Probleme auftreten:
  - Da NetApp Disaster Recovery SnapMirror verwendet und das System ganze ONTAP Volumes repliziert, wird die genutzte Kapazität dieses Volumes für Lizenzierungsüberlegungen verwendet. In diesem Fall würde der von geschützten und ungeschützten VMs belegte Volume-Speicherplatz in diese Berechnung einbezogen.
  - Wenn ein Failover der Ressourcengruppe und der zugehörigen Datenspeicher auf den Disaster Recovery-Standort durchgeführt werden muss, sind alle ungeschützten VMs (VMs, die nicht Teil der Ressourcengruppe sind, aber auf dem ONTAP Volume gehostet werden) durch den Failover-Prozess nicht mehr auf dem Quellstandort vorhanden, was zu einem Ausfall ungeschützter VMs am Quellstandort führt. Außerdem startet NetApp Disaster Recovery diese ungeschützten VMs nicht am Failover-vCenter-Standort.
- Um eine VM zu schützen, muss sie in eine Ressourcengruppe aufgenommen werden.

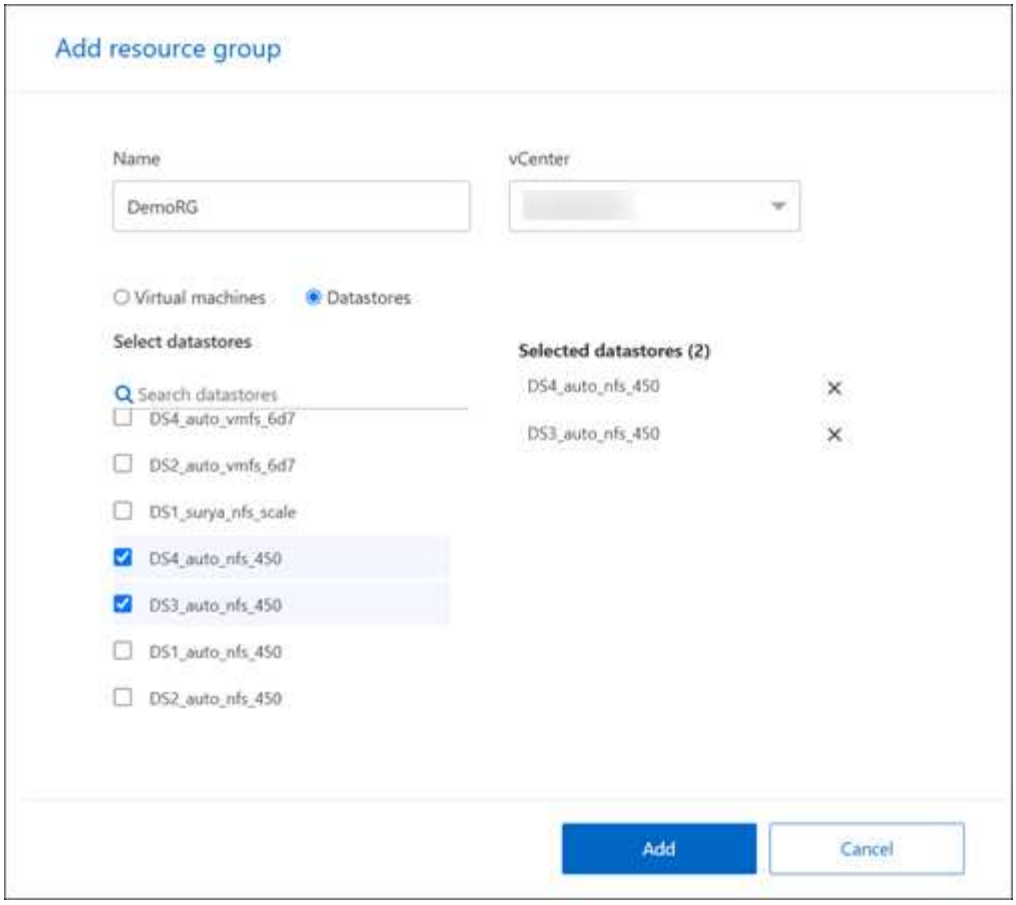
BEST PRACTICE: Organisieren Sie Ihre VMs, bevor Sie NetApp Disaster Recovery bereitstellen, um die

Ausbreitung von Datenspeichern zu minimieren. Platzieren Sie VMs, die Schutz benötigen, auf einer Teilmenge von Datenspeichern und platzieren Sie VMs, die nicht geschützt werden sollen, auf einer anderen Teilmenge von Datenspeichern. Stellen Sie sicher, dass die VMs auf einem bestimmten Datenspeicher nicht durch unterschiedliche Replikationspläne geschützt sind.

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im NetApp Disaster Recovery Menü **Ressourcengruppen** aus.
4. Wählen Sie **Hinzufügen**.
5. Geben Sie einen Namen für die Ressourcengruppe ein.
6. Wählen Sie den Quell-vCenter-Cluster aus, in dem sich die VMs befinden.
7. Wählen Sie je nach gewünschter Suchmethode entweder **Virtuelle Maschinen** oder **Datenspeicher** aus.
8. Wählen Sie die Registerkarte **Ressourcengruppen hinzufügen**. Das System listet alle Datenspeicher oder VMs im ausgewählten vCenter-Cluster auf. Wenn Sie **Datenspeicher** ausgewählt haben, listet das System alle Datenspeicher im ausgewählten vCenter-Cluster auf. Wenn Sie **Virtuelle Maschinen** ausgewählt haben, listet das System alle VMs im ausgewählten vCenter-Cluster auf.
9. Wählen Sie auf der linken Seite der Seite „Ressourcengruppen hinzufügen“ die VMs aus, die Sie schützen möchten.





10. Ändern Sie optional die Reihenfolge der VMs auf der rechten Seite, indem Sie jede VM in der Liste nach oben oder unten ziehen. Die VMs werden basierend auf der Reihenfolge eingeschaltet, in der Sie sie einschließen.
11. Wählen Sie **Hinzufügen**.

Erstellen eines Replikationsplans in NetApp Disaster Recovery

Nachdem Sie vCenter-Sites hinzugefügt haben, können Sie einen Notfallwiederherstellungs- oder Replikationsplan erstellen. Replikationspläne verwalten den Datenschutz der VMware-Infrastruktur. Wählen Sie die Quell- und Ziel-vCenter aus, wählen Sie die Ressourcengruppen aus und gruppieren Sie, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen. Sie können beispielsweise virtuelle Maschinen (VMs) gruppieren, die einer Anwendung zugeordnet sind, oder Sie können Anwendungen gruppieren, die ähnliche Ebenen haben. Solche Pläne werden manchmal als „Blaupausen“ bezeichnet.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator oder Disaster Recovery-Anwendungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Über diese Aufgabe

Sie können einen Replikationsplan erstellen und auch Zeitpläne für Compliance und Tests bearbeiten. Führen Sie Test-Failover von VMs durch, ohne die Produktionsarbeitslasten zu beeinträchtigen.

Sie können mehrere VMs auf mehreren Datenspeichern schützen. NetApp Disaster Recovery erstellt ONTAP Konsistenzgruppen für alle ONTAP Volumes, die geschützte VM-Datenspeicher hosten.

VMs können nur geschützt werden, wenn sich der Replikationsplan in einem der folgenden Zustände befindet:

- Bereit
- Failback durchgeführt
- Test-Failover festgeschrieben

Replikationsplan-Snapshots

Disaster Recovery verwaltet die gleiche Anzahl von Snapshots auf den Quell- und Zielclustern. Standardmäßig führt der Dienst alle 24 Stunden einen Snapshot-Abgleichprozess durch, um sicherzustellen, dass die Anzahl der Snapshots auf den Quell- und Zielclustern gleich ist.

Die folgenden Situationen können dazu führen, dass die Anzahl der Snapshots zwischen den Quell- und Zielclustern unterschiedlich ist:

- In einigen Situationen können ONTAP -Vorgänge außerhalb der Notfallwiederherstellung dazu führen, dass Snapshots zum Volume hinzugefügt oder daraus entfernt werden:
  - Wenn auf der Quellsite Snapshots fehlen, werden die entsprechenden Snapshots auf der Zielsite möglicherweise gelöscht, abhängig von der Standard SnapMirror -Richtlinie für die Beziehung.
  - Wenn auf der Zielsite Snapshots fehlen, löscht der Dienst möglicherweise die entsprechenden Snapshots auf der Quellsite während des nächsten geplanten Snapshot-Abgleichprozesses, abhängig von der SnapMirror Standardrichtlinie für die Beziehung.
- Eine Reduzierung der Snapshot-Aufbewahrungsanzahl des Replikationsplans kann dazu führen, dass der Dienst die ältesten Snapshots sowohl auf der Quell- als auch auf der Zielsite löscht, um die neu reduzierte Aufbewahrungsanzahl einzuhalten.

In diesen Fällen entfernt Disaster Recovery bei der nächsten Konsistenzprüfung ältere Snapshots aus den Quell- und Zielclustern. Alternativ kann der Administrator eine sofortige Snapshot-Bereinigung durchführen, indem er die **Aktionen** auswählt. ••• Symbol im Replikationsplan und Auswahl von **Snapshots bereinigen**.

Der Dienst führt alle 24 Stunden Snapshot-Symmetrieprüfungen durch.

Bevor Sie beginnen

- Bevor Sie eine SnapMirror -Beziehung erstellen, richten Sie das Cluster- und SVM-Peering außerhalb der Notfallwiederherstellung ein.
- Mit Google Cloud können Sie einem Replikationsplan nur ein Volume oder einen Datenspeicher hinzufügen.

Organisieren Sie Ihre VMs vor der Bereitstellung von NetApp Disaster Recovery , um die „Datenspeicherausbreitung“ zu minimieren. Platzieren Sie VMs, die Schutz benötigen, auf einer Teilmenge von Datenspeichern und platzieren Sie VMs, die nicht geschützt werden sollen, auf einer anderen Teilmenge von Datenspeichern. Verwenden Sie datenspeicherbasierten Schutz, um sicherzustellen, dass die VMs auf jedem beliebigen Datenspeicher geschützt sind.

Erstellen Sie den Plan

Ein Assistent führt Sie durch die folgenden Schritte:

- Wählen Sie vCenter-Server aus.
- Wählen Sie die VMs oder Datenspeicher aus, die Sie replizieren möchten, und weisen Sie Ressourcengruppen zu.
- Ordnen Sie zu, wie Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden.
- Legen Sie fest, wie oft der Plan ausgeführt wird, führen Sie ein vom Gast gehostetes Skript aus, legen Sie die Startreihenfolge fest und wählen Sie das Wiederherstellungspunktziel aus.
- Überprüfen Sie den Plan.

Beim Erstellen des Plans sollten Sie die folgenden Richtlinien befolgen:

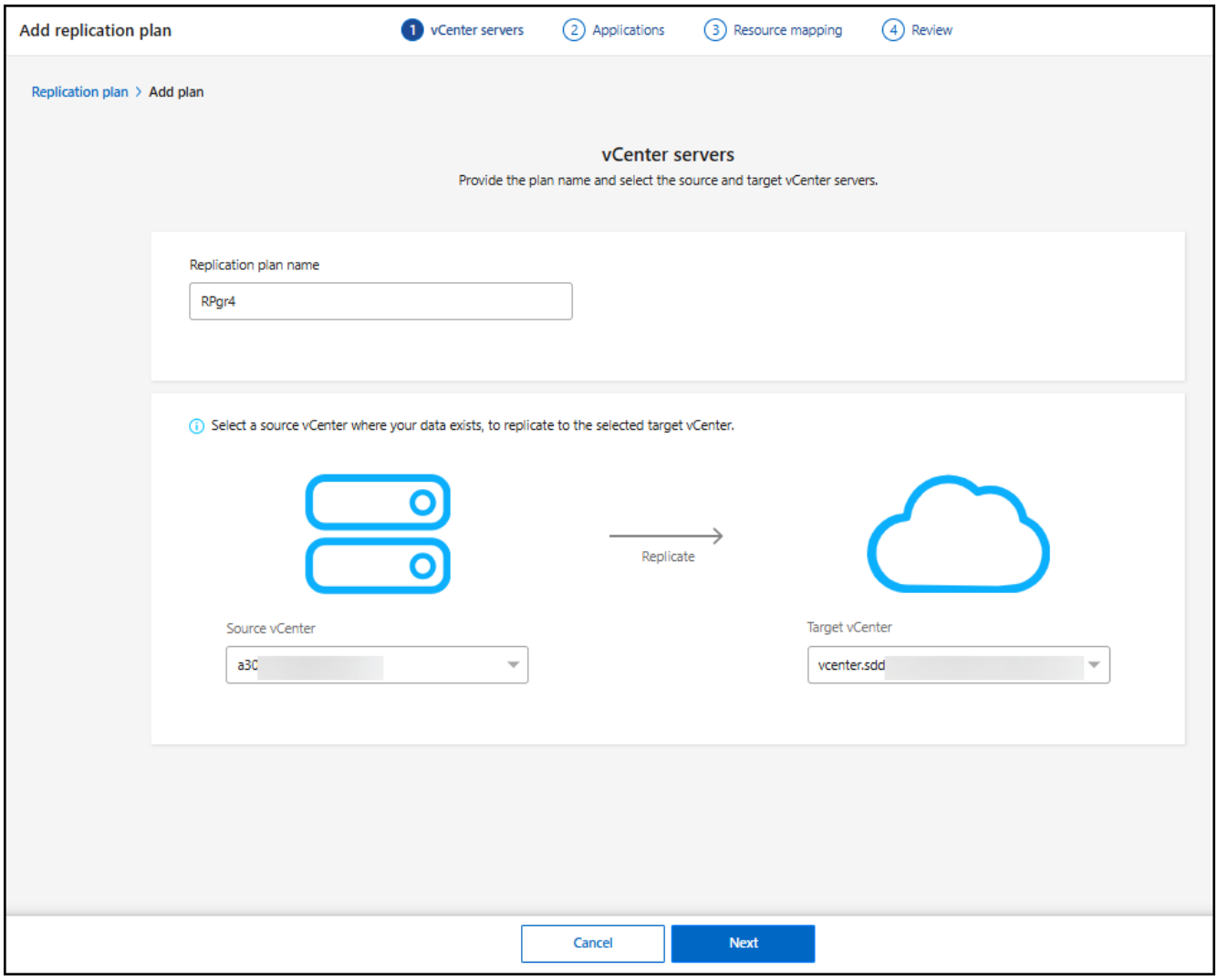
- Verwenden Sie für alle VMs im Plan dieselben Anmeldeinformationen.
- Verwenden Sie für alle VMs im Plan dasselbe Skript.
- Verwenden Sie für alle VMs im Plan dasselbe Subnetz, DNS und Gateway.

vCenter-Server auswählen

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

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** und dann **Hinzufügen**. Oder wählen Sie im Dashboard „Replikationsplan hinzufügen“ aus, wenn Sie den Dienst gerade erst nutzen.



