NetApp Disaster Recovery -Dokumentation

NetApp Disaster Recovery

NetApp
October 14, 2025

Inhalt

NetApp Disaster Recovery -Dokumentation

Versionshinweise

Was ist neu bei NetApp Disaster Recovery ?

Erfahren Sie, was es Neues bei NetApp Disaster Recovery gibt.

06. Oktober 2025

BlueXP disaster recovery heißt jetzt NetApp Disaster Recovery

BlueXP disaster recovery wurde in NetApp Disaster Recovery umbenannt.

BlueXP heißt jetzt NetApp Console

Die NetApp Console basiert auf der verbesserten und neu strukturierten BlueXP -Grundlage und ermöglicht die zentrale Verwaltung von NetApp -Speicher und NetApp Data Services in On-Premises- und Cloud-Umgebungen auf Unternehmensniveau. Sie liefert Einblicke in Echtzeit, schnellere Arbeitsabläufe und eine vereinfachte Verwaltung mit hoher Sicherheit und Konformität.

Einzelheiten zu den Änderungen finden Sie im"Versionshinweise zur NetApp Console" .

Weitere Updates

- Die Unterstützung für Amazon Elastic VMware Service (EVS) mit Amazon FSx for NetApp ONTAP befand sich in einer öffentlichen Vorschau. Mit dieser Version ist es nun allgemein verfügbar. Weitere Einzelheiten finden Sie unter"Einführung von NetApp Disaster Recovery mit Amazon Elastic VMware Service und Amazon FSx for NetApp ONTAP" .
- Verbesserungen bei der Speichererkennung, einschließlich verkürzter Erkennungszeiten für lokale Bereitstellungen
- Unterstützung für Identity and Access Management (IAM), einschließlich rollenbasierter Zugriffskontrolle (RBAC) und erweiterter Benutzerberechtigungen
- Private Preview-Unterstützung für Azure VMware-Lösung und Cloud Volumes ONTAP. Mit dieser Unterstützung können Sie jetzt mithilfe des Cloud Volumes ONTAP Speichers den Notfallwiederherstellungsschutz von lokalen Standorten auf die Azure VMware-Lösung konfigurieren.

04. August 2025

Version 4.2.5P2

NetApp Disaster Recovery -Updates

Diese Version enthält die folgenden Updates:

- Die VMFS-Unterstützung wurde verbessert, um dieselbe LUN zu verarbeiten, die von mehreren virtuellen Speichermaschinen bereitgestellt wird.
- Die Bereinigung beim Test-Teardown wurde verbessert, um den Datenspeicher zu verarbeiten, der bereits ausgehängt und/oder gelöscht wurde.
- Verbesserte Subnetzzuordnung, sodass jetzt überprüft wird, ob das eingegebene Gateway im bereitgestellten Netzwerk enthalten ist.

- Ein Problem wurde behoben, das dazu führen konnte, dass der Replikationsplan fehlschlug, wenn der VM-Name „.com“ enthielt.
- Eine Einschränkung wurde entfernt, die verhinderte, dass das Zielvolume beim Erstellen des Volumes im Rahmen der Erstellung des Replikationsplans mit dem Quellvolume identisch war.
- Unterstützung für ein Pay-as-you-go-Abonnement (PAYGO) für NetApp Intelligent Services im Azure Marketplace hinzugefügt und im Dialogfeld „Kostenlose Testversion“ ein Link zum Azure Marketplace hinzugefügt.

  Weitere Einzelheiten finden Sie unter "NetApp Disaster Recovery -Lizenzierung" Und "Einrichten der Lizenzierung für NetApp Disaster Recovery" .

14. Juli 2025

Version 4.2.5

Benutzerrollen in NetApp Disaster Recovery

NetApp Disaster Recovery verwendet jetzt Rollen, um den Zugriff jedes Benutzers auf bestimmte Funktionen und Aktionen zu regeln.

Der Dienst verwendet die folgenden Rollen, die spezifisch für NetApp Disaster Recovery sind.

- **Disaster Recovery-Administrator**: Führen Sie beliebige Aktionen in NetApp Disaster Recovery aus.
- **Disaster Recovery-Failover-Administrator**: Führen Sie Failover- und Migrationsaktionen in NetApp Disaster Recovery durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Erstellen und ändern Sie Replikationspläne und starten Sie Test-Failover.
- **Disaster Recovery Viewer**: Informationen in NetApp Disaster Recovery anzeigen, aber keine Aktionen ausführen.

Wenn Sie auf den NetApp Disaster Recovery -Dienst klicken und ihn zum ersten Mal konfigurieren, müssen Sie über die Berechtigung **SnapCenterAdmin** oder die Rolle **Organisationsadministrator** verfügen.

Weitere Informationen finden Sie unter "Benutzerrollen und Berechtigungen in NetApp Disaster Recovery" .

"Erfahren Sie mehr über Zugriffsrollen für alle Dienste" .

Weitere Updates in NetApp Disaster Recovery

- Verbesserte Netzwerkerkennung
- Verbesserungen der Skalierbarkeit:
  - Filtern nach den benötigten Metadaten statt nach allen Details
  - Verbesserungen bei der Erkennung zum schnelleren Abrufen und Aktualisieren von VM-Ressourcen
  - Speicheroptimierung und Leistungsoptimierung für Datenabruf und Datenaktualisierung
  - Verbesserungen bei der Clienterstellung und Poolverwaltung im vCenter SDK
- Verwaltung veralteter Daten bei der nächsten geplanten oder manuellen Erkennung:
  - Wenn eine VM im vCenter gelöscht wird, entfernt NetApp Disaster Recovery sie jetzt automatisch aus dem Replikationsplan.

    - Wenn ein Datenspeicher oder Netzwerk im vCenter gelöscht wird, löscht NetApp Disaster Recovery es jetzt aus dem Replikationsplan und der Ressourcengruppe.
    - Wenn ein Cluster, Host oder Rechenzentrum im vCenter gelöscht wird, löscht NetApp Disaster Recovery es jetzt aus dem Replikationsplan und der Ressourcengruppe.
- Sie können jetzt im Inkognitomodus Ihres Browsers auf die Swagger-Dokumentation zugreifen. Sie können innerhalb von NetApp Disaster Recovery über die Option „Einstellungen“ > „API-Dokumentation“ oder direkt über die folgende URL im Inkognitomodus Ihres Browsers darauf zugreifen: "Swagger-Dokumentation" .
- In einigen Situationen blieb die iGroup nach Abschluss eines Failback-Vorgangs zurück. Dieses Update entfernt die iGroup, wenn sie veraltet ist.
- Wenn der NFS-FQDN im Replikationsplan verwendet wurde, löst NetApp Disaster Recovery ihn jetzt in eine IP-Adresse auf. Dieses Update ist nützlich, wenn der FQDN am Standort zur Notfallwiederherstellung nicht aufgelöst werden kann.
- Verbesserungen der UI-Ausrichtung
- Protokollverbesserungen zur Erfassung der vCenter-Größendetails nach der erfolgreichen Erkennung

30. Juni 2025

Version 4.2.4P2

Verbesserungen bei der Erkennung

Dieses Update verbessert den Erkennungsprozess und verkürzt so die für die Erkennung benötigte Zeit.

23. Juni 2025

Version 4.2.4P1

Verbesserungen der Subnetzzuordnung

Dieses Update erweitert den Dialog „Subnetzzuordnung hinzufügen und bearbeiten“ um eine neue Suchfunktion. Sie können jetzt durch Eingabe von Suchbegriffen schnell bestimmte Subnetze finden, was die Verwaltung von Subnetzzuordnungen vereinfacht.

09. Juni 2025

Version 4.2.4

Unterstützung für Windows Local Administrator Password Solution (LAPS)

Windows Local Administrator Password Solution (Windows LAPS) ist eine Windows-Funktion, die das Kennwort eines lokalen Administratorkontos im Active Directory automatisch verwaltet und sichert.

Sie können jetzt Subnetzzuordnungsoptionen auswählen und die LAPS-Option überprüfen, indem Sie die Domänencontrollerdetails angeben. Wenn Sie diese Option verwenden, müssen Sie nicht für jede Ihrer virtuellen Maschinen ein Kennwort angeben.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

13. Mai 2025

Version 4.2.3

Subnetzzuordnung

Mit dieser Version können Sie IP-Adressen beim Failover auf eine neue Art und Weise verwalten, indem Sie die Subnetzzuordnung verwenden, die es Ihnen ermöglicht, für jedes vCenter Subnetze hinzuzufügen. Dabei definieren Sie das IPv4-CIDR, das Standard-Gateway und das DNS für jedes virtuelle Netzwerk.

Beim Failover ermittelt NetApp Disaster Recovery die entsprechende IP-Adresse jeder vNIC, indem es sich den für das zugeordnete virtuelle Netzwerk bereitgestellten CIDR ansieht und daraus die neue IP-Adresse ableitet.

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.

Weitere Informationen zum Einbinden der Subnetzzuordnung in Ihre Sites finden Sie unter "vCenter-Server-Sites hinzufügen" .

Skip-Schutz

Sie können jetzt den Schutz überspringen, sodass der Dienst nach einem Failover des Replikationsplans nicht automatisch eine umgekehrte Schutzbeziehung erstellt. Dies ist nützlich, wenn Sie zusätzliche Vorgänge auf der wiederhergestellten Site durchführen möchten, bevor Sie sie in NetApp Disaster Recovery wieder online schalten.

Wenn Sie ein Failover initiieren, erstellt der Dienst standardmäßig automatisch eine umgekehrte Schutzbeziehung für jedes Volume im Replikationsplan, sofern die ursprüngliche Quellsite online ist. Dies bedeutet, dass der Dienst eine SnapMirror Beziehung von der Zielsite zurück zur Quellsite erstellt. Der Dienst kehrt die SnapMirror -Beziehung auch automatisch um, wenn Sie ein Failback initiieren.

Beim Einleiten eines Failovers können Sie jetzt die Option **Schutz überspringen** auswählen. Damit kehrt der Dienst die SnapMirror -Beziehung nicht automatisch um. Stattdessen belässt es das beschreibbare Volume auf beiden Seiten des Replikationsplans.

Nachdem die ursprüngliche Quellsite wieder online ist, können Sie 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.

Einzelheiten zum Überspringschutz finden Sie unter "Failover von Anwendungen auf einen Remote-Standort" .

SnapMirror -Zeitplanaktualisierungen im Replikationsplan

NetApp Disaster Recovery unterstützt jetzt die Verwendung externer Snapshot-Management-Lösungen wie den nativen ONTAP SnapMirror Policy Scheduler oder Drittanbieter-Integrationen mit ONTAP. 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.

Aktivieren Sie zur Konfiguration im Abschnitt Replikationsplan > Ressourcenzuordnung das Kontrollkästchen **Von der Plattform verwaltete Sicherungen und Aufbewahrungspläne verwenden**, wenn Sie die Datenspeicherzuordnung konfigurieren.

Wenn die 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.

Einzelheiten zur Verwendung externer Snapshot-Lösungen im Replikationsplan finden Sie unter "Erstellen eines Replikationsplans" .

16. April 2025

Version 4.2.2

Geplante Erkennung für VMs

NetApp Disaster Recovery führt alle 24 Stunden eine Erkennung durch. Mit dieser Version können Sie jetzt den Erkennungszeitplan an Ihre Anforderungen anpassen und die Auswirkungen auf die Leistung bei Bedarf reduzieren. Wenn Sie beispielsweise über eine große Anzahl VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 48 Stunden 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 die Erkennung nicht planen möchten, können Sie die Option zur geplanten Erkennung deaktivieren und die Erkennung jederzeit manuell aktualisieren.

Weitere Einzelheiten finden Sie unter "vCenter-Server-Sites hinzufügen" .

Unterstützung für Ressourcengruppen-Datenspeicher

Bisher konnten Sie Ressourcengruppen nur nach VMs erstellen. Mit dieser Version können Sie eine Ressourcengruppe nach Datenspeichern erstellen. Wenn Sie einen Replikationsplan erstellen und eine Ressourcengruppe für diesen Plan erstellen, werden alle VMs in einem Datenspeicher aufgelistet. Dies ist nützlich, wenn Sie über eine große Anzahl VMs verfügen und diese nach Datenspeicher gruppieren möchten.

Sie können eine Ressourcengruppe mit einem Datenspeicher 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.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Benachrichtigungen zum Ablauf der kostenlosen Testversion oder Lizenz

Diese Version enthält Benachrichtigungen, dass die kostenlose Testversion in 60 Tagen abläuft, um sicherzustellen, dass Sie Zeit haben, eine Lizenz zu erwerben. Diese Version bietet auch Benachrichtigungen am Tag des Lizenzablaufs.

Benachrichtigung über Service-Updates

Mit dieser Version wird oben ein Banner angezeigt, das darauf hinweist, dass die Dienste aktualisiert werden und der Dienst in den Wartungsmodus versetzt wird. Das Banner wird angezeigt, wenn der Dienst aktualisiert wird, und verschwindet, wenn die Aktualisierung abgeschlossen ist. Während des Upgrades können Sie zwar weiterhin in der Benutzeroberfläche arbeiten, Sie können jedoch keine neuen Aufträge übermitteln. Geplante Jobs werden ausgeführt, nachdem das Update abgeschlossen ist und der Dienst in den Produktionsmodus zurückkehrt.

10. März 2025

Version 4.2.1

Intelligente Proxy-Unterstützung

Der NetApp Console Agent unterstützt intelligente Proxys. Intelligent Proxy ist eine einfache, sichere und effiziente Möglichkeit, Ihr lokales System mit NetApp Disaster Recovery zu verbinden. Es bietet eine sichere Verbindung zwischen Ihrem System und NetApp Disaster Recovery, ohne dass ein VPN oder direkter Internetzugang erforderlich ist. Diese optimierte Proxy-Implementierung entlastet den API-Verkehr innerhalb des lokalen Netzwerks.

Wenn ein Proxy konfiguriert ist, versucht NetApp Disaster Recovery, direkt mit VMware oder ONTAP zu kommunizieren und verwendet den konfigurierten Proxy, wenn die direkte Kommunikation fehlschlägt.

Die Implementierung des NetApp Disaster Recovery -Proxys erfordert eine Kommunikation über Port 443 zwischen dem Konsolenagenten und allen vCenter-Servern und ONTAP Arrays unter Verwendung eines HTTPS-Protokolls. Der NetApp Disaster Recovery -Agent innerhalb des Konsolen-Agenten kommuniziert bei der Durchführung von Aktionen direkt mit VMware vSphere, dem VC oder ONTAP .

Weitere Informationen zum intelligenten Proxy für NetApp Disaster Recovery finden Sie unter "Richten Sie Ihre Infrastruktur für NetApp Disaster Recovery ein" .

Weitere Informationen zum Einrichten eines allgemeinen Proxys in der NetApp Console finden Sie unter "Konfigurieren des Konsolenagenten zur Verwendung eines Proxyservers" .

Beenden Sie die kostenlose Testversion jederzeit

Sie können die kostenlose Testversion jederzeit beenden oder warten, bis sie abläuft.

Sehen "Kostenlose Testversion beenden" .

19. Februar 2025

Version 4.2

ASA R2-Unterstützung für VMs und Datenspeicher auf VMFS-Speicher

Diese Version von NetApp Disaster Recovery bietet Unterstützung für ASA r2 für VMs und Datenspeicher auf VMFS-Speicher. Auf einem ASA R2-System unterstützt die ONTAP -Software wesentliche SAN-Funktionen und entfernt Funktionen, die in SAN-Umgebungen nicht unterstützt werden.

Diese Version unterstützt die folgenden Funktionen für ASA r2:

- Bereitstellung von Konsistenzgruppen für Primärspeicher (nur flache Konsistenzgruppen, d. h. nur eine Ebene ohne hierarchische Struktur)
- Backup-Vorgänge (Konsistenzgruppe) einschließlich SnapMirror Automatisierung

Die Unterstützung für ASA r2 in NetApp Disaster Recovery verwendet ONTAP 9.16.1.

Während Datenspeicher auf einem ONTAP Volume oder einer ASA r2-Speichereinheit gemountet werden können, kann eine Ressourcengruppe in NetApp Disaster Recovery nicht sowohl einen Datenspeicher von ONTAP als auch einen von ASA r2 enthalten. Sie können in einer Ressourcengruppe entweder einen Datenspeicher von ONTAP oder einen Datenspeicher von ASA r2 auswählen.

30. Oktober 2024

Berichterstattung

Sie können jetzt Berichte erstellen und herunterladen, die Ihnen bei der Analyse Ihrer Landschaft helfen. Vorgefertigte Berichte fassen Failovers und Failbacks zusammen, zeigen Replikationsdetails auf allen Sites und zeigen Jobdetails für die letzten sieben Tage.

Siehe "Erstellen von Disaster Recovery-Berichten" .

30 Tage kostenlos testen

Sie können sich jetzt für eine 30-tägige kostenlose Testversion von NetApp Disaster Recovery anmelden. Bisher waren kostenlose Testversionen 90 Tage lang verfügbar.

Siehe "Einrichten der Lizenzierung" .

Deaktivieren und Aktivieren von Replikationsplänen

Eine frühere Version enthielt Aktualisierungen der Failover-Testplanstruktur, die zur Unterstützung täglicher und wöchentlicher Zeitpläne erforderlich waren. Für dieses Update war es erforderlich, dass Sie alle vorhandenen Replikationspläne deaktivieren und erneut aktivieren, damit Sie die neuen täglichen und wöchentlichen Failover-Testpläne verwenden können. Dies ist eine einmalige Anforderung.

So geht’s:

1. Wählen Sie im Menü **Replikationspläne** aus.
2. Wählen Sie einen Plan aus und klicken Sie auf das Symbol „Aktionen“, um das Dropdown-Menü anzuzeigen.
3. Wählen Sie **Deaktivieren**.

4. Wählen Sie nach einigen Minuten **Aktivieren**.

Ordnerzuordnung

Wenn Sie einen Replikationsplan erstellen und Rechenressourcen zuordnen, können Sie jetzt Ordner zuordnen, sodass VMs in einem Ordner wiederhergestellt werden, den Sie für Rechenzentrum, Cluster und Host angeben.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

VM-Details für Failover, Failback und Test-Failover verfügbar

Wenn ein Fehler auftritt und Sie ein Failover starten, ein Failback durchführen oder das Failover testen, können Sie jetzt Details der VMs anzeigen und feststellen, welche VMs nicht neu gestartet wurden.

Siehe "Failover von Anwendungen auf einen Remote-Standort" .

VM-Startverzögerung mit geordneter Startsequenz

Wenn Sie einen Replikationsplan erstellen, können Sie jetzt für jede VM im Plan eine Startverzögerung festlegen. Auf diese Weise können Sie eine Reihenfolge für den Start der VMs festlegen, um sicherzustellen, dass alle Ihre VMs mit Priorität eins ausgeführt werden, bevor die VMs mit nachfolgender Priorität gestartet werden.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Informationen zum VM-Betriebssystem

Wenn Sie einen Replikationsplan erstellen, können Sie jetzt das Betriebssystem für jede VM im Plan sehen. Dies ist hilfreich bei der Entscheidung, wie VMs in einer Ressourcengruppe zusammengefasst werden sollen.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

VM-Namensaliasing

Wenn Sie einen Replikationsplan erstellen, können Sie den VM-Namen auf der Disaster-Recovery-Site jetzt ein Präfix und ein Suffix hinzufügen. Dadurch können Sie für die VMs im Plan einen aussagekräftigeren Namen verwenden.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Bereinigen Sie alte Snapshots

Sie können alle Snapshots löschen, die Sie nach der von Ihnen angegebenen Aufbewahrungsdauer nicht mehr benötigen. Wenn Sie die Anzahl der Snapshot-Aufbewahrungen verringern, können sich mit der Zeit Snapshots ansammeln. Sie können diese jetzt entfernen, um Speicherplatz freizugeben. Sie können dies jederzeit bei Bedarf oder beim Löschen eines Replikationsplans tun.

Weitere Einzelheiten finden Sie unter "Verwalten Sie Sites, Ressourcengruppen, Replikationspläne, Datenspeicher und Informationen zu virtuellen Maschinen" .

Snapshots abgleichen

Sie können jetzt Snapshots abgleichen, die zwischen Quelle und Ziel nicht synchron sind. Dies kann auftreten, wenn Snapshots auf einem Ziel außerhalb von NetApp Disaster Recovery gelöscht werden. Der Dienst löscht

den Snapshot auf der Quelle automatisch alle 24 Stunden. Sie können dies jedoch auf Anfrage durchführen. Mit dieser Funktion können Sie sicherstellen, dass die Snapshots auf allen Sites konsistent sind.

Weitere Einzelheiten finden Sie unter "Verwalten von Replikationsplänen" .

20. September 2024

Unterstützung für lokale VMware VMFS-Datenspeicher

Diese Version umfasst Unterstützung für VMs, die auf VMware vSphere Virtual Machine File System (VMFS)-Datenspeichern für iSCSI und FC gemountet sind und auf lokalem Speicher geschützt sind. Zuvor bot der Dienst eine *Technologievorschau*, die VMFS-Datenspeicher für iSCSI und FC unterstützte.

Hier sind einige zusätzliche Überlegungen zu den iSCSI- und FC-Protokollen:

- FC-Unterstützung gilt für Client-Front-End-Protokolle, nicht für die Replikation.
- NetApp Disaster Recovery unterstützt nur eine einzige LUN pro ONTAP -Volume. Das Volume sollte nicht mehrere LUNs haben.
- Für jeden Replikationsplan sollte das Ziel ONTAP -Volume dieselben Protokolle verwenden wie das Quell ONTAP -Volume, auf dem die geschützten VMs gehostet werden. Wenn die Quelle beispielsweise ein FC-Protokoll verwendet, sollte das Ziel auch FC verwenden.

02. August 2024

Unterstützung für lokale VMware VMFS-Datenspeicher für FC

Diese Version enthält eine *Technologievorschau* der Unterstützung für VMs, die auf VMware vSphere Virtual Machine File System (VMFS)-Datenspeichern für FC gemountet sind, die auf lokalem Speicher geschützt sind. Zuvor bot der Dienst eine Technologievorschau, die VMFS-Datenspeicher für iSCSI unterstützte.

NetApp berechnet Ihnen keine Kosten für die in der Vorschau angezeigte Workload-Kapazität.

Job abbrechen

Mit dieser Version können Sie jetzt einen Job in der Job Monitor-Benutzeroberfläche abbrechen.

Siehe "Überwachen von Jobs" .

17. Juli 2024

Failover-Testpläne

Diese Version enthält Aktualisierungen der Failover-Testplanstruktur, die zur Unterstützung täglicher und wöchentlicher Zeitpläne erforderlich waren. Dieses Update erfordert, dass Sie alle vorhandenen Replikationspläne deaktivieren und erneut aktivieren, damit Sie die neuen täglichen und wöchentlichen Failover-Testpläne verwenden können. Dies ist eine einmalige Anforderung.

So geht’s:

1. Wählen Sie im Menü **Replikationspläne** aus.
2. Wählen Sie einen Plan aus und klicken Sie auf das Symbol „Aktionen“, um das Dropdown-Menü anzuzeigen.

3. Wählen Sie **Deaktivieren**.
4. Wählen Sie nach einigen Minuten **Aktivieren**.

Aktualisierungen des Replikationsplans

Diese Version enthält Aktualisierungen der Replikationsplandaten, die das Problem „Snapshot nicht gefunden“ beheben. Dazu müssen Sie die Aufbewahrungsanzahl in allen Replikationsplänen auf 1 ändern und einen On-Demand-Snapshot initiieren. Dieser Vorgang erstellt ein neues Backup und entfernt alle älteren Backups.

So geht’s:

1. Wählen Sie im Menü **Replikationspläne** aus.
2. Wählen Sie den Replikationsplan aus, klicken Sie auf die Registerkarte **Failover-Zuordnung** und dann auf das Bleistiftsymbol **Bearbeiten**.
3. Klicken Sie auf den Pfeil **Datenspeicher**, um ihn zu erweitern.
4. Notieren Sie den Wert der Aufbewahrungsanzahl im Replikationsplan. Sie müssen diesen ursprünglichen Wert wiederherstellen, wenn Sie mit diesen Schritten fertig sind.
5. Reduzieren Sie die Anzahl auf 1.
6. Starten Sie einen On-Demand-Snapshot. Wählen Sie dazu auf der Seite „Replikationsplan“ den Plan aus, klicken Sie auf das Symbol „Aktionen“ und wählen Sie „Jetzt Snapshot erstellen“ aus.
7. Nachdem der Snapshot-Job erfolgreich abgeschlossen wurde, erhöhen Sie die Anzahl im Replikationsplan wieder auf den ursprünglichen Wert, den Sie im ersten Schritt notiert haben.
8. Wiederholen Sie diese Schritte für alle vorhandenen Replikationspläne.

05. Juli 2024

Diese NetApp Disaster Recovery -Version enthält die folgenden Updates:

Unterstützung für AFF A-Serie

Diese Version unterstützt die Hardwareplattformen der NetApp AFF A-Serie.

Unterstützung für lokale VMware VMFS-Datenspeicher

Diese Version enthält eine *Technologievorschau* der Unterstützung für VMs, die auf VMware vSphere Virtual Machine File System (VMFS)-Datenspeichern gemountet sind, die auf lokalem Speicher geschützt sind. Mit dieser Version wird die Notfallwiederherstellung in einer Technologievorschau für lokale VMware-Workloads in einer lokalen VMware-Umgebung mit VMFS-Datenspeichern unterstützt.

NetApp berechnet Ihnen keine Kosten für die in der Vorschau angezeigte Workload-Kapazität.

Aktualisierungen des Replikationsplans

Sie können einen Replikationsplan einfacher hinzufügen, indem Sie VMs auf der Seite „Anwendungen“ nach Datenspeicher filtern und auf der Seite „Ressourcenzuordnung“ weitere Zieldetails auswählen. Siehe "Erstellen eines Replikationsplans" .

Replikationspläne bearbeiten

Mit dieser Version wurde die Seite „Failover-Zuordnungen“ zur besseren Übersichtlichkeit verbessert.

Siehe "Pläne verwalten" .

VMs bearbeiten

Mit dieser Version wurden beim Bearbeiten von VMs im Plan einige kleinere Verbesserungen der Benutzeroberfläche vorgenommen.

Siehe "Verwalten von VMs" .

Failover-Updates

Bevor Sie ein Failover einleiten, können Sie jetzt den Status der VMs ermitteln und feststellen, ob sie ein- oder ausgeschaltet sind. Der Failover-Prozess ermöglicht es Ihnen nun, sofort einen Snapshot zu erstellen oder die Snapshots auszuwählen.

Siehe "Failover von Anwendungen auf einen Remote-Standort" .

Failover-Testpläne

Sie können jetzt die Failover-Tests bearbeiten und tägliche, wöchentliche und monatliche Zeitpläne für den Failover-Test festlegen.

Siehe "Pläne verwalten" .

Aktualisierungen der erforderlichen Informationen

Die Informationen zu den Voraussetzungen für NetApp Disaster Recovery wurden aktualisiert.

Siehe "Voraussetzungen für NetApp Disaster Recovery" .

15. Mai 2024

Diese NetApp Disaster Recovery -Version enthält die folgenden Updates:

Replizieren von VMware-Workloads von On-Premises zu On-Premises

Dies wird jetzt als allgemein verfügbare Funktion veröffentlicht. Zuvor handelte es sich um eine Technologievorschau mit eingeschränkter Funktionalität.

Lizenzierungsupdates

Bei NetApp Disaster Recovery können Sie sich für eine kostenlose 90-Tage-Testversion anmelden, ein Pay-as-you-go-Abonnement (PAYGO) bei Amazon Marketplace erwerben oder Ihre eigene Lizenz (BYOL) mitbringen. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter oder von der NetApp -Support-Site (NSS) erhalten.

Einzelheiten zum Einrichten der Lizenzierung für NetApp Disaster Recovery finden Sie unter"Einrichten der Lizenzierung" .

"Erfahren Sie mehr über NetApp Disaster Recovery" .

05. März 2024

Dies ist die allgemein verfügbare Version von NetApp Disaster Recovery, die die folgenden Updates enthält.

Lizenzierungsupdates

Bei NetApp Disaster Recovery können Sie sich für eine kostenlose 90-Tage-Testversion anmelden oder Ihre eigene Lizenz (BYOL) mitbringen. Dabei handelt es sich um eine NetApp -Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL in den NetApp Console -Abonnements zu aktivieren. Die Gebühren für NetApp Disaster Recovery basieren auf der bereitgestellten Kapazität der Datenspeicher.

Einzelheiten zum Einrichten der Lizenzierung für NetApp Disaster Recovery finden Sie unter "Einrichten der Lizenzierung" .

Weitere Informationen zur Verwaltung von Lizenzen für **alle** NetApp Console -Datendienste finden Sie unter "Verwalten Sie Lizenzen für alle NetApp Console Datendienste" .

Zeitpläne bearbeiten

Mit dieser Version können Sie jetzt Zeitpläne zum Testen von Konformitäts- und Failover-Tests einrichten, um sicherzustellen, dass sie bei Bedarf ordnungsgemäß funktionieren.

Weitere Einzelheiten finden Sie unter "Erstellen des Replikationsplans" .

01. Februar 2024

Diese Vorschauversion von NetApp Disaster Recovery enthält die folgenden Updates:

Netzwerkerweiterung

Mit dieser Version können Sie jetzt die Größe der VM-CPU- und RAM-Werte ändern. Sie können jetzt auch eine Netzwerk-DHCP- oder statische IP-Adresse für die VM auswählen.

- DHCP: Wenn Sie diese Option wählen, geben Sie Anmeldeinformationen für die VM an.
- Statische IP: Sie können dieselben oder andere Informationen aus der Quell-VM auswählen. 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, die Subnetzmaske, DNS und Gateway-Informationen angeben.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Benutzerdefinierte Skripte

Können jetzt als Prozesse nach dem Failover einbezogen werden. Mit benutzerdefinierten Skripten können Sie NetApp Disaster Recovery Ihr Skript nach einem Failover-Prozess ausführen lassen. Sie können beispielsweise ein benutzerdefiniertes Skript verwenden, um alle Datenbanktransaktionen nach Abschluss des Failovers fortzusetzen.

Weitere Einzelheiten finden Sie unter "Failover zu einem Remotestandort" .

SnapMirror -Beziehung

Sie können jetzt beim Entwickeln des Replikationsplans eine SnapMirror -Beziehung erstellen. Bisher mussten

Sie die Beziehung außerhalb von NetApp Disaster Recovery erstellen.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Konsistenzgruppen

Wenn Sie einen Replikationsplan erstellen, können Sie VMs aus unterschiedlichen Volumes und unterschiedlichen SVMs einschließen. NetApp Disaster Recovery erstellt einen Consistency Group Snapshot, indem es alle Volumes einbezieht und alle sekundären Standorte aktualisiert.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Option zur VM-Einschaltverzögerung

Wenn Sie einen Replikationsplan erstellen, können Sie VMs zu einer Ressourcengruppe hinzufügen. Mit Ressourcengruppen können Sie für jede VM eine Verzögerung festlegen, sodass sie in einer verzögerten Reihenfolge hochgefahren werden.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

Anwendungskonsistente Snapshot-Kopien

Sie können angeben, dass 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.

Weitere Einzelheiten finden Sie unter "Erstellen eines Replikationsplans" .

11. Januar 2024

Diese Vorschauversion von NetApp Disaster Recovery enthält die folgenden Updates:

Schneller Dashboard

Mit dieser Version können Sie vom Dashboard aus schneller auf Informationen auf anderen Seiten zugreifen.

"Erfahren Sie mehr über NetApp Disaster Recovery" .

20. Oktober 2023

Diese Vorabversion von NetApp Disaster Recovery enthält die folgenden Updates.

Schützen Sie lokale, NFS-basierte VMware-Workloads

Mit NetApp Disaster Recovery können Sie jetzt Ihre lokalen, NFS-basierten VMware-Workloads zusätzlich zur öffentlichen Cloud vor Katastrophen in einer anderen lokalen, NFS-basierten VMware-Umgebung schützen. NetApp Disaster Recovery orchestriert die Durchführung der Notfallwiederherstellungspläne.

Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

"Erfahren Sie mehr über NetApp Disaster Recovery" .

27. September 2023

Diese Vorschauversion von NetApp Disaster Recovery enthält die folgenden Updates:

Dashboard-Updates

Sie können jetzt auf die Optionen im Dashboard klicken, was Ihnen die schnelle Überprüfung der Informationen erleichtert. Außerdem zeigt das Dashboard jetzt den Status von Failovers und Migrationen an.

Siehe "Sehen Sie sich den Zustand Ihrer Notfallwiederherstellungspläne auf dem Dashboard an" .

Aktualisierungen des Replikationsplans

- **RPO**: Sie können jetzt das Recovery Point Objective (RPO) und die Aufbewahrungsanzahl im Abschnitt „Datenspeicher“ des Replikationsplans eingeben. Dies gibt die Menge an Daten an, die vorhanden sein müssen und nicht älter als die eingestellte Zeit sind. Wenn Sie ihn beispielsweise auf 5 Minuten einstellen, kann das System im Katastrophenfall bis zu 5 Minuten Daten verlieren, ohne dass geschäftskritische Anforderungen beeinträchtigt werden.

  Siehe "Erstellen eines Replikationsplans" .

- **Netzwerkverbesserungen**: Wenn Sie im Abschnitt „Virtuelle Maschinen“ des Replikationsplans das Netzwerk zwischen Quell- und Zielstandorten zuordnen, bietet NetApp Disaster Recovery jetzt zwei Optionen: DHCP oder statische IP. Bisher wurde nur DHCP unterstützt. Für statische IPs konfigurieren Sie das Subnetz, das Gateway und die DNS-Server. Darüber hinaus können Sie jetzt Anmeldeinformationen für virtuelle Maschinen eingeben.

  Siehe "Erstellen eines Replikationsplans" .

- **Zeitpläne bearbeiten**: Sie können jetzt Zeitpläne für Replikationspläne aktualisieren.

  Siehe "Ressourcen verwalten" .

- * SnapMirror Automatisierung*: Während Sie in dieser Version den Replikationsplan erstellen, können Sie die SnapMirror Beziehung zwischen Quell- und Zielvolumes in einer der folgenden Konfigurationen definieren:
  - 1 bis 1
  - 1 zu viele in einer Fanout-Architektur
  - Viele zu 1 als Konsistenzgruppe
  - Viele zu viele

    Siehe "Erstellen eines Replikationsplans" .