4. Erstellen Sie einen Namen für den Replikationsplan.
5. Wählen Sie die Quell- und Ziel-vCenter aus den Listen „Quell-“ und „Ziel-vCenter“ aus.
6. Wählen Sie **Weiter**.

Auswählen von Anwendungen zum Replizieren und Zuweisen von Ressourcengruppen

Der nächste Schritt besteht darin, die erforderlichen VMs oder Datenspeicher in funktionale Ressourcengruppen zu gruppieren. Mithilfe von Ressourcengruppen können Sie eine Reihe von VMs oder Datenspeichern mit einem gemeinsamen Snapshot schützen.

Wenn Sie im Replikationsplan Anwendungen auswählen, können Sie das Betriebssystem für jede VM oder jeden Datenspeicher im Plan sehen. Dies ist hilfreich bei der Entscheidung, wie VMs oder Datenspeicher in einer Ressourcengruppe zusammengefasst werden sollen.

Jede Ressourcengruppe kann eine oder mehrere VMs oder Datenspeicher enthalten.

Berücksichtigen Sie beim Erstellen von Ressourcengruppen die folgenden Punkte:

- Bevor Sie Datenspeicher zu Ressourcengruppen hinzufügen, starten Sie zunächst eine manuelle oder geplante Erkennung der VMs. Dadurch wird sichergestellt, dass die VMs erkannt und in der Ressourcengruppe aufgelistet werden. Wenn Sie keine manuelle Erkennung auslösen, werden die VMs

möglicherweise nicht in der Ressourcengruppe aufgeführt.

- Stellen Sie sicher, dass sich mindestens eine VM im Datenspeicher befindet. Wenn sich im Datenspeicher keine VMs befinden, wird der Datenspeicher nicht erkannt.
- Ein einzelner Datenspeicher sollte keine VMs hosten, die durch mehr als einen Replikationsplan geschützt sind.
- Hosten Sie geschützte und ungeschützte VMs nicht auf demselben Datenspeicher. Wenn geschützte und ungeschützte VMs auf demselben Datenspeicher gehostet werden, können die folgenden Probleme auftreten:
  - Da NetApp Disaster Recovery SnapMirror verwendet und das System ganze ONTAP Volumes repliziert, wird die genutzte Kapazität dieses Volumes für Lizenzierungsüberlegungen verwendet. In diesem Fall würde der von geschützten und ungeschützten VMs belegte Volume-Speicherplatz in diese Berechnung einbezogen.
  - Wenn ein Failover der Ressourcengruppe und der zugehörigen Datenspeicher auf den Disaster Recovery-Standort durchgeführt werden muss, sind alle ungeschützten VMs (VMs, die nicht Teil der Ressourcengruppe sind, aber auf dem ONTAP Volume gehostet werden) durch den Failover-Prozess nicht mehr auf dem Quellstandort vorhanden, was zu einem Ausfall ungeschützter VMs am Quellstandort führt. Außerdem startet NetApp Disaster Recovery diese ungeschützten VMs nicht am Failover-vCenter-Standort.
- Um eine VM zu schützen, muss sie in eine Ressourcengruppe aufgenommen werden.

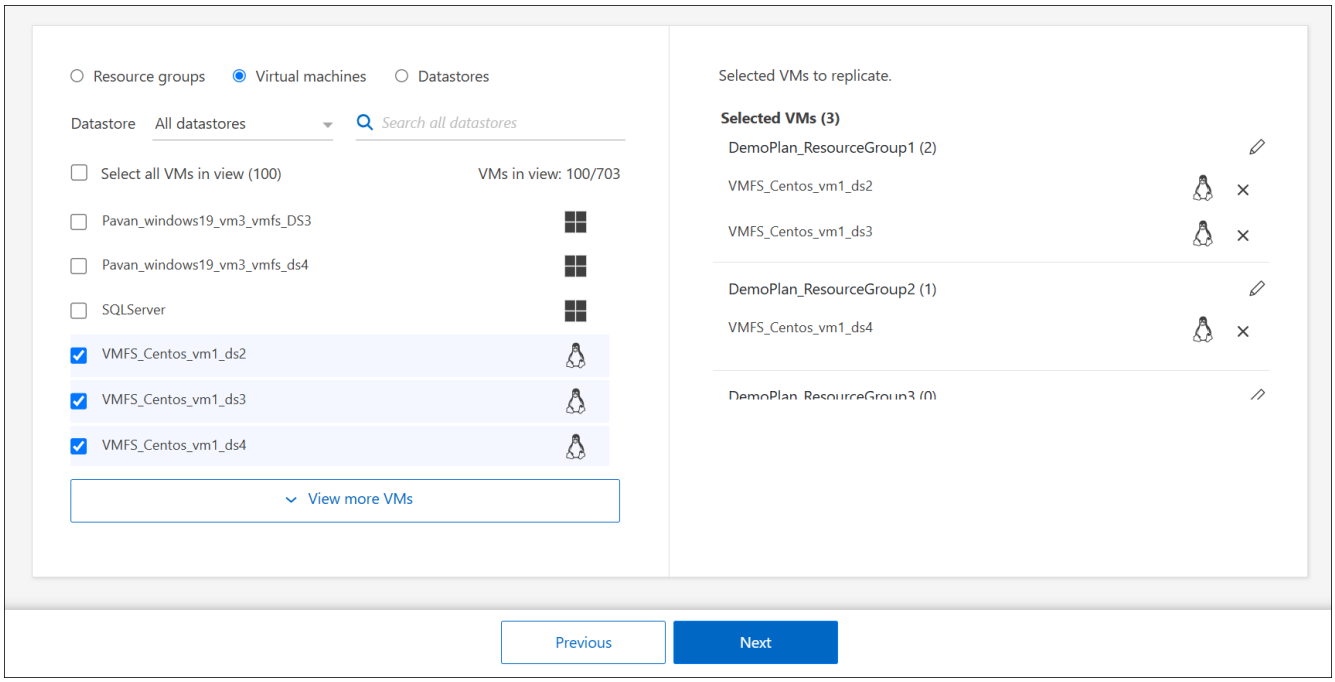
Erstellen Sie für Ihre Failover-Tests einen separaten, dedizierten Satz von Zuordnungen, um zu verhindern, dass VMS mit Produktionsnetzwerken über dieselben IP-Adressen verbunden wird.

Schritte

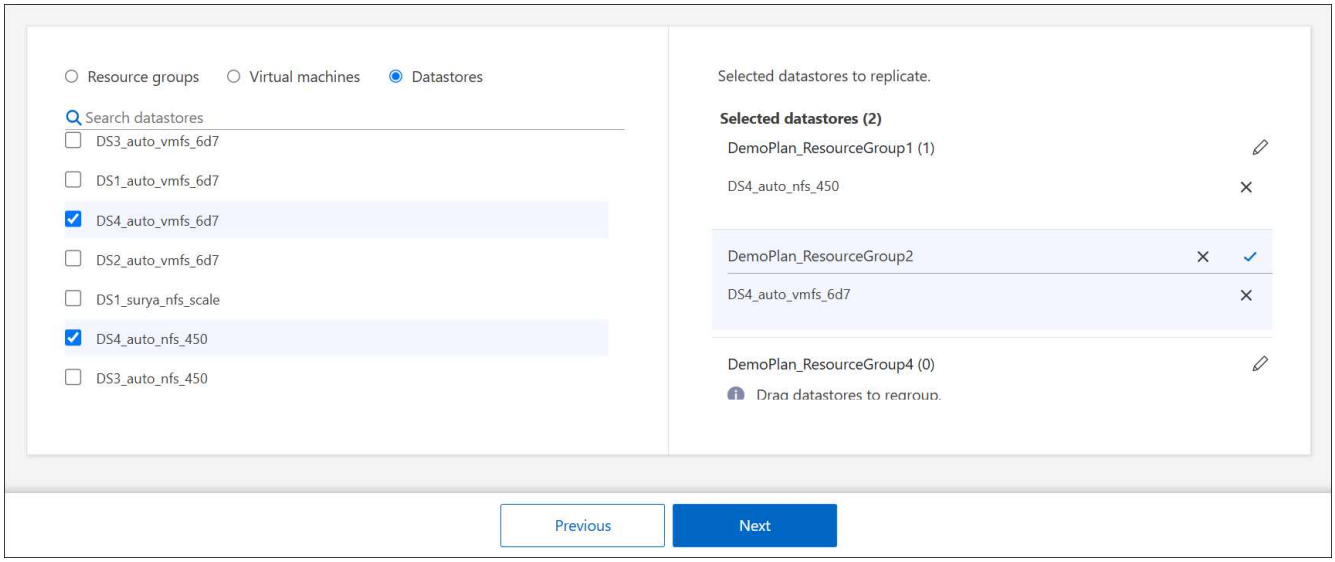
1. Wähle Sie **Virtuelle Maschinen** oder **Datenspeicher**.
2. Suchen Sie optional nach bestimmten VMs oder Datenspeichern anhand des Namens.
3. Wählen Sie auf der linken Seite der Anwendungsseite die VMs oder Datenspeicher aus, die Sie schützen möchten, und weisen Sie sie der ausgewählten Gruppe zu.

   Der Quell-vCenter-Server muss sich auf dem lokalen vCenter-Server befinden. Das Ziel-vCenter kann ein zweites lokales vCenter am selben Standort oder an einem entfernten Standort sein, oder ein cloudbasiertes softwaredefiniertes Rechenzentrum (SDDC) wie VMware Cloud on AWS. Beide vCenter-Server sollten bereits in Ihrer Disaster-Recovery-Arbeitsumgebung hinzugefügt sein.

   Die ausgewählte Ressource wird automatisch zur Gruppe 1 hinzugefügt und eine neue Gruppe 2 wird gestartet. Jedes Mal, wenn Sie der letzten Gruppe eine Ressource hinzufügen, wird eine weitere Gruppe hinzugefügt.



Oder für Datenspeicher:



4. Führen Sie optional einen der folgenden Schritte aus:
   - Um den Namen der Gruppe zu ändern, klicken Sie auf die Gruppe *Bearbeiten* Symbol.
   - Um eine Ressource aus einer Gruppe zu entfernen, wählen Sie **X** neben der Ressource aus.
   - Um eine Ressource in eine andere Gruppe zu verschieben, ziehen Sie sie per Drag & Drop in die neue Gruppe.

   Um einen Datenspeicher in eine andere Ressourcengruppe zu verschieben, heben Sie die Auswahl des nicht gewünschten Datenspeichers auf und übermitteln Sie den Replikationsplan. Erstellen oder bearbeiten Sie dann den anderen Replikationsplan und wählen Sie den Datenspeicher erneut aus.

5. Wählen Sie **Weiter**.

Ordnen Sie Quellressourcen dem Ziel zu

Geben Sie im Schritt „Ressourcenzuordnung“ an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden sollen. Wenn Sie einen Replikationsplan erstellen, können Sie für jede VM im Plan eine Startverzögerung und -reihenfolge festlegen. Dadurch können Sie eine Reihenfolge für den Start der VMs festlegen.

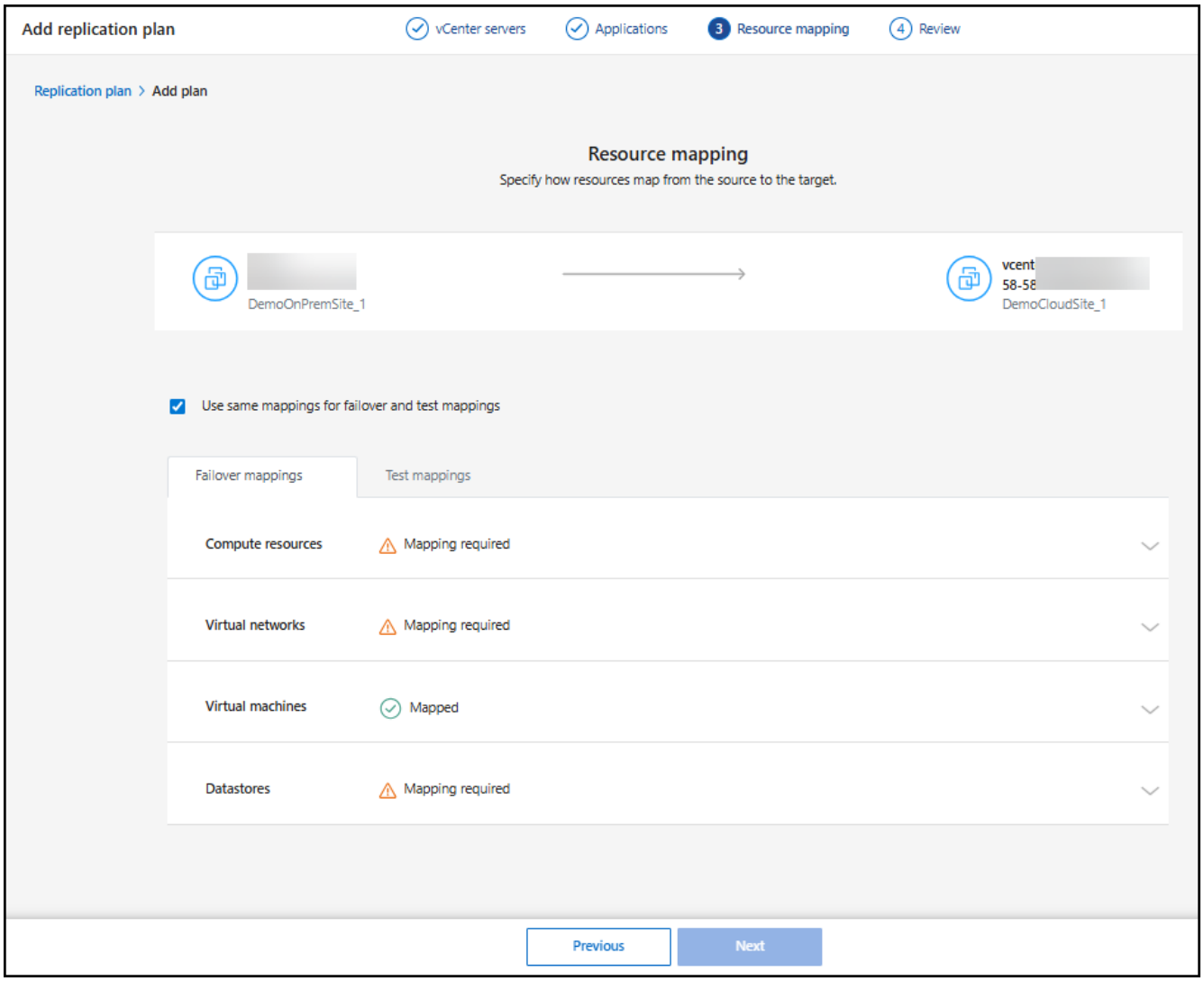
Wenn Sie im Rahmen Ihres DR-Plans Test-Failover durchführen möchten, sollten Sie eine Reihe von Test-Failover-Zuordnungen bereitstellen, um sicherzustellen, dass während des Failover-Tests gestartete VMs keine Produktions-VMs stören. Sie können dies erreichen, indem Sie entweder Test-VMs mit unterschiedlichen IP-Adressen bereitstellen oder indem Sie die virtuellen Netzwerkkarten der Test-VMs einem anderen Netzwerk zuordnen, das von der Produktion isoliert ist, aber dieselbe IP-Konfiguration aufweist (als *Bubble* oder *Testnetzwerk* bezeichnet).

Bevor Sie beginnen

Wenn Sie in diesem Dienst eine SnapMirror -Beziehung erstellen möchten, sollten der Cluster und sein SVM-Peering bereits außerhalb von NetApp Disaster Recovery eingerichtet worden sein.

Schritte

1. Aktivieren Sie auf der Seite „Ressourcenzuordnung“ das Kontrollkästchen, um für Failover- und Testvorgänge dieselben Zuordnungen zu verwenden.



2. Wählen Sie auf der Registerkarte „Failover-Zuordnungen“ den Abwärtspfeil rechts neben jeder Ressource aus und ordnen Sie die Ressourcen in jedem Abschnitt zu:
    - Rechenressourcen
    - Virtuelle Netzwerke
    - Virtuelle Maschinen
    - Datenspeicher

Kartenressourcen > Abschnitt „Compute-Ressourcen“

Der Abschnitt „Compute-Ressourcen“ definiert, wo VMs nach einem Failover wiederhergestellt werden. Ordnen Sie das Quell-vCenter-Rechenzentrum und den Cluster einem Ziel-Rechenzentrum und -Cluster zu.

Optional können VMs auf einem bestimmten vCenter ESXi-Host neu gestartet werden. Wenn VMWare DRS aktiviert ist, können Sie die VM bei Bedarf automatisch auf einen anderen Host verschieben, um die konfigurierte DR-Richtlinie einzuhalten.

Optional können Sie alle VMs in diesem Replikationsplan in einem eindeutigen Ordner mit dem vCenter platzieren. Dies bietet eine einfache Möglichkeit, ausgefallene VMs schnell innerhalb des vCenter zu organisieren.

Wählen Sie den Abwärtspfeil neben **Compute-Ressourcen** aus.

- **Quell- und Ziel-Rechenzentren**
- **Zielcluster**
- **Zielhost** (optional): Nachdem Sie den Cluster ausgewählt haben, können Sie diese Informationen festlegen.

Wenn ein vCenter über einen Distributed Resource Scheduler (DRS) verfügt, der für die Verwaltung mehrerer Hosts in einem Cluster konfiguriert ist, müssen Sie keinen Host auswählen. Wenn Sie einen Host auswählen, platziert NetApp Disaster Recovery alle VMs auf dem ausgewählten Host. * **Ziel-VM-Ordner** (optional): Erstellen Sie einen neuen Stammordner zum Speichern der ausgewählten VMs.

Kartenressourcen > Abschnitt „Virtuelle Netzwerke“

VMs verwenden virtuelle Netzwerkkarten, die mit virtuellen Netzwerken verbunden sind. Beim Failover-Prozess verbindet der Dienst diese virtuellen Netzwerkkarten mit virtuellen Netzwerken, die in der VMware-Zielumgebung definiert sind. Für jedes von den VMs in der Ressourcengruppe verwendete virtuelle Quellnetzwerk erfordert der Dienst die Zuweisung eines virtuellen Zielnetzwerks.

Sie können demselben virtuellen Zielnetzwerk mehrere virtuelle Quellnetzwerke zuweisen. Dies kann jedoch zu Konflikten bei der IP-Netzwerkkonfiguration führen. Sie können mehrere Quellnetzwerke einem einzigen Zielnetzwerk zuordnen, um sicherzustellen, dass alle Quellnetzwerke dieselbe Konfiguration haben.

Wählen Sie auf der Registerkarte „Failover-Zuordnungen“ den Abwärtspfeil neben „Virtuelle Netzwerke“ aus. Wählen Sie das virtuelle Quell-LAN und das virtuelle Ziel-LAN aus.

Wählen Sie die Netzwerkzuordnung zum entsprechenden virtuellen LAN aus. Die virtuellen LANs sollten bereits bereitgestellt sein. Wählen Sie daher das entsprechende virtuelle LAN aus, um die VM zuzuordnen.

Kartenressourcen > Abschnitt Virtuelle Maschinen

Sie können jede VM in der durch den Replikationsplan geschützten Ressourcengruppe so konfigurieren, dass sie zur virtuellen vCenter-Zielumgebung passt, indem Sie eine der folgenden Optionen festlegen:

- Die Anzahl der virtuellen CPUs
- Die Menge an virtuellem DRAM
- Die IP-Adresskonfiguration
- Die Möglichkeit, Shell-Skripte des Gastbetriebssystems als Teil des Failover-Prozesses auszuführen
- Die Möglichkeit, Failover-VM-Namen durch die Verwendung eines eindeutigen Präfixes und Suffixes zu ändern
- Die Möglichkeit, die Neustartreihenfolge während des VM-Failovers festzulegen

Wählen Sie auf der Registerkarte „Failover-Zuordnungen“ den Abwärtspfeil neben „Virtuelle Maschinen“ aus.

Der Standardwert für die VMs ist „Mapped“. Die Standardzuordnung verwendet dieselben Einstellungen, die die VMs in der Produktionsumgebung verwenden (dieselbe IP-Adresse, Subnetzmaske und dasselbe Gateway).

Wenn Sie Änderungen an den Standardeinstellungen vornehmen, müssen Sie das Feld „Ziel-IP“ in „Unterscheidet sich von der Quelle“ ändern.

Wenn Sie die Einstellungen auf „Abweichend von der Quelle“ ändern, müssen Sie die Anmeldeinformationen des VM-Gastbetriebssystems angeben.

In diesem Abschnitt werden je nach Ihrer Auswahl möglicherweise unterschiedliche Felder angezeigt.

Sie können die Anzahl der virtuellen CPUs, die jeder VM zugewiesen sind, die ausgefallen ist, erhöhen oder verringern. Allerdings benötigt jede VM mindestens eine virtuelle CPU. Sie können die Anzahl der virtuellen CPUs und des virtuellen DRAM ändern, die jeder VM zugewiesen sind. Der häufigste Grund, warum Sie die Standardeinstellungen für virtuelle CPU und virtuellen DRAM ändern möchten, liegt darin, dass die Zielknoten des vCenter-Clusters nicht über so viele verfügbare Ressourcen verfügen wie der Quell-vCenter-Cluster.

Netzwerkeinstellungen Disaster Recovery unterstützt eine umfangreiche Reihe von Konfigurationsoptionen für VM-Netzwerke. Eine Änderung dieser Einstellungen kann erforderlich sein, wenn die Zielsite über virtuelle Netzwerke verfügt, die andere TCP/IP-Einstellungen verwenden als die virtuellen Produktionsnetzwerke auf der Quellsite.

Auf der grundlegendsten (und standardmäßigen) Ebene verwenden die Einstellungen einfach dieselben TCP/IP-Netzwerkeinstellungen für jede VM auf der Zielsite, die auch auf der Quellsite verwendet werden. Dies erfordert, dass Sie in den virtuellen Quell- und Zielnetzwerken dieselben TCP/IP-Einstellungen konfigurieren.

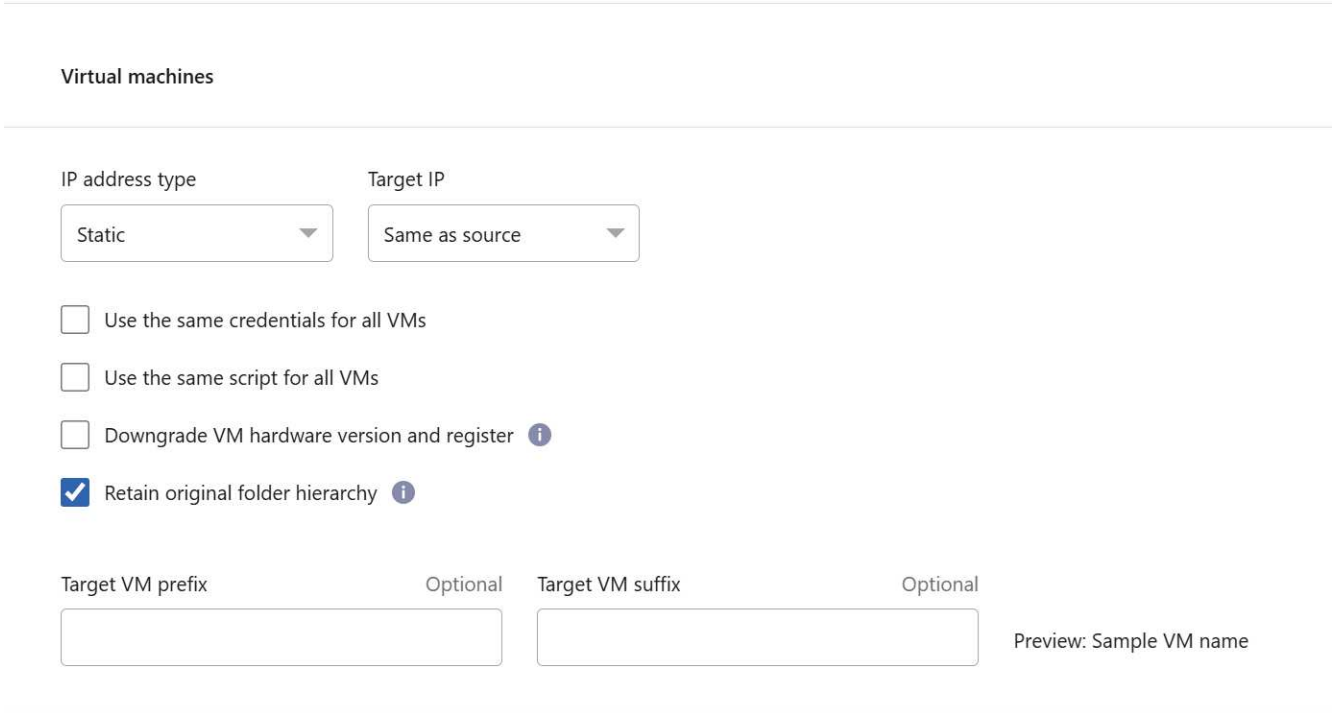
Der Dienst unterstützt Netzwerkeinstellungen der statischen oder Dynamic Host Configuration Protocol (DHCP)-IP-Konfiguration für VMs. DHCP bietet eine standardbasierte Methode zur dynamischen Konfiguration der TCP/IP-Einstellungen eines Host-Netzwerkports. DHCP muss mindestens eine TCP/IP-Adresse bereitstellen und kann auch eine Standard-Gateway-Adresse (zum Routing zu einer externen Internetverbindung), eine Subnetzmaske und eine DNS-Serveradresse bereitstellen. DHCP wird häufig für Computergeräte von Endbenutzern verwendet, beispielsweise für Desktop-, Laptop- und Mobiltelefonverbindungen von Mitarbeitern. Es kann jedoch auch für alle anderen Computergeräte im Netzwerk, beispielsweise Server, verwendet werden.

- Option **Gleiche Subnetzmaske, DNS und Gateway-Einstellungen verwenden**: Da diese Einstellungen

normalerweise für alle VMs, die mit denselben virtuellen Netzwerken verbunden sind, gleich sind, ist es möglicherweise einfacher, diese einmal zu konfigurieren und Disaster Recovery die Einstellungen für alle VMs in der durch den Replikationsplan geschützten Ressourcengruppe verwenden zu lassen. Wenn einige VMs unterschiedliche Einstellungen verwenden, müssen Sie dieses Kontrollkästchen deaktivieren und diese Einstellungen für jede VM angeben.

- **IP-Adresstyp**: Konfigurieren Sie die VM-Konfiguration neu, damit sie den Anforderungen des virtuellen Zielnetzwerks entspricht. NetApp Disaster Recovery bietet zwei Optionen: DHCP oder statische IP. Konfigurieren Sie für statische IPs die Subnetzmaske, das Gateway und die DNS-Server. Geben Sie außerdem Anmeldeinformationen für VMs ein.
  - **DHCP**: Wählen Sie diese Einstellung, wenn Ihre VMs Netzwerkkonfigurationsinformationen von einem DHCP-Server beziehen sollen. Wenn Sie diese Option wählen, geben Sie nur die Anmeldeinformationen für die VM an.
  - **Statische IP**: Wählen Sie diese Einstellung, wenn Sie die IP-Konfigurationsinformationen manuell angeben möchten. Sie können eine der folgenden Optionen auswählen: „Gleich wie Quelle“, „Unterscheidet sich von Quelle“ oder „Subnetzzuordnung“. Wenn Sie dasselbe wie die Quelle wählen, müssen Sie keine Anmeldeinformationen eingeben. Wenn Sie andererseits andere Informationen als die Quelle verwenden möchten, können Sie die Anmeldeinformationen, die IP-Adresse der VM, die Subnetzmaske, DNS und Gateway-Informationen angeben. Die Anmeldeinformationen des VM-Gastbetriebssystems sollten entweder auf globaler Ebene oder auf jeder VM-Ebene bereitgestellt werden.