01. August 2023

NetApp Disaster Recovery -Vorschau

NetApp Disaster Recovery Preview ist ein Cloud-basierter Disaster Recovery-Dienst, der Disaster Recovery-Workflows automatisiert. Mit der Vorschau von NetApp Disaster Recovery können Sie zunächst Ihre lokalen, NFS-basierten VMware-Workloads, auf denen NetApp -Speicher ausgeführt wird, mit Amazon FSx für ONTAP in VMware Cloud (VMC) auf AWS schützen.

Bei diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitplan vor der allgemeinen Verfügbarkeit zu ändern.

"Erfahren Sie mehr über NetApp Disaster Recovery" .

Diese Version enthält die folgenden Updates:

Ressourcengruppen-Update für die Startreihenfolge

Wenn Sie einen Notfallwiederherstellungs- oder Replikationsplan erstellen, können Sie virtuelle Maschinen zu funktionalen Ressourcengruppen hinzufügen. Mithilfe von Ressourcengruppen können Sie eine Reihe abhängiger virtueller Maschinen in logische Gruppen einteilen, die Ihren Anforderungen entsprechen. Beispielsweise könnten Gruppen eine Startreihenfolge enthalten, die bei der Wiederherstellung ausgeführt werden kann. Mit dieser Version kann jede Ressourcengruppe eine oder mehrere virtuelle Maschinen enthalten. Die virtuellen Maschinen werden basierend auf der Reihenfolge eingeschaltet, in der Sie sie in den Plan aufnehmen. Siehe "Auswählen von Anwendungen zum Replizieren und Zuweisen von Ressourcengruppen" .

Replikationsüberprüfung

Nachdem Sie den Disaster Recovery- oder Replikationsplan erstellt, die Wiederholung im Assistenten identifiziert und eine Replikation zu einem Disaster Recovery-Standort 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. Weitere Informationen finden Sie unter "Replizieren von Anwendungen auf eine andere Site" .

Der Replikationsplan zeigt die Übertragungspläne für das Recovery Point Objective (RPO)

Wenn Sie einen Notfallwiederherstellungs- oder Replikationsplan erstellen, wählen Sie die VMs aus. In dieser Version können Sie jetzt den SnapMirror anzeigen, der mit jedem der Volumes verknüpft ist, die mit dem Datenspeicher oder der VM verknüpft sind. Sie können auch die RPO-Übertragungspläne sehen, die mit dem SnapMirror -Zeitplan verknüpft sind. Mithilfe von RPO können Sie feststellen, ob Ihr Sicherungsplan für die Wiederherstellung nach einem Notfall ausreicht. Siehe "Erstellen eines Replikationsplans" .

Job Monitor-Update

Die Seite „Job Monitor“ enthält jetzt eine Aktualisierungsoption, sodass Sie einen aktuellen Status der Vorgänge erhalten. Weitere Informationen finden Sie unter "Überwachen von Disaster Recovery-Jobs" .

18. Mai 2023

Dies ist die Erstveröffentlichung von NetApp Disaster Recovery.

Cloudbasierter Disaster-Recovery-Dienst

NetApp Disaster Recovery ist ein Cloud-basierter Disaster-Recovery-Dienst, der Disaster-Recovery-Workflows automatisiert. Mit der Vorschau von NetApp Disaster Recovery können Sie zunächst Ihre lokalen, NFS-basierten VMware-Workloads, auf denen NetApp -Speicher ausgeführt wird, mit Amazon FSx für ONTAP in VMware Cloud (VMC) auf AWS schützen.

"Erfahren Sie mehr über NetApp Disaster Recovery" .

Einschränkungen bei der NetApp Disaster Recovery

Bekannte Einschränkungen identifizieren Plattformen, Geräte oder Funktionen, die von dieser Version des Dienstes nicht unterstützt werden oder nicht ordnungsgemäß mit ihm zusammenarbeiten.

Warten Sie, bis das Failback abgeschlossen ist, bevor Sie die Erkennung ausführen

Starten Sie nach Abschluss eines Failovers die Erkennung im Quell-vCenter nicht manuell. Warten Sie, bis das Failback abgeschlossen ist, und starten Sie dann die Erkennung im Quell-vCenter.

Die NetApp Console erkennt Amazon FSx for NetApp ONTAP möglicherweise nicht

Manchmal erkennt die NetApp Console Amazon FSx for NetApp ONTAP -Cluster nicht. Dies kann daran liegen, dass die FSx-Anmeldeinformationen nicht korrekt waren.

Problemumgehung: Fügen Sie den Amazon FSx for NetApp ONTAP -Cluster in der NetApp Console hinzu und aktualisieren Sie den Cluster regelmäßig, um alle Änderungen anzuzeigen.

Wenn Sie den ONTAP FSx-Cluster aus NetApp Disaster Recovery entfernen müssen, führen Sie die folgenden Schritte aus:

1. Verwenden Sie im NetApp Console Agent die Konnektivitätsoptionen Ihres Cloud-Anbieters, stellen Sie eine Verbindung zur Linux-VM her, auf der der Console-Agent ausgeführt wird, und starten Sie den Dienst "occm" mithilfe des `docker restart occm` Befehl.

Siehe "Vorhandene Konsolenagenten verwalten" .

1. Fügen Sie auf der Seite „NetApp Console Systems“ das Amazon FSx for ONTAP -System erneut hinzu und geben Sie die FSx-Anmeldeinformationen ein.

   Siehe "Erstellen Sie ein Amazon FSx for NetApp ONTAP -Dateisystem" .

2. Wählen Sie in NetApp Disaster Recovery*Sites* aus und wählen Sie in der vCenter-Zeile die Option *Actions* , und wählen Sie im Menü „Aktionen“ die Option „Aktualisieren“ aus, um die FSx-Erkennung in NetApp Disaster Recovery zu aktualisieren.

   Dadurch werden der Datenspeicher, seine virtuellen Maschinen und seine Zielbeziehung neu erkannt.

Erste Schritte

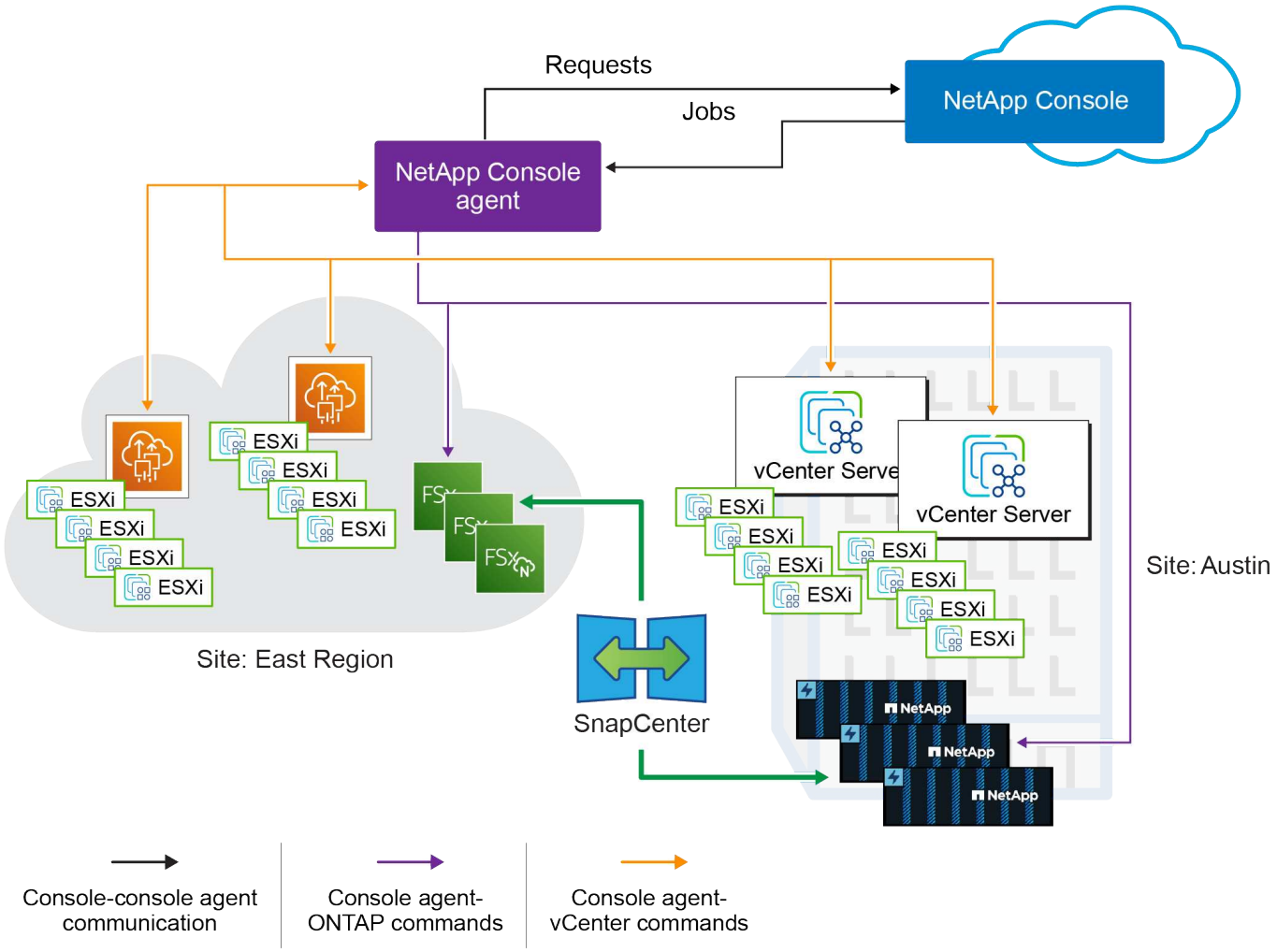
Erfahren Sie mehr über NetApp Disaster Recovery für VMware

Die Notfallwiederherstellung in der Cloud ist eine robuste und kostengünstige Möglichkeit, Workloads vor Standortausfällen und Datenbeschädigungen zu schützen. Mit NetApp Disaster Recovery für VMware können Sie Ihre lokalen VMware-VM- oder Datastore-Workloads mit ONTAP -Speicher in ein softwaredefiniertes VMware-Rechenzentrum in einer öffentlichen Cloud mit NetApp Cloud-Speicher oder in eine andere lokale VMware-Umgebung mit ONTAP -Speicher als Disaster-Recovery-Site replizieren. Sie können Disaster Recovery auch verwenden, um VM-Workloads von einem Standort zu einem anderen zu migrieren.

NetApp Disaster Recovery ist ein Cloud-basierter Disaster-Recovery-Dienst, der Disaster-Recovery-Workflows automatisiert. Mit NetApp Disaster Recovery können Sie Ihre lokalen, NFS-basierten Workloads und VMware vSphere Virtual Machine File System (VMFS)-Datenspeicher für iSCSI und FC mit NetApp -Speicher auf einem der folgenden Systeme schützen:

- VMware Cloud (VMC) auf AWS mit Amazon FSx for NetApp ONTAP
- Amazon Elastic VMware Service (EVS) mit Amazon FSx for NetApp ONTAP Weitere Informationen finden Sie unter"Einführung von NetApp Disaster Recovery mit Amazon Elastic VMware Service und Amazon FSx for NetApp ONTAP" .
- Azure VMware Solution (AVS) mit NetApp Cloud Volumes ONTAP (iSCSI) (Private Vorschau)
- Eine weitere lokale NFS- und/oder VMFS-basierte (iSCSI/FC) VMware-Umgebung mit ONTAP Speicher

NetApp Disaster Recovery verwendet die ONTAP SnapMirror -Technologie mit integrierter nativer VMware-Orchestrierung, um VMware-VMs und die zugehörigen On-Disk-Betriebssystemimages zu schützen und gleichzeitig alle Speichereffizienzvorteile von ONTAP beizubehalten. Disaster Recovery verwendet diese Technologien als Replikationstransport zum Disaster Recovery-Standort. Dies ermöglicht die branchenweit beste Speichereffizienz (Komprimierung und Deduplizierung) an primären und sekundären Standorten.



NetApp Console

Auf NetApp Disaster Recovery kann über die NetApp Console zugegriffen werden.

Die NetApp Console ermöglicht eine zentrale Verwaltung von NetApp -Speicher- und Datendiensten in lokalen und Cloud-Umgebungen auf Unternehmensebene. Die Konsole ist für den Zugriff auf und die Nutzung der NetApp -Datendienste erforderlich. Als Verwaltungsschnittstelle ermöglicht es Ihnen, viele Speicherressourcen über eine Schnittstelle zu verwalten. Konsolenadministratoren können den Zugriff auf Speicher und Dienste für alle Systeme innerhalb des Unternehmens steuern.

Sie benötigen weder eine Lizenz noch ein Abonnement, um die NetApp Console zu verwenden. Es fallen nur dann Kosten an, wenn Sie Konsolenagenten in Ihrer Cloud bereitstellen müssen, um die Konnektivität zu Ihren Speichersystemen oder NetApp -Datendiensten sicherzustellen. Einige NetApp -Datendienste, auf die über die Konsole zugegriffen werden kann, sind jedoch lizenz- oder abonnementbasiert.

Erfahren Sie mehr über die "NetApp Console" .

Vorteile der Verwendung von NetApp Disaster Recovery für VMware

NetApp Disaster Recovery bietet die folgenden Vorteile:

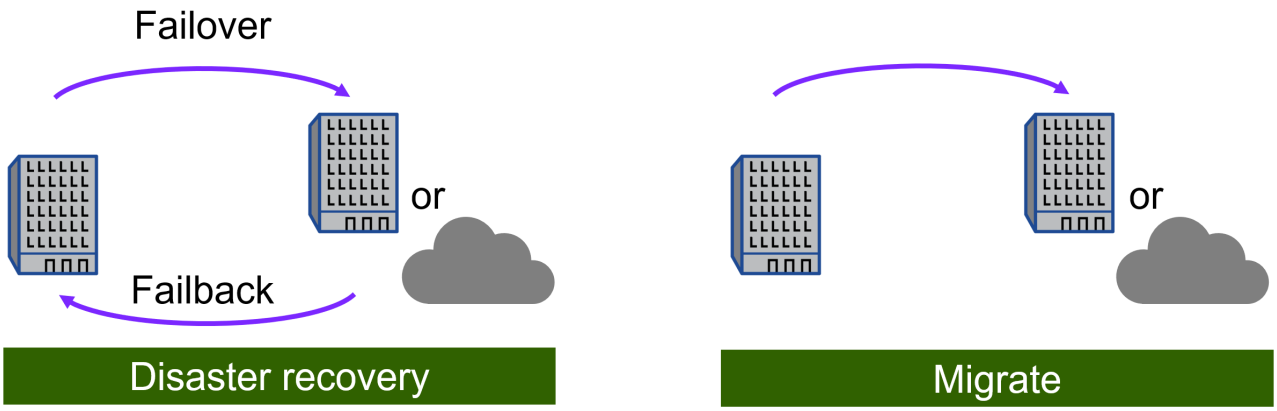
- Vereinfachte Benutzererfahrung für die vCenter-Erkennung und -Wiederherstellung von Anwendungen mit mehreren zeitpunktbezogenen Wiederherstellungsvorgängen.

- Niedrigere Gesamtbetriebskosten durch reduzierte Betriebskosten und die Möglichkeit, Notfallwiederherstellungspläne mit minimalem Ressourcenaufwand zu erstellen und anzupassen.
- Kontinuierliche Notfallwiederherstellungsbereitschaft mit virtuellen Failover-Tests, die den Betrieb nicht unterbrechen. Sie können Ihre DR-Failover-Pläne regelmäßig testen, ohne die Produktionsarbeitslast zu beeinträchtigen.
- Schnellere Wertschöpfung durch dynamische Änderungen in Ihrer IT-Umgebung und die Möglichkeit, diese in Ihren Notfallwiederherstellungsplänen zu berücksichtigen.
- Möglichkeit, sowohl die Speicher- als auch die virtuellen Ebenen durch Backend-Orchestrierung von ONTAP und VMware gleichzeitig zu verwalten, ohne dass virtuelle Server-Appliances (VSAs) bereitgestellt und gewartet werden müssen.
- DR-Lösungen für VMware können ressourcenintensiv sein. Viele DR-Lösungen replizieren VMs auf der virtuellen VMware-Ebene mithilfe von VSAs, was mehr Rechenressourcen verbrauchen und zu einem Verlust der wertvollen Speichereffizienz von ONTAP führen kann. Da Disaster Recovery die ONTAP SnapMirror -Technologie verwendet, kann es mithilfe unseres inkrementellen Replikationsmodells mit allen nativen Datenkomprimierungs- und Deduplizierungseffizienzen von ONTAP Daten von Produktionsdatenspeichern zum DR-Standort replizieren.

Was Sie mit NetApp Disaster Recovery für VMware tun können

NetApp Disaster Recovery bietet Ihnen die volle Nutzung mehrerer NetApp -Technologien, um die folgenden Ziele zu erreichen:

- Replizieren Sie VMware-Apps auf Ihrem lokalen Produktionsstandort mithilfe der SnapMirror -Replikation an einen Remote-Standort zur Notfallwiederherstellung in der Cloud oder vor Ort.
- Migrieren Sie VMware-Workloads von Ihrem ursprünglichen Standort zu einem anderen Standort.
- Führen Sie einen Failover-Test durch. Wenn Sie dies tun, erstellt der Dienst temporäre virtuelle Maschinen. Disaster Recovery erstellt aus dem ausgewählten Snapshot ein neues FlexClone Volume und ein temporärer Datenspeicher, der durch das FlexClone -Volume gesichert ist, wird den ESXi-Hosts zugeordnet. Dieser Prozess verbraucht keine zusätzliche physische Kapazität auf dem lokalen ONTAP -Speicher oder FSx für NetApp ONTAP -Speicher in AWS. Das ursprüngliche Quellvolume wird nicht geändert und Replikationsaufträge können auch während der Notfallwiederherstellung fortgesetzt werden.
- Führen Sie im Katastrophenfall bei Bedarf ein Failover Ihres primären Standorts auf den Disaster Recovery-Standort durch. Dabei kann es sich um VMware Cloud auf AWS mit Amazon FSx for NetApp ONTAP oder eine lokale VMware-Umgebung mit ONTAP handeln.
- Nachdem der Notfall behoben wurde, führen Sie bei Bedarf ein Failback vom Notfallwiederherstellungsstandort zum primären Standort durch.
- Gruppieren Sie VMs oder Datenspeicher für eine effiziente Verwaltung in logische Ressourcengruppen.



Die Konfiguration des vSphere-Servers erfolgt außerhalb von NetApp Disaster Recovery im vSphere-Server.

Kosten

NetApp berechnet Ihnen für die Nutzung der Testversion von NetApp Disaster Recovery keine Gebühren.

NetApp Disaster Recovery kann entweder mit einer NetApp -Lizenz oder einem jährlichen Abonnementplan über Amazon Web Services verwendet werden.

Einige Versionen enthalten eine Technologievorschau. NetApp berechnet Ihnen keine Kosten für die in der Vorschau angezeigte Workload-Kapazität. Sehen"Was ist neu bei NetApp Disaster Recovery ?" für Informationen zu den neuesten Technologievorschauen.

Lizenzierung

Sie können die folgenden Lizenztypen verwenden:

- Melden Sie sich für eine 30-tägige kostenlose Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) über den Amazon Web Services (AWS) Marketplace oder den Microsoft Azure Marketplace. Mit dieser Lizenz können Sie eine Lizenz mit fester, geschützter Kapazität ohne langfristige Bindung erwerben.
- Bringen Sie Ihre eigene Lizenz (BYOL) mit. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL in der NetApp Console zu aktivieren.

Lizenzen für alle NetApp -Datendienste werden über Abonnements in der NetApp Console verwaltet. Nachdem Sie Ihr BYOL eingerichtet haben, können Sie in der Konsole eine aktive Lizenz für den Dienst sehen.

Die Lizenzierung des Dienstes erfolgt auf Grundlage der auf geschützten ONTAP Volumes gehosteten Datenmenge. Der Dienst ermittelt, welche Volumes für Lizenzierungszwecke berücksichtigt werden sollten, indem er geschützte VMs ihren vCenter-Datenspeichern zuordnet. Jeder Datenspeicher wird auf einem ONTAP Volume oder LUN gehostet. Die von ONTAP für dieses Volume oder LUN gemeldete genutzte Kapazität wird für Lizenzierungsbestimmungen verwendet.

Geschützte Volumes können viele VMs hosten. Einige sind möglicherweise nicht Teil einer NetApp Disaster Recovery -Ressourcengruppe. Unabhängig davon wird der von allen VMs auf diesem Volume oder LUN verbrauchte Speicher auf die maximale Lizenzkapazität angerechnet.

> Die Gebühren für NetApp Disaster Recovery basieren auf der genutzten Kapazität der Datenspeicher am Quellstandort, wenn mindestens eine VM über einen Replikationsplan verfügt. Die Kapazität für einen ausgefallenen Datenspeicher ist nicht in der Kapazitätszuteilung enthalten. Wenn bei einem BYOL die Daten die zulässige Kapazität überschreiten, sind die Vorgänge im Dienst eingeschränkt, bis Sie eine zusätzliche Kapazitätslizenz erwerben oder die Lizenz in der NetApp Console aktualisieren.

Einzelheiten zum Einrichten der Lizenzierung für NetApp Disaster Recovery finden Sie unter"Einrichten der NetApp Disaster Recovery -Lizenzierung" .

30 Tage kostenlos testen

Sie können NetApp Disaster Recovery mit einer 30-tägigen kostenlosen Testversion ausprobieren.

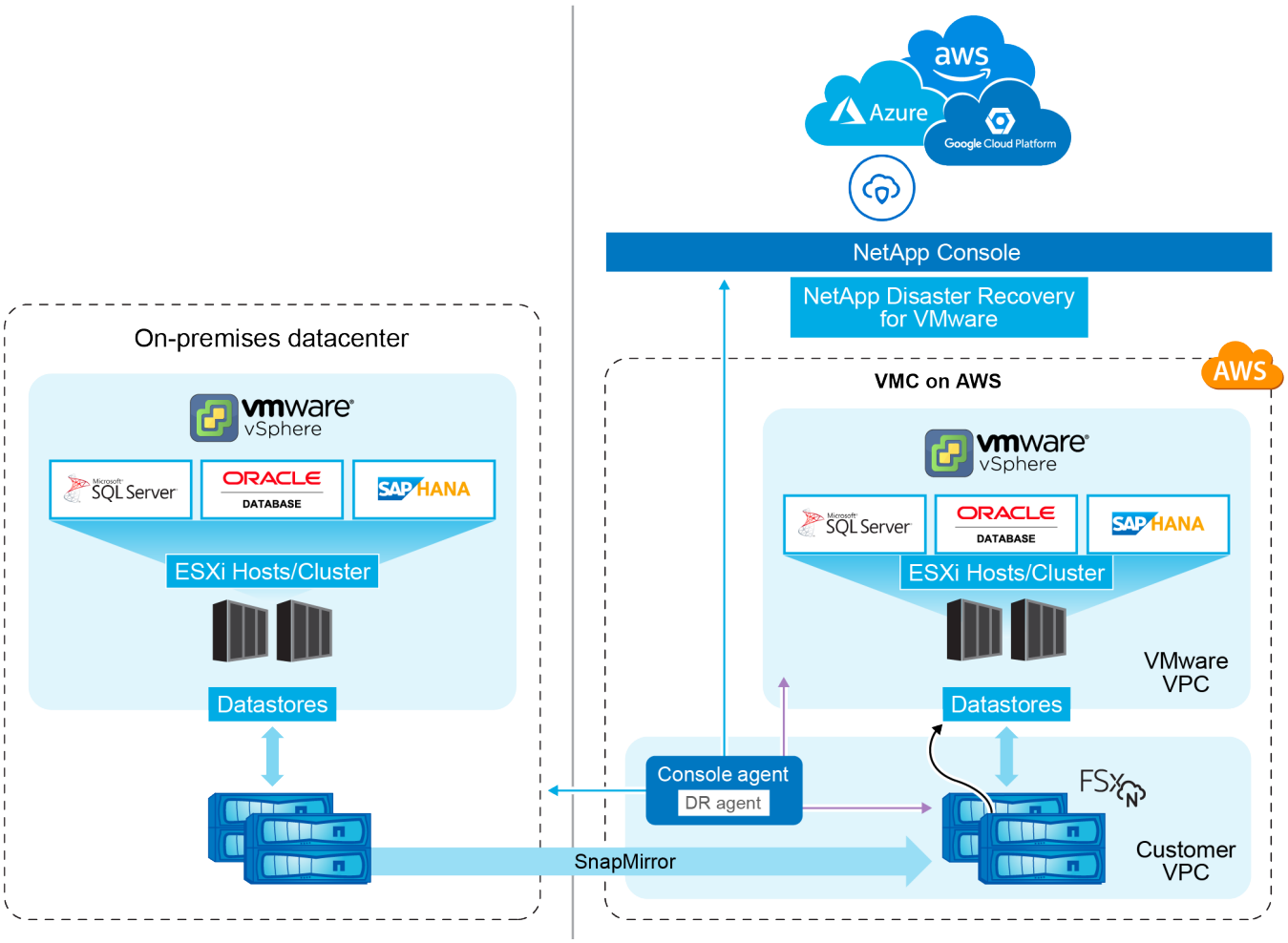
Um nach der 30-tägigen Testphase fortzufahren, müssen Sie ein Pay-as-you-go-Abonnement (PAYGO) von Ihrem Cloud-Anbieter erwerben oder eine BYOL-Lizenz von NetApp kaufen.

Sie können jederzeit eine Lizenz erwerben und es fallen erst nach Ablauf der 30-tägigen Testphase Kosten für Sie an.

So funktioniert NetApp Disaster Recovery

NetApp Disaster Recovery ist ein Dienst, der in der NetApp Console -Software als Serviceumgebung (SaaS) gehostet wird. Disaster Recovery kann Workloads wiederherstellen, die von einem lokalen Standort auf Amazon FSx for ONTAP oder einen anderen lokalen Standort repliziert wurden. Dieser Service automatisiert die Wiederherstellung von der SnapMirror -Ebene über die Registrierung virtueller Maschinen in VMware Cloud auf AWS bis hin zu Netzwerkzuordnungen direkt auf der VMware-Netzwerkvirtualisierungs- und Sicherheitsplattform NSX-T. Diese Funktion ist in allen Virtual Machine Cloud-Umgebungen enthalten.

NetApp Disaster Recovery verwendet die ONTAP SnapMirror -Technologie, die eine hocheffiziente Replikation ermöglicht und die Effizienz der inkrementellen Snapshots von ONTAP für immer bewahrt. Die SnapMirror Replikation stellt sicher, dass anwendungskonsistente Snapshot-Kopien immer synchron sind und die Daten nach einem Failover sofort nutzbar sind.



Im Katastrophenfall unterstützt Sie dieser Dienst bei der Wiederherstellung virtueller Maschinen in der anderen lokalen VMware-Umgebung oder VMC, indem er die SnapMirror -Beziehungen auflöst und die Zielsite aktiviert.

- Mit dem Dienst können Sie außerdem ein Failback virtueller Maschinen auf den ursprünglichen Quellspeicherort durchführen.
- Sie können den Failover-Prozess für die Notfallwiederherstellung testen, ohne die ursprünglichen virtuellen Maschinen zu unterbrechen. Der Test stellt virtuelle Maschinen in einem isolierten Netzwerk wieder her, indem ein FlexClone des Volumes erstellt wird.
- Für den Failover- oder Test-Failover-Prozess können Sie den neuesten (Standard) oder ausgewählten Snapshot auswählen, von dem aus Ihre virtuelle Maschine wiederhergestellt werden soll.

Komponenten der Notfallwiederherstellung

Disaster Recovery verwendet die folgenden Komponenten, um die Notfallwiederherstellung für VMware-Workloads bereitzustellen:

- * NetApp Console*: Die Benutzeroberfläche zum Verwalten Ihrer Notfallwiederherstellungspläne. Mit der NetApp Console können Sie Replikationspläne, Ressourcengruppen und Failover-Vorgänge in Ihren lokalen und Cloud-Umgebungen erstellen und verwalten.
- **Konsolenagent**: Eine leichtgewichtige Softwarekomponente, die in Ihrem Cloud-gehosteten Netzwerk oder Ihrer lokalen VMware-Umgebung ausgeführt wird. Es kommuniziert mit der NetApp Console und verwaltet die Datenreplikation zwischen Ihrer lokalen Umgebung und dem Disaster-Recovery-Standort. Der Konsolenagent wird auf einer virtuellen Maschine in Ihrer VMware-Umgebung installiert.

- * ONTAP -Speichercluster*: Die ONTAP -Speichercluster sind die primären Speichersysteme, die Ihre VMware-Workloads hosten. Die ONTAP Speichercluster stellen die zugrunde liegende Speicherinfrastruktur für Ihre Notfallwiederherstellungspläne bereit. Disaster Recovery verwendet ONTAP Speicher-APIs zum Verwalten von ONTAP Speicherclustern wie lokalen Arrays und Cloud-basierten Lösungen wie Amazon FSx for NetApp ONTAP.
- **vCenter-Server**: Das VMware vCenter ist der Verwaltungsserver für Ihre VMware-Umgebung. Es verwaltet die ESXi-Hosts und die zugehörigen Datenspeicher. Der Konsolenagent kommuniziert mit dem VMware vCenter, um die Datenreplikation zwischen Ihrer lokalen Umgebung und dem Notfallwiederherstellungsstandort zu verwalten. Dazu gehört das Registrieren von ONTAP -LUNs und -Volumes als Datenspeicher, das Neukonfigurieren von VMs sowie das Starten und Stoppen von VMs.

Der Disaster Recovery-Schutz-Workflow

Wenn einer Ressourcengruppe ein Replikationsplan zugewiesen wird, führt Disaster Recovery eine Erkennungsprüfung aller Komponenten in der Ressourcengruppe und im Plan durch, um sicherzustellen, dass der Plan aktiviert werden kann.

Wenn diese Prüfung erfolgreich ist, führt Disaster Recovery die folgenden Initialisierungsschritte durch:

1. Identifizieren Sie für jede VM in der Zielressourcengruppe den VMware-Hostdatenspeicher.
2. Identifizieren Sie für jeden gefundenen VMware-Datenspeicher das Host ONTAP FlexVol volume oder die LUN.
3. Stellen Sie für jedes gefundene ONTAP Volume und LUN fest, ob eine vorhandene SnapMirror Beziehung zwischen den Quellvolumes und einem Zielvolume am Zielstandort besteht.
    a. Wenn keine SnapMirror -Beziehung vorhanden ist, erstellen Sie alle neuen Zielvolumes und erstellen Sie eine neue SnapMirror -Beziehung zwischen jedem ungeschützten Quellvolume.
    b. Wenn bereits eine SnapMirror -Beziehung besteht, verwenden Sie diese Beziehung, um alle Replikationsvorgänge durchzuführen.

Nachdem Disaster Recovery alle Beziehungen erstellt und initialisiert hat, führt der Dienst bei jeder geplanten Sicherung die folgenden Schritte zum Datenschutz aus:

1. Verwenden Sie für jede als „anwendungskonsistent“ gekennzeichnete VM VMtools, um die unterstützte Anwendung in einen Sicherungszustand zu versetzen.
2. Erstellen Sie einen neuen Snapshot aller ONTAP -Volumes, die geschützte VMware-Datenspeicher hosten.
3. Führen Sie einen SnapMirror Aktualisierungsvorgang durch, um diese Snapshots auf den Ziel ONTAP -Cluster zu replizieren.
4. Stellen Sie fest, ob die Anzahl der aufbewahrten Snapshots die im Replikationsplan definierte maximale Snapshot-Aufbewahrung überschritten hat, und löschen Sie alle überflüssigen Snapshots sowohl vom Quell- als auch vom Zielvolume.

Unterstützte Schutzziele und Datenspeichertypen

Unterstützte Datenspeichertypen NetApp Disaster Recovery unterstützt die folgenden Datenspeichertypen:

- NFS-Datenspeicher, die auf ONTAP FlexVol -Volumes gehostet werden, die sich auf ONTAP Clustern befinden.
- VMware vSphere Virtual Machine File System (VMFS)-Datenspeicher mit dem iSCSI- oder FC-Protokoll

Unterstützte Schutzziele

- VMware Cloud (VMC) auf AWS mit Amazon FSx for NetApp ONTAP
- Eine weitere lokale, NFS-basierte VMware-Umgebung mit ONTAP Speicher oder eine lokale FC/iSCSI-VMSF
- Amazon Elastic VMware Service
- Azure VMware Solution (AVS) mit NetApp Cloud Volumes ONTAP (iSCSI) (Private Vorschau)

Begriffe, die Ihnen bei NetApp Disaster Recovery helfen könnten

Es kann für Sie von Vorteil sein, einige Begriffe im Zusammenhang mit der Notfallwiederherstellung zu verstehen.

- **Datenspeicher**: Ein VMware vCenter-Datencontainer, der ein Dateisystem zum Speichern von VMDK-Dateien verwendet. Typische Datenspeichertypen sind NFS, VMFS, vSAN oder vVol. Disaster Recovery unterstützt NFS- und VMFS-Datenspeicher. Jeder VMware-Datenspeicher wird auf einem einzelnen ONTAP Volume oder LUN gehostet. Disaster Recovery unterstützt NFS- und VMFS-Datenspeicher, die auf FlexVol Volumes gehostet werden, die sich auf ONTAP Clustern befinden.
- **Replikationsplan**: Ein Satz von Regeln darüber, wie oft Sicherungen durchgeführt werden und wie mit Failover-Ereignissen umgegangen wird. Pläne werden einer oder mehreren Ressourcengruppen zugewiesen.
- **Recovery Point Objective (RPO)**: Der maximale Datenverlust, der im Katastrophenfall akzeptabel ist. RPO wird in der Häufigkeit der Datenreplikation oder im Replikationszeitplan des Replikationsplans definiert.
- **Recovery Time Objective (RTO)**: Die maximal akzeptable Zeitspanne für die Wiederherstellung nach einem Desaster. RTO ist im Replikationsplan definiert und ist die Zeit, die für das Failover zum DR-Standort und den Neustart aller VMs benötigt wird.
- **Ressourcengruppe**: Ein logischer Container, der es Ihnen ermöglicht, mehrere VMs als eine Einheit zu verwalten. Eine VM kann sich jeweils nur in einer Ressourcengruppe befinden. Sie können für jede Anwendung oder Arbeitslast, die Sie schützen möchten, eine Ressourcengruppe erstellen.
- **Site**: Ein logischer Container, der normalerweise mit einem physischen Rechenzentrum oder Cloud-Standort verknüpft ist, der einen oder mehrere vCenter-Cluster und ONTAP Speicher hostet.