    Dies kann sehr hilfreich sein, wenn große Umgebungen auf kleineren Zielclustern wiederhergestellt werden oder wenn Disaster-Recovery-Tests durchgeführt werden, ohne dass eine physische Eins-zu-eins-VMware-Infrastruktur bereitgestellt werden muss.



- **Skripte**: Sie können benutzerdefinierte, im Gastbetriebssystem gehostete Skripte im .sh-, .bat- oder .ps1-Format als Nachbearbeitung einbinden. Mithilfe von benutzerdefinierten Skripten kann Disaster Recovery Ihr Skript nach einem Failover, Failback und der Migration von Prozessen ausführen. Beispielsweise können Sie ein benutzerdefiniertes Skript verwenden, um alle Datenbanktransaktionen nach Abschluss des Failovers fortzusetzen. Der Dienst kann Skripte in virtuellen Maschinen ausführen, auf denen Microsoft Windows oder eine beliebige unterstützte Linux-Variante mit Unterstützung für Befehlszeilenparameter

läuft. Sie können ein Skript einzelnen VMs oder allen VMs im Replikationsplan zuweisen.

Um die Skriptausführung mit dem VM-Gastbetriebssystem zu ermöglichen, müssen die folgenden Bedingungen erfüllt sein:

- VMware Tools müssen auf der VM installiert sein.
- Zum Ausführen des Skripts müssen entsprechende Benutzeranmeldeinformationen mit ausreichenden Gastbetriebssystemberechtigungen bereitgestellt werden.
- Geben Sie optional einen Timeout-Wert in Sekunden für das Skript an.

  VMs mit Microsoft Windows: können entweder Windows-Batch-Skripts (.bat) oder PowerShell-Skripts (ps1) ausführen. Windows-Skripte können Befehlszeilenargumente verwenden. Formatieren Sie jedes Argument im `arg_name$value` Format, wobei `arg_name` ist der Name des Arguments und `$value` ist der Wert des Arguments und ein Semikolon trennt jedes `argument$value` Paar.

VMs mit Linux: können jedes Shell-Skript (.sh) ausführen, das von der von der VM verwendeten Linux-Version unterstützt wird. Linux-Skripte können Befehlszeilenargumente verwenden. Geben Sie Argumente in einer durch Semikolons getrennten Werteliste an. Benannte Argumente werden nicht unterstützt. Fügen Sie jedes Argument zum `Arg[x]` Argumentliste und verweisen Sie auf jeden Wert mit einem Zeiger in die `Arg[x]` Array, zum Beispiel `value1;value2;value3` .

- **VM-Hardwareversion herabstufen und registrieren**: Wählen Sie diese Option, wenn die Version des Ziel-ESX-Hosts älter ist als die des Quell-ESX-Hosts, damit diese bei der Registrierung übereinstimmen.
- **Ursprüngliche Ordnerhierarchie beibehalten**: Standardmäßig behält Disaster Recovery die VM-Inventarhierarchie (Ordnerstruktur) beim Failover bei. Falls das Wiederherstellungsziel die ursprüngliche Ordnerhierarchie nicht aufweist, erstellt Disaster Recovery diese.

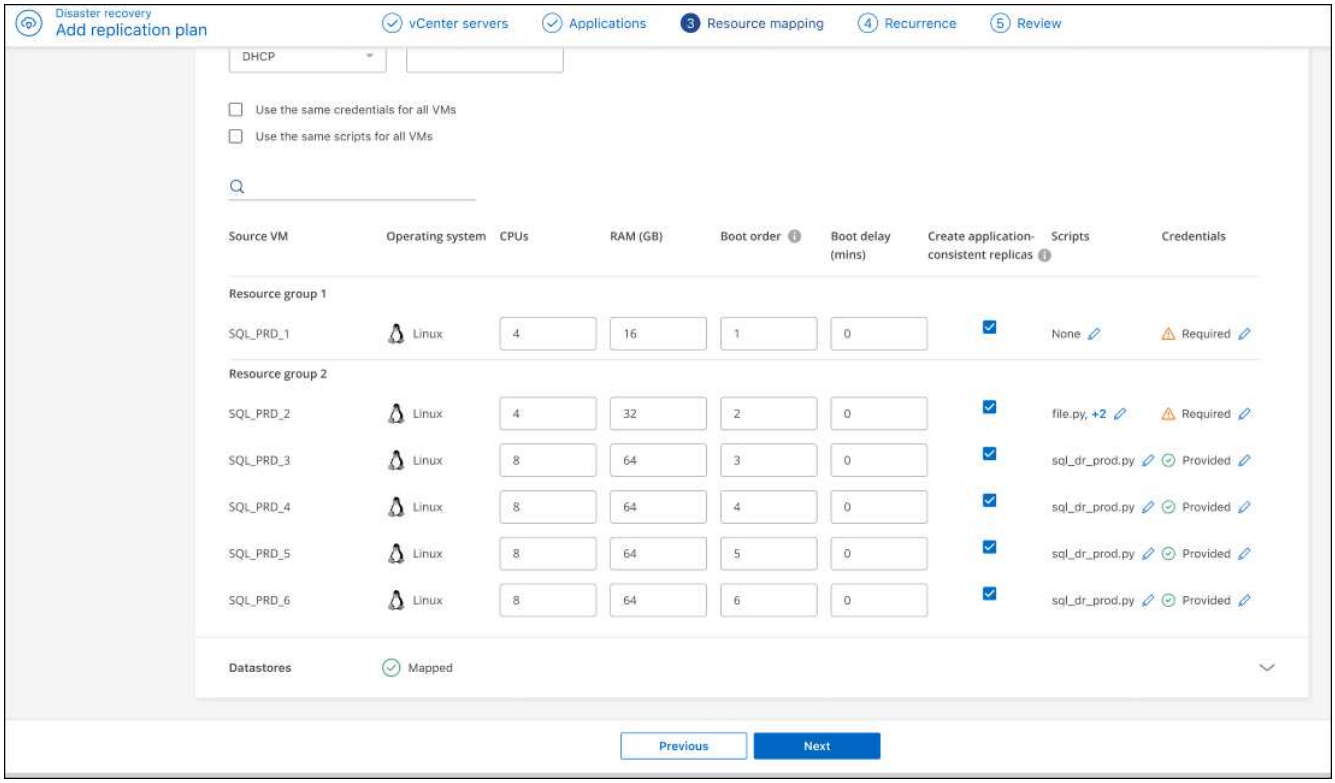
  Deaktivieren Sie dieses Kontrollkästchen, um die ursprüngliche Ordnerhierarchie zu ignorieren.

- **Präfix und Suffix der Ziel-VM**: Unter den Details der virtuellen Maschinen können Sie optional jedem VM-Namen, für den ein Failover durchgeführt wurde, ein Präfix und ein Suffix hinzufügen. Dies kann hilfreich sein, um die VMs, für die ein Failover durchgeführt wurde, von den Produktions-VMs zu unterscheiden, die auf demselben vCenter-Cluster ausgeführt werden. Sie können dem VM-Namen beispielsweise das Präfix „DR-“ und das Suffix „-failover“ hinzufügen. Manche Leute fügen ein zweites Produktions-vCenter hinzu, um VMs im Katastrophenfall vorübergehend an einem anderen Standort zu hosten. Durch das Hinzufügen eines Präfixes oder Suffixes können Sie VMs, bei denen ein Failover stattgefunden hat, schnell identifizieren. Sie können das Präfix oder Suffix auch in benutzerdefinierten Skripten verwenden.

  Sie können die alternative Methode zum Festlegen des Ziel-VM-Ordners im Abschnitt „Compute-Ressourcen“ verwenden.

- **CPU und RAM der Quell-VM**: Unter den Details der virtuellen Maschinen können Sie optional die Größe der VM-CPU- und RAM-Parameter ändern.

  Sie können DRAM entweder in Gigabyte (GiB) oder Megabyte (MiB) konfigurieren. Obwohl jede VM mindestens ein MiB RAM benötigt, muss die tatsächliche Menge sicherstellen, dass das VM-Gastbetriebssystem und alle laufenden Anwendungen effizient arbeiten können.



- **Startreihenfolge**: Sie können die Startreihenfolge nach einem Failover für alle ausgewählten virtuellen Maschinen in den Ressourcengruppen ändern. Standardmäßig werden alle VMs parallel gestartet. Sie können in dieser Phase jedoch Änderungen vornehmen. Dies ist hilfreich, um sicherzustellen, dass alle Ihre VMs mit der Priorität 1 ausgeführt werden, bevor die VMs mit der nachfolgenden Priorität gestartet werden.

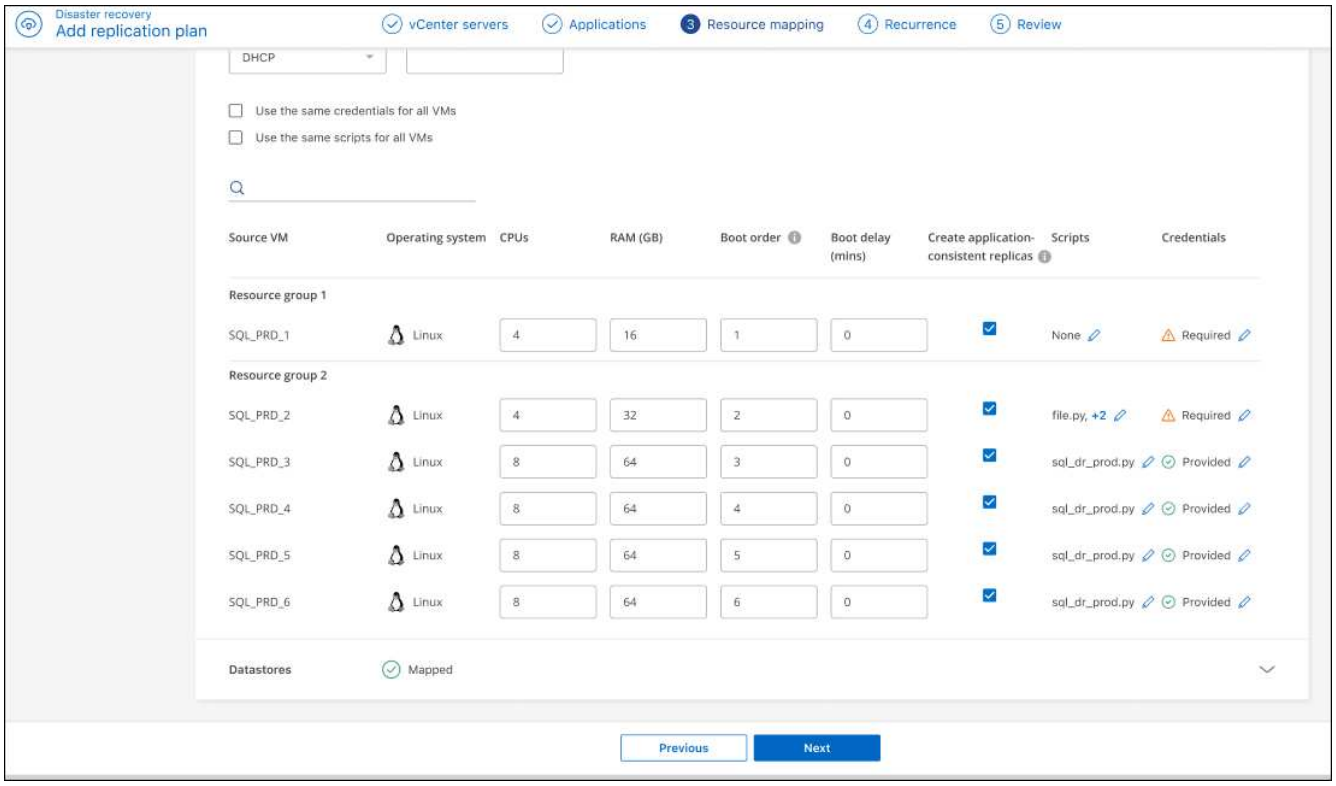
  Die Notfallwiederherstellung startet alle VMs mit der gleichen Startreihenfolgenummer parallel.

  - Sequentielles Booten: Weisen Sie jeder VM eine eindeutige Nummer zu, um sie in der zugewiesenen Reihenfolge zu booten, z. B. 1, 2, 3, 4, 5.
  - Gleichzeitiger Start: Weisen Sie allen VMs dieselbe Nummer zu, um sie gleichzeitig zu starten, z. B. 1,1,1,1,2,2,3,4,4.
- **Startverzögerung**: Passen Sie die Verzögerung des Startvorgangs in Minuten an und geben Sie die Zeit an, die die VM wartet, bevor sie mit dem Einschaltvorgang beginnt. Geben Sie einen Wert zwischen 0 und 10 Minuten ein.

> Um die Startreihenfolge auf die Standardeinstellung zurückzusetzen, wählen Sie **VM-Einstellungen auf Standard zurücksetzen** und wählen Sie dann aus, welche Einstellungen Sie wieder auf die Standardeinstellung zurücksetzen möchten.

- **Anwendungskonsistente Replikate erstellen**: Geben Sie an, ob anwendungskonsistente Snapshot-Kopien erstellt werden sollen. Der Dienst legt die Anwendung still und erstellt dann einen Snapshot, um einen konsistenten Zustand der Anwendung zu erhalten. Diese Funktion wird von Oracle unter Windows und Linux sowie von SQL Server unter Windows unterstützt. Weitere Einzelheiten finden Sie weiter unten.
- **Windows LAPS verwenden**: Wenn Sie die Windows Local Administrator Password Solution (Windows LAPS) verwenden, aktivieren Sie dieses Kontrollkästchen. Diese Option ist nur verfügbar, wenn Sie die Option **Statische IP** ausgewählt haben. Wenn Sie dieses Kontrollkästchen aktivieren, müssen Sie nicht für jede Ihrer virtuellen Maschinen ein Kennwort angeben. Stattdessen geben Sie die Domänencontrollerdetails an.

Wenn Sie Windows LAPS nicht verwenden, handelt es sich bei der VM um eine Windows-VM und die Anmeldeinformationsoption in der VM-Zeile ist aktiviert. Sie können die Anmeldeinformationen für die VM angeben.



Erstellen anwendungskonsistenter Replikate

Viele VMs hosten Datenbankserver wie Oracle oder Microsoft SQL Server. Diese Datenbankserver erfordern anwendungskonsistente Snapshots, um sicherzustellen, dass sich die Datenbank zum Zeitpunkt der Snapshot-Erstellung in einem konsistenten Zustand befindet.

Anwendungskonsistente Snapshots stellen sicher, dass sich die Datenbank zum Zeitpunkt der Snapshot-Erstellung in einem konsistenten Zustand befindet. Dies ist wichtig, da dadurch sichergestellt wird, dass die Datenbank nach einem Failover- oder Failback-Vorgang in einen konsistenten Zustand zurückversetzt werden kann.

Die vom Datenbankserver verwalteten Daten können auf demselben Datenspeicher wie die VM gehostet werden, auf der der Datenbankserver gehostet wird, oder sie können auf einem anderen Datenspeicher gehostet werden. Die folgende Tabelle zeigt die unterstützten Konfigurationen für anwendungskonsistente Snapshots in der Notfallwiederherstellung:

Datenstandort	Unterstützt	Hinweise
Innerhalb desselben vCenter-Datenspeichers wie die VM	Ja	Da sich der Datenbankserver und die Datenbank beide im selben Datenspeicher befinden, sind sowohl der Server als auch die Daten beim Failover synchron.

Datenstandort	Unterstützt	Hinweise
Innerhalb eines anderen vCenter-Datenspeichers als die VM	Nein	Disaster Recovery kann nicht erkennen, wenn sich die Daten eines Datenbankservers auf einem anderen vCenter-Datenspeicher befinden. Der Dienst kann die Daten nicht replizieren, aber die Datenbankserver-VM. Obwohl die Datenbankdaten nicht repliziert werden können, stellt der Dienst sicher, dass der Datenbankserver alle erforderlichen Schritte durchführt, um sicherzustellen, dass die Datenbank zum Zeitpunkt der VM-Sicherung in den Ruhezustand versetzt wird.
Innerhalb einer externen Datenquelle	Nein	Wenn sich die Daten auf einer vom Gast bereitgestellten LUN- oder NFS-Freigabe befinden, kann Disaster Recovery die Daten nicht replizieren, aber die Datenbankserver-VM kann replizieren. Obwohl die Datenbankdaten nicht repliziert werden können, stellt der Dienst sicher, dass der Datenbankserver alle erforderlichen Schritte durchführt, um sicherzustellen, dass die Datenbank zum Zeitpunkt der VM-Sicherung in den Ruhezustand versetzt wird.

Während einer geplanten Sicherung legt Disaster Recovery den Datenbankserver still und erstellt dann einen Snapshot der VM, auf der der Datenbankserver gehostet wird. Dadurch wird sichergestellt, dass sich die Datenbank zum Zeitpunkt der Erstellung des Snapshots in einem konsistenten Zustand befindet.

- Für Windows-VMs verwendet der Dienst den Microsoft Volume Shadow Copy Service (VSS) zur Koordination mit den beiden Datenbankservern.
- Für Linux-VMs verwendet der Dienst eine Reihe von Skripts, um den Oracle-Server in den Sicherungsmodus zu versetzen.

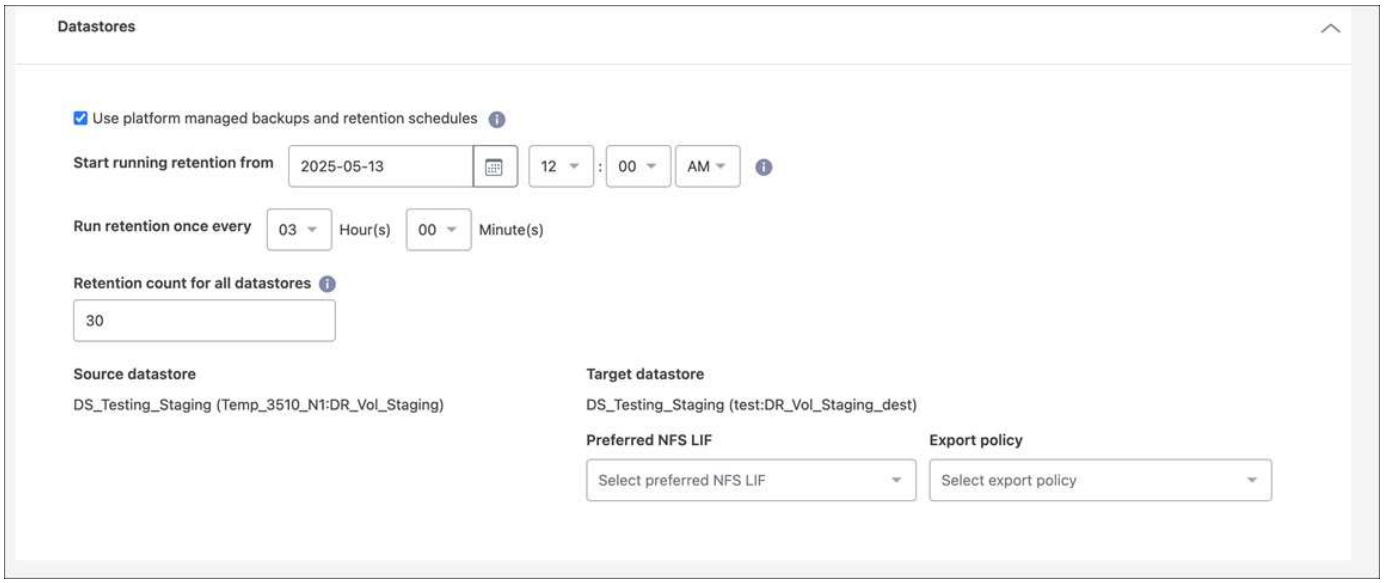
Um anwendungskonsistente Replikate der VMs und ihrer Hosting-Datenspeicher zu aktivieren, aktivieren Sie das Kontrollkästchen neben **Anwendungskonsistente Replikate erstellen** für jede VM und geben Sie Gastanmeldeinformationen mit den entsprechenden Berechtigungen an.

Kartenressourcen > Abschnitt „Datenspeicher“

VMware-Datenspeicher werden auf ONTAP FlexVol -Volumes oder ONTAP iSCSI- oder FC-LUNs unter Verwendung von VMware VMFS gehostet. Verwenden Sie den Abschnitt „Datenspeicher“, um den Ziel ONTAP Cluster, die Storage Virtual Machine (SVM) und das Volume oder LUN zu definieren, um die Daten auf der Festplatte zum Ziel zu replizieren.

Wählen Sie den Abwärtspfeil neben **Datenspeicher**. Basierend auf der Auswahl der VMs werden Datenspeicherzuordnungen automatisch ausgewählt.

Dieser Abschnitt kann je nach Ihrer Auswahl aktiviert oder deaktiviert sein.



- **Plattformverwaltete Backups und Aufbewahrungspläne verwenden**: Wenn Sie eine externe Snapshot-Verwaltungslösung verwenden, aktivieren Sie dieses Kontrollkästchen. NetApp Disaster Recovery unterstützt die Verwendung externer Snapshot-Management-Lösungen wie den nativen ONTAP SnapMirror Policy Scheduler oder Integrationen von Drittanbietern. Wenn jeder Datenspeicher (Volume) im Replikationsplan bereits über eine SnapMirror -Beziehung verfügt, die anderswo verwaltet wird, können Sie diese Snapshots als Wiederherstellungspunkte in NetApp Disaster Recovery verwenden.

  Wenn diese Option ausgewählt ist, konfiguriert NetApp Disaster Recovery keinen Sicherungszeitplan. Sie müssen jedoch weiterhin einen Aufbewahrungszeitplan konfigurieren, da möglicherweise weiterhin Snapshots für Test-, Failover- und Failback-Vorgänge erstellt werden.

  Nach der Konfiguration erstellt der Dienst keine regelmäßig geplanten Snapshots, sondern verlässt sich stattdessen darauf, dass die externe Entität diese Snapshots erstellt und aktualisiert.

- **Startzeit**: Geben Sie das Datum und die Uhrzeit ein, zu der die Sicherungen und die Aufbewahrung beginnen sollen.
- **Ausführungsintervall**: Geben Sie das Zeitintervall in Stunden und Minuten ein. Wenn Sie beispielsweise 1 Stunde eingeben, erstellt der Dienst jede Stunde einen Snapshot.
- **Aufbewahrungsanzahl**: Geben Sie die Anzahl der Snapshots ein, die Sie aufbewahren möchten.

  Die Anzahl der beibehaltenen Snapshots sowie die Datenänderungsrate zwischen den einzelnen Snapshots bestimmen die Menge des sowohl auf der Quelle als auch auf dem Ziel verbrauchten Speicherplatzes. Je mehr Snapshots Sie behalten, desto mehr Speicherplatz wird verbraucht.

- **Quell- und Zieldatenspeicher**: Wenn mehrere (Fan-Out-) SnapMirror Beziehungen vorhanden sind, können Sie das zu verwendende Ziel auswählen. Wenn für ein Volume bereits eine SnapMirror -Beziehung besteht, werden die entsprechenden Quell- und Zieldatenspeicher angezeigt. Wenn ein Volume keine SnapMirror -Beziehung hat, können Sie jetzt eines erstellen, indem Sie einen Zielcluster auswählen, eine Ziel-SVM auswählen und einen Volumenamen angeben. Der Dienst erstellt die Volume- und SnapMirror -Beziehung.

  Wenn Sie in diesem Dienst eine SnapMirror -Beziehung erstellen möchten, sollten der Cluster und sein SVM-Peering bereits außerhalb von NetApp Disaster Recovery eingerichtet worden sein.

- Wenn die VMs vom selben Volume und derselben SVM stammen, führt der Dienst einen Standard-ONTAP Snapshot durch und aktualisiert die sekundären Ziele.
- Wenn die VMs aus unterschiedlichen Volumes und derselben SVM stammen, erstellt der Dienst einen Snapshot der Konsistenzgruppe, indem er alle Volumes einschließt und die sekundären Ziele aktualisiert.
- Wenn die VMs aus unterschiedlichen Volumes und unterschiedlichen SVMs stammen, führt der Dienst einen Snapshot der Startphase und der Commit-Phase der Konsistenzgruppe durch, indem er alle Volumes im selben oder in einem anderen Cluster einschließt und die sekundären Ziele aktualisiert.
- Während des Failovers können Sie einen beliebigen Snapshot auswählen. Wenn Sie den neuesten Snapshot auswählen, erstellt der Dienst ein On-Demand-Backup, aktualisiert das Ziel und verwendet diesen Snapshot für das Failover.

- **Bevorzugtes NFS-LIF** und **Exportrichtlinie**: Lassen Sie den Dienst normalerweise das bevorzugte NFS-LIF und die Exportrichtlinie auswählen. Wenn Sie eine bestimmte NFS-LIF- oder Exportrichtlinie verwenden möchten, wählen Sie den Abwärtspfeil neben jedem Feld und wählen Sie die entsprechende Option aus.

  Sie können optional bestimmte Datenschnittstellen (LIFs) für ein Volume nach einem Failover-Ereignis verwenden. Dies ist für den Datenverkehrsausgleich nützlich, wenn die Ziel-SVM über mehrere LIFs verfügt.

  Zur zusätzlichen Kontrolle der NAS-Datenzugriffssicherheit kann der Dienst verschiedenen Datenspeichervolumes spezifische NAS-Exportrichtlinien zuweisen. Exportrichtlinien definieren die Zugriffskontrollregeln für NFS-Clients, die auf die Datenspeichervolumes zugreifen. Wenn Sie keine Exportrichtlinie angeben, verwendet der Dienst die Standardexportrichtlinie für die SVM.

> Es wird empfohlen, eine dedizierte Exportrichtlinie zu erstellen, die den Zugriff auf das Volume *ausschließlich* auf die Quell- und Ziel-vCenter-ESXi-Hosts beschränkt, auf denen die geschützten VMs gehostet werden. Dadurch wird sichergestellt, dass externe Entitäten keinen Zugriff auf den NFS-Export erhalten.

Test-Failover-Zuordnungen hinzufügen

Schritte

1. Um andere Zuordnungen für die Testumgebung festzulegen, deaktivieren Sie das Kontrollkästchen und wählen Sie die Registerkarte **Testzuordnungen**.
2. Gehen Sie die einzelnen Registerkarten wie zuvor durch, diesmal jedoch für die Testumgebung.

   Auf der Registerkarte „Testzuordnungen“ sind die Zuordnungen „Virtuelle Maschinen“ und „Datenspeicher“ deaktiviert.

> Sie können den gesamten Plan später testen. Im Moment richten Sie die Zuordnungen für die Testumgebung ein.

Überprüfen des Replikationsplans

Nehmen Sie sich abschließend einen Moment Zeit, um den Replikationsplan zu überprüfen.

> Sie können den Replikationsplan später deaktivieren oder löschen.

Schritte

1. Überprüfen Sie die Informationen auf jeder Registerkarte: Plandetails, Failover-Zuordnung und VMs.
2. Wählen Sie **Plan hinzufügen**.

   Der Plan wird der Liste der Pläne hinzugefügt.

Bearbeiten Sie Zeitpläne, um die Konformität zu testen und sicherzustellen, dass Failover-Tests funktionieren

Möglicherweise möchten Sie Zeitpläne zum Testen der Konformität und des Failovers einrichten, um sicherzustellen, dass diese bei Bedarf ordnungsgemäß funktionieren.