Voraussetzungen für NetApp Disaster Recovery

Bevor Sie NetApp Disaster Recovery verwenden, sollten Sie sicherstellen, dass Ihre Umgebung die Anforderungen für ONTAP -Speicher, VMware vCenter-Cluster und NetApp Console erfüllt.

Softwareversionen

Komponente	Mindestversion
ONTAP Software	ONTAP 9.10.0 oder höher
VMware vCenter vor Ort	7.0u3 oder höher
VMware Cloud für AWS	Neuste verfügbare Version

Komponente	Mindestversion
Amazon FSx for NetApp ONTAP	Neuste verfügbare Version

ONTAP -Speichervoraussetzungen

Diese Voraussetzungen gelten entweder für ONTAP oder Amazon FSX für NetApp ONTAP Instanzen.

- Quell- und Zielcluster müssen eine Peer-Beziehung haben.
- Die SVM, die die Disaster Recovery-Volumes hosten wird, muss auf dem Zielcluster vorhanden sein.
- Zwischen Quell-SVM und Ziel-SVM muss eine Peer-Beziehung bestehen.
- Bei der Bereitstellung mit Amazon FSx for NetApp ONTAP gilt die folgende Voraussetzung:
  - In Ihrer VPC muss eine Amazon FSx for NetApp ONTAP -Instanz zum Hosten von VMware DR-Datenspeichern vorhanden sein. Weitere Informationen finden Sie in der Amazon FSx for ONTAP -Dokumentation unter "Erste Schritte" .

Voraussetzungen für VMware vCenter-Cluster

Diese Voraussetzungen gelten sowohl für lokale vCenter-Cluster als auch für das softwaredefinierte Rechenzentrum (SDDC) von VMware Cloud für AWS.

- Rezension"vCenter-Berechtigungen" erforderlich für NetApp Disaster Recovery.
- Alle VMware-Cluster, die von NetApp Disaster Recovery verwaltet werden sollen, verwenden ONTAP Volumes zum Hosten aller VMs, die Sie schützen möchten.
- Alle VMware-Datenspeicher, die von NetApp Disaster Recovery verwaltet werden sollen, müssen eines der folgenden Protokolle verwenden:
  - NFS
  - VMFS mit dem iSCSI- oder FC-Protokoll
- VMware vSphere Version 7.0 Update 3 (7.0v3) oder höher
- Wenn Sie VMware Cloud SDDC verwenden, gelten diese Voraussetzungen.
  - Verwenden Sie in der VMware Cloud Console die Dienstrollen „Administrator“ und „NSX Cloud-Administrator“. Verwenden Sie den Organisationseigentümer auch für die Organisationsrolle. Siehe "Dokumentation zur Verwendung von VMware Cloud Foundations mit AWS FSx für NetApp ONTAP" .
  - Verknüpfen Sie das VMware Cloud SDDC mit der Amazon FSx for NetApp ONTAP Instanz. Siehe "VMware Cloud auf AWS-Integration mit Amazon FSx for NetApp ONTAP -Bereitstellungsinformationen" .

Voraussetzungen für die NetApp Console

Erste Schritte mit der NetApp Console

Falls Sie dies noch nicht getan haben, "Melden Sie sich bei der NetApp Console an und erstellen Sie eine Organisation" .

Sammeln Sie Anmeldeinformationen für ONTAP und VMware

- Amazon FSx für ONTAP und AWS-Anmeldeinformationen müssen dem System innerhalb des NetApp

Console hinzugefügt werden, das zur Verwaltung der NetApp Disaster Recovery verwendet wird.

- Für NetApp Disaster Recovery sind vCenter-Anmeldeinformationen erforderlich. Sie geben die vCenter-Anmeldeinformationen ein, wenn Sie eine Site in NetApp Disaster Recovery hinzufügen.

  Eine Liste der erforderlichen vCenter-Berechtigungen finden Sie unter"Für NetApp Disaster Recovery erforderliche vCenter-Berechtigungen" . Anweisungen zum Hinzufügen einer Site finden Sie unter"Hinzufügen einer Site" .

Erstellen Sie den NetApp Console Agenten

Der Konsolenagent ist eine Softwarekomponente, die es der Konsole ermöglicht, mit Ihrem ONTAP Speicher und Ihren VMware vCenter-Clustern zu kommunizieren. Es ist erforderlich, damit die Notfallwiederherstellung ordnungsgemäß funktioniert. Der Agent befindet sich in Ihrem privaten Netzwerk (entweder in einem lokalen Rechenzentrum oder in einem Cloud-VPC) und kommuniziert mit Ihren ONTAP Speicherinstanzen und allen zusätzlichen Server- und Anwendungskomponenten. Für die Notfallwiederherstellung ist dies der Zugriff auf Ihre verwalteten vCenter-Cluster.

In der NetApp Console muss ein Konsolenagent eingerichtet werden. Wenn Sie den Agenten verwenden, enthält er die entsprechenden Funktionen für den Disaster Recovery-Dienst.

- NetApp Disaster Recovery funktioniert nur mit der Agent-Bereitstellung im Standardmodus. Sehen "Erste Schritte mit der NetApp Console im Standardmodus" .
- Stellen Sie sicher, dass sowohl das Quell- als auch das Ziel-vCenter denselben Konsolenagenten verwenden.
- Benötigter Konsolenagenttyp:
  - **Notfallwiederherstellung von vor Ort zu vor Ort**: Installieren Sie den lokalen Konsolen-Agenten am Standort für die Notfallwiederherstellung. Bei dieser Methode verhindert ein Ausfall des primären Standorts nicht, dass der Dienst Ihre virtuellen Ressourcen am DR-Standort neu startet. Siehe "Installieren und Einrichten des Konsolen-Agenten vor Ort" .
  - **Vor Ort zu AWS**: Installieren Sie den Konsolenagenten für AWS in Ihrem AWS VPC. Siehe "Installationsoptionen für Konsolenagenten in AWS" .

    Verwenden Sie für die lokale Übertragung den lokalen Konsolenagenten. Verwenden Sie für die lokale Verbindung zu AWS den AWS-Konsolenagenten, der Zugriff auf das lokale Quell-vCenter und das lokale Ziel-vCenter hat.

  - Der installierte Konsolenagent muss auf alle VMware-Cluster zugreifen können, die von NetApp Disaster Recovery verwaltet werden.
- Alle ONTAP Arrays, die von NetApp Disaster Recovery verwaltet werden sollen, müssen zu jedem System innerhalb des NetApp Console -Projekts hinzugefügt werden, das zur Verwaltung von NetApp Disaster Recovery verwendet wird.

  Sehen "Entdecken Sie lokale ONTAP -Cluster" .

- Informationen zum Einrichten eines intelligenten Proxys für NetApp Disaster Recovery finden Sie unter"Richten Sie Ihre Infrastruktur für NetApp Disaster Recovery ein" .

Workload-Voraussetzungen

Um sicherzustellen, dass die Prozesse zur Anwendungskonsistenz erfolgreich sind, müssen Sie die folgenden Voraussetzungen erfüllen:

- Stellen Sie sicher, dass VMware-Tools (oder Open VM-Tools) auf den zu schützenden VMs ausgeführt werden.
- Bei Windows-VMs, auf denen Microsoft SQL Server oder Oracle Database oder beides ausgeführt wird, sollten die VSS Writer der Datenbanken aktiviert sein.
- Bei Oracle-Datenbanken, die auf einem Linux-Betriebssystem ausgeführt werden, sollte die Betriebssystem-Benutzerauthentifizierung für die SYSDBA-Rolle der Oracle-Datenbank aktiviert sein.

Schnellstart für NetApp Disaster Recovery

Hier finden Sie eine Übersicht über die erforderlichen Schritte für den Einstieg in NetApp Disaster Recovery. Über die Links in den einzelnen Schritten gelangen Sie zu einer Seite mit weiteren Einzelheiten.

1 Überprüfen der Voraussetzungen

"Stellen Sie sicher, dass Ihr System diese Anforderungen erfüllt" .

2 Einrichten von NetApp Disaster Recovery

- "Einrichten der Infrastruktur für den Dienst" .
- "Einrichten der Lizenzierung" .

3 Wie geht es weiter?

Nachdem Sie den Dienst eingerichtet haben, können Sie als Nächstes Folgendes tun.

- "Fügen Sie Ihre vCenter-Sites zu NetApp Disaster Recovery" .
- "Erstellen Sie Ihre erste Ressourcengruppe" .
- "Erstellen Sie Ihren ersten Replikationsplan" .
- "Replizieren von Anwendungen auf eine andere Site" .
- "Failover von Anwendungen auf einen Remote-Standort" .
- "Failback von Anwendungen auf die ursprüngliche Quellsite" .
- "Verwalten von Sites, Ressourcengruppen und Replikationsplänen" .
- "Überwachen von Notfallwiederherstellungsvorgängen" .

Richten Sie Ihre Infrastruktur für NetApp Disaster Recovery ein

Um NetApp Disaster Recovery zu verwenden, führen Sie einige Schritte aus, um es sowohl in Amazon Web Services (AWS) als auch in der NetApp Console einzurichten.

Rezension"Voraussetzungen" um sicherzustellen, dass Ihr System bereit ist.

Sie können NetApp Disaster Recovery in folgenden Infrastrukturen verwenden:

- Hybrid Cloud DR, das ein lokales VMware plus ONTAP -Rechenzentrum in eine AWS DR-Infrastruktur repliziert, die auf VMware Cloud on AWS und Amazon FSx for NetApp ONTAP basiert.
- Private Cloud-DR, die ein lokales VMware plus ONTAP vCenter auf ein anderes lokales VMware plus ONTAP vCenter repliziert.

Hybrid Cloud mit VMware Cloud und Amazon FSx for NetApp ONTAP

Diese Methode besteht aus einer lokalen vCenter-Produktionsinfrastruktur mit Datenspeichern, die auf ONTAP FlexVol -Volumes mithilfe eines NFS-Protokolls gehostet werden. Die DR-Site besteht aus einer oder mehreren VMware Cloud SDDC-Instanzen, die Datenspeicher verwenden, die auf FlexVol -Volumes gehostet werden, die von einer oder mehreren FSx for ONTAP -Instanzen mithilfe eines NFS-Protokolls bereitgestellt werden.

Die Produktions- und DR-Standorte sind über eine AWS-kompatible sichere Verbindung verbunden. Gängige Verbindungstypen sind ein sicheres VPN (privat oder von AWS bereitgestellt), AWS Direct Connect oder andere genehmigte Verbindungsmethoden.

Für die Notfallwiederherstellung mit AWS-Cloud-Infrastruktur müssen Sie den Konsolenagenten für AWS verwenden. Der Agent sollte im selben VPC wie die FSx for ONTAP -Instanz installiert werden. Wenn zusätzliche FSx for ONTAP -Instanzen in anderen VPCs bereitgestellt wurden, muss die VPC, die den Agenten hostet, Zugriff auf die anderen VPCs haben.

AWS-Verfügbarkeitszonen

AWS unterstützt die Bereitstellung von Lösungen in einer oder mehreren Verfügbarkeitszonen (AZ) innerhalb einer bestimmten Region. Disaster Recovery verwendet zwei von AWS gehostete Dienste: VMware Cloud für AWS und AWS FSx für NetApp ONTAP.

- **VMware Cloud für AWS**: Unterstützt die Bereitstellung in einer Single-AZ- oder in einer Dual-AZ-Stretch-Cluster-SDDC-Umgebung. Disaster Recovery unterstützt eine Single-AZ-SDDC-Bereitstellung nur für Amazon VMware Cloud für AWS.
- **AWS FSx für NetApp ONTAP**: Wenn dies in einer Dual-AZ-Konfiguration bereitgestellt wird, gehört jedes Volume einem einzelnen FSx-System. Jedes Volume gehört einem einzelnen FSx-System. Die Daten des Volumes werden auf das zweite FSx-System gespiegelt. Die FSx für ONTAP -Systeme können entweder in Single- oder Dual-AZ-Bereitstellungen eingesetzt werden. Disaster Recovery unterstützt sowohl Single- als auch Multi-AZ-FSx für FSx für ONTAP Bereitstellungen.

BEST PRACTICE: Für die AWS DR-Site-Konfiguration empfiehlt NetApp die Verwendung von Single-AZ-Bereitstellungen sowohl für VMware Cloud als auch für AWS FSx für ONTAP -Instanzen. Da AWS für DR verwendet wird, bietet die Einführung mehrerer AZs keinen Vorteil. Mehrere AZs können die Kosten und die Komplexität erhöhen.

Von On-Premises zu AWS

AWS bietet die folgenden Methoden zum Verbinden privater Rechenzentren mit der AWS-Cloud. Jede Lösung hat ihre Vorteile und Kostenaspekte.

- **AWS Direct Connect**: Dies ist eine AWS-Cloud-Verbindung, die sich im selben geografischen Gebiet wie Ihr privates Rechenzentrum befindet und von einem AWS-Partner bereitgestellt wird. Diese Lösung bietet eine sichere, private Verbindung zwischen Ihrem lokalen Rechenzentrum und der AWS-Cloud, ohne dass eine öffentliche Internetverbindung erforderlich ist. Dies ist die direkteste und effizienteste Verbindungsmethode, die von AWS angeboten wird.
- **AWS Internet Gateway**: Dies bietet öffentliche Konnektivität zwischen AWS-Cloud-Ressourcen und

externen Rechenressourcen. Dieser Verbindungstyp wird normalerweise verwendet, um externen Kunden Serviceangebote bereitzustellen, beispielsweise HTTP/HTTPS-Dienste, bei denen Sicherheit keine Voraussetzung ist. Es gibt keine Kontrolle der Dienstqualität, Sicherheit oder Konnektivitätsgarantie. Aus diesem Grund wird diese Verbindungsmethode nicht für die Verbindung eines Produktionsrechenzentrums mit der Cloud empfohlen.

- **AWS Site-Site VPN**: Diese virtuelle private Netzwerkverbindung kann verwendet werden, um sichere Zugriffsverbindungen zusammen mit einem öffentlichen Internetdienstanbieter bereitzustellen. Das VPN verschlüsselt und entschlüsselt alle Daten, die zur und von der AWS-Cloud übertragen werden. VPNs können entweder software- oder hardwarebasiert sein. Für Unternehmensanwendungen sollte der öffentliche Internetdienstanbieter (ISP) Qualitätsgarantien bieten, um sicherzustellen, dass für die DR-Replikation ausreichend Bandbreite und Latenz zur Verfügung stehen.

BEST PRACTICE: Für die AWS DR-Site-Konfiguration empfiehlt NetApp die Verwendung von AWS Direct Connect. Diese Lösung bietet höchste Leistung und Sicherheit für Unternehmensanwendungen. Wenn dies nicht möglich ist, sollte eine leistungsstarke öffentliche ISP-Verbindung zusammen mit einem VPN verwendet werden. Stellen Sie sicher, dass der ISP kommerzielle QoS-Dienstlevel anbietet, um eine angemessene Netzwerkleistung sicherzustellen.

VPC-zu-VPC-Verbindungen

AWS bietet die folgenden Arten von VPC-zu-VPC-Verbindungen an. Jede Lösung hat ihre Vorteile und Kostenaspekte.

- **VPC-Peering**: Dies ist eine private Verbindung zwischen zwei VPCs. Es ist die direkteste und effizienteste Verbindungsmethode, die von AWS angeboten wird. VPC-Peering kann verwendet werden, um VPCs in derselben oder in verschiedenen AWS-Regionen zu verbinden.
- **AWS Internet Gateway**: Dies wird normalerweise verwendet, um Verbindungen zwischen AWS VPC-Ressourcen und Nicht-AWS-Ressourcen und -Endpunkten bereitzustellen. Der gesamte Datenverkehr folgt einem „Haarnadelpfad“, bei dem VPC-Datenverkehr, der für eine andere VPC bestimmt ist, die AWS-Infrastruktur über das Internet-Gateway verlässt und über dasselbe oder ein anderes Gateway zur AWS-Infrastruktur zurückkehrt. Dies ist kein geeigneter VPC-Verbindungstyp für VMware-Unternehmenslösungen.
- **AWS Transit Gateway**: Dies ist ein zentralisierter, routerbasierter Verbindungstyp, der es jedem VPC ermöglicht, eine Verbindung zu einem einzigen, zentralen Gateway herzustellen, das als zentraler Hub für den gesamten VPC-zu-VPC-Verkehr fungiert. Dies kann auch mit Ihrer VPN-Lösung verbunden werden, um lokalen Rechenzentrumsressourcen den Zugriff auf von AWS VPC gehostete Ressourcen zu ermöglichen. Für die Implementierung dieser Verbindungsart fallen in der Regel zusätzliche Kosten an.

BEST PRACTICE: Für DR-Lösungen mit VMware Cloud und einem einzelnen FSx für ONTAP VPC empfiehlt NetApp die Verwendung der VPC-Peer-Verbindung. Wenn mehrere FSx für ONTAP VPCs bereitgestellt werden, empfehlen wir die Verwendung eines AWS Transit Gateway, um den Verwaltungsaufwand mehrerer VPC-Peer-Verbindungen zu reduzieren.

Machen Sie sich bereit für den On-Premises-to-Cloud-Schutz mit AWS

Um NetApp Disaster Recovery für den On-Premises-to-Cloud-Schutz mit AWS einzurichten, müssen Sie Folgendes einrichten:

- AWS FSx für NetApp ONTAP einrichten
- Einrichten von VMware Cloud on AWS SDDC

AWS FSx für NetApp ONTAP einrichten

- Erstellen Sie ein Amazon FSx for NetApp ONTAP -Dateisystem.
  - Stellen Sie FSx für ONTAP bereit und konfigurieren Sie es. Amazon FSx for NetApp ONTAP ist ein vollständig verwalteter Service, der äußerst zuverlässigen, skalierbaren, leistungsstarken und funktionsreichen Dateispeicher bietet, der auf dem NetApp ONTAP Dateisystem basiert.
  - Befolgen Sie die Schritte in "Technischer Bericht 4938: Mounten Sie Amazon FSx ONTAP als NFS-Datenspeicher mit VMware Cloud auf AWS" Und "Schnellstart für Amazon FSx for NetApp ONTAP" zum Bereitstellen und Konfigurieren von FSx für ONTAP.
- Fügen Sie dem System Amazon FSx for ONTAP hinzu und fügen Sie AWS-Anmeldeinformationen für FSx for ONTAP hinzu.
- Erstellen oder überprüfen Sie Ihr Ziel ONTAP SVM in AWS FSx für die ONTAP Instanz.
- Konfigurieren Sie die Replikation zwischen Ihrem lokalen ONTAP Quellcluster und Ihrer FSx for ONTAP Instanz in der NetApp Console.

Siehe "So richten Sie ein FSx für ONTAP -System ein" für detaillierte Schritte.

Einrichten von VMware Cloud on AWS SDDC

"VMware Cloud auf AWS"bietet eine Cloud-native Erfahrung für VMware-basierte Workloads im AWS-Ökosystem. Jedes VMware-Software-Defined Data Center (SDDC) läuft in einer Amazon Virtual Private Cloud (VPC) und bietet einen vollständigen VMware-Stack (einschließlich vCenter Server), NSX-T-Software-Defined Networking, vSAN-Software-Defined Storage und einen oder mehrere ESXi-Hosts, die den Workloads Rechen- und Speicherressourcen bereitstellen.

Um eine VMware Cloud-Umgebung auf AWS zu konfigurieren, befolgen Sie die Schritte in "Bereitstellen und Konfigurieren der Virtualisierungsumgebung auf AWS" Ein Pilotlichtcluster kann auch für die Notfallwiederherstellung verwendet werden.

Private Cloud

Sie können NetApp Disaster Recovery verwenden, um VMware-VMs zu schützen, die auf einem oder mehreren vCenter-Clustern gehostet werden, indem Sie VM-Datenspeicher auf einen anderen vCenter-Cluster replizieren, entweder im selben privaten Rechenzentrum oder in einem entfernten privaten oder am selben Standort befindlichen Rechenzentrum.

Installieren Sie den Konsolenagenten für On-Premises-Situationen an einem der physischen Standorte.

Disaster Recovery unterstützt die Site-to-Site-Replikation über Ethernet und TCP/IP. Stellen Sie sicher, dass ausreichend Bandbreite zur Verfügung steht, um die Datenänderungsraten auf den VMs des Produktionsstandorts zu unterstützen, sodass alle Änderungen innerhalb des RPO-Zeitrahmens (Recovery Point Objective) auf den DR-Standort repliziert werden können.

Machen Sie sich bereit für den On-Premises-zu-On-Premises-Schutz

Stellen Sie sicher, dass die folgenden Anforderungen erfüllt sind, bevor Sie NetApp Disaster Recovery für den On-Premises-zu-On-Premises-Schutz einrichten:

- ONTAP-Speicher
  - Stellen Sie sicher, dass Sie über ONTAP Anmeldeinformationen verfügen.
  - Erstellen oder überprüfen Sie Ihre Disaster-Recovery-Site.

- Erstellen oder überprüfen Sie Ihr Ziel ONTAP SVM.
- Stellen Sie sicher, dass Ihre Quell- und Ziel ONTAP -SVMs per Peering verbunden sind.

- vCenter-Cluster
  - Stellen Sie sicher, dass die VMs, die Sie schützen möchten, auf NFS-Datenspeichern (mithilfe von ONTAP NFS-Volumes) oder VMFS-Datenspeichern (mithilfe von NetApp iSCSI LUNs) gehostet werden.
  - Rezension"vCenter-Berechtigungen" erforderlich für NetApp Disaster Recovery.
  - Erstellen Sie ein Benutzerkonto für die Notfallwiederherstellung (nicht das standardmäßige vCenter-Administratorkonto) und weisen Sie dem Konto die vCenter-Berechtigungen zu.

Intelligente Proxy-Unterstützung

Der NetApp Console Agent unterstützt intelligente Proxys. Intelligent Proxy ist eine einfache, sichere und effiziente Möglichkeit, Ihre lokale Umgebung mit der NetApp Console zu verbinden. Es bietet eine sichere Verbindung zwischen Ihrem System und dem Konsolendienst, ohne dass ein VPN oder direkter Internetzugang erforderlich ist. Diese optimierte Proxy-Implementierung entlastet den API-Verkehr innerhalb des lokalen Netzwerks.

Wenn ein Proxy konfiguriert ist, versucht NetApp Disaster Recovery, direkt mit VMware oder ONTAP zu kommunizieren und verwendet den konfigurierten Proxy, wenn die direkte Kommunikation fehlschlägt.

Die Implementierung des NetApp Disaster Recovery -Proxys erfordert eine Kommunikation über Port 443 zwischen dem Konsolenagenten und allen vCenter-Servern und ONTAP Arrays unter Verwendung eines HTTPS-Protokolls. Der NetApp Disaster Recovery -Agent innerhalb des Konsolen-Agenten kommuniziert bei der Durchführung von Aktionen direkt mit VMware vSphere, dem VC oder ONTAP .

Weitere Informationen zum Einrichten eines allgemeinen Proxys in der NetApp Console finden Sie unter "Konfigurieren des Konsolenagenten zur Verwendung eines Proxyservers" .

Zugriff auf NetApp Disaster Recovery

Sie verwenden die NetApp Console , um sich beim NetApp Disaster Recovery -Dienst anzumelden.

Zum Anmelden können Sie Ihre Anmeldeinformationen für die NetApp Support-Site verwenden oder sich mit Ihrer E-Mail-Adresse und einem Kennwort für eine NetApp Cloud-Anmeldung registrieren. "Erfahren Sie mehr über die Anmeldung" .

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

Schritte

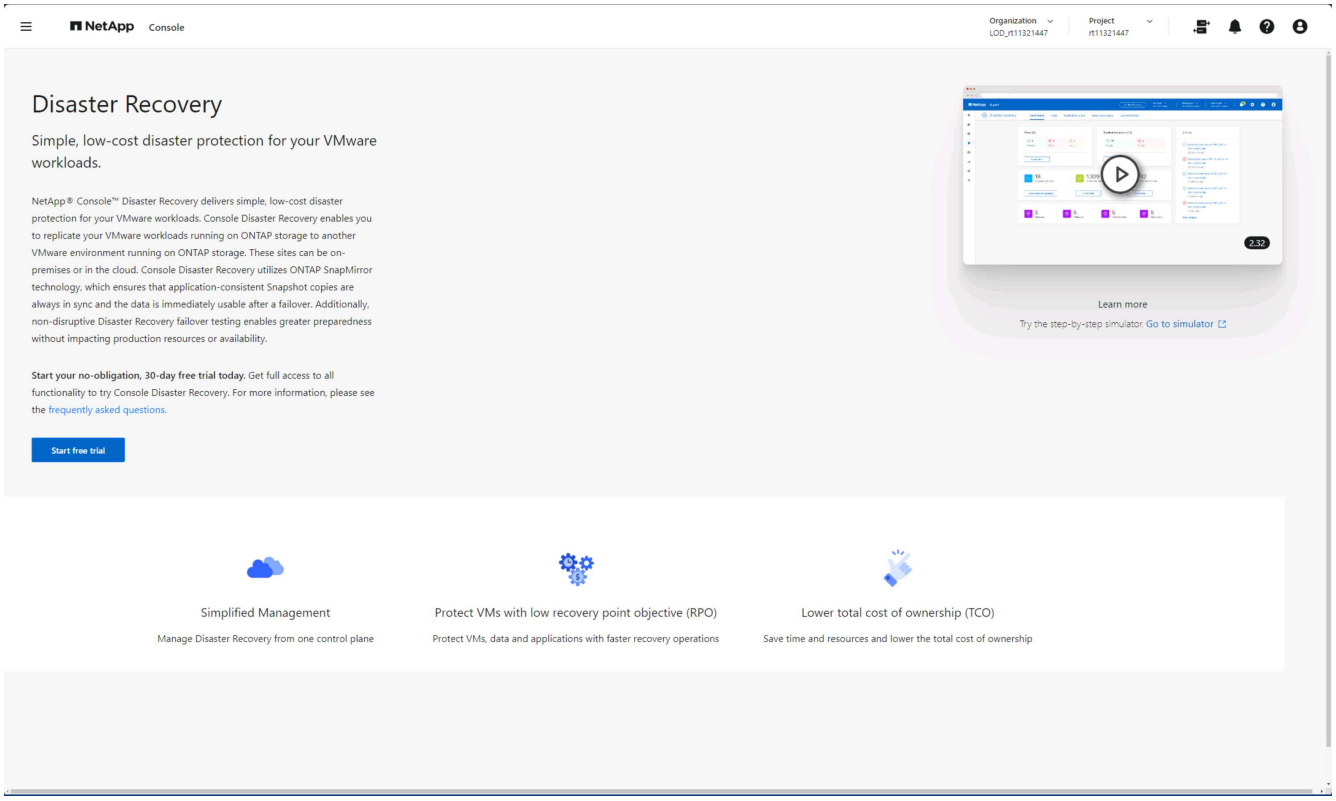
1. Öffnen Sie einen Webbrowser und gehen Sie zu "NetApp Console" .

   Die Anmeldeseite der NetApp Console wird angezeigt.

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

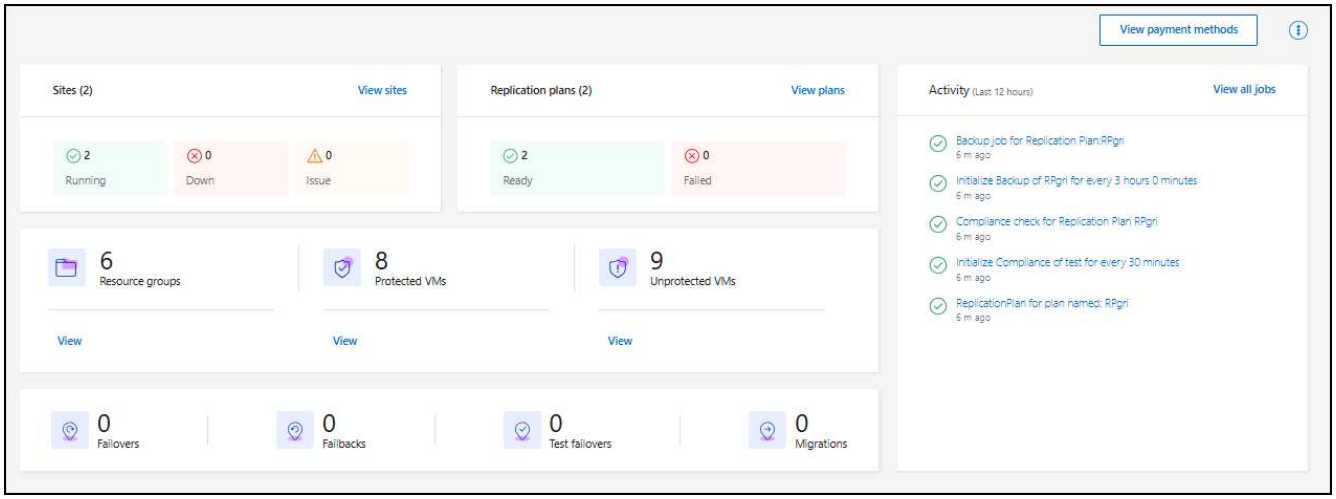
   Wenn Sie sich zum ersten Mal bei diesem Dienst anmelden, wird die Zielseite angezeigt und Sie können

sich für eine kostenlose Testversion anmelden.



Andernfalls wird das NetApp Disaster Recovery Dashboard angezeigt.

- Wenn Sie noch keinen NetApp Console Agenten hinzugefügt haben, müssen Sie einen hinzufügen. Informationen zum Hinzufügen des Agenten finden Sie unter "Erfahren Sie mehr über Konsolenagenten" .
- Wenn Sie ein NetApp Console mit einem vorhandenen Agenten sind und „Notfallwiederherstellung“ auswählen, wird eine Meldung zur Anmeldung angezeigt.
- Wenn Sie den Dienst bereits verwenden und „Notfallwiederherstellung“ auswählen, wird das Dashboard angezeigt.



Einrichten der Lizenzierung für NetApp Disaster Recovery

Mit NetApp Disaster Recovery können Sie verschiedene Lizenzierungspläne nutzen, darunter eine kostenlose Testversion, ein Pay-as-you-go-Abonnement oder die Nutzung Ihrer eigenen Lizenz.

*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 Zugriffsrollen für alle Dienste" .

Lizenzierungsoptionen Sie können die folgenden Lizenzierungsoptionen nutzen:

- Melden Sie sich für eine 30-tägige kostenlose Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) für den Amazon Web Services (AWS) Marketplace oder den Microsoft Azure Marketplace.
- Bringen Sie Ihre eigene Lizenz (BYOL) mit. Dabei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um BYOL in der NetApp Console zu aktivieren.

> Die Gebühren für NetApp Disaster Recovery basieren auf der genutzten Kapazität der Datenspeicher am Quellstandort, wenn mindestens eine VM über einen Replikationsplan verfügt. Die Kapazität für einen ausgefallenen Datenspeicher ist nicht in der Kapazitätszuteilung enthalten. Wenn bei einem BYOL die Daten die zulässige Kapazität überschreiten, sind die Vorgänge im Dienst eingeschränkt, bis Sie eine zusätzliche Kapazitätslizenz erwerben oder die Lizenz in der NetApp Console aktualisieren.

"Mehr über Abonnements erfahren" .

Nach Ablauf der kostenlosen Testversion oder der Lizenz können Sie im Dienst weiterhin Folgendes tun:

- Zeigen Sie beliebige Ressourcen an, beispielsweise eine Arbeitslast oder einen Replikationsplan.
- Löschen Sie beliebige Ressourcen, beispielsweise eine Arbeitslast oder einen Replikationsplan.
- Führen Sie alle geplanten Vorgänge aus, die während der Testphase oder unter der Lizenz erstellt wurden.

Probieren Sie es mit einer 30-tägigen kostenlosen Testversion aus

Sie können NetApp Disaster Recovery mit einer 30-tägigen kostenlosen Testversion ausprobieren.

> Während der Testphase gelten keine Kapazitätsbeschränkungen.

Um nach der Testphase fortzufahren, müssen Sie eine BYOL-Lizenz oder ein PAYGO-AWS-Abonnement erwerben. Sie können jederzeit eine Lizenz erwerben und es entstehen Ihnen erst nach Ablauf der Testphase Kosten.

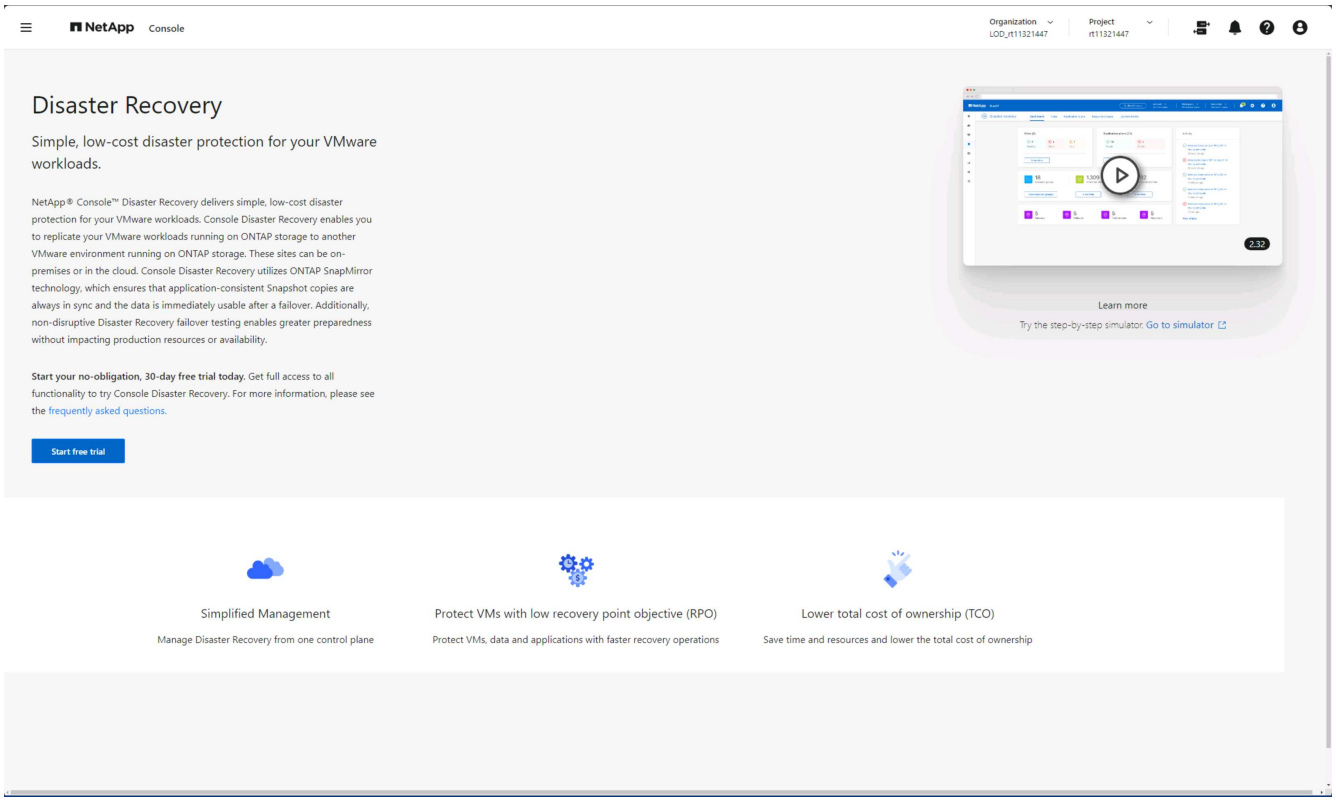
Während der Testphase steht Ihnen die volle Funktionalität zur Verfügung.