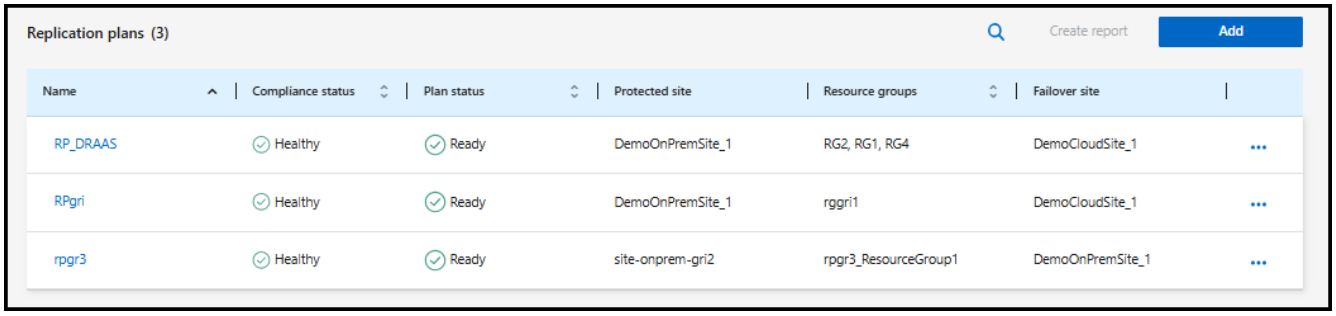
- **Auswirkungen auf die Compliance-Zeit**: Wenn ein Replikationsplan erstellt wird, erstellt der Dienst standardmäßig einen Compliance-Zeitplan. Die Standard-Compliance-Zeit beträgt 30 Minuten. Um diese Zeit zu ändern, können Sie den Zeitplan im Replikationsplan bearbeiten.
- **Auswirkungen des Failovers testen**: Sie können einen Failover-Prozess bei Bedarf oder nach Zeitplan testen. Auf diese Weise können Sie das Failover virtueller Maschinen zu einem in einem Replikationsplan angegebenen Ziel testen.

  Bei einem Test-Failover wird ein FlexClone -Volume erstellt, der Datenspeicher wird bereitgestellt und die Arbeitslast wird auf diesen Datenspeicher verschoben. Ein Test-Failover-Vorgang hat *keine* Auswirkungen auf Produktions-Workloads, die auf der Testsite verwendete SnapMirror -Beziehung und geschützte Workloads, die weiterhin normal ausgeführt werden müssen.

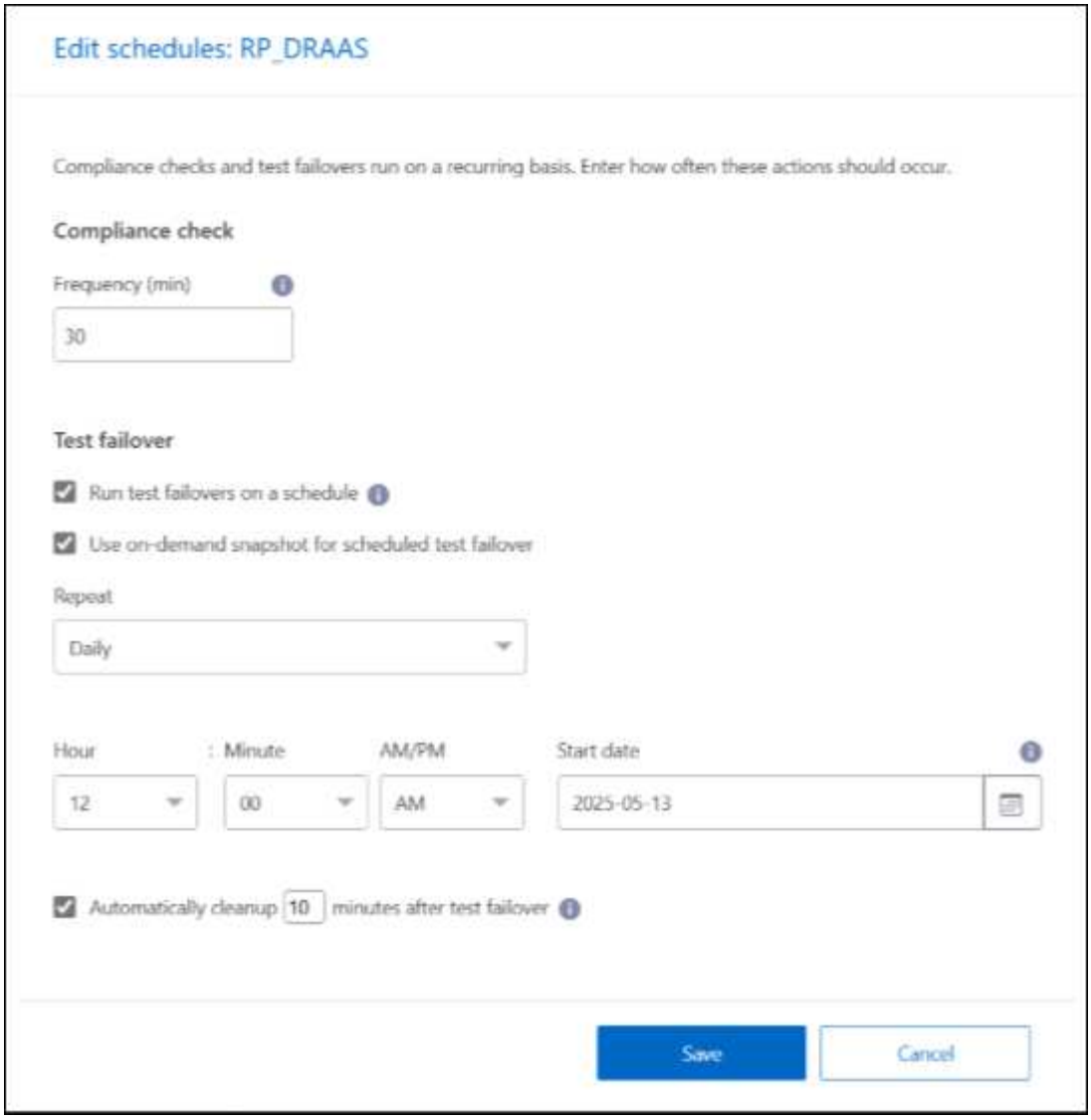
Basierend auf dem Zeitplan wird der Failover-Test ausgeführt und stellt sicher, dass die Workloads an das im Replikationsplan angegebene Ziel verschoben werden.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.



2. Wählen Sie die **Aktionen*** ••• **Symbol und wählen Sie *Zeitpläne bearbeiten**.
3. Geben Sie in Minuten ein, wie oft NetApp Disaster Recovery die Testkonformität überprüfen soll.
4. Um zu überprüfen, ob Ihre Failover-Tests fehlerfrei sind, aktivieren Sie **Führen Sie Failover monatlich aus**.
   a. Wählen Sie den Tag des Monats und die Uhrzeit aus, zu der diese Tests ausgeführt werden sollen.
   b. Geben Sie das Datum im Format JJJJ-MM-TT ein, an dem der Test beginnen soll.



5. **On-Demand-Snapshot für geplantes Test-Failover verwenden**: Aktivieren Sie dieses Kontrollkästchen, um vor dem Starten des automatisierten Test-Failovers einen neuen Snapshot zu erstellen.
6. Um die Testumgebung nach Abschluss des Failovertests zu bereinigen, aktivieren Sie **Automatisch bereinigen nach Testfailover** und geben Sie die Anzahl der Minuten ein, die Sie warten möchten, bevor die Bereinigung beginnt.

> Dieser Vorgang deregistriert die temporären VMs vom Teststandort, löscht das erstellte FlexClone -Volume und hebt die Bereitstellung der temporären Datenspeicher auf.

7. Wählen Sie **Speichern**.

Replizieren Sie Anwendungen an einen anderen Standort mit NetApp Disaster Recovery

Mit NetApp Disaster Recovery können Sie VMware-Apps auf Ihrem Quellstandort mithilfe der SnapMirror -Replikation auf einen Remote-Standort zur Notfallwiederherstellung in der Cloud replizieren.

Nachdem Sie den Notfallwiederherstellungsplan erstellt, die Wiederholung im Assistenten identifiziert und eine Replikation an einen Notfallwiederherstellungsstandort initiiert haben, überprüft NetApp Disaster Recovery alle 30 Minuten, ob die Replikation tatsächlich gemäß Plan erfolgt. Sie können den Fortschritt auf der Seite „Job Monitor“ überwachen.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster-Recovery-Administrator oder Disaster-Recovery-Failover-Administratorrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Bevor Sie beginnen

Bevor Sie die Replikation starten, sollten Sie einen Replikationsplan erstellt und die Replikation der Apps ausgewählt haben. Anschließend wird im Menü „Aktionen“ die Option „Replizieren“ angezeigt.

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im Menü **Replikationspläne** aus.
4. Wählen Sie den Replikationsplan aus.
5. Wählen Sie rechts die Option **Aktionen*** ••• **und wählen Sie *Replizieren**.

Migrieren Sie Anwendungen mit NetApp Disaster Recovery an einen anderen Standort

Mit NetApp Disaster Recovery können Sie VMware-Apps von Ihrem Quellstandort auf einen anderen Standort migrieren.

Nachdem Sie den Replikationsplan erstellt, die Wiederholung im Assistenten identifiziert und die Migration initiiert haben, überprüft NetApp Disaster Recovery alle 30 Minuten, ob die Migration tatsächlich gemäß Plan erfolgt. Sie können den Fortschritt auf der Seite „Job Monitor“ überwachen.

Bevor Sie beginnen

Bevor Sie die Migration starten, sollten Sie einen Replikationsplan erstellt und die Migration der Apps ausgewählt haben. Anschließend wird im Menü „Aktionen“ die Option „Migrieren“ angezeigt.

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im Menü **Replikationspläne** aus.
4. Wählen Sie den Replikationsplan aus.
5. Wählen Sie rechts die Option **Aktionen*** ••• **und wählen Sie *Migrieren**.

Failover von Anwendungen an einen Remote-Standort mit NetApp Disaster Recovery

Führen Sie im Katastrophenfall ein Failover Ihres primären VMware-Standorts vor Ort auf einen anderen VMware-Standort vor Ort oder auf VMware Cloud auf AWS durch. Sie können den Failover-Prozess testen, um sicherzustellen, dass er bei Bedarf erfolgreich ist.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster-Recovery-Administrator oder Disaster-Recovery-Failover-Administratorrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Über diese Aufgabe

Im Falle eines Failovers verwendet Disaster Recovery standardmäßig die aktuellste SnapMirror Snapshot-Kopie. Sie können jedoch einen bestimmten Snapshot aus einem Point-in-Time-Snapshot auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Verwenden Sie die Option „Zeitpunkt“.

Dieser Prozess unterscheidet sich, je nachdem, ob der Produktionsstandort fehlerfrei ist und Sie aus anderen Gründen als einem kritischen Infrastrukturausfall ein Failover zum Disaster Recovery-Standort durchführen:

- Kritischer Produktionsstandortausfall, bei dem auf das Quell-vCenter oder den ONTAP Cluster nicht zugegriffen werden kann: Mit NetApp Disaster Recovery können Sie einen beliebigen verfügbaren Snapshot für die Wiederherstellung auswählen.
- Die Produktionsumgebung ist fehlerfrei: Sie können entweder „Jetzt einen Snapshot erstellen“ oder einen zuvor erstellten Snapshot auswählen.

Dieses Verfahren unterbricht die Replikationsbeziehung, setzt die vCenter-Quell-VMs offline, registriert die Volumes als Datenspeicher im Disaster Recovery-vCenter, startet die geschützten VMs unter Verwendung der Failover-Regeln im Plan neu und aktiviert das Lesen/Schreiben auf der Zielsite.

Testen des Failover-Prozesses

Bevor Sie das Failover starten, können Sie den Vorgang testen. Der Test schaltet die virtuellen Maschinen nicht offline.

Während eines Failover-Tests erstellt Disaster Recovery vorübergehend virtuelle Maschinen. Risaster Recovery ordnet einen temporären Datenspeicher, der das FlexClone Volume unterstützt, den ESXi-Hosts zu.

Dieser Prozess beansprucht keine zusätzliche physische Kapazität auf dem lokalen ONTAP Speicher oder dem FSx für NetApp ONTAP -Speicher in AWS. Das ursprüngliche Quellvolume wird nicht verändert, und Replikationsaufträge können auch während der Notfallwiederherstellung fortgesetzt werden.

Wenn Sie den Test abgeschlossen haben, sollten Sie die virtuellen Maschinen mit der Option **Test bereinigen** zurücksetzen. Dies wird zwar empfohlen, ist jedoch nicht erforderlich.

Ein Test-Failover-Vorgang hat *keine* Auswirkungen auf Produktions-Workloads, die auf der Testsite verwendete SnapMirror -Beziehung und geschützte Workloads, die weiterhin normal ausgeführt werden müssen.

Für ein Test-Failover führt Disaster Recovery die folgenden Vorgänge aus:

- Führen Sie Vorprüfungen des Zielclusters und der SnapMirror -Beziehung durch.
- Erstellen Sie aus dem ausgewählten Snapshot für jedes geschützte ONTAP Volume auf dem ONTAP -Cluster des Zielstandorts ein neues FlexClone Volume.
- Wenn es sich bei einem der Datenspeicher um VMFS handelt, erstellen Sie eine iGroup und ordnen Sie sie jeder LUN zu.
- Registrieren Sie die virtuellen Zielmaschinen in vCenter als neue Datenspeicher.
- Schalten Sie die virtuellen Zielmaschinen basierend auf der auf der Seite „Ressourcengruppen“ erfassten Startreihenfolge ein.
- Führen Sie eine Stilllegung aller unterstützten Datenbankanwendungen in VMs durch, die als „anwendungskonsistent“ gekennzeichnet sind.
- Wenn die Quell-vCenter- und ONTAP Cluster noch aktiv sind, erstellen Sie eine SnapMirror -Beziehung in umgekehrter Richtung, um alle Änderungen im Failover-Zustand zurück auf die ursprüngliche Quellsite zu replizieren.

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.
4. Wählen Sie den Replikationsplan aus.
5. Wählen Sie rechts die Option **Aktionen*** ••• **und wählen Sie *Failover testen**.
6. Geben Sie auf der Seite „Testfailover“ „Testfailover“ ein und wählen Sie **Testfailover** aus.
7. Nachdem der Test abgeschlossen ist, bereinigen Sie die Testumgebung.