Schritte

1. Melden Sie sich an bei "NetApp Console" .

2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.

   Wenn Sie sich zum ersten Mal bei diesem Dienst anmelden, wird die Zielseite angezeigt.



3. Wenn Sie noch keinen Konsolenagenten für andere Dienste hinzugefügt haben, fügen Sie einen hinzu.

   Informationen zum Hinzufügen eines Konsolenagenten finden Sie unter "Erfahren Sie mehr über Konsolenagenten" .

4. Nachdem Sie den Agenten eingerichtet haben, ändert sich auf der Zielseite von NetApp Disaster Recovery die Schaltfläche zum Hinzufügen des Agenten in eine Schaltfläche zum Starten einer kostenlosen Testversion. Wählen Sie **Kostenlose Testversion starten**.
5. Beginnen Sie mit dem Hinzufügen von vCenters.

   Weitere Informationen finden Sie unter "vCenter-Sites hinzufügen" .

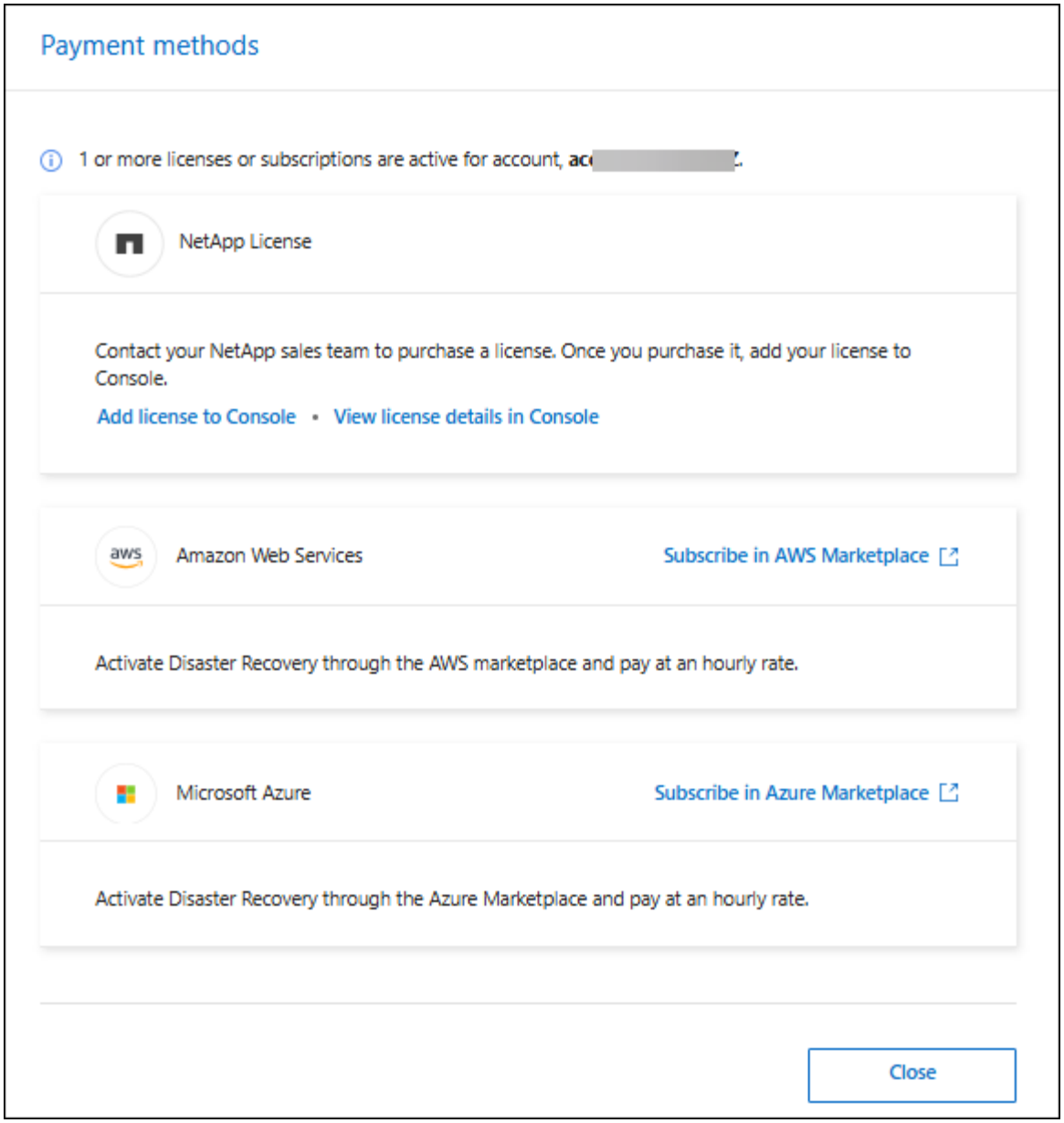
Nach Ablauf der Testphase abonnieren Sie über einen der Marketplaces

Nach Ablauf der kostenlosen Testversion können Sie entweder eine Lizenz von NetApp erwerben oder ein Abonnement über AWS Marketplace oder Microsoft Azure Marketplace abschließen. Dieses Verfahren bietet einen allgemeinen Überblick darüber, wie Sie sich direkt bei einem der Marktplätze anmelden können.

Schritte

1. In NetApp Disaster Recovery wird eine Meldung angezeigt, dass die kostenlose Testversion abläuft. Wählen Sie in der Nachricht **Abonnieren oder Lizenz kaufen** aus.

   Oder wählen Sie im die Option **Zahlungsmethoden anzeigen** aus.



2. Wählen Sie **Im AWS Marketplace abonnieren** oder **Im Azure Marketplace abonnieren**.
3. Verwenden Sie AWS Marketplace oder Microsoft Azure Marketplace, um * NetApp Disaster Recovery* zu abonnieren.
4. Wenn Sie zu NetApp Disaster Recovery zurückkehren, wird eine Meldung angezeigt, dass Sie abonniert sind.

   Sie können Abonnementdetails auf der Abonnementseite der NetApp Console anzeigen. "Erfahren Sie mehr über die Verwaltung von Abonnements mit der NetApp Console" .

Nach Ablauf der Testphase können Sie über NetApp eine BYOL-Lizenz erwerben.

Nach Ablauf der Testphase können Sie über Ihren NetApp Vertriebsmitarbeiter eine Lizenz erwerben.

Wenn Sie Ihre eigene Lizenz mitbringen (BYOL), umfasst die Einrichtung den Kauf der Lizenz, das Abrufen der NetApp -Lizenzdatei (NLF) und das Hinzufügen der Lizenz zur NetApp Console.

Fügen Sie die Lizenz zur NetApp Console hinzu. * Nachdem Sie Ihre NetApp Disaster Recovery -Lizenz von einem NetApp Vertriebsmitarbeiter erworben haben, können Sie die Lizenz in der Konsole verwalten.

"Erfahren Sie mehr über das Hinzufügen von Lizenzen mit der NetApp Console" .

Aktualisieren Sie Ihre Lizenz, wenn sie abläuft

Wenn sich Ihre Lizenzlaufzeit dem Ablaufdatum nähert oder Ihre lizenzierte Kapazität das Limit erreicht, werden Sie in der NetApp Disaster Recovery Benutzeroberfläche benachrichtigt. Sie können Ihre NetApp Disaster Recovery -Lizenz vor Ablauf aktualisieren, sodass Ihr Zugriff auf die gescannten Daten ohne Unterbrechung möglich ist.

Diese Meldung erscheint auch in der NetApp Console und in "Benachrichtigungen" .

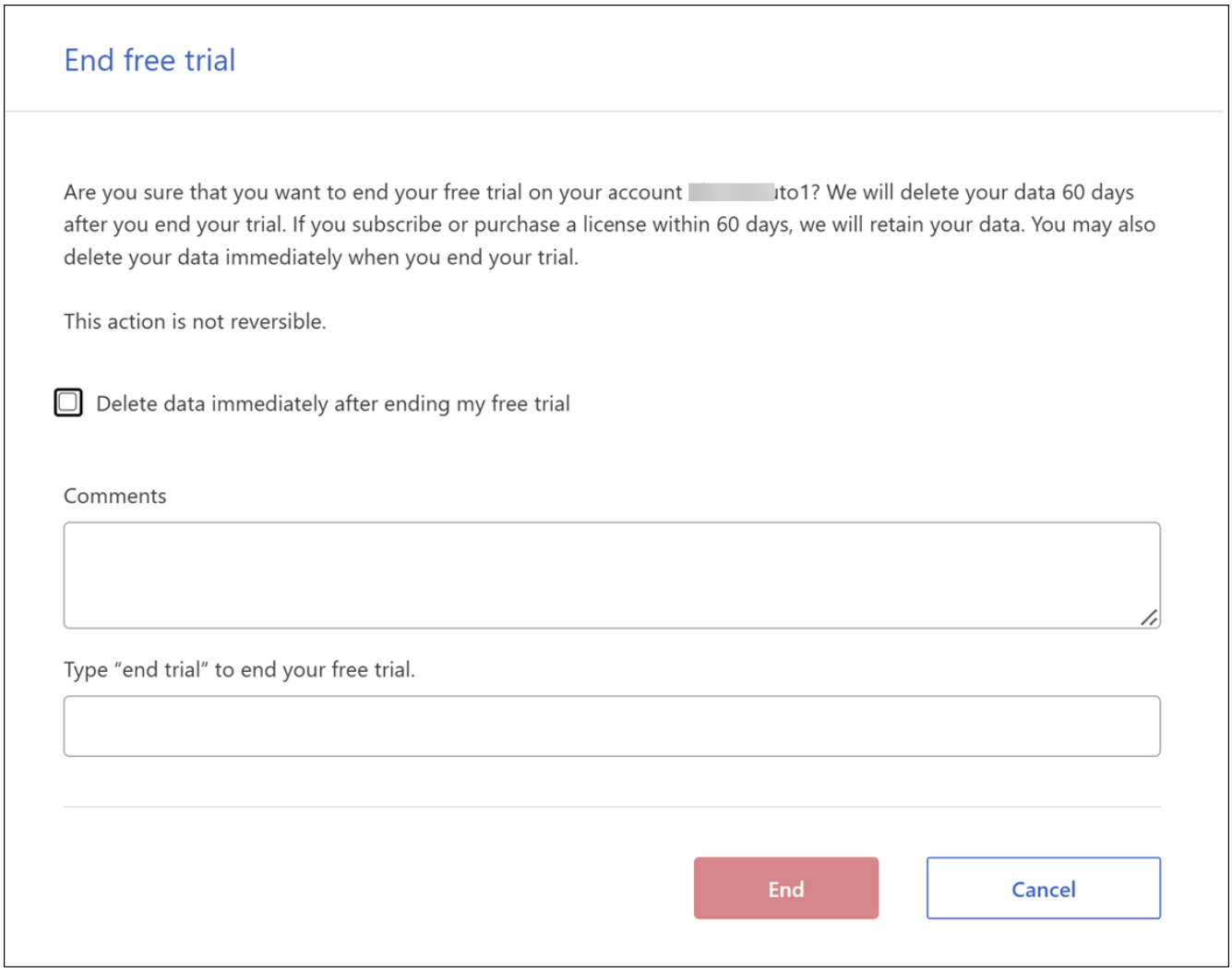
"Erfahren Sie mehr über die Aktualisierung von Lizenzen mit der NetApp Console" .

Kostenlose Testversion beenden

Sie können die kostenlose Testversion jederzeit beenden oder warten, bis sie abläuft.

Schritte

1. Wählen Sie in NetApp Disaster Recovery*Kostenlose Testversion – Details anzeigen* aus.
2. Wählen Sie in den Dropdown-Details **Kostenlose Testversion beenden** aus.



3. Wenn Sie alle Daten löschen möchten, aktivieren Sie **Daten sofort nach Beendigung meiner kostenlosen Testversion löschen**.

   Dadurch werden alle Zeitpläne, Replikationspläne, Ressourcengruppen, vCenter und Sites gelöscht. Prüfdaten, Betriebsprotokolle und Auftragsverläufe werden bis zum Ende der Produktlebensdauer aufbewahrt.

   Wenn Sie die kostenlose Testversion beenden, keine Datenlöschung angefordert haben und keine Lizenz oder kein Abonnement erwerben, löscht NetApp Disaster Recovery 60 Tage nach Ablauf der kostenlosen Testversion alle Ihre Daten.

4. Geben Sie „Testversion beenden“ in das Textfeld ein.
5. Wählen Sie **Ende**.

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

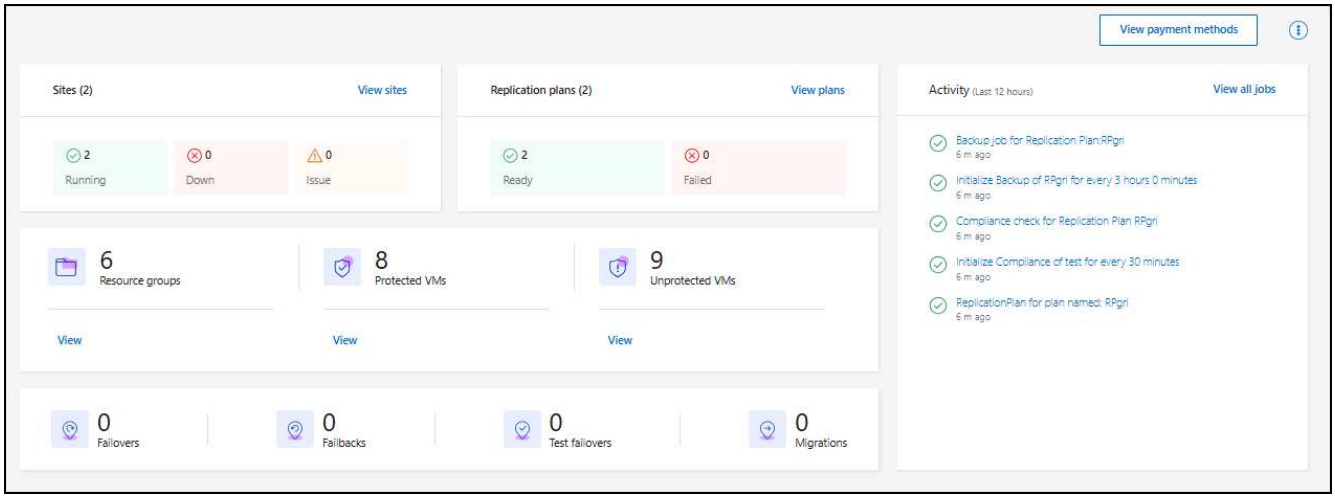
Mithilfe des NetApp Disaster Recovery Dashboards können Sie den Zustand Ihrer Disaster Recovery-Sites und Replikationspläne ermitteln. Sie können schnell feststellen, welche Websites und Pläne fehlerfrei, getrennt oder beeinträchtigt sind.

*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

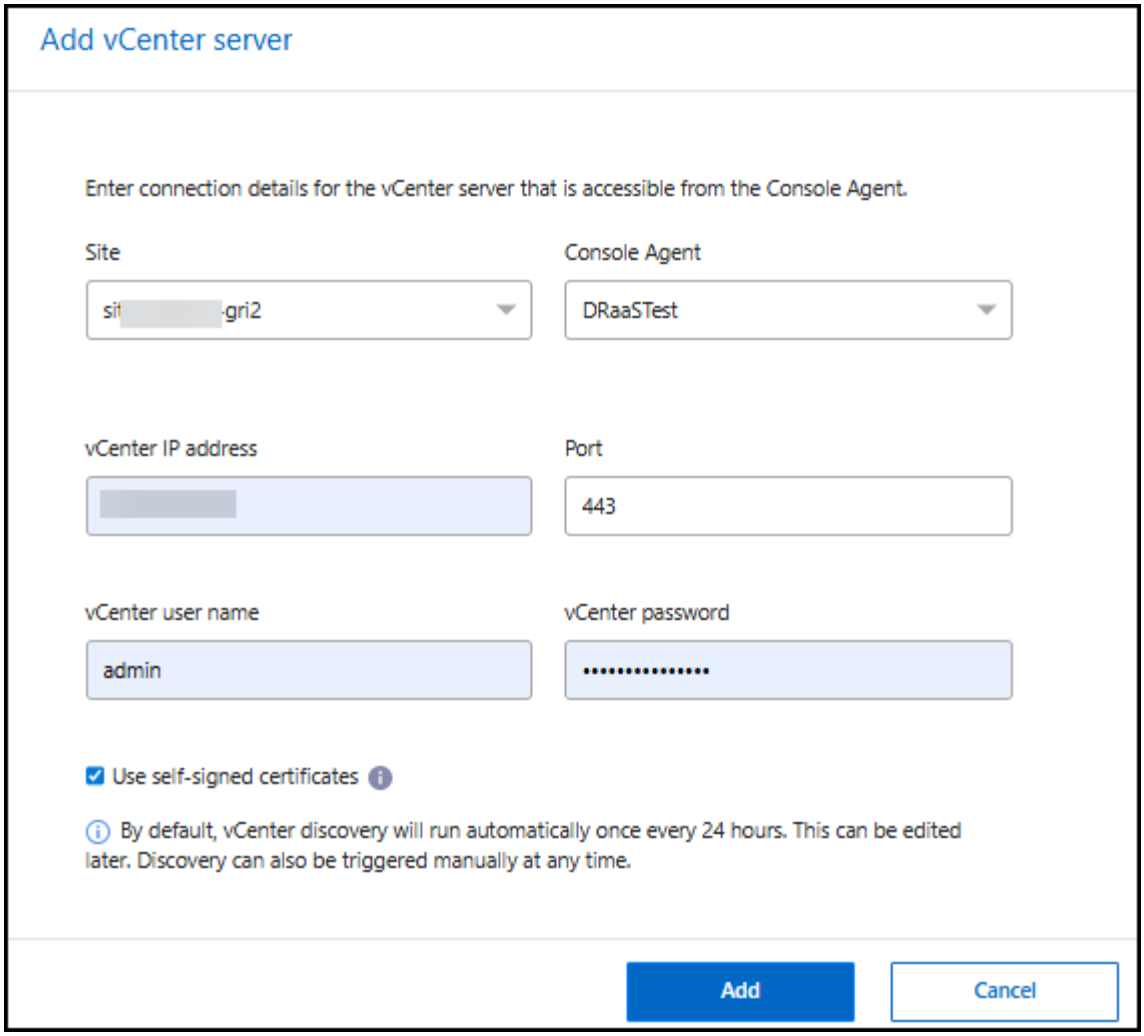
1. Melden Sie sich an bei "NetApp Console" .
2. Wählen Sie in der linken Navigation der NetApp Console **Schutz** > **Notfallwiederherstellung**.

   Sie landen auf der NetApp Disaster Recovery Dashboard-Seite. Wenn Sie den Dienst zum ersten Mal starten, müssen Sie vCenter-Informationen hinzufügen. Später zeigt das Dashboard Daten zu Ihren Sites und Replikationsplänen an.

   > 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.

   > Wenn bereits einige vCenter-Sites vorhanden sind und Sie weitere hinzufügen möchten, wählen Sie im oberen Menü **Sites** und dann **Hinzufügen** aus.



- Wählen Sie eine Site aus, wählen Sie den NetApp Console Agenten aus und geben Sie die vCenter-Anmeldeinformationen ein.
- (Gilt nur für lokale Sites) Aktivieren Sie das Kontrollkästchen, um selbstsignierte Zertifikate für das Quell-vCenter zu akzeptieren.

> 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.

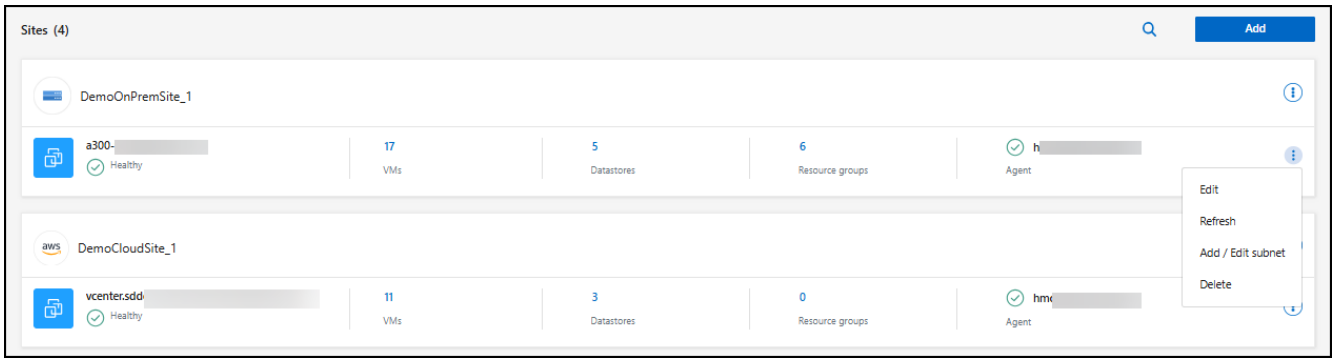
Zusammenfassend lässt sich sagen, dass die Hostadresse gleich bleibt, während die Netzwerkadresse durch die in der Site-Subnetzzuordnung konfigurierte Adresse ersetzt wird. Auf diese Weise können Sie die Neuzuweisung von IP-Adressen bei einem Failover einfacher verwalten, insbesondere wenn Sie Hunderte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

Die Verwendung der Subnetzzuordnung ist ein optionaler zweistufiger Prozess:

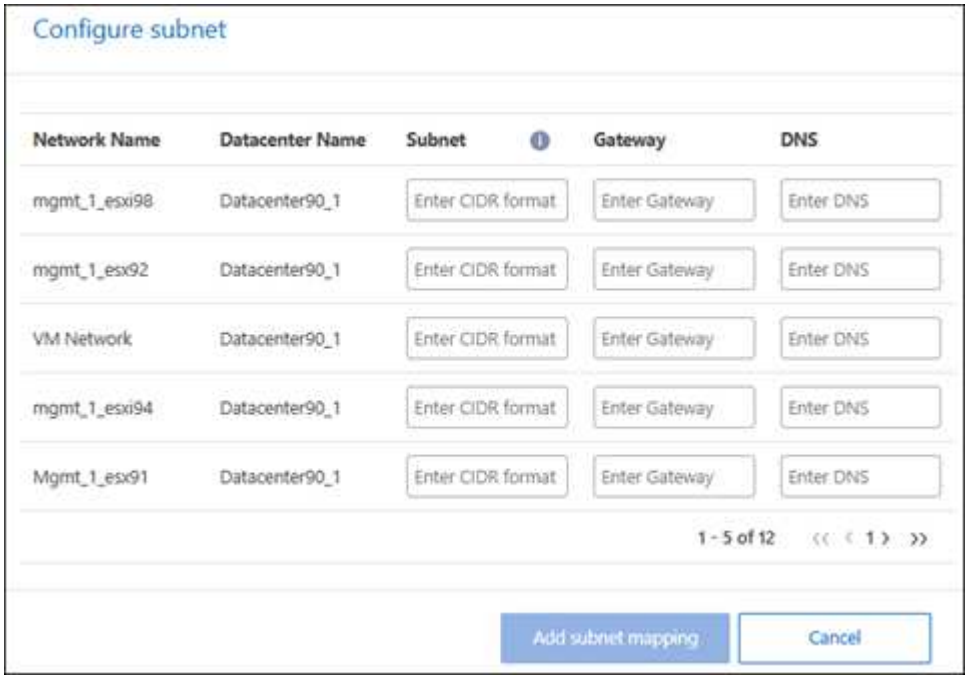
- Fügen Sie zunächst die Subnetzzuordnung für jeden vCenter-Standort hinzu.
- Geben Sie zweitens im Replikationsplan auf der Registerkarte „Virtuelle Maschinen“ und im Feld „Ziel-IP“ an, dass Sie die Subnetzzuordnung verwenden möchten.

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

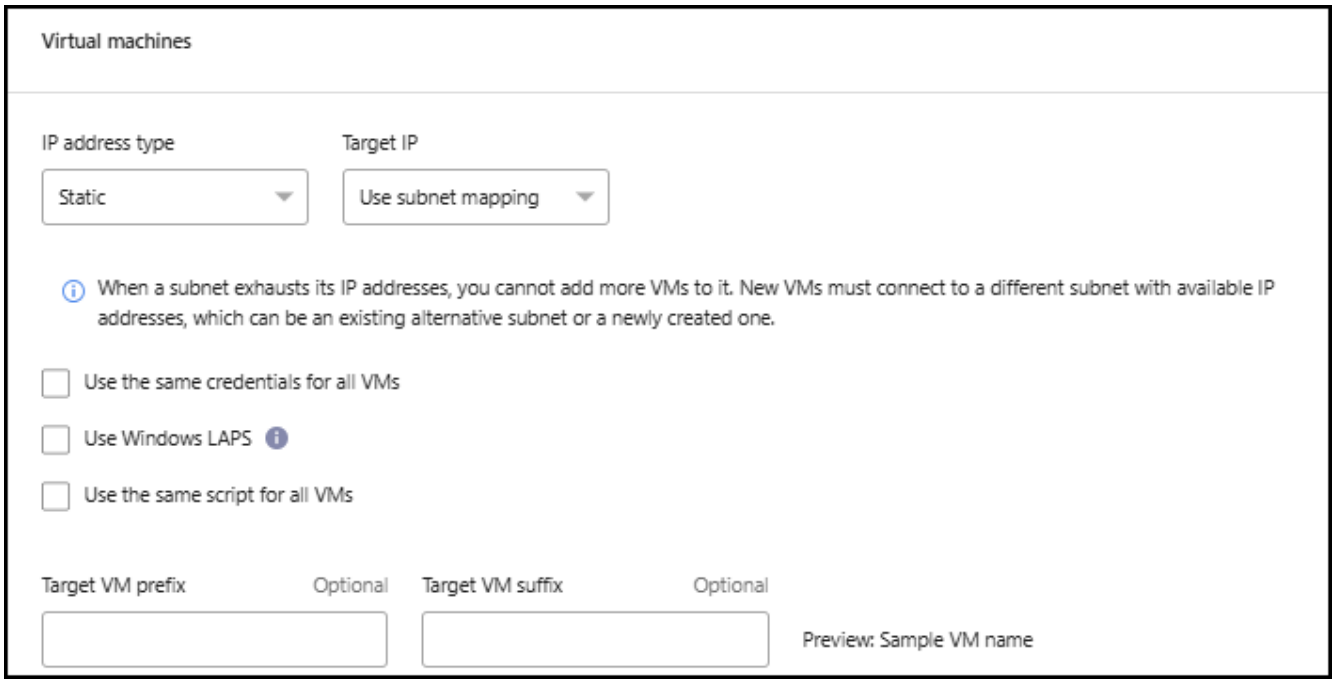
Wenn Sie einen Replikationsplan erstellen, können Sie die Subnetzzuordnung für den Replikationsplan auswählen.

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,

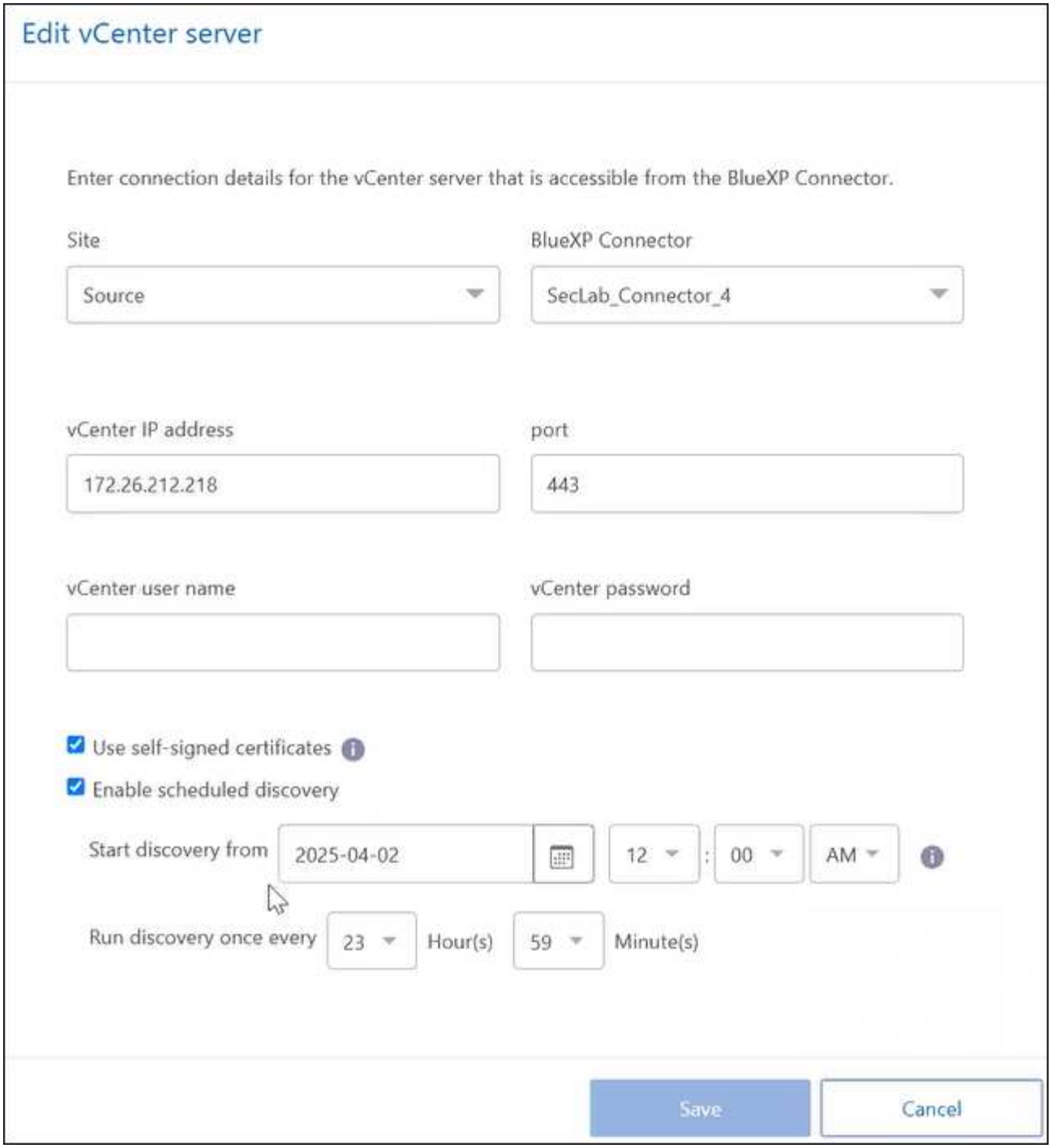
dass er alle 23 Stunden und 59 Minuten ausgeführt wird. Wenn Sie nur eine kleine Anzahl von VMs haben, können Sie den Erkennungszeitplan so einstellen, dass er alle 12 Stunden ausgeführt wird.

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:

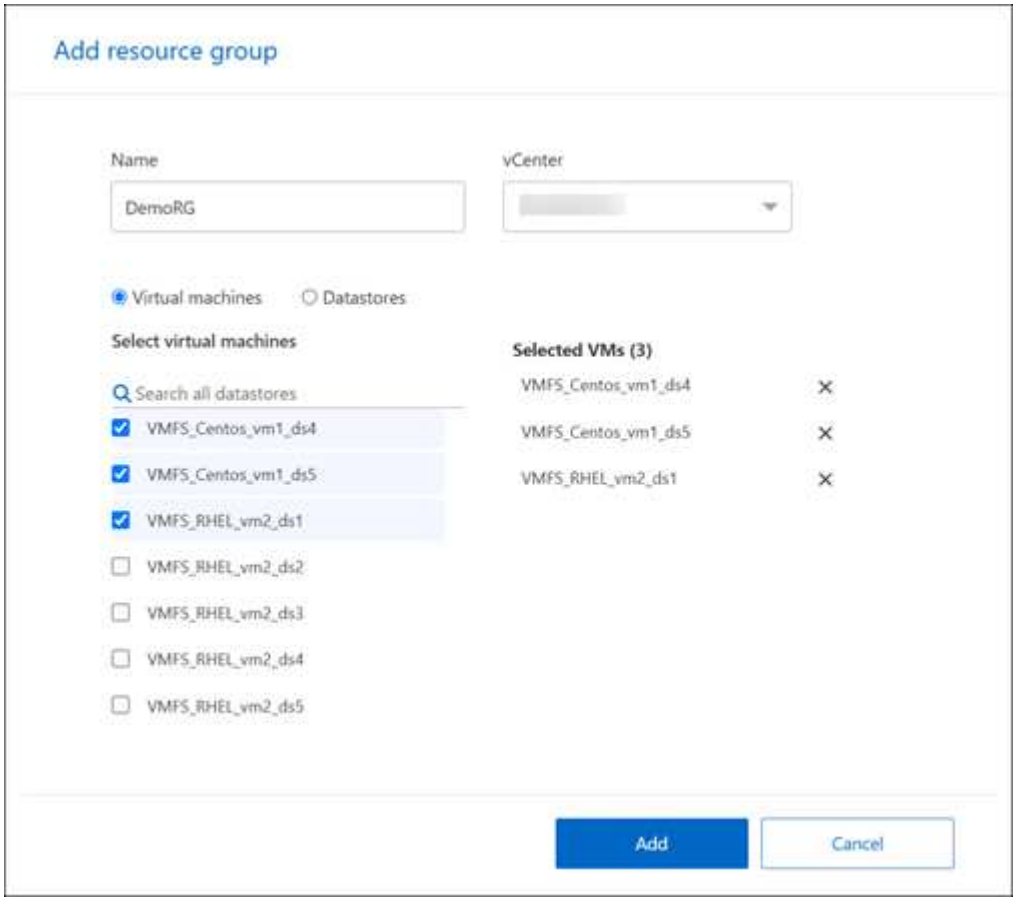
- Bevor Sie Datenspeicher zu Ressourcengruppen hinzufügen, starten Sie zunächst eine manuelle oder geplante Erkennung der VMs. Dadurch wird sichergestellt, dass die VMs erkannt und in der Ressourcengruppe aufgelistet werden. Wenn Sie keine manuelle Erkennung starten, werden die VMs möglicherweise nicht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

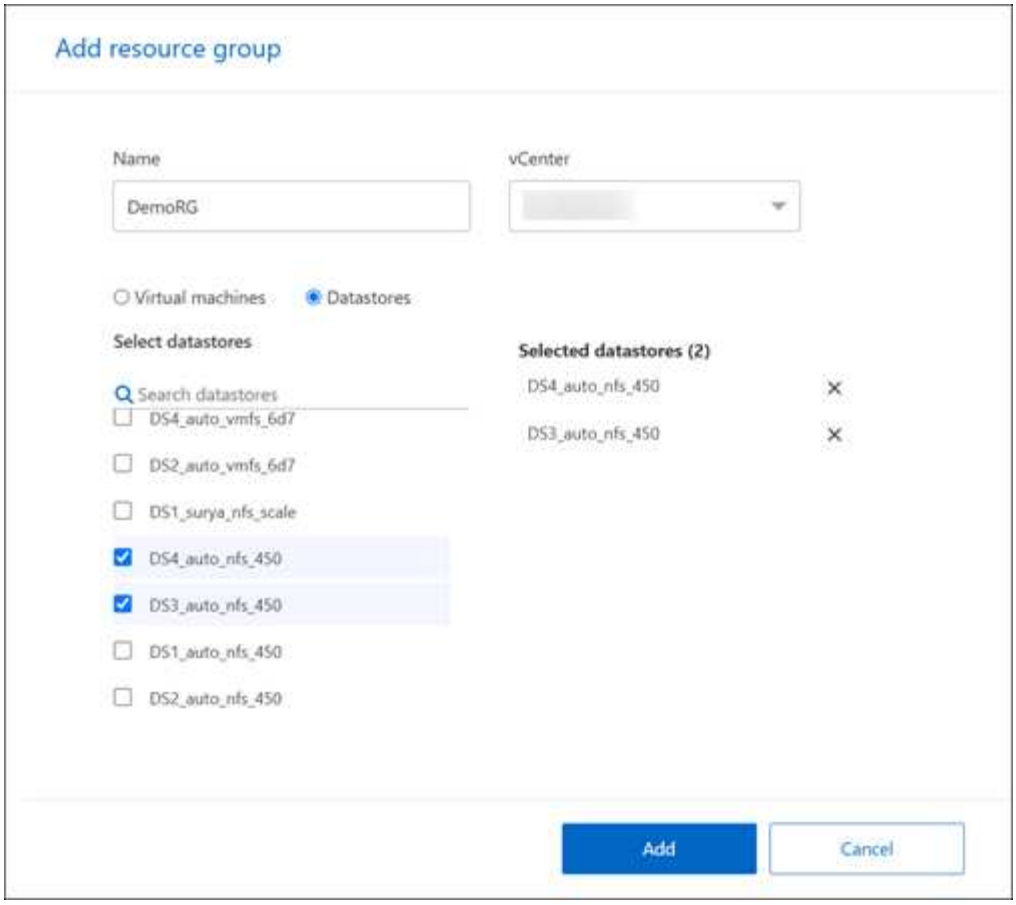
BEST PRACTICE: Organisieren Sie Ihre VMs, bevor Sie NetApp Disaster Recovery bereitstellen, um die

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.

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. 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:

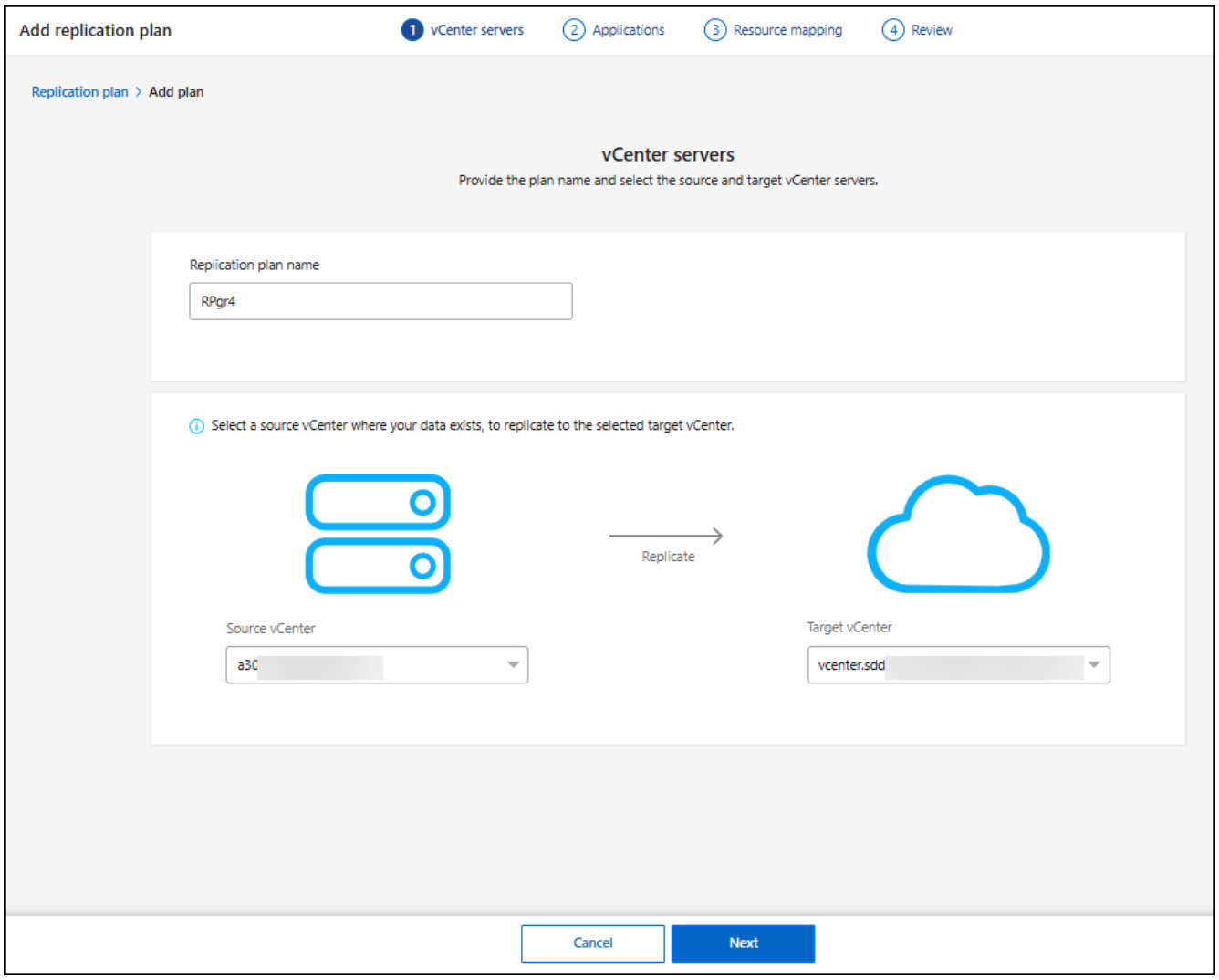
- Verwenden Sie für alle VMs im Plan dieselben Anmeldeinformationen.
- Verwenden Sie für alle VMs im Plan dasselbe Skript.
- Verwenden Sie für alle VMs im Plan dasselbe Subnetz, DNS und Gateway.

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.

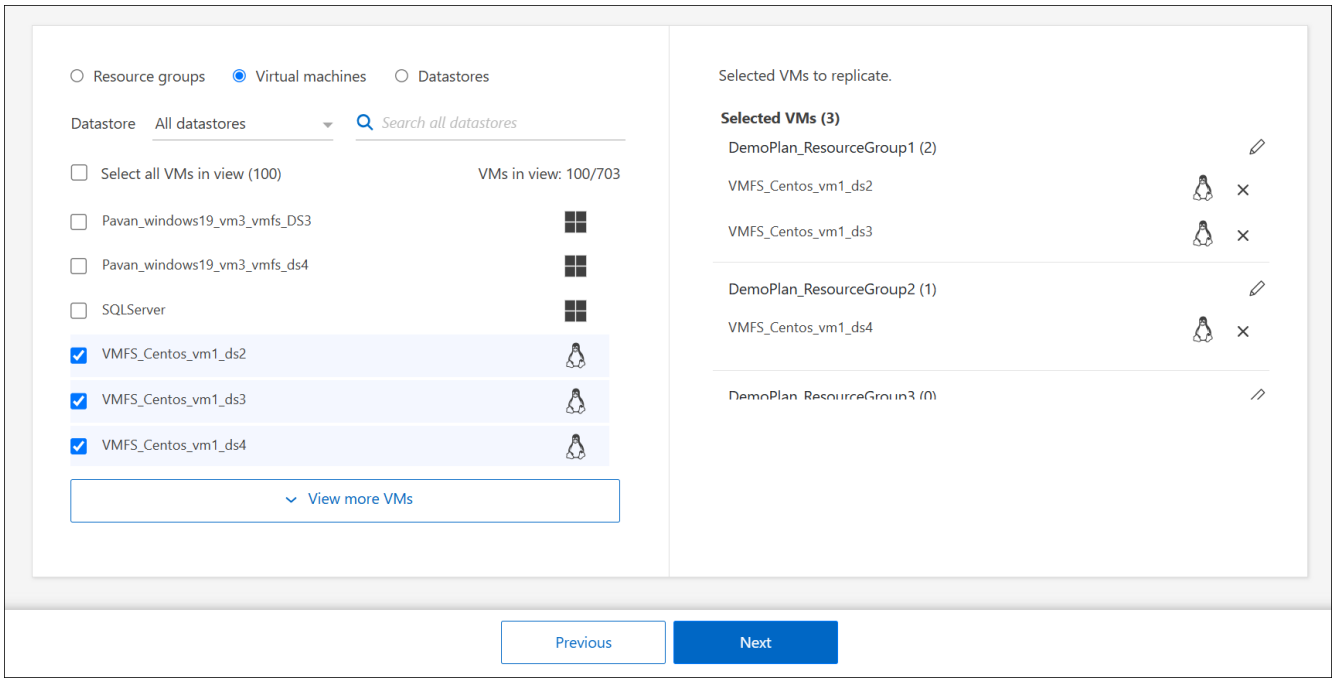
BEST PRACTICE: Erstellen Sie einen separaten dedizierten Satz von Zuordnungen für Ihre Failover-Tests, um zu verhindern, dass VMS über dieselben IP-Adressen mit Produktionsnetzwerken verbunden werden.

Schritte

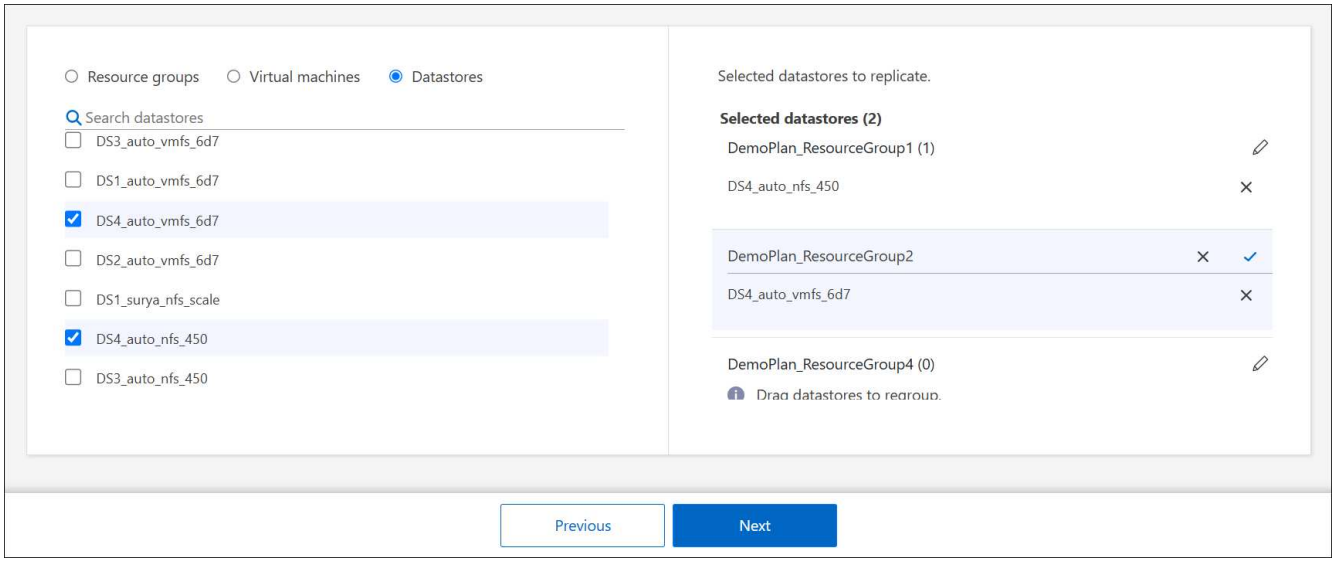
1. Wählen Sie **Virtuelle Maschinen** oder **Datenspeicher**.
2. Suchen Sie optional nach bestimmten VMs oder Datenspeichern anhand des Namens.
3. Wählen Sie auf der linken Seite der Anwendungsseite die VMs oder Datenspeicher aus, die Sie schützen möchten, und weisen Sie sie der ausgewählten Gruppe zu.

   Das Quell-vCenter muss sich auf dem lokalen vCenter befinden. Das Ziel-vCenter kann ein zweites lokales vCenter am selben Standort oder an einem Remote-Standort oder ein Cloud-basiertes Software Defined Data Center (SDDC) wie VMware Cloud on AWS sein. Beide vCenter sollten bereits zu Ihrer BlueXP disaster recovery 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.

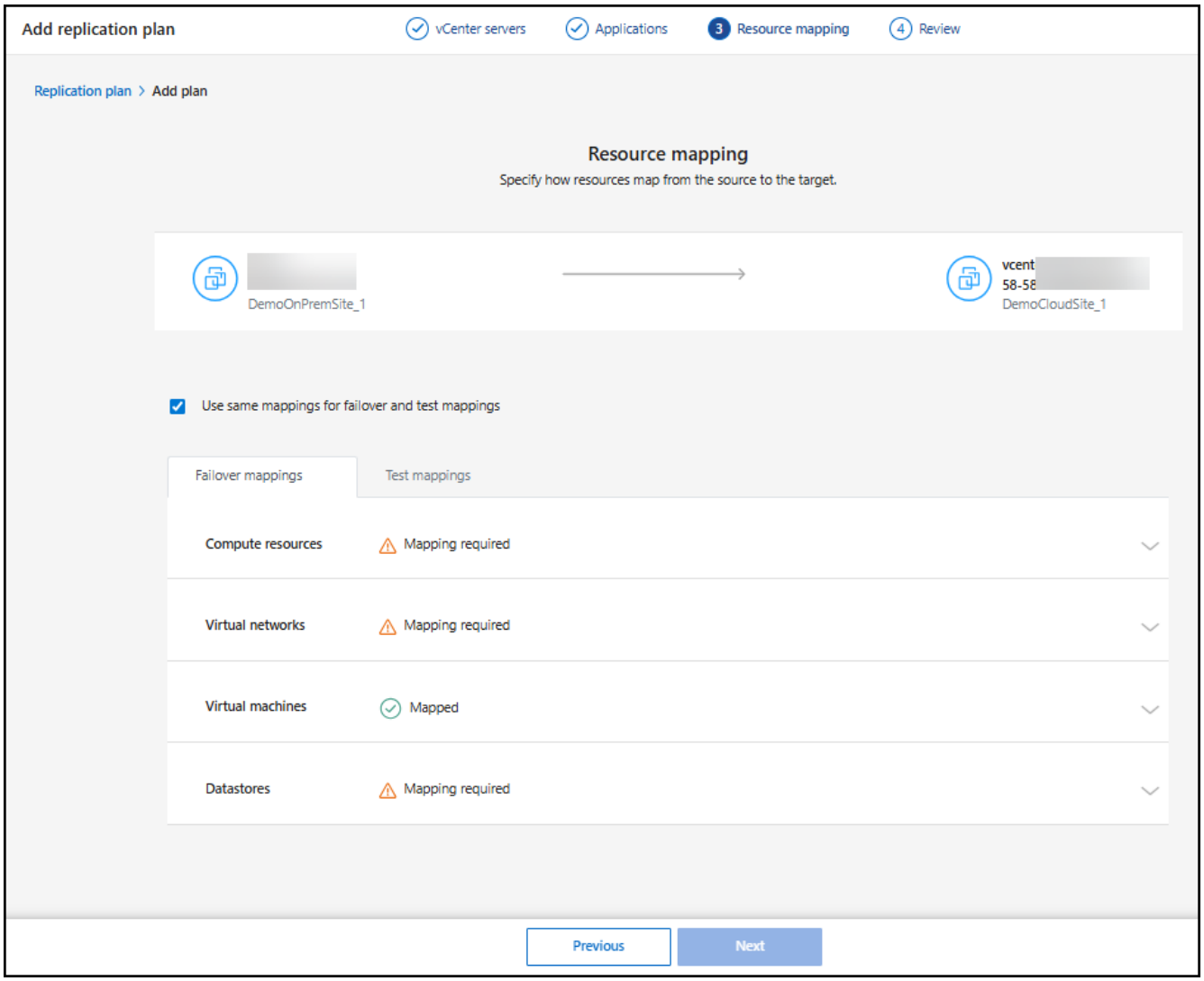
Wenn Sie im Rahmen Ihres DR-Plans Test-Failover durchführen möchten, sollten Sie eine Reihe von Test-Failover-Zuordnungen bereitstellen, um sicherzustellen, dass während des Failover-Tests gestartete VMs keine Produktions-VMs stören. Sie können dies erreichen, indem Sie entweder Test-VMs mit unterschiedlichen 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.

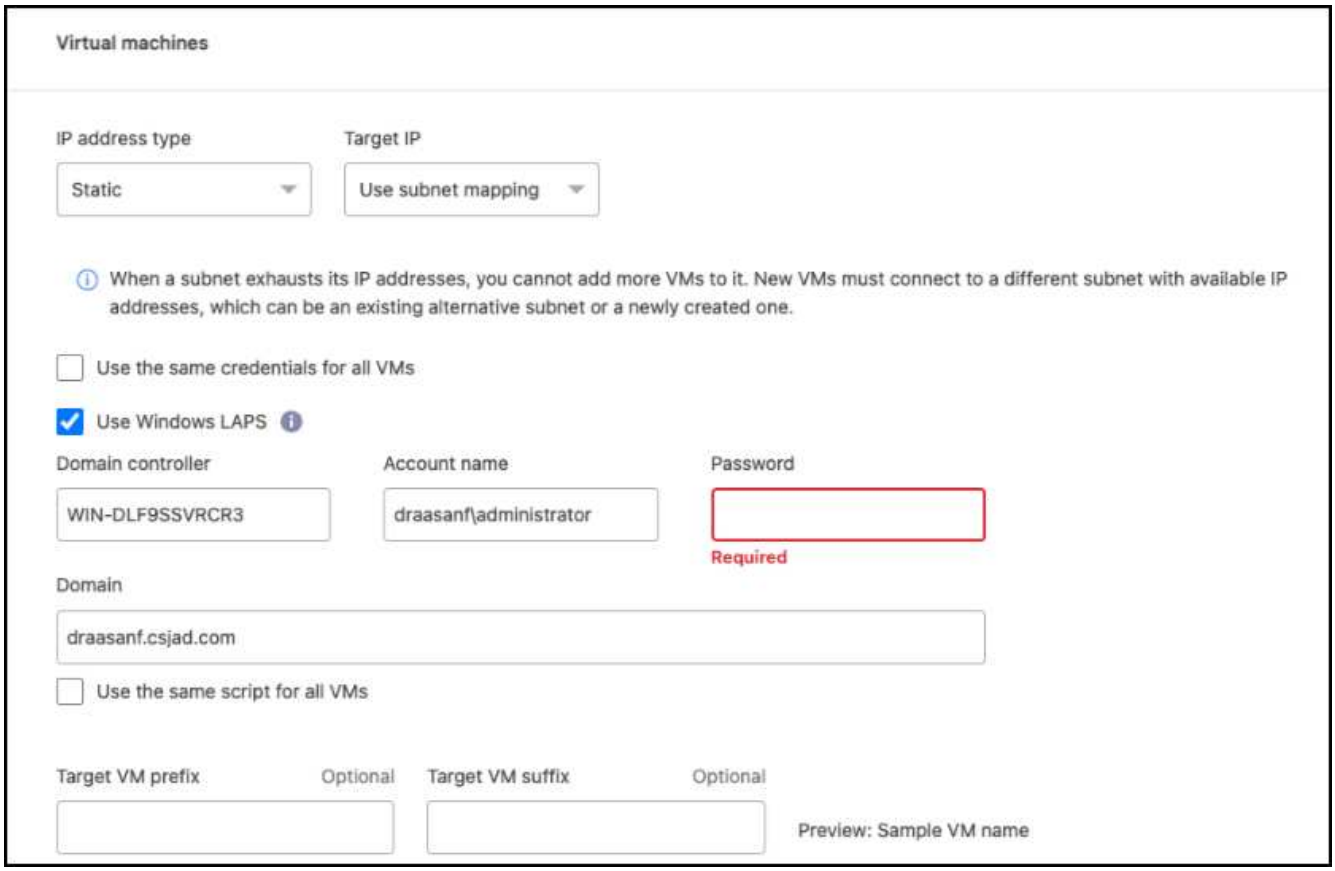
Der Dienst unterstützt Netzwerkeinstellungen der statischen oder Dynamic Host Configuration Protocol (DHCP)-IP-Konfiguration für VMs. DHCP bietet eine standardbasierte Methode zur dynamischen Konfiguration der TCP/IP-Einstellungen eines Host-Netzwerkports. DHCP muss mindestens eine TCP/IP-Adresse bereitstellen 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, vom Gastbetriebssystem gehostete Skripte im .sh-, .bat- oder .ps1-Format als Postprozesse einbinden. Mit benutzerdefinierten Skripten kann die BlueXP disaster

recovery Ihr Skript nach einem Failover, Failback und Migrationsprozessen ausführen. Sie können beispielsweise ein benutzerdefiniertes Skript verwenden, um alle Datenbanktransaktionen nach Abschluss des Failovers fortzusetzen. Der Dienst kann Skripte in VMs ausführen, auf denen Microsoft Windows oder eine beliebige unterstützte Linux-Variante mit unterstützten Befehlszeilenparametern 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.

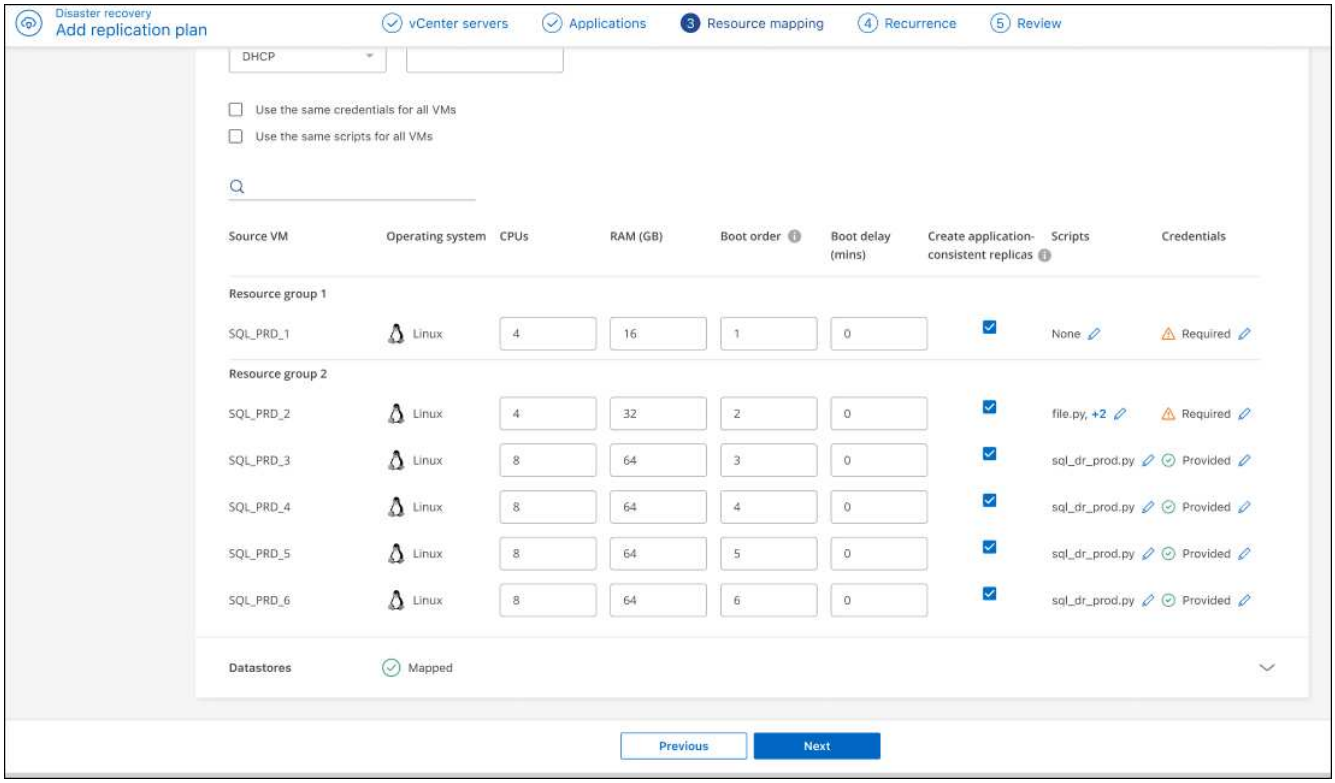
VMs mit Linux: können jedes Shell-Skript (.sh) ausführen, das von der von der VM verwendeten Linux-Version unterstützt wird. Linux-Skripte können Befehlszeilenargumente verwenden. Geben Sie Argumente in einer durch Semikolons getrennten Werteliste an. Benannte Argumente werden nicht unterstützt. Fügen 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` .

- **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.

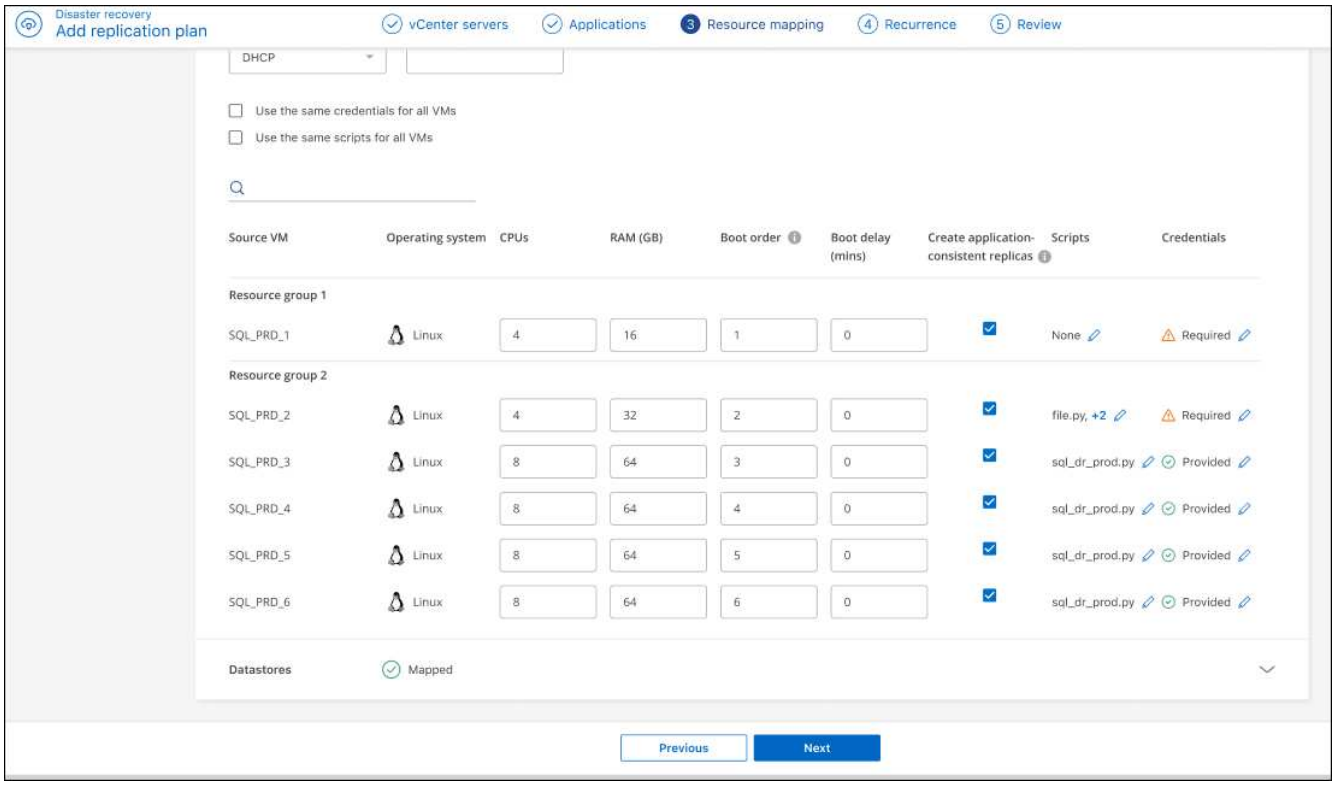
  BlueXP disaster recovery bootet alle VMs mit der gleichen Bootreihenfolgenummer parallel.

  - 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.

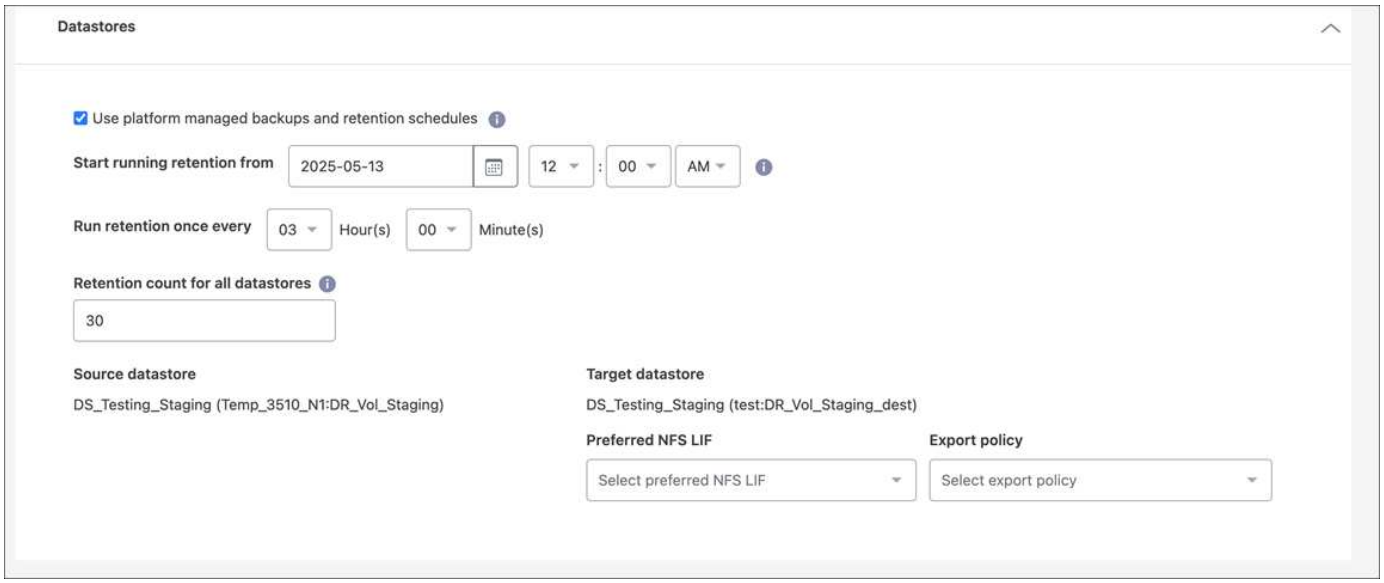
Um anwendungskonsistente Replikate der VMs und ihrer Hosting-Datenspeicher zu aktivieren, aktivieren Sie das Kontrollkästchen neben **Anwendungskonsistente Replikate erstellen** für jede VM und geben Sie Gastanmeldeinformationen mit den entsprechenden Berechtigungen an.

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.

BEST PRACTICE: Wir empfehlen dringend, eine dedizierte Exportrichtlinie zu erstellen, die den Volumezugriff nur 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.