Bereinigen der Testumgebung nach einem Failovertest

Nachdem der Failover-Test abgeschlossen ist, sollten Sie die Testumgebung bereinigen. Dieser Prozess entfernt die temporären VMs vom Teststandort, den FlexClones und den temporären Datenspeichern.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.
2. Wählen Sie den Replikationsplan aus.
3. Wählen Sie rechts die Option **Aktionen** aus. ••• dann **Failover-Test bereinigen**.
4. Geben Sie auf der Seite „Test-Failover“ die Option „Failover bereinigen“ ein und wählen Sie dann **Failover-Test bereinigen** aus.

Führen Sie ein Failover des Quellstandorts auf einen Notfallwiederherstellungsstandort durch

Führen Sie im Katastrophenfall bei Bedarf ein Failover Ihres primären VMware-Standorts vor Ort auf einen anderen VMware-Standort vor Ort oder auf VMware Cloud auf AWS mit FSx für NetApp ONTAP durch.

Der Failover-Prozess umfasst die folgenden Vorgänge:

- Disaster Recovery führt Vorprüfungen des Zielclusters und der SnapMirror -Beziehung durch.
- Wenn Sie den neuesten Snapshot ausgewählt haben, wird das SnapMirror Update durchgeführt, um die neuesten Änderungen zu replizieren.

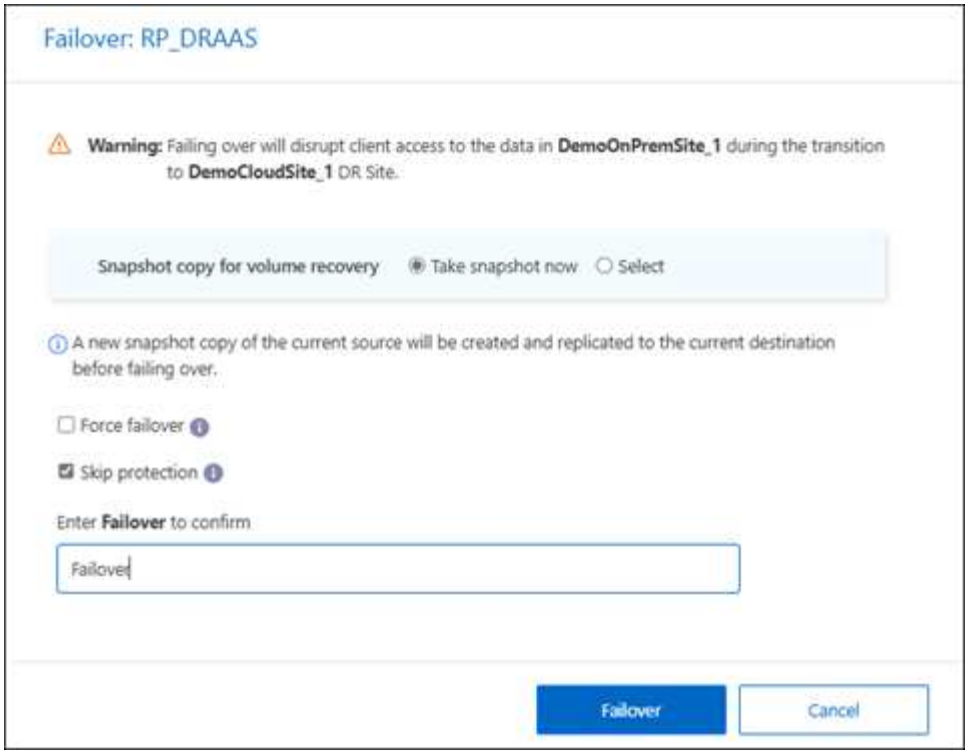
- Die virtuellen Quellmaschinen werden heruntergefahren.
- Die SnapMirror -Beziehung wird unterbrochen und das Zielvolume wird lese-/schreibgeschützt.
- Basierend auf der Auswahl des Snapshots wird das aktive Dateisystem auf den angegebenen Snapshot (neuester oder ausgewählter) wiederhergestellt.
- Datenspeicher werden basierend auf den im Replikationsplan erfassten Informationen erstellt und im VMware- oder VMC-Cluster oder -Host bereitgestellt. Wenn es sich bei einem der Datenspeicher um VMFS handelt, erstellen Sie eine iGroup und ordnen Sie sie jeder LUN zu.
- Die virtuellen Zielmaschinen werden in vCenter als neue Datenspeicher registriert.
- Die virtuellen Zielmaschinen werden basierend auf der auf der Seite „Ressourcengruppen“ erfassten Startreihenfolge eingeschaltet.
- Wenn das Quell-vCenter noch aktiv ist, schalten Sie alle VMs auf der Quellseite aus, für die ein Failover durchgeführt wird.
- Führen Sie eine Stilllegung aller unterstützten Datenbankanwendungen in VMs durch, die als „anwendungskonsistent“ gekennzeichnet sind.
- Wenn die Quell-vCenter- und ONTAP Cluster noch aktiv sind, erstellen Sie eine SnapMirror -Beziehung in umgekehrter Richtung, um alle Änderungen im Failover-Zustand zurück auf die ursprüngliche Quellsite zu replizieren. Die SnapMirror -Beziehung wird von der Ziel- zur Quell-VM umgekehrt.

Bei datenspeicherbasierten Replikationsplänen werden VMs, die Sie hinzugefügt und erkannt haben, für die aber keine Zuordnungsdetails angegeben wurden, in das Failover einbezogen. Der Failover schlägt fehl und es wird eine Benachrichtigung in den Jobs angezeigt. Sie müssen die Zuordnungsdetails angeben, um das Failover erfolgreich abzuschließen.

Nachdem das Failover gestartet wurde, können Sie die wiederhergestellten VMs im vCenter der Disaster-Recovery-Site sehen (virtuelle Maschinen, Netzwerke und Datenspeicher). Standardmäßig werden die virtuellen Maschinen im Workload-Ordner wiederhergestellt.

Schritte

1. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.
2. Wählen Sie den Replikationsplan aus.
3. Wählen Sie rechts die Option **Aktionen*** ••• **und wählen Sie *Failover**.



4. Auf der Failover-Seite können Sie entweder jetzt einen neuen Snapshot erstellen oder einen vorhandenen Snapshot für den Datenspeicher auswählen, der als Grundlage für die Wiederherstellung dienen soll. Standardmäßig wird die neueste Version verwendet.

   Vor dem Failover wird ein Snapshot der aktuellen Quelle erstellt und zum aktuellen Ziel repliziert.

5. Wählen Sie optional **Failover erzwingen** aus, wenn das Failover auch dann erfolgen soll, wenn ein Fehler erkannt wird, der das Failover normalerweise verhindern würde.
6. Wählen Sie optional **Schutz überspringen** aus, wenn der Dienst nach einem Failover des Replikationsplans nicht automatisch eine umgekehrte SnapMirror -Schutzbeziehung erstellen soll. Dies ist nützlich, wenn Sie zusätzliche Vorgänge auf der wiederhergestellten Site durchführen möchten, bevor Sie sie in NetApp Disaster Recovery wieder online schalten.

   Sie können einen umgekehrten Schutz einrichten, indem Sie im Menü „Aktionen“ des Replikationsplans die Option „Ressourcen schützen“ auswählen. Dadurch wird versucht, für jedes Volume im Plan eine umgekehrte Replikationsbeziehung zu erstellen. Sie können diesen Job wiederholt ausführen, bis der Schutz wiederhergestellt ist. Wenn der Schutz wiederhergestellt ist, können Sie auf die übliche Weise ein Failback einleiten.

7. Geben Sie „Failover“ in das Feld ein.
8. Wählen Sie **Failover**.
9. Um den Fortschritt zu überprüfen, wählen Sie im Menü **Jobüberwachung**.

Failback von Anwendungen auf die ursprüngliche Quelle mit NetApp Disaster Recovery

Nachdem ein Notfall behoben wurde, führen Sie ein Failback vom Notfallwiederherstellungsstandort zum Quellstandort durch, um zum Normalbetrieb

zurückzukehren. Sie können den Snapshot auswählen, von dem die Wiederherstellung erfolgen soll.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster-Recovery-Administrator oder Disaster-Recovery-Failover-Administratorrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Über Failback

Im Failback-Modus repliziert (resynchronisiert) NetApp Disaster Recovery alle Änderungen zurück auf die ursprüngliche virtuelle Quellmaschine, bevor die Replikationsrichtung umgekehrt wird. Dieser Prozess beginnt mit einer Beziehung, die vollständig auf ein Ziel umgeschaltet wurde, und umfasst die folgenden Schritte:

- Führen Sie eine Konformitätsprüfung auf der wiederhergestellten Site durch.
- Aktualisieren Sie die vCenter-Informationen für jeden vCenter-Cluster, der sich am wiederhergestellten Standort befindet.
- Schalten Sie auf der Zielsite die virtuellen Maschinen aus, heben Sie die Registrierung auf und heben Sie die Bereitstellung der Volumes auf.
- Unterbrechen Sie die SnapMirror -Beziehung zur Originalquelle, um Lese-/Schreibzugriff zu ermöglichen.
- Synchronisieren Sie die SnapMirror -Beziehung erneut, um die Replikation umzukehren.
- Schalten Sie die virtuellen Quellmaschinen ein, registrieren Sie sie und mounten Sie die Volumes auf der Quelle.

Bevor Sie beginnen

Wenn Sie einen datenspeicherbasierten Schutz verwenden, können VMs, die dem Datenspeicher hinzugefügt wurden, im Failover-Prozess ebenfalls dem Datenspeicher hinzugefügt werden. Falls dies der Fall ist, stellen Sie sicher, dass Sie die zusätzlichen Mapping-Informationen für diese VMs bereitstellen, bevor Sie das Failback einleiten. Informationen zum Bearbeiten der Ressourcenzuordnung finden Sie unter "Verwalten von Replikationsplänen"Die

Schritte

1. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
2. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.
3. Wählen Sie den Replikationsplan aus.
4. Wählen Sie rechts die Option **Aktionen*** ••• **und wählen Sie *Failback**.
5. Geben Sie den Namen des Replikationsplans ein, um das Failback zu starten.
6. Wählen Sie den Snapshot für den Datenspeicher aus, aus dem die Wiederherstellung erfolgen soll. Die Standardeinstellung ist die neueste Version.
7. Um den Fortschritt des Auftrags zu überwachen, wählen Sie im Menü „Notfallwiederherstellung“ die Option „Auftragsüberwachung“.

Verwalten Sie Sites, Ressourcengruppen, Replikationspläne, Datenspeicher und Informationen zu virtuellen Maschinen mit NetApp Disaster Recovery

NetApp Disaster Recovery bietet Übersichten und detailliertere Einblicke in alle Ihre Ressourcen:

- Seiten
- Ressourcengruppen
- Replikationspläne
- Datenspeicher
- Virtuelle Maschinen

Für die Aufgaben sind unterschiedliche NetApp Console erforderlich. Weitere Informationen finden Sie im Abschnitt *Erforderliche NetApp Console * in jeder Aufgabe.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Verwalten von vCenter-Sites

Sie können den vCenter-Sitenamen und den Sitetyp (vor Ort oder AWS) bearbeiten.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator oder Notfallwiederherstellungsadministratorrolle.

Schritte

1. Wählen Sie im Menü **Sites** aus.
2. Wählen Sie die Option **Aktionen***  **rechts neben dem vCenter-Namen und wählen Sie *Bearbeiten**.
3. Bearbeiten Sie den Namen und den Standort der vCenter-Site.

Verwalten von Ressourcengruppen

Sie können Ressourcengruppen nach VMs oder Datenspeichern erstellen. Sie können beim Erstellen des Replikationsplans oder auch später hinzugefügt werden.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Notfallwiederherstellungsanwendungsadministrator.

Sie können eine Ressourcengruppe nach Datenspeichern auf folgende Weise erstellen:

- Wenn Sie eine Ressourcengruppe mithilfe von Datenspeichern hinzufügen, wird eine Liste der Datenspeicher angezeigt. Sie können einen oder mehrere Datenspeicher auswählen, um eine Ressourcengruppe zu erstellen.
- Wenn Sie einen Replikationsplan erstellen und innerhalb des Plans eine Ressourcengruppe erstellen, können Sie die VMs in den Datenspeichern sehen.

Mit Ressourcengruppen können Sie folgende Aufgaben ausführen:

- Ändern Sie den Namen der Ressourcengruppe.
- Fügen Sie der Ressourcengruppe VMs hinzu.
- Entfernen Sie VMs aus der Ressourcengruppe.
- Ressourcengruppen löschen.

Einzelheiten zum Erstellen einer Ressourcengruppe finden Sie unter"Erstellen Sie eine Ressourcengruppe, um VMs gemeinsam zu organisieren" .

Schritte

1. Wählen Sie im Menü **Ressourcengruppen** aus.
2. Um eine Ressourcengruppe hinzuzufügen, wählen Sie **Gruppe hinzufügen**.
3. Sie können die Ressourcengruppe ändern oder löschen, indem Sie die Option **Aktionen** auswählen. ••• Die

Verwalten von Replikationsplänen

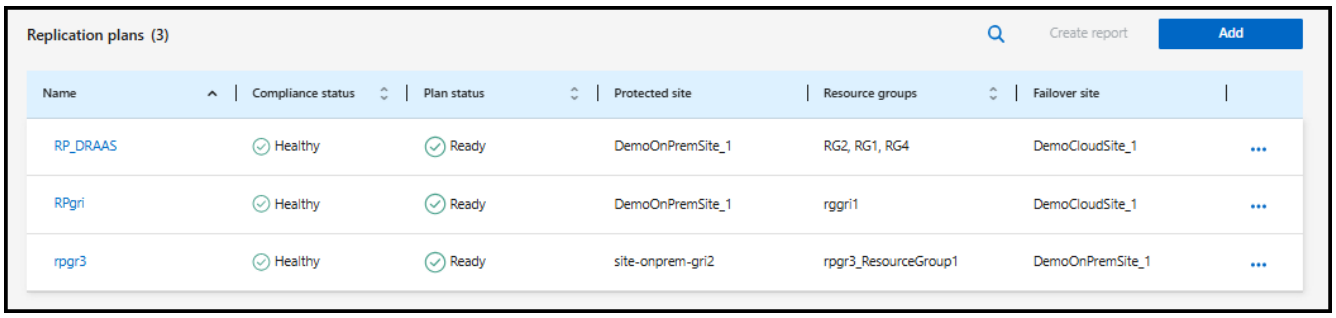
Sie können Replikationspläne deaktivieren, aktivieren und löschen. Sie können Zeitpläne ändern.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator oder Disaster Recovery-Anwendungsadministrator.