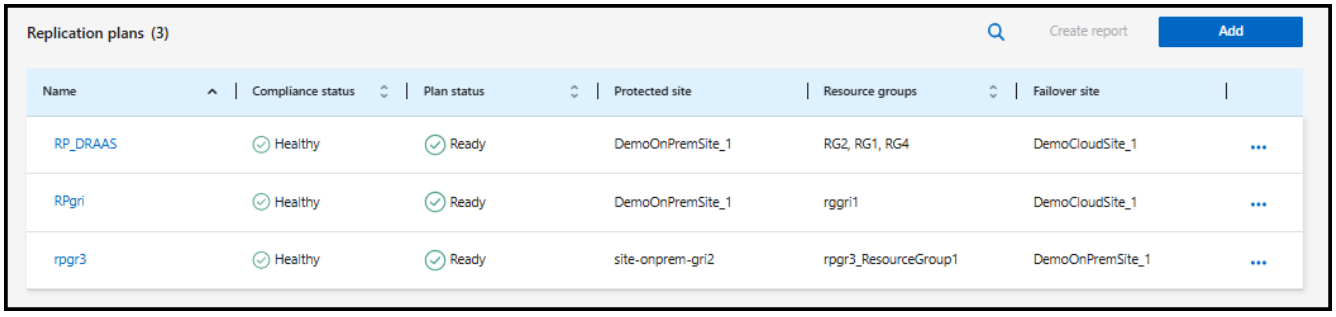
- **Auswirkungen auf die Compliance-Zeit**: Wenn ein Replikationsplan erstellt wird, erstellt der Dienst standardmäßig einen Compliance-Zeitplan. Die Standard-Compliance-Zeit beträgt 30 Minuten. Um diese Zeit zu ändern, können Sie den Zeitplan im Replikationsplan bearbeiten.
- **Auswirkungen des Failovers 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.

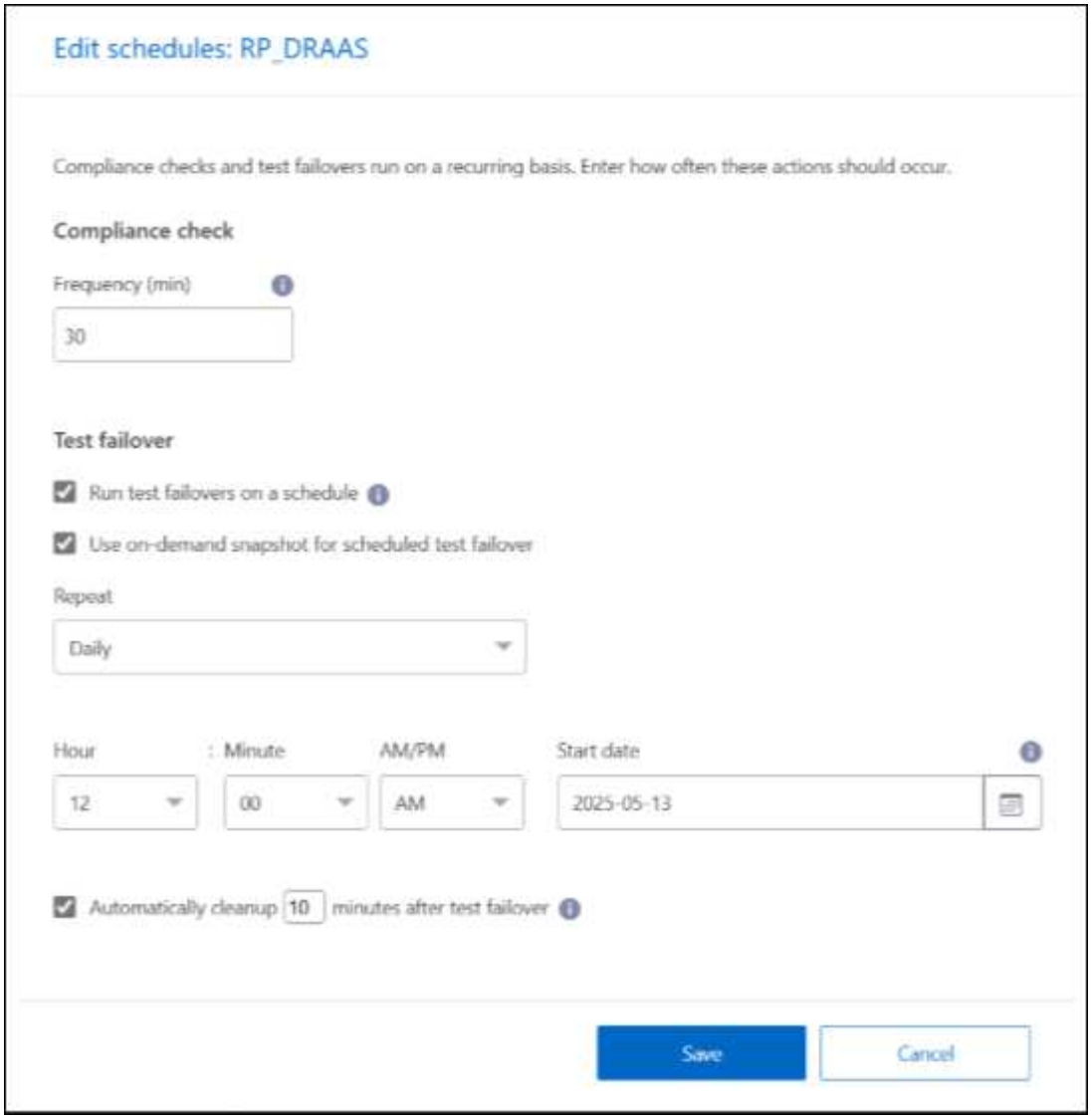
Basierend auf dem Zeitplan wird der Failover-Test ausgeführt und stellt sicher, dass die Workloads an das im Replikationsplan angegebene Ziel verschoben werden.

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

Während eines Failovers verwendet Disaster Recovery die aktuellste SnapMirror Snapshot-Kopie. Oder Sie können einen bestimmten Snapshot aus einem Point-in-Time-Snapshot auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror).

Verwenden Sie die Point-in-Time-Option, wenn die aktuellsten Replikate kompromittiert wurden, beispielsweise während eines Ransomware-Angriffs. BlueXP disaster recovery zeigt alle verfügbaren Zeitpunkte an.

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 BlueXP disaster recovery vorübergehend virtuelle Maschinen. BlueXP disaster recovery ordnet den ESXi-Hosts einen temporären Datenspeicher zu, der das FlexClone -Volume sichert.

Dieser Prozess verbraucht keine zusätzliche physische Kapazität auf dem lokalen ONTAP -Speicher oder FSx für NetApp ONTAP -Speicher in AWS. Das ursprüngliche Quellvolume wird nicht geändert 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*** ••• **und wählen Sie *Failover-Test bereinigen**.
4. Geben Sie auf der Seite „Failover testen“ „Failover bereinigen“ ein und wählen Sie **Failovertest 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.

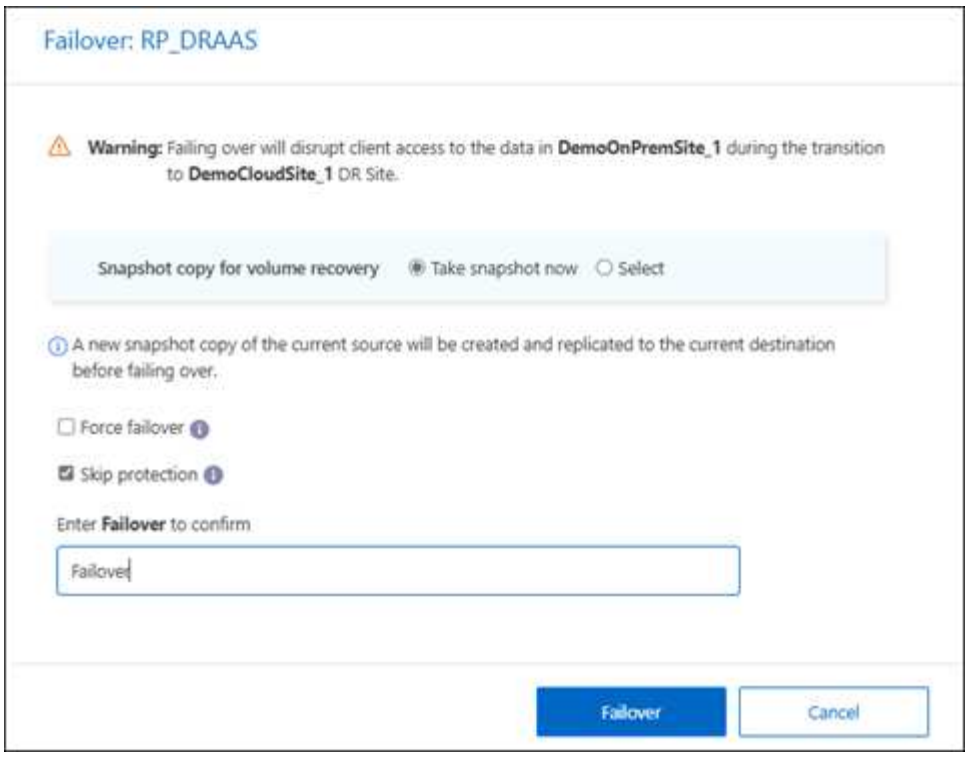
Der Failover-Prozess umfasst die folgenden Vorgänge:

- 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.

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. Initiieren Sie auf der Seite „Failover“ entweder jetzt einen Snapshot oder wählen Sie den Snapshot für den Datenspeicher aus, von dem die Wiederherstellung erfolgen soll. Die Standardeinstellung ist die neueste Version.

   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 diese Aufgabe

In diesem Workflow repliziert (resynchronisiert) NetApp Disaster Recovery alle Änderungen zurück zur ursprünglichen virtuellen Quellmaschine, bevor die Replikationsrichtung umgekehrt wird. Dieser Prozess beginnt mit einer Beziehung, deren Failover zu einem Ziel abgeschlossen ist, 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.

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 *Failback**.
6. Geben Sie den Namen des Replikationsplans ein, um das Failback zu bestätigen und zu starten.
7. Wählen Sie den Snapshot für den Datenspeicher aus, aus dem die Wiederherstellung erfolgen soll. Die Standardeinstellung ist die neueste Version.
8. Um den Fortschritt zu überprüfen, wählen Sie im Menü **Jobüberwachung**.

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

Sie können einen schnellen Überblick über alle Ihre NetApp Disaster Recovery -Ressourcen erhalten oder sich jede im Detail ansehen:

- 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 zwar beim Erstellen eines Replikationsplans eine Ressourcengruppe hinzufügen, es ist jedoch möglicherweise praktischer, die Gruppen separat hinzuzufügen und diese Gruppen später im Plan zu verwenden. Sie erstellen Ressourcengruppen nach VMs oder nach Datenspeichern.

*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 die folgenden 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. Um Aktionen mit der Ressourcengruppe durchzuführen, wählen Sie die Option **Aktionen*** ••• **und wählen Sie eine der Optionen aus, z. B. *Ressourcengruppe bearbeiten** oder **Ressourcengruppe löschen**.

Verwalten von Replikationsplänen

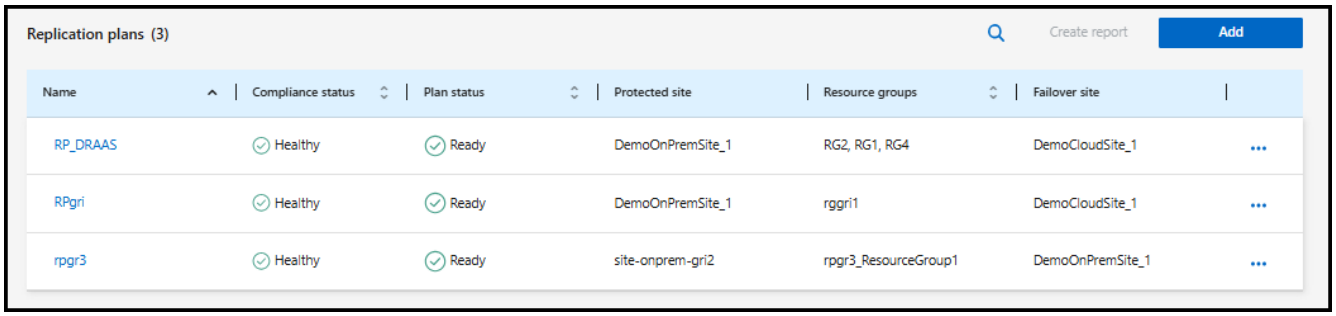
Sie können Replikationspläne deaktivieren, aktivieren und löschen. Sie können Zeitpläne ändern.

*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**.

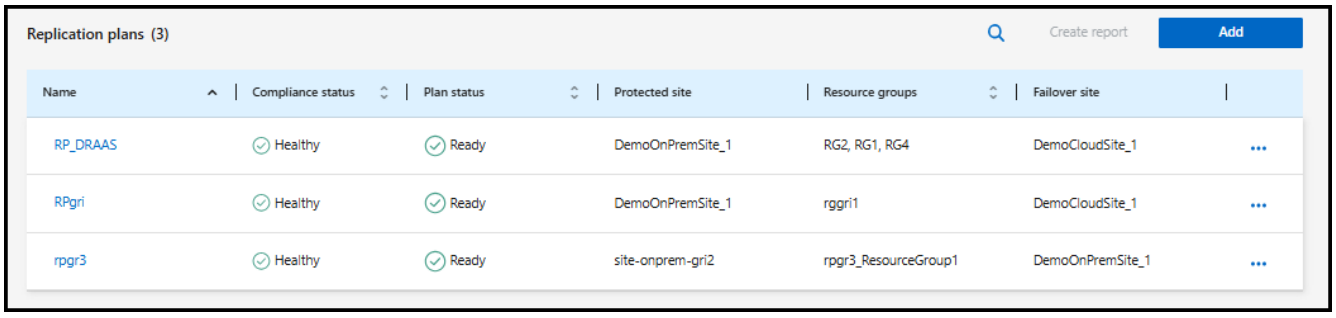
Snapshots bei Bedarf abgleichen

Sie können Snapshots abgleichen, die zwischen Quelle und Ziel nicht synchron sind. Dies kann auftreten, wenn Snapshots auf einem Ziel außerhalb von NetApp Disaster Recovery gelöscht werden. Der Dienst löscht den Snapshot auf der Quelle automatisch alle 24 Stunden. Sie können dies jedoch auf Anfrage durchführen. Mit dieser Funktion können Sie sicherstellen, dass die Snapshots auf allen Sites konsistent sind.

*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 aus der Liste der Replikationspläne die Option **Aktionen*** ••• **rechts neben dem Plan und wählen Sie *Snapshots abgleichen**.

3. Überprüfen Sie die Abstimmungsinformationen.

4. Wählen Sie **Abgleichen**.

Löschen eines Replikationsplans

Sie können einen Replikationsplan löschen, wenn Sie ihn nicht mehr benötigen. 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, sekundären Snapshots oder nur die vom Plan erstellten Metadaten löschen möchten.

4. Geben Sie „delete“ ein, um den Löschvorgang zu bestätigen.
5. Wählen Sie **Löschen**.

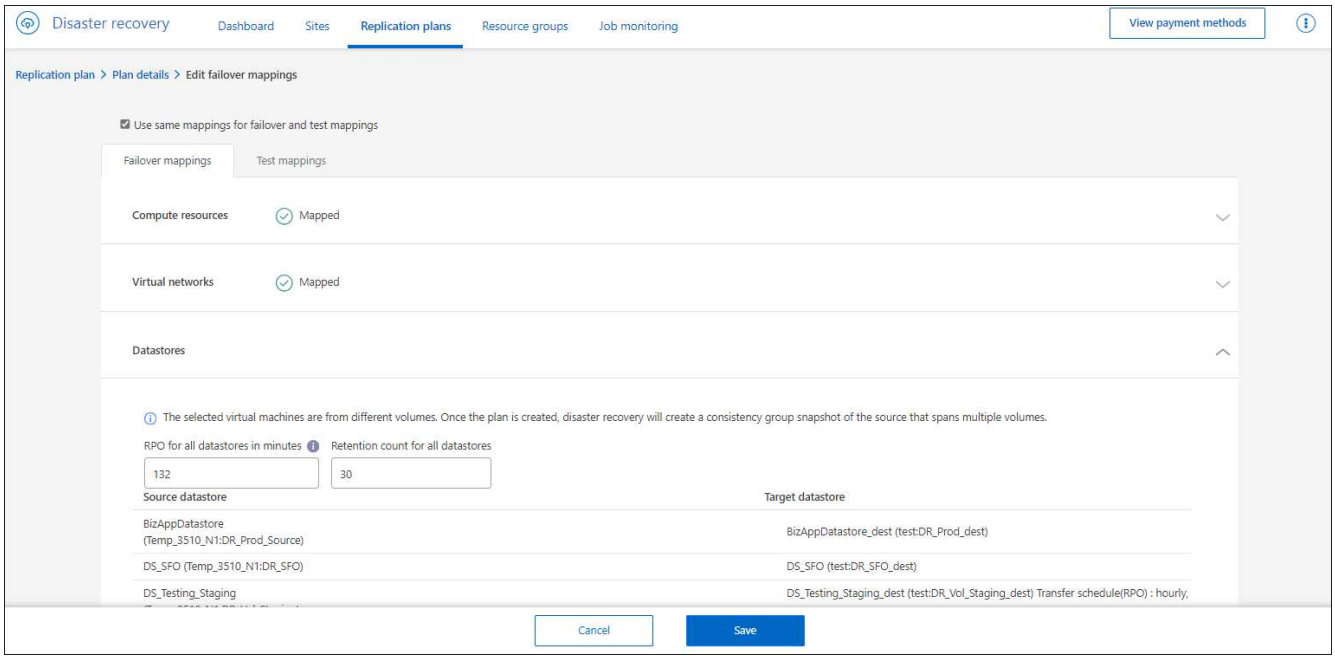
Ändern der Aufbewahrungsanzahl für Failover-Zeitpläne

Sie können ändern, wie viele Datenspeicher beibehalten werden.

*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 aus, wählen Sie die Registerkarte **Failover-Zuordnung** und wählen Sie das Bleistiftsymbol **Bearbeiten**.
3. Wählen Sie den Pfeil **Datenspeicher** aus, um ihn zu erweitern.



4. Ändern Sie den Wert der Aufbewahrungsanzahl im Replikationsplan.
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.

Referenz

Für NetApp Disaster Recovery erforderliche vCenter-Berechtigungen

Das vCenter-Konto muss über einen Mindestsatz an vCenter-Berechtigungen verfügen, damit NetApp Disaster Recovery seine Dienste ausführen kann, z. B. das Registrieren und Aufheben der Registrierung von Datenspeichern, das Starten und Stoppen von VMs und die Neukonfiguration virtueller Maschinen (VMs). In der folgenden Tabelle sind alle Berechtigungen aufgeführt, die NetApp Disaster Recovery für die Schnittstelle mit einem vCenter-Cluster benötigt.

Typ	Berechtigungsname	Beschreibung
Datenspeicher	Datastore.Datenspeicher konfigurieren	Wird zum Konfigurieren eines Datenspeichers verwendet.
	Datastore.Datenspeicher entfernen	Wird zum Entfernen eines Datenspeichers verwendet.
Virtuelle Maschine	Virtuelle Maschine.Konfiguration.Einstellungen ändern	Wird verwendet, um allgemeine VM-Einstellungen zu ändern.
	Virtuelle Maschine.Konfiguration.Geräteeinstellungen ändern	Dient zum Ändern der Eigenschaften eines vorhandenen Geräts.
	Virtuelle Maschine.Konfiguration.Neu laden vom Pfad	Wird verwendet, um einen VM-Konfigurationspatch zu ändern und gleichzeitig die Identität der VM beizubehalten. Lösungen wie VMware vCenter Site Recovery Manager verwenden diesen Vorgang, um die VM-Identität während eines Failovers und Failbacks aufrechtzuerhalten.
	Virtuelle Maschine.Konfiguration.Umbenennen	Wird verwendet, um eine VM umzubenennen oder die zugehörigen Knoten einer VM zu ändern.
	Virtuelle Maschine.Konfiguration.Gastinformationen zurücksetzen	Wird verwendet, um die Informationen zum Gastbetriebssystem für eine VM zu bearbeiten.

Typ	Berechtigungsname	Beschreibung
	Virtuelle Maschine.Konfiguration.Speicher ändern	Verwenden Sie diese Option, um die der VM zugewiesene Speichermenge zu ändern.
	Virtuelle Maschine.Konfiguration.CPU-Anzahl ändern	Dient zum Ändern der Anzahl der virtuellen CPUs.
Virtuelle Maschine als Gast	Virtuelle Maschine.Gastvorgänge.Änderungen an Gastvorgängen	Ermöglicht VM-Gastvorgänge, die Änderungen an einem Gastbetriebssystem in einer VM beinhalten, beispielsweise das Übertragen einer Datei auf die VM.
Interaktion mit virtuellen Maschinen	Virtuelle Maschine.Interaktion.Ausschalten	Wird zum Ausschalten einer eingeschalteten VM verwendet. Dieser Vorgang schaltet das Gastbetriebssystem ab.
	Virtuelle Maschine.Interaktion.Einschalten	Wird verwendet, um eine ausgeschaltete VM einzuschalten und eine angehaltene VM fortzusetzen.
	Virtuelle Maschine.Interaktion.VMware Tools installieren	Wird zum Mounten und Unmounten des VMware Tools-CD-Installationsprogramms als CD-ROM für das Gastbetriebssystem verwendet.
Inventar virtueller Maschinen	Virtuelle Maschine.Inventar.Neu erstellen	Wird verwendet, um eine VM zu erstellen und Ressourcen für ihre Ausführung zuzuweisen.
	Virtuelle Maschine.Inventar.Registrieren	Wird verwendet, um eine vorhandene VM zu einem vCenter Server oder Host-Inventar hinzuzufügen.
	Virtuelle Maschine.Inventar.Registrierung aufheben	Wird verwendet, um die Registrierung einer VM von einem vCenter Server oder Host-Inventar aufzuheben.
Status der virtuellen Maschine	Virtuelle Maschine.Snapshot-Verwaltung.Snapshot erstellen	Wird verwendet, um einen Snapshot vom aktuellen Status der VM zu erstellen.
	Virtuelle Maschine.Snapshot-Verwaltung.Snapshot entfernen	Wird verwendet, um einen Snapshot aus dem Snapshot-Verlauf zu entfernen.

Typ	Berechtigungsname	Beschreibung
	Virtuelle Maschine.Snapshot-Verwaltung.Zurück zum Snapshot	Wird verwendet, um die VM auf den Zustand zurückzusetzen, in dem sie sich bei einem bestimmten Snapshot befand.

Rollenbasierter Zugriff auf Funktionen von NetApp Disaster Recovery

NetApp Disaster Recovery verwendet Rollen, um den Zugriff jedes Benutzers auf bestimmte Funktionen und Aktionen zu regeln.

Der Dienst verwendet die folgenden Rollen, die spezifisch für NetApp Disaster Recovery sind.

- **Disaster Recovery-Administrator**: Führen Sie beliebige Aktionen in NetApp Disaster Recovery aus.
- **Disaster Recovery-Failover-Administrator**: Führen Sie Failover- und Migrationsaktionen in NetApp Disaster Recovery durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Erstellen und ändern Sie Replikationspläne und starten Sie Test-Failover.
- **Disaster Recovery Viewer**: Informationen in NetApp Disaster Recovery anzeigen, aber keine Aktionen ausführen.

Diese Rollen sind spezifisch für NetApp Disaster Recovery und nicht identisch mit den Plattformrollen, die in der NetApp Console verwendet werden. Einzelheiten zu allen NetApp Console Plattformrollen finden Sie unter "die Dokumentation zur Einrichtung und Administration der NetApp Console" .

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Disaster Recovery -Rolle ausführen kann.

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Ja	Nein	Nein	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Ja	Nein
Bei der Option „Sites“:				
Websites anzeigen	Ja	Ja	Ja	Ja

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Hinzufügen, Ändern oder Löschen von Sites	Ja	Nein	Nein	Nein
Zur Option „Replikationspläne“:				
Replikationspläne anzeigen	Ja	Ja	Ja	Ja
Anzeigen von Replikationsplandetails	Ja	Ja	Ja	Ja
Erstellen oder Ändern von Replikationsplänen	Ja	Ja	Ja	Nein
Erstellen von Berichten	Ja	Nein	Nein	Nein
Snapshots anzeigen	Ja	Ja	Ja	Ja
Durchführen von Failover-Tests	Ja	Ja	Ja	Nein
Durchführen von Failovers	Ja	Ja	Nein	Nein
Failbacks durchführen	Ja	Ja	Nein	Nein
Migrationen durchführen	Ja	Ja	Nein	Nein
Zur Option „Ressourcengruppen“:				
Anzeigen von Ressourcengruppen	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Ressourcengruppen	Ja	Nein	Ja	Nein
Option zur Überwachung am Arbeitsplatz:				
Jobs anzeigen	Ja	Nein	Ja	Ja
Aufträge abbrechen	Ja	Ja	Ja	Nein

Verwenden Sie NetApp Disaster Recovery mit Amazon EVS

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

Kunden sind für Produktions-Rechenlasten zunehmend auf virtualisierte Infrastrukturen angewiesen, beispielsweise auf Basis von VMware vSphere. Da diese virtuellen

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

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

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

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

Informationen zu Amazon FSx for NetApp ONTAP finden Sie unter "Erste Schritte mit Amazon FSx for NetApp ONTAP" .

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

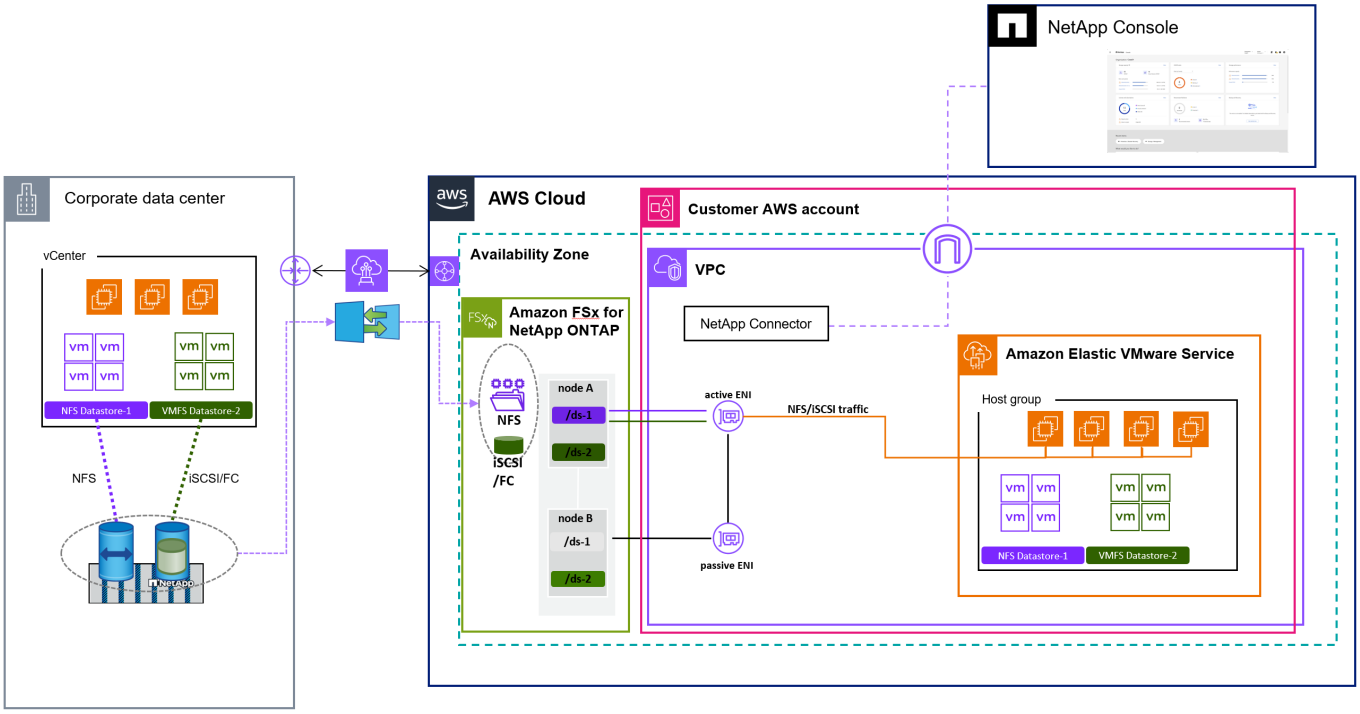
NetApp Disaster Recovery ist ein Mehrwertdienst, der in der Software-as-a-Service-Umgebung der NetApp Console gehostet wird und auf der Kernarchitektur der NetApp Console basiert. Der DR-Dienst für den VMware-Schutz innerhalb der Konsole besteht aus mehreren Hauptkomponenten.

Eine vollständige Übersicht über die NetApp Disaster Recovery -Lösung finden Sie unter"Erfahren Sie mehr über NetApp Disaster Recovery für VMware" .

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

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

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



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

geschützte VM beim Amazon EVS vCenter und startet jede gemäß den im Replikationsplan enthaltenen vordefinierten Regeln.

Installieren Sie den NetApp Console -Agenten für NetApp Disaster Recovery

Ein NetApp Console Agent ist eine NetApp -Software, die in Ihrer Cloud oder Ihrem lokalen Netzwerk ausgeführt wird. Es führt die Aktionen aus, die die NetApp Console zur Verwaltung Ihrer Dateninfrastruktur ausführen muss. Der Konsolenagent fragt die NetApp Disaster Recovery -Software als Serviceebene ständig nach erforderlichen Aktionen ab.

Bei NetApp Disaster Recovery werden mit den ausgeführten Aktionen VMware vCenter-Cluster und ONTAP Speicherinstanzen mithilfe nativer APIs für jeden jeweiligen Dienst orchestriert, um Schutz für Produktions-VMs zu bieten, die an einem lokalen Standort ausgeführt werden. Obwohl der Konsolenagent an jedem Ihrer Netzwerkstandorte installiert werden kann, empfehlen wir für NetApp Disaster Recovery, den Konsolenagenten am DR-Standort zu installieren. Dadurch wird sichergestellt, dass im Falle eines Ausfalls des primären Standorts die Cloud-basierte Konsolen-Benutzeroberfläche von NetApp weiterhin Kontakt mit dem Konsolenagenten hat und den Wiederherstellungsprozess innerhalb dieses DR-Standorts orchestrieren kann.

Um den Dienst zu verwenden, installieren Sie den Konsolenagenten im Standardmodus. Weitere Informationen zu den verschiedenen Konsolen-Agent-Installationsarten finden Sie unter "Erfahren Sie mehr über die Bereitstellungsmodi der NetApp Console | NetApp Dokumentation" .

Obwohl der Konsolenagent für die Verwendung des Dienstes von entscheidender Bedeutung ist, hängen die Installationsschritte zur Installation des Konsolenagenten von Ihren Anforderungen und der Netzwerkkonfiguration ab. Es geht über den Rahmen dieser Informationen hinaus, spezifische Anweisungen zur Installation bereitzustellen.

Die einfachste Methode zum Installieren des Konsolenagenten mit Amazon AWS ist die Verwendung des AWS Marketplace. Weitere Informationen zur Installation des Konsolenagenten über den AWS Marketplace finden Sie unter "Erstellen Sie einen Konsolenagenten aus dem AWS Marketplace | NetApp Dokumentation" .

Konfigurieren Sie NetApp Disaster Recovery für Amazon EVS

Übersicht: Konfigurieren von NetApp Disaster Recovery für Amazon EVS

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

- "Voraussetzungen für Amazon EVS mit NetApp Disaster Recovery"
- "Fügen Sie ONTAP Speicher-Arrays zu NetApp Disaster Recovery hinzu"
- "Aktivieren Sie NetApp Disaster Recovery für Amazon EVS"
- "vCenter-Sites zu NetApp Disaster Recovery hinzufügen"
- "vCenter-Cluster zu NetApp Disaster Recovery hinzufügen"

Voraussetzungen für Amazon EVS mit NetApp Disaster Recovery

Sie sollten sicherstellen, dass mehrere Voraussetzungen erfüllt sind, bevor Sie mit der Konfiguration von Amazon EVS mit NetApp Disaster Recovery fortfahren.

Gehen Sie insbesondere wie folgt vor:

- Erstellen Sie ein vCenter-Benutzerkonto mit den spezifischen VMware-Berechtigungen, die für NetApp Disaster Recovery erforderlich sind, um die erforderlichen Vorgänge auszuführen.

> Wir empfehlen nicht, das standardmäßige Administratorkonto „administrator@vsphere.com“ zu verwenden. Stattdessen sollten Sie auf allen vCenter-Clustern, die am DR-Prozess teilnehmen, ein NetApp Disaster Recovery spezifisches Benutzerkonto erstellen. Eine Liste der erforderlichen Berechtigungen finden Sie unter"Für NetApp Disaster Recovery erforderliche vCenter-Berechtigungen" .

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

  Der Dienst unterstützt NFS und VMFS auf iSCSI (und nicht FC) bei Verwendung von Amazon FSx auf NetApp ONTAP. Während der Dienst FC unterstützt, ist dies bei Amazon FSx for NetApp ONTAP nicht der Fall.

- Stellen Sie sicher, dass Ihr Amazon EVS vCenter mit einem Amazon FSx for NetApp ONTAP Speichercluster verbunden ist.
- Stellen Sie sicher, dass auf allen geschützten VMs VMware-Tools installiert sind.
- Stellen Sie sicher, dass Ihr lokales Netzwerk über eine von Amazon genehmigte Verbindungsmethode mit Ihrem AWS VPC-Netzwerk verbunden ist. Wir empfehlen Ihnen, AWS Direct Connect, AWS Private Link oder ein AWS Site-to-Site-VPN zu verwenden.