- Wenn Sie einen Replikationsplan vorübergehend anhalten möchten, können Sie ihn deaktivieren und später aktivieren.
- Wenn Sie den Plan nicht mehr benötigen, können Sie ihn löschen.

Schritte

1. Wählen Sie im Menü **Replikationspläne** aus.



2. Um die Plandetails anzuzeigen, wählen Sie die Option **Aktionen*** ••• **und wählen Sie *Plandetails anzeigen**.
3. Führen Sie einen der folgenden Schritte aus:
   - Um die Plandetails zu bearbeiten (die Wiederholung zu ändern), wählen Sie die Registerkarte **Plandetails** und dann rechts das Symbol **Bearbeiten**.
   - Um die Ressourcenzuordnungen zu bearbeiten, wählen Sie die Registerkarte **Failover-Zuordnung** und dann das Symbol **Bearbeiten**.
   - Um die virtuellen Maschinen hinzuzufügen oder zu bearbeiten, wählen Sie die Registerkarte **Virtuelle Maschinen** und wählen Sie die Option **VMs hinzufügen** oder das Symbol **Bearbeiten**.

4. Kehren Sie zur Liste der Pläne zurück, indem Sie in der Breadcrumb-Navigation links „Replikationspläne“ auswählen.
5. Um Aktionen mit dem Plan auszuführen, wählen Sie aus der Liste der Replikationspläne die Option **Aktionen*** ••• **rechts neben dem Plan und wählen Sie eine der Optionen aus, z. B. *Zeitpläne bearbeiten**, **Failover testen**, **Failover**, **Failback**, **Migrieren**, **Jetzt Snapshot erstellen**, **Alte Snapshots bereinigen**, **Deaktivieren**, **Aktivieren** oder **Löschen**.
6. Um einen Test-Failover-Zeitplan festzulegen oder zu ändern oder die Konformitätshäufigkeitsprüfung festzulegen, wählen Sie die Option **Aktionen*** ••• **rechts neben dem Plan und wählen Sie *Zeitpläne bearbeiten**.
   a. Geben Sie auf der Seite „Zeitpläne bearbeiten“ ein, wie oft (in Minuten) die Failover-Konformitätsprüfung durchgeführt werden soll.
   b. Aktivieren Sie **Test-Failover nach Zeitplan ausführen**.
   c. Wählen Sie in der Option „Wiederholen“ den täglichen, wöchentlichen oder monatlichen Zeitplan aus.
   d. Wählen Sie **Speichern**.

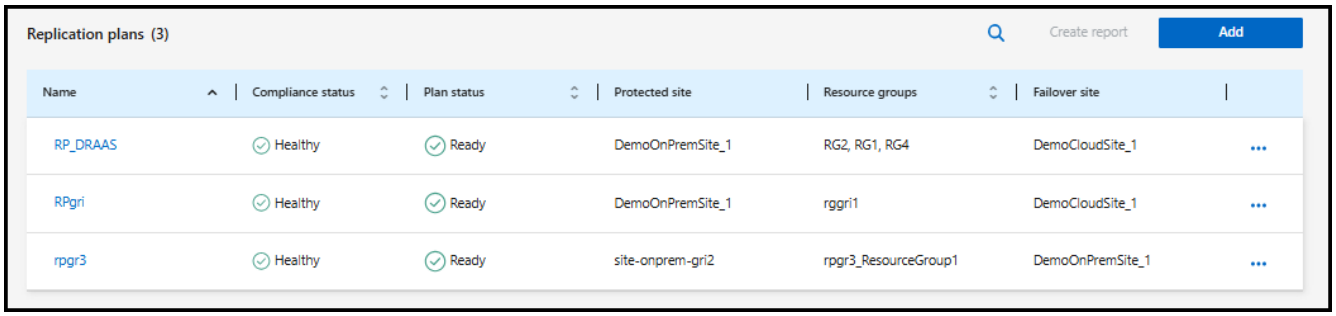
Snapshots bei Bedarf abgleichen

Die Disaster-Recovery-Funktion löscht automatisch alle 24 Stunden Snapshots auf dem Quellsystem. Sollten Sie feststellen, dass die Snapshots zwischen Quelle und Ziel nicht synchron sind, müssen Sie die Diskrepanz zwischen den Snapshots beheben, um die Konsistenz über alle Standorte hinweg zu gewährleisten.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator oder Disaster Recovery-Anwendungsadministrator.

Schritte

1. Wählen Sie im Menü **Replikationspläne** aus.



2. Wählen Sie in der Liste der Replikationspläne die Option **Aktionen** aus. ••• dann **Snapshots abgleichen**.
3. Überprüfen Sie die Abstimmungsinformationen.
4. Wählen Sie **Abgleichen**.

Löschen eines Replikationsplans

Wenn Sie einen Replikationsplan löschen, können Sie auch die vom Plan erstellten primären und sekundären Snapshots löschen.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator oder Disaster Recovery-Anwendungsadministrator.

Schritte

1. Wählen Sie im Menü **Replikationspläne** aus.
2. Wählen Sie die Option **Aktionen*** ••• **rechts neben dem Plan und wählen Sie *Löschen**.
3. Wählen Sie aus, ob Sie die primären Snapshots, die sekundären Snapshots oder nur die vom Plan erstellten Metadaten löschen möchten.
4. Geben Sie „Löschen“ ein, um den Löschvorgang zu bestätigen.
5. Wählen Sie **Löschen**.

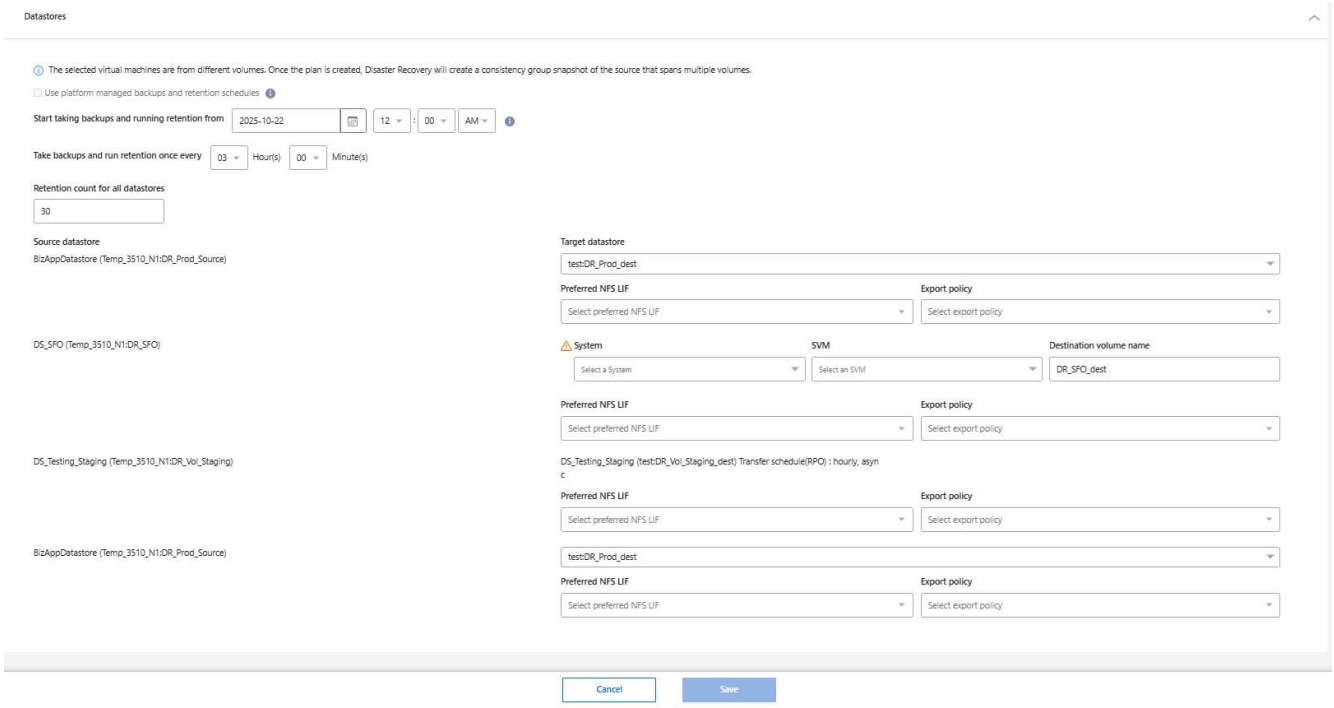
Ändern der Aufbewahrungsanzahl für Failover-Zeitpläne

Durch die Änderung der Aufbewahrungsanzahl können Sie die Anzahl der gespeicherten Datenspeicher erhöhen oder verringern.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator oder Disaster Recovery-Anwendungsadministrator.

Schritte

1. Wählen Sie im Menü **Replikationspläne** aus.
2. Wählen Sie den Replikationsplan und anschließend die Registerkarte **Failover-Zuordnung** aus. Wählen Sie das Stiftsymbol **Bearbeiten** aus.
3. Klicken Sie auf den Abwärtspfeil in der Zeile **Datenspeicher**, um diese zu erweitern.



4. Ändern Sie den Wert der **Aufbewahrungsanzahl für alle Datenspeicher**.
5. Wählen Sie bei ausgewähltem Replikationsplan das Menü „Aktionen“ und dann „Alte Snapshots bereinigen“ aus, um alte Snapshots auf dem Ziel zu entfernen und sie an die neue Aufbewahrungsanzahl anzupassen.

Anzeigen von Datenspeicherinformationen

Sie können Informationen darüber anzeigen, wie viele Datenspeicher auf der Quelle und auf dem Ziel vorhanden sind.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator, Disaster Recovery-Anwendungsadministrator oder Disaster Recovery-Viewer-Rolle.

Schritte

1. Wählen Sie im Menü **Dashboard** aus.
2. Wählen Sie das vCenter in der Sitezeile aus.
3. Wählen Sie **Datenspeicher** aus.
4. Zeigen Sie die Datenspeicherinformationen an.

Anzeigen von Informationen zu virtuellen Maschinen

Sie können Informationen darüber anzeigen, wie viele virtuelle Maschinen auf der Quelle und auf dem Ziel vorhanden sind, sowie Informationen zu CPU, Arbeitsspeicher und verfügbarer Kapazität.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator, Disaster Recovery-Anwendungsadministrator oder Disaster Recovery-Viewer-Rolle.

Schritte

1. Wählen Sie im Menü **Dashboard** aus.
2. Wählen Sie das vCenter in der Sitezeile aus.
3. Wählen Sie **Virtuelle Maschinen** aus.
4. Zeigen Sie die Informationen zu virtuellen Maschinen an.

Überwachen Sie NetApp Disaster Recovery -Jobs

Sie können alle NetApp Disaster Recovery -Jobs überwachen und ihren Fortschritt bestimmen.

Jobs anzeigen

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Anwendungsadministrator oder Disaster Recovery-Viewer-Rolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie im Menü **Jobüberwachung** aus.
4. Erkunden Sie alle betriebsbezogenen Jobs und überprüfen Sie deren Zeitstempel und Status.

5. Um Details zu einem bestimmten Job anzuzeigen, wählen Sie die entsprechende Zeile aus.
6. Um die Informationen zu aktualisieren, wählen Sie **Aktualisieren**.

Abbrechen eines Auftrags

Wenn ein Auftrag ausgeführt wird oder sich in einer Warteschlange befindet und Sie nicht möchten, dass er fortgesetzt wird, können Sie ihn abbrechen. Möglicherweise möchten Sie einen Auftrag abbrechen, wenn er im gleichen Zustand feststeckt und Sie den nächsten Vorgang in der Warteschlange freigeben möchten. Möglicherweise möchten Sie einen Auftrag abbrechen, bevor die Zeit abläuft.

*Erforderliche NetApp Console * Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator oder Disaster Recovery-Anwendungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen in NetApp Disaster Recovery". "Erfahren Sie mehr über die Zugriffsrollen der NetApp Console für alle Dienste".

Schritte

1. Wählen Sie in der linken Navigationsleiste der NetApp Console **Schutz** > **Notfallwiederherstellung**.
2. Wählen Sie im Menü **Jobüberwachung** aus.
3. Notieren Sie auf der Job-Monitor-Seite die ID des Jobs, den Sie abbrechen möchten.

   Der Auftrag muss sich im Status „In Bearbeitung“ oder „In der Warteschlange“ befinden.

4. Wählen Sie in der Spalte „Aktionen“ die Option „Auftrag abbrechen“ aus.

Erstellen Sie NetApp Disaster Recovery -Berichte

Durch die Überprüfung der NetApp Disaster Recovery -Berichte können Sie Ihre Disaster Recovery-Vorbereitung analysieren. Vorgefertigte Berichte enthalten eine Zusammenfassung der Test-Failover, Replikationsplandetails und Jobdetails für alle Sites innerhalb eines Kontos für die letzten sieben Tage.

Sie können Berichte im PDF-, HTML- oder JSON-Format herunterladen.

Der Download-Link ist sechs Stunden gültig.

Schritte

1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.
3. Wählen Sie in der linken Navigationsleiste der NetApp Console **Replikationspläne** aus.
4. Wählen Sie **Bericht erstellen**.
5. Wählen Sie den Dateiformattyp und den Zeitraum innerhalb der letzten 7 Tage aus.
6. Wählen Sie **Erstellen**.

   Die Anzeige des Berichts kann einige Minuten dauern.

7. Um einen Bericht herunterzuladen, wählen Sie **Bericht herunterladen** und wählen Sie ihn im Download-

Ordner des Administrators aus.