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

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

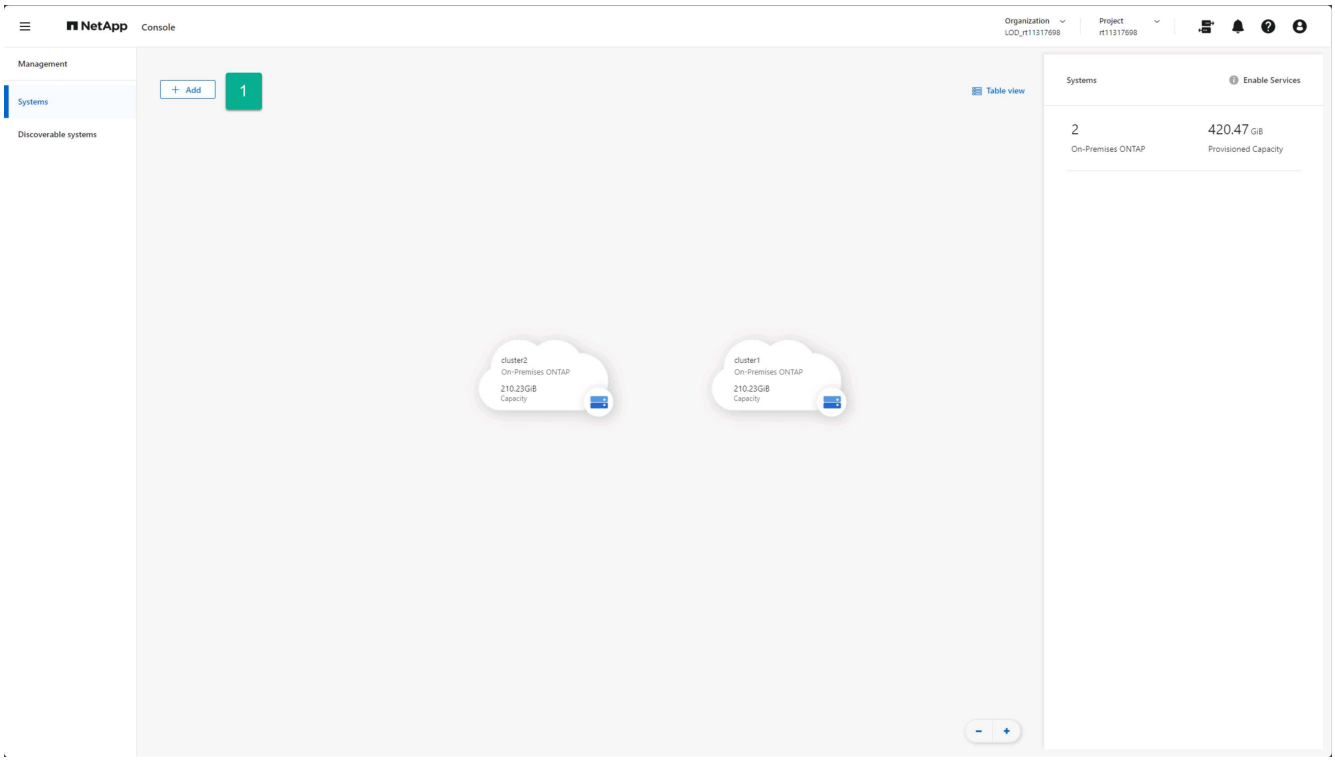
Sie müssen Folgendes tun:

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

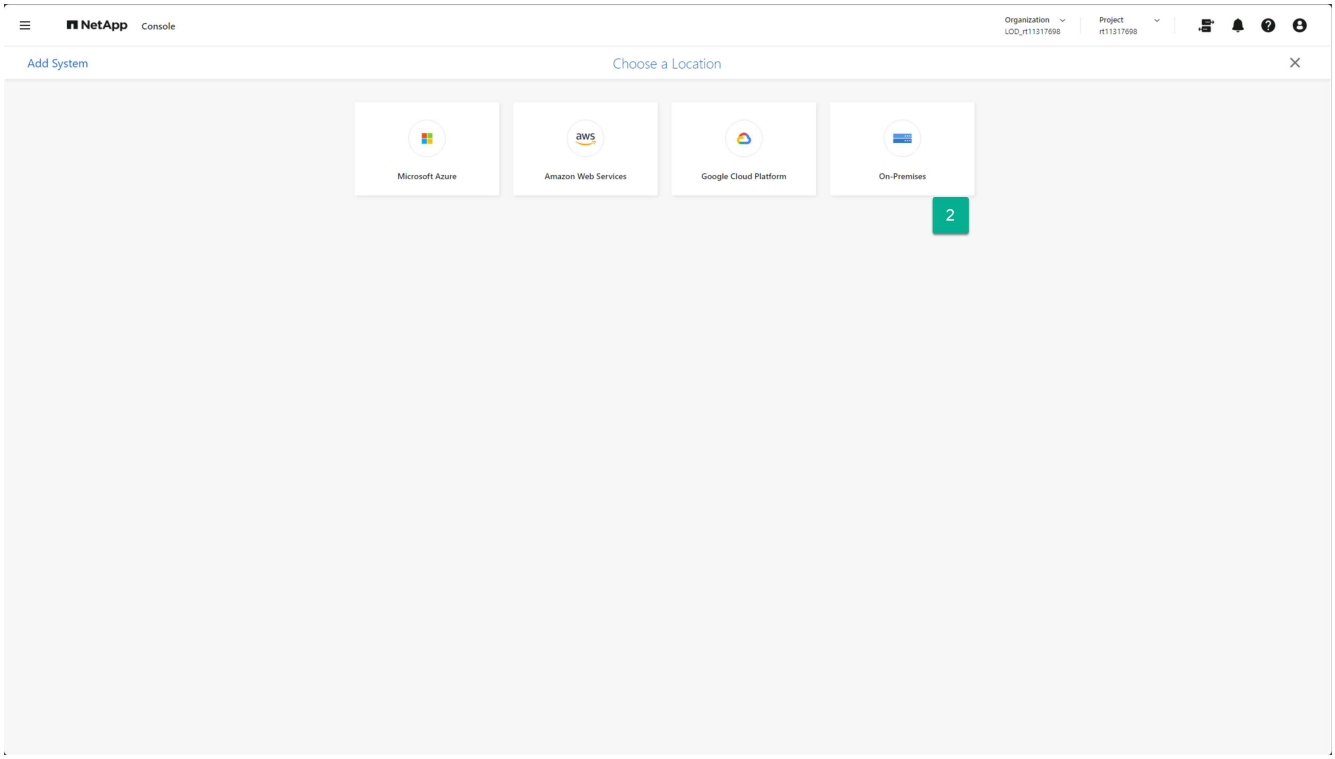
Fügen Sie dem NetApp Console lokale Speicher-Arrays hinzu

Fügen Sie Ihrem NetApp Console lokale ONTAP Speicherressourcen hinzu.

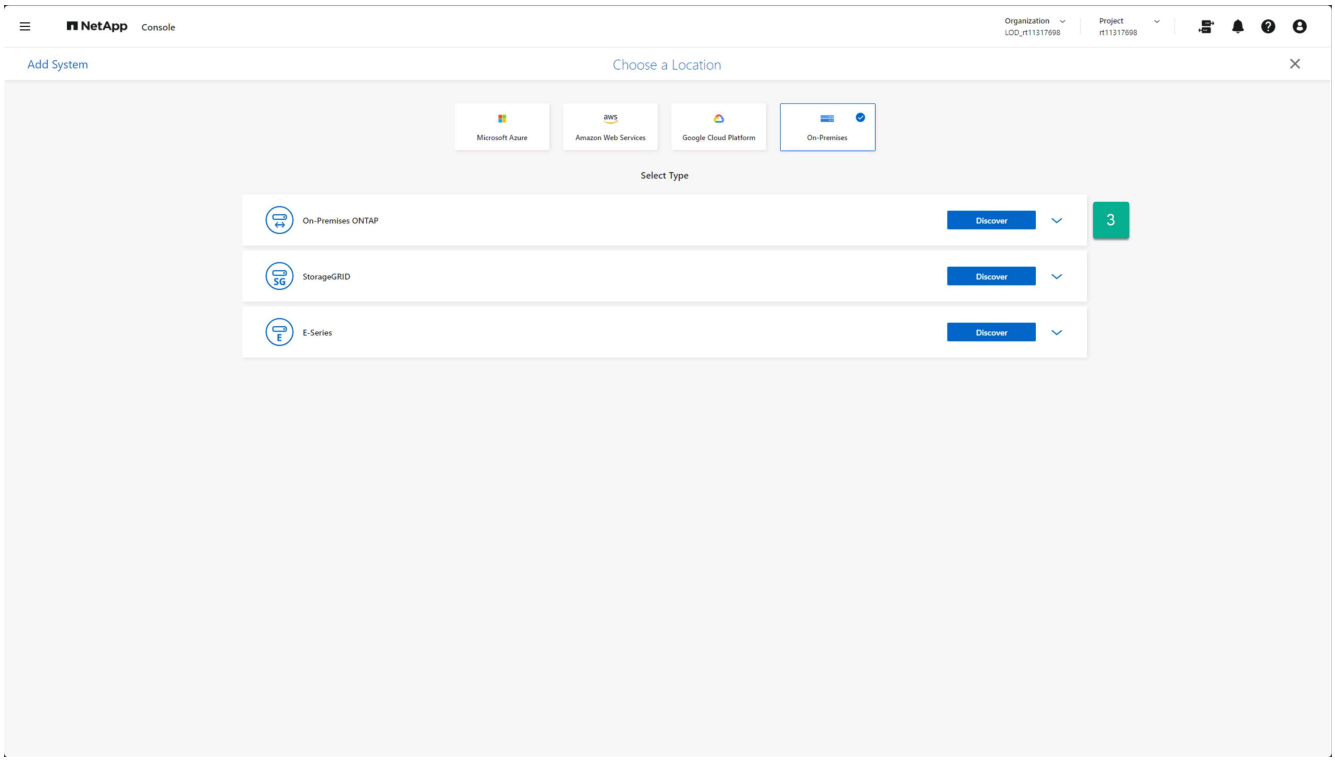
1. Wählen Sie auf der Seite „NetApp Console “ die Option „System hinzufügen“ aus.



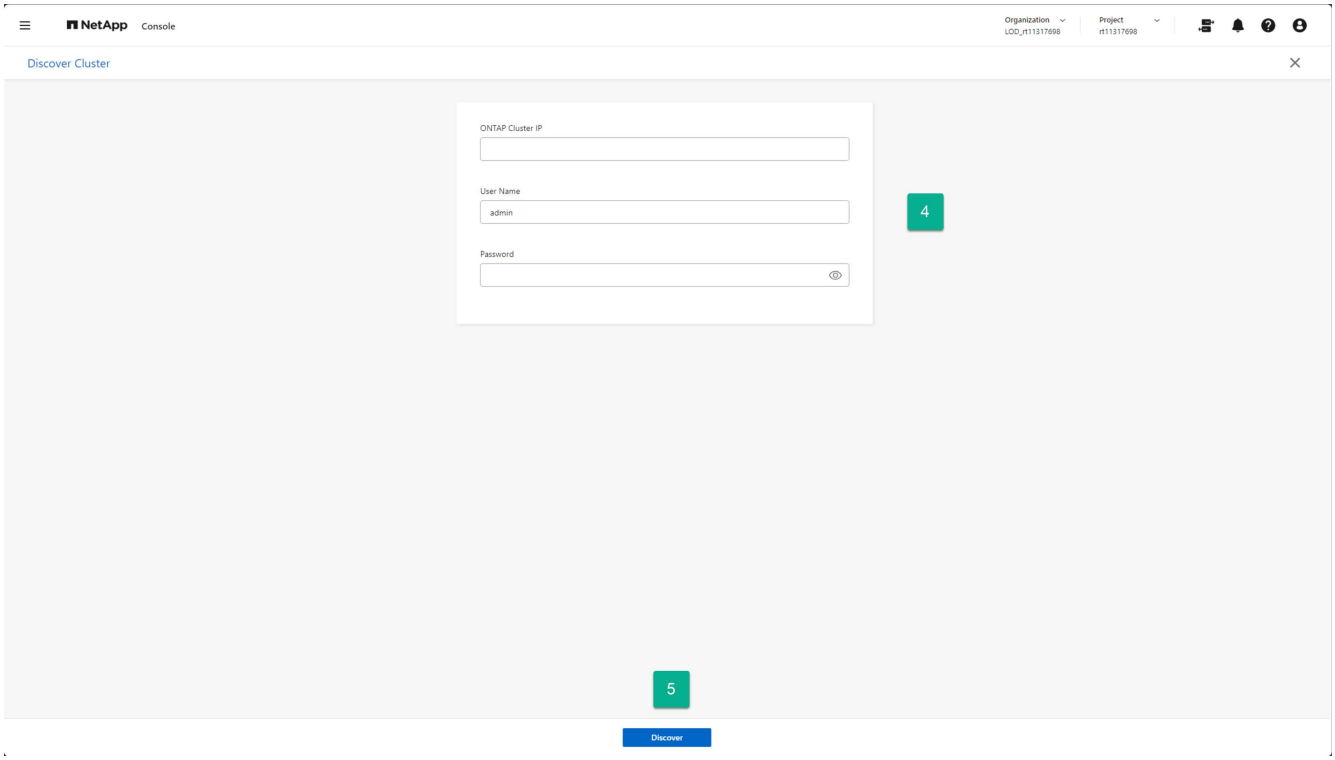
2. Wählen Sie auf der Seite „System hinzufügen“ die Karte **On-Premises** aus.



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



4. Geben Sie auf der Seite „Cluster ermitteln“ die folgenden Informationen ein:
   a. Die IP-Adresse des ONTAP -Array-Cluster-Management-Ports
   b. Der Administrator-Benutzername
   c. Das Administratorkennwort
5. Wählen Sie unten auf der Seite **Entdecken** aus.

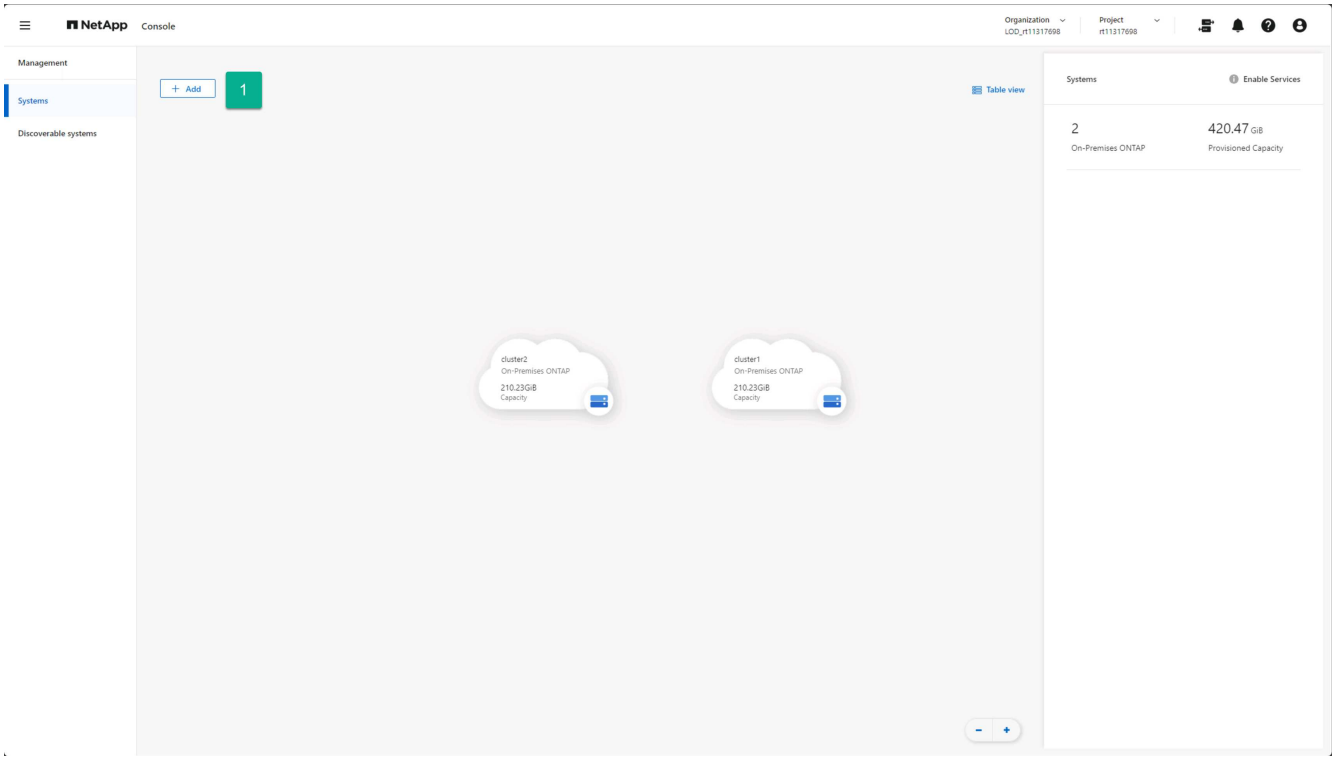


6. Wiederholen Sie die Schritte 1–5 für jedes ONTAP Array, das vCenter-Datenspeicher hosten soll.

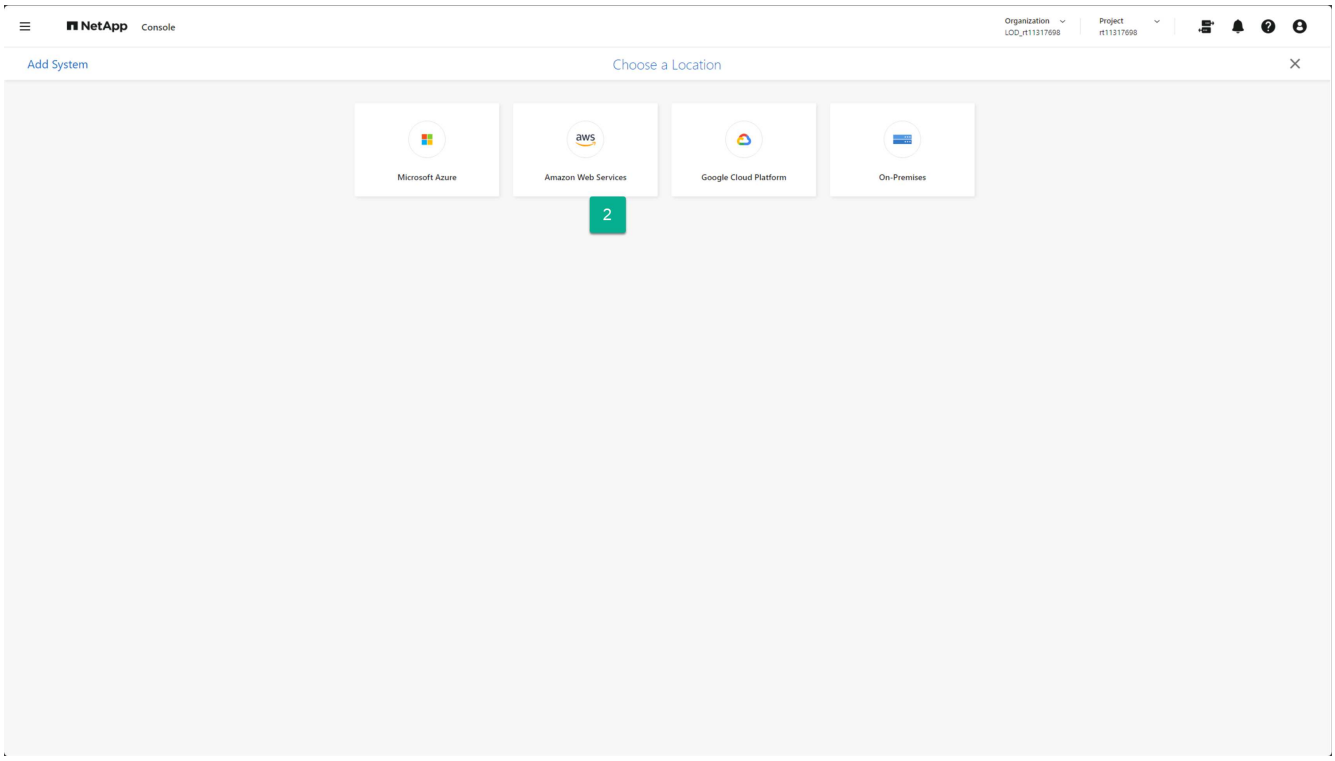
Fügen Sie Amazon FSx for NetApp ONTAP Speicherinstanzen zum NetApp Console hinzu

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

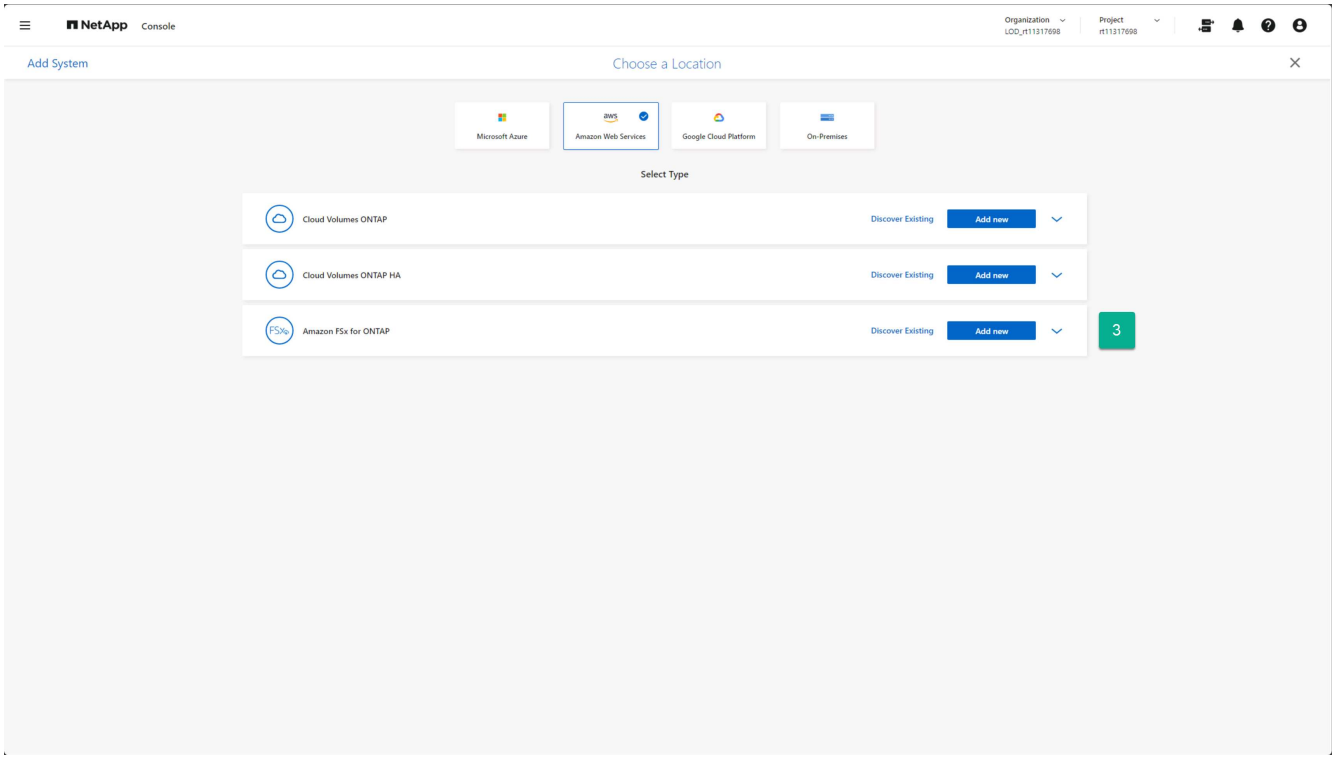
1. Wählen Sie auf der Seite „NetApp Console “ die Option „System hinzufügen“ aus.



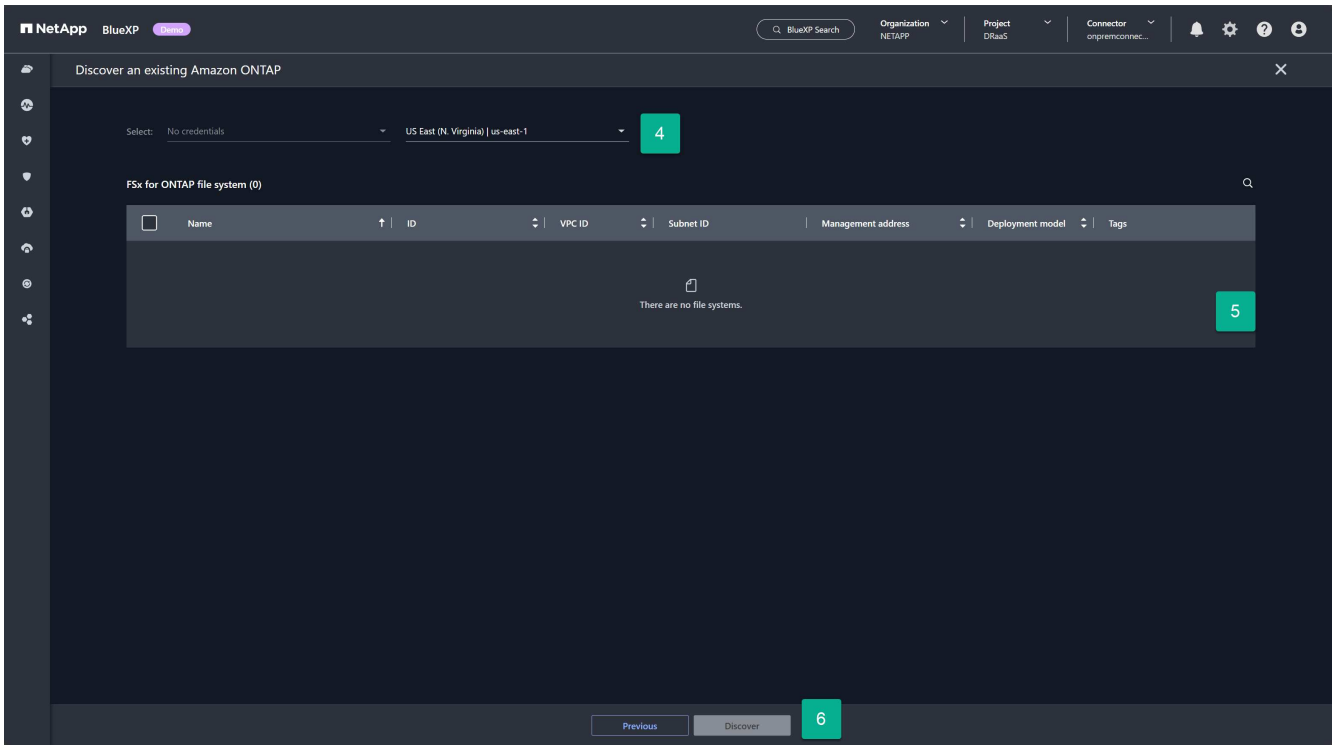
2. Wählen Sie auf der Seite „System hinzufügen“ die Karte **Amazon Web Services** aus.



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



4. Wählen Sie die Anmeldeinformationen und die AWS-Region aus, in der die FSx for ONTAP Instanz gehostet wird.
5. Wählen Sie ein oder mehrere FSx for ONTAP -Dateisysteme aus, die hinzugefügt werden sollen.
6. Wählen Sie unten auf der Seite **Entdecken** aus.



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

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

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

Weitere Informationen zu NetApp Disaster Recovery Lizenzen finden Sie unter"Einrichten der Lizenzierung für NetApp Disaster Recovery" .

Lizenztypen

Es gibt zwei primäre Lizenztypen:

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

Bemessen Sie Ihren Kapazitätsbedarf für die Notfallwiederherstellung

Bevor Sie Ihre Lizenz erwerben, sollten Sie wissen, wie viel ONTAP Speicherkapazität Sie schützen müssen. Einer der Vorteile der Verwendung von NetApp ONTAP Speicher ist die hohe Effizienz, mit der NetApp Ihre Daten speichert. Alle in einem ONTAP Volume gespeicherten Daten – beispielsweise VMware-Datenspeicher, die VMs hosten – werden auf hocheffiziente Weise gespeichert. ONTAP verwendet beim Schreiben von Daten in den physischen Speicher standardmäßig drei Arten der Speichereffizienz: Komprimierung, Deduplizierung und Komprimierung. Das Nettoergebnis ist eine Speichereffizienz zwischen 1,5:1 und 4:1, abhängig von den gespeicherten Datentypen. Tatsächlich bietet NetApp eine "Speichereffizienzgarantie" für bestimmte Arbeitslasten.

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

Schritte

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

   Beispiel:

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

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

Hinzufügen von Sites in NetApp Disaster Recovery für Amazon EVS

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

Sie müssen Folgendes erstellen:

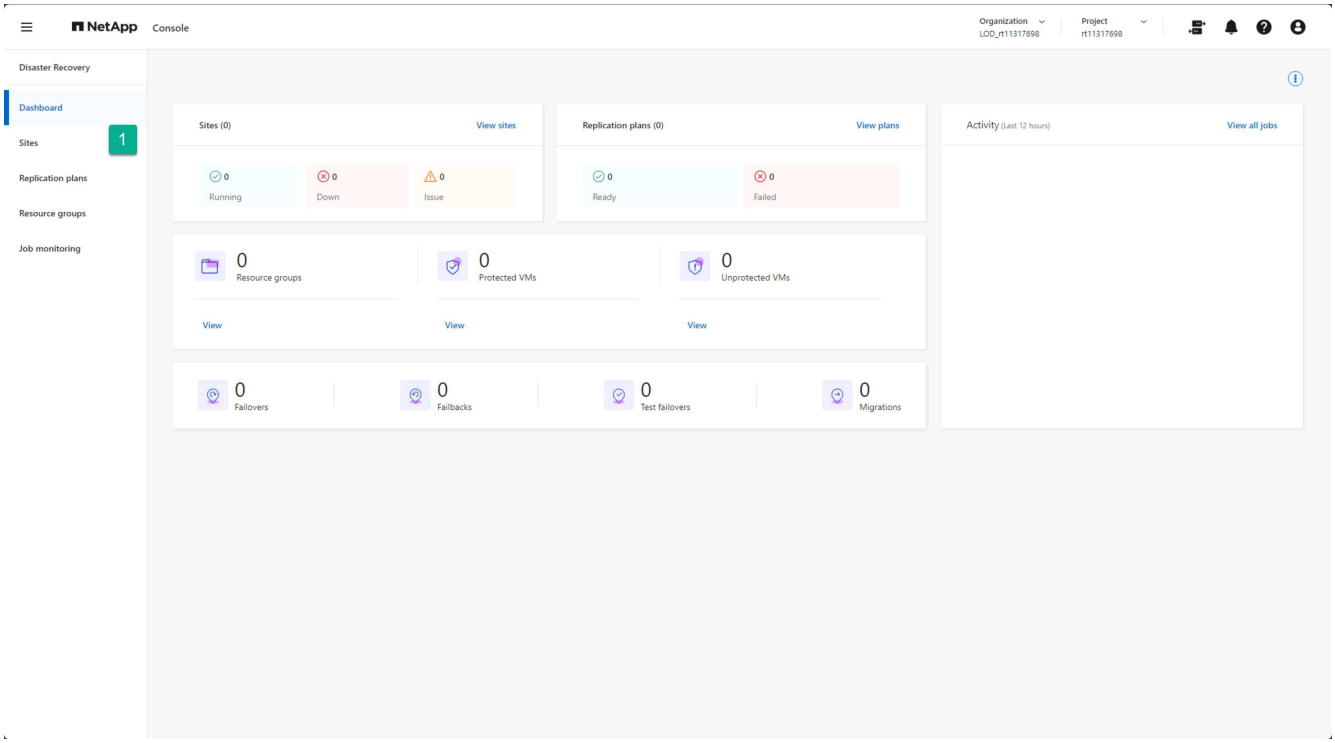
- Eine Site zur Darstellung jedes Produktionsrechenzentrums, in dem sich Ihre Produktions-vCenter-Cluster befinden
- Eine Site für Ihr Amazon EVS/ Amazon FSx for NetApp ONTAP Cloud-Rechenzentrum

Erstellen lokaler Websites

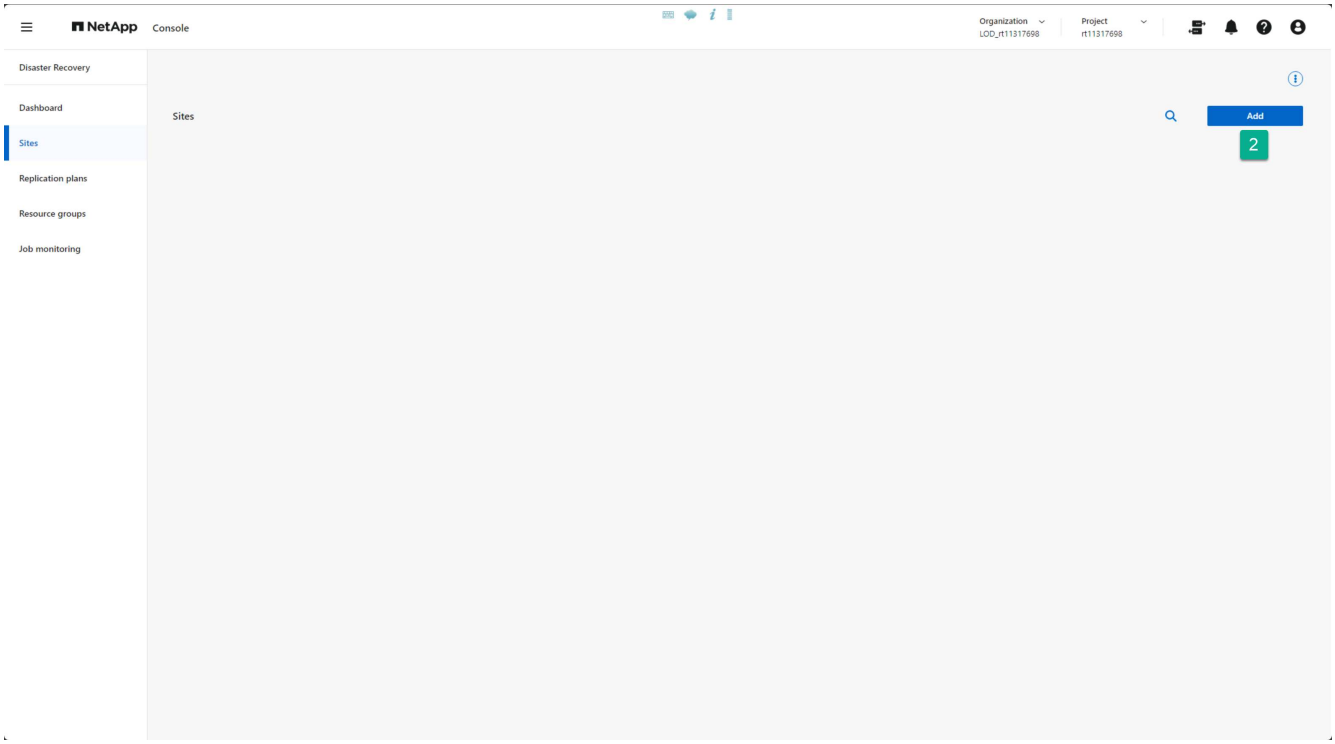
Erstellen Sie eine vCenter-Produktionssite.

Schritte

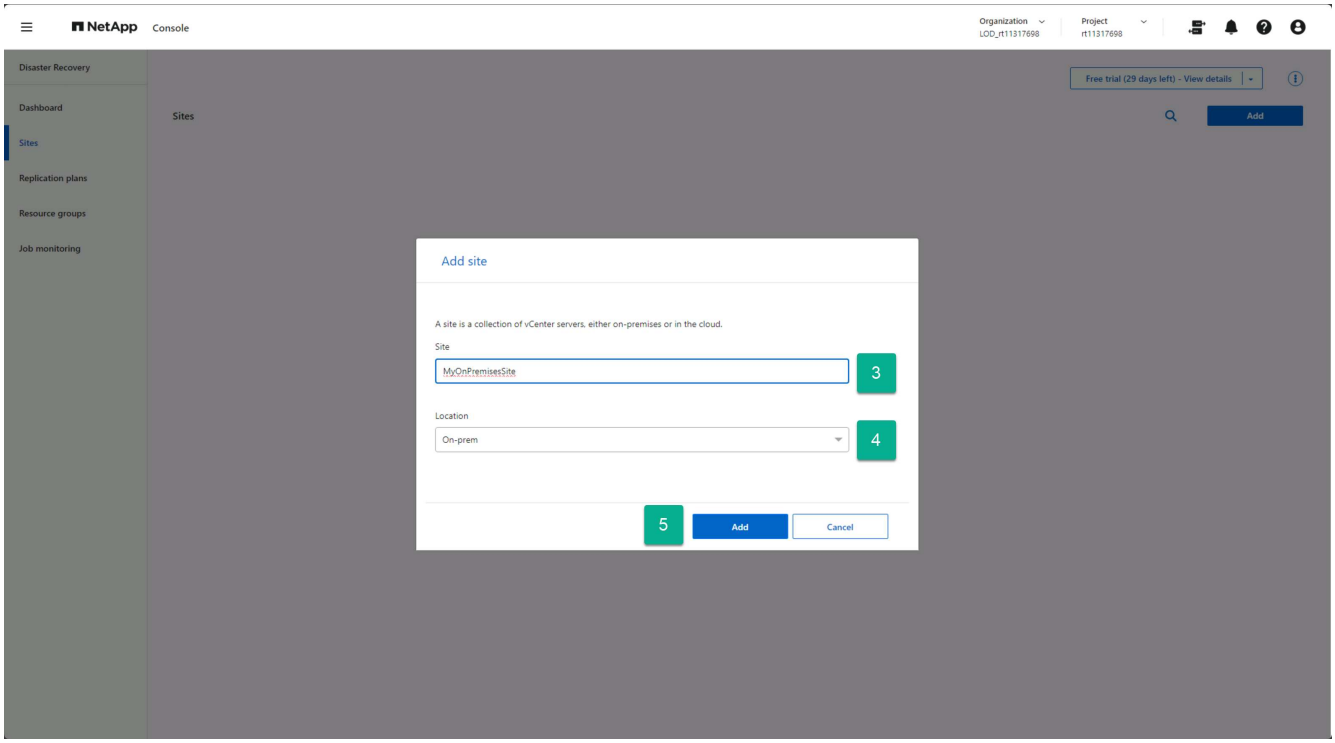
1. Wählen Sie in der linken Navigationsleiste der NetApp Console **Schutz** > **Notfallwiederherstellung**.
2. Wählen Sie auf einer beliebigen Seite in NetApp Disaster Recovery die Option **Sites** aus.



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



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

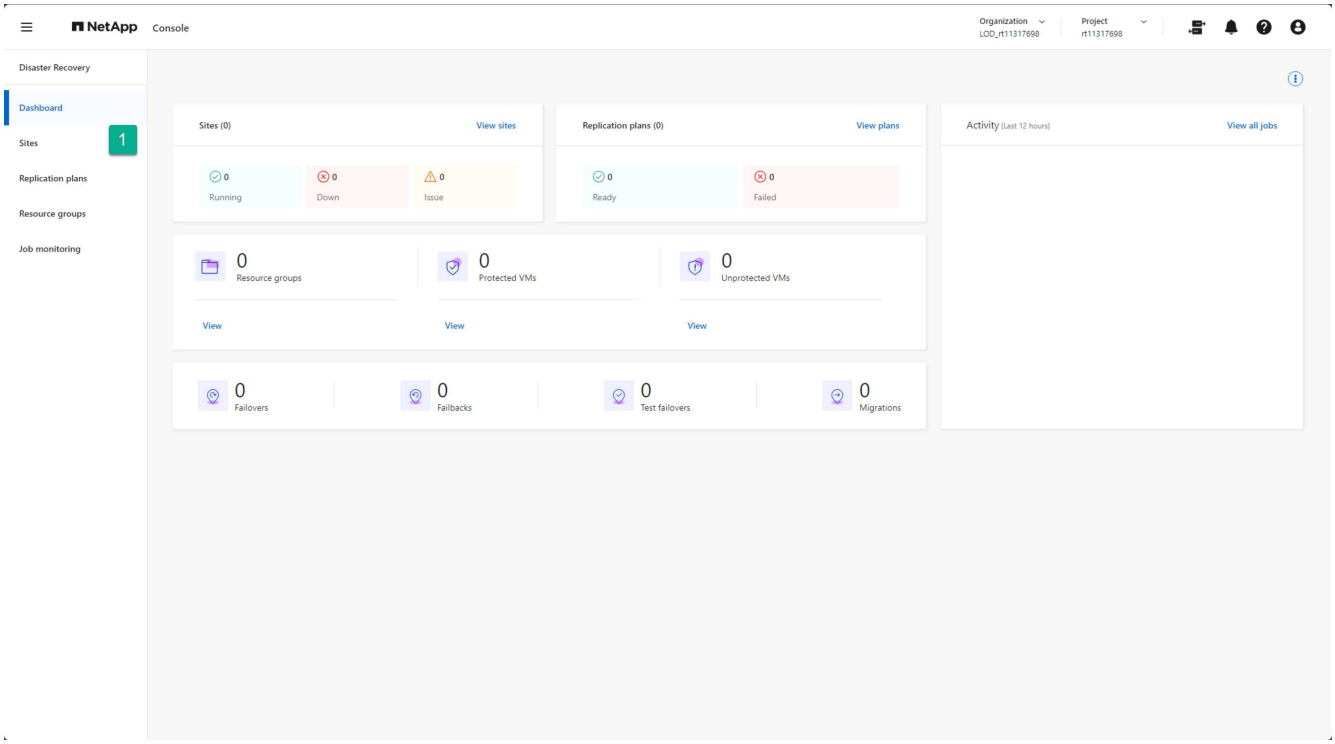


Wenn Sie über andere vCenter-Produktionssites verfügen, können Sie diese mit denselben Schritten hinzufügen.

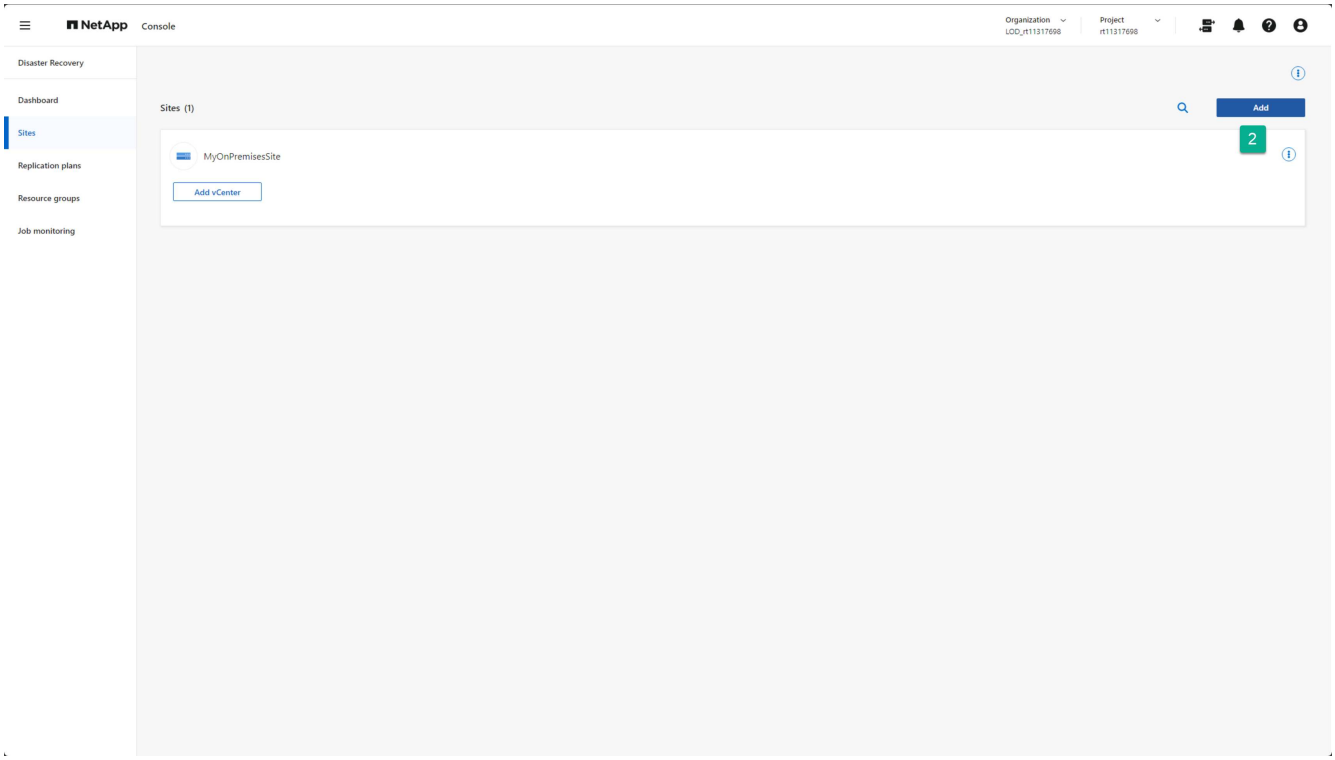
Erstellen Sie Amazon Cloud-Sites

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

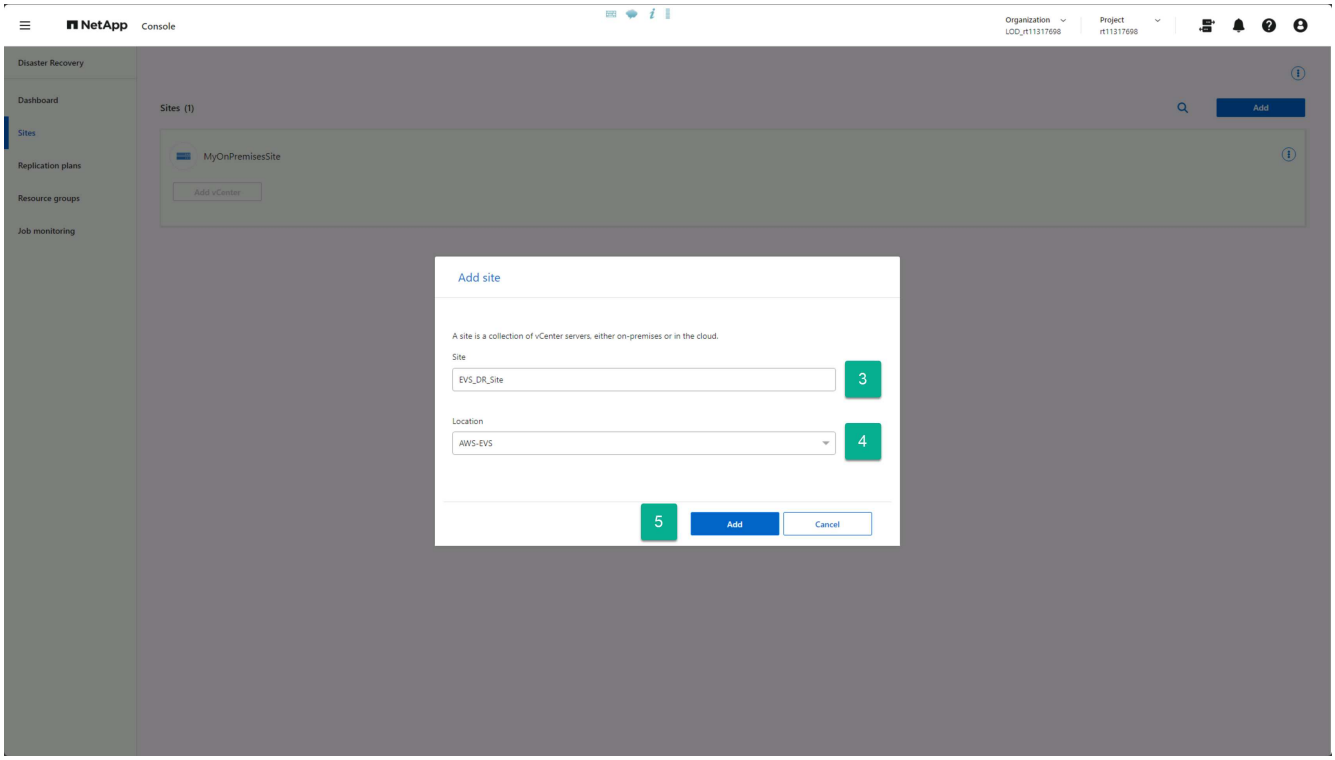
1. Wählen Sie auf einer beliebigen Seite in NetApp Disaster Recovery die Option **Sites** aus.



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



3. Geben Sie im Dialogfeld „Site hinzufügen“ einen Sitenamen ein.
4. Wählen Sie „AWS-EVS“ als Standort aus.
5. Wählen Sie **Hinzufügen**.



Ergebnis

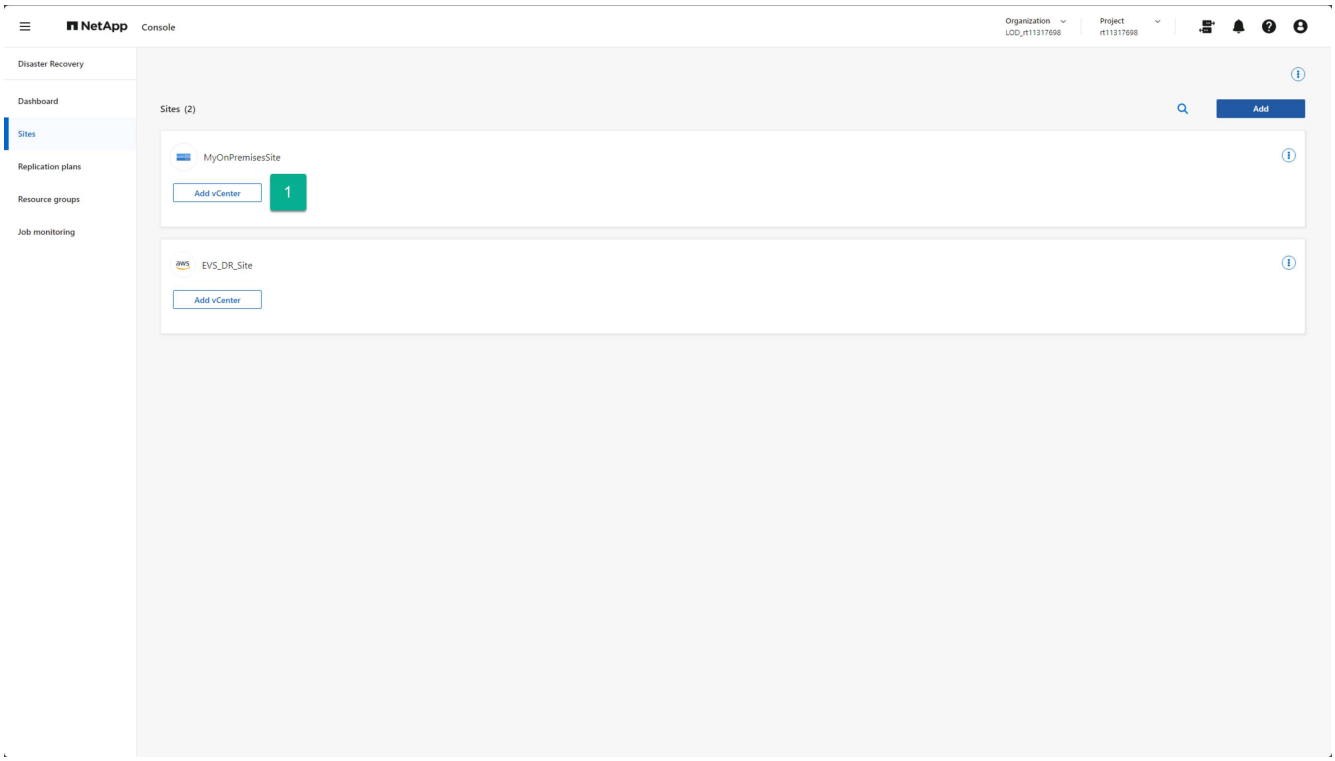
Sie haben jetzt einen Produktionsstandort (Quellstandort) und einen DR-Standort (Zielstandort) erstellt.

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

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

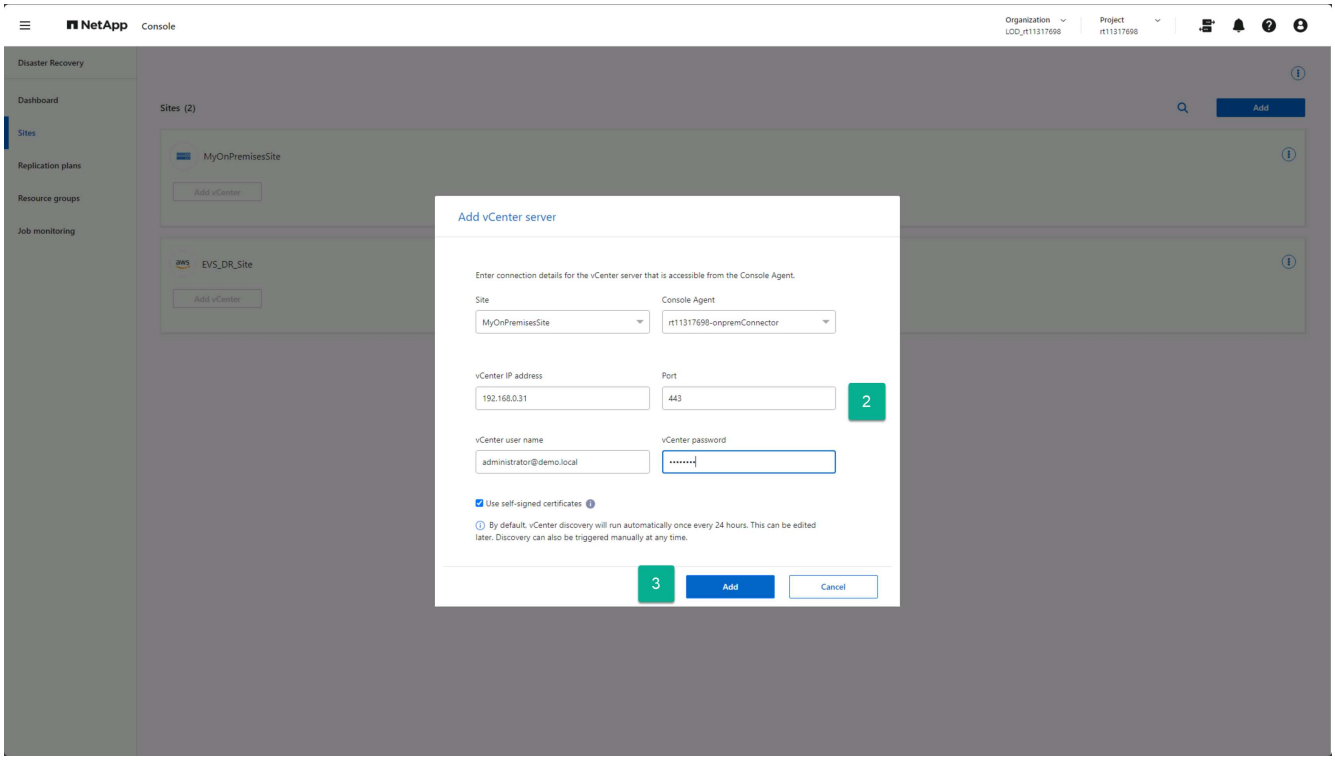
Schritte zum Hinzufügen eines vCenters zu jeder Site

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



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

3. Wählen Sie **Hinzufügen**.



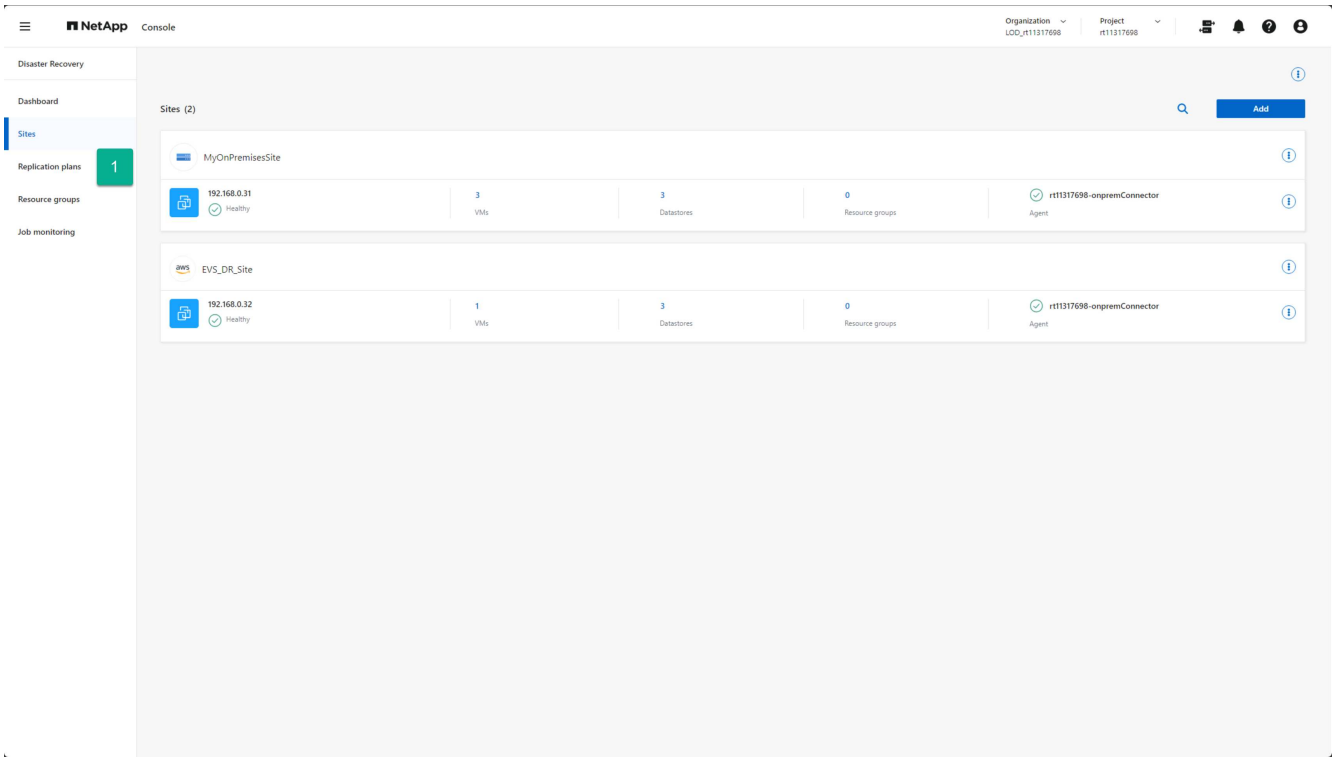
Erstellen von Replikationsplänen für Amazon EVS

Erstellen von Replikationsplänen in der NetApp Disaster Recovery Übersicht

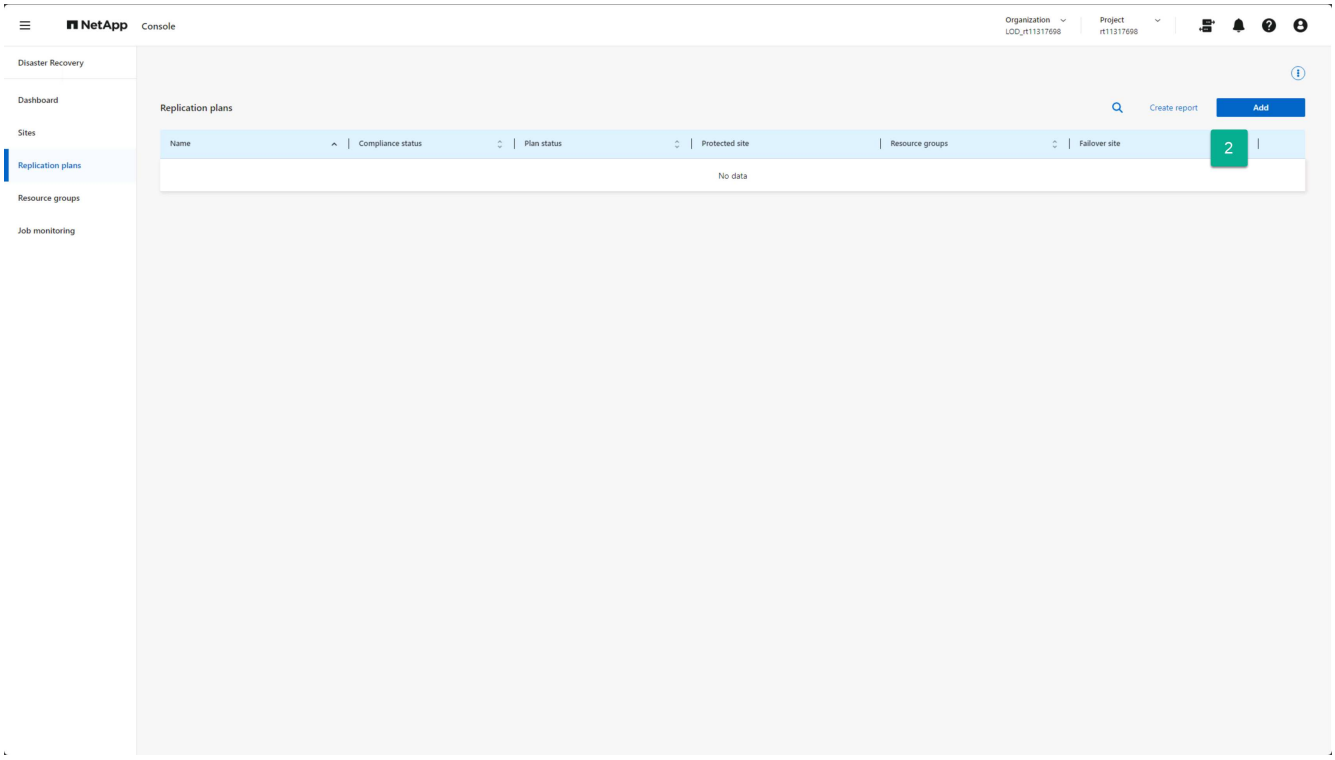
Nachdem Sie vCenter zum Schutz auf der lokalen Site haben und eine Amazon EVS-Site für die Verwendung von Amazon FSx for NetApp ONTAP konfiguriert haben, die Sie als DR-Ziel verwenden können, können Sie einen Replikationsplan (RP) erstellen, um alle auf dem vCenter-Cluster innerhalb Ihrer lokalen Site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

So starten Sie den Prozess zur Erstellung des Replikationsplans:

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



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



Dadurch wird der Assistent „Replikationsplan erstellen“ geöffnet.

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

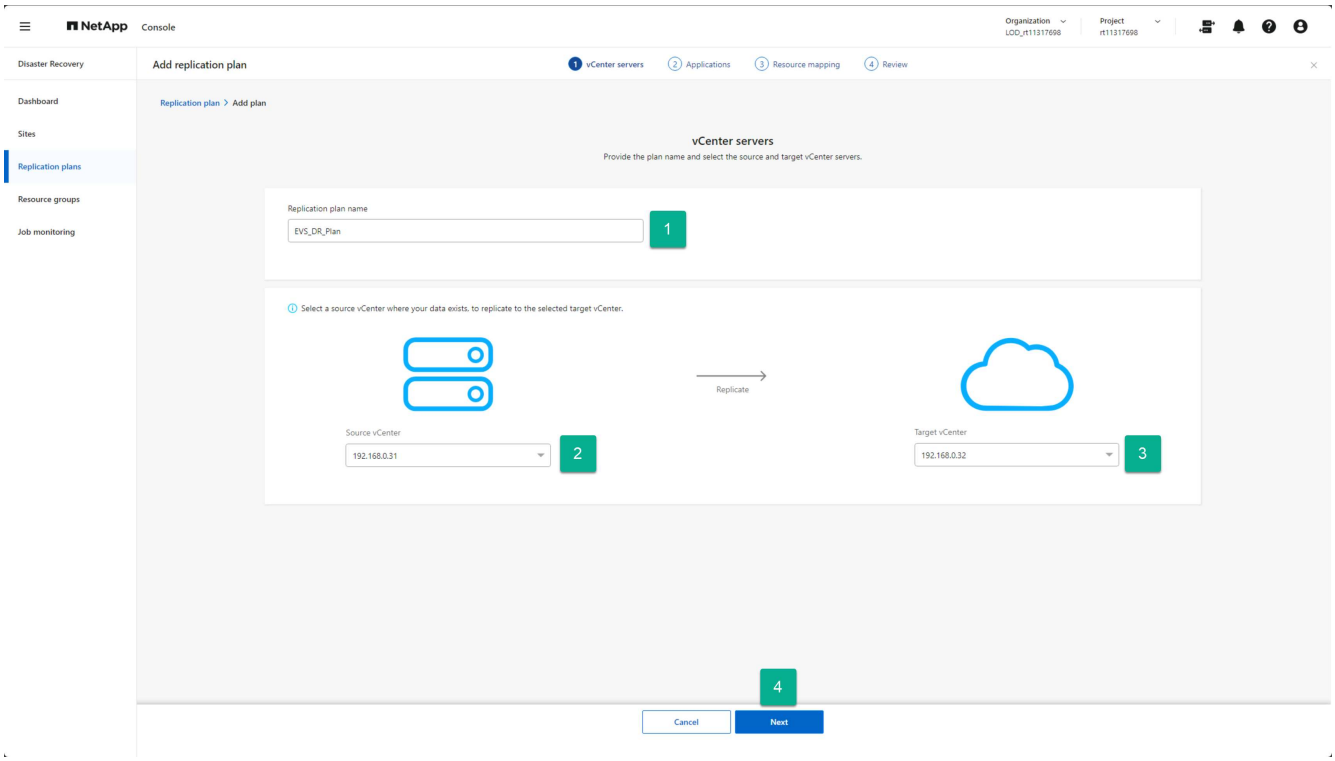
Erstellen eines Replikationsplans: Schritt 1 – Auswählen von vCentern in NetApp Disaster Recovery

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

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

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

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



Weiter mit"Assistent zum Erstellen eines Replikationsplans – Schritt 2" .

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

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

Es gibt mehrere Möglichkeiten, VMs zum Schutz auszuwählen:

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

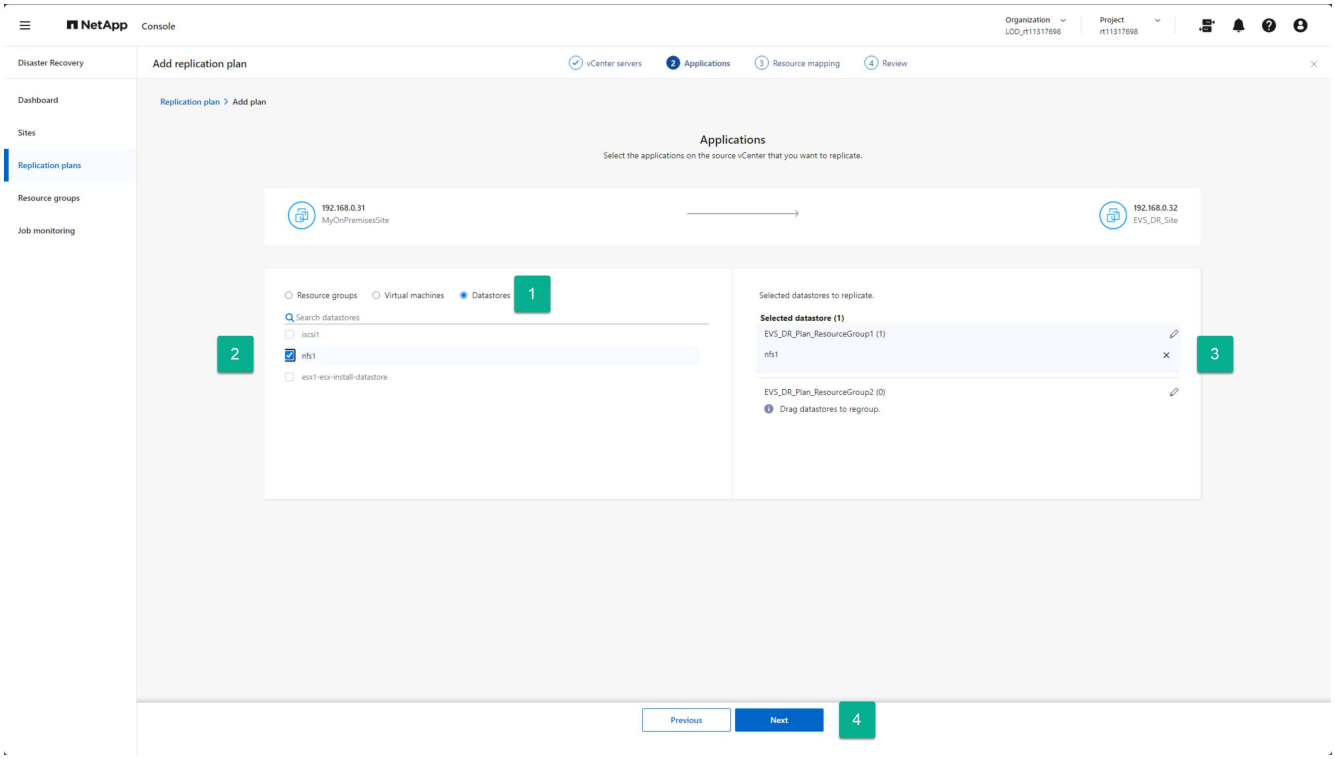
Menü verwenden. Dies ist keine Voraussetzung, da Sie die beiden anderen Methoden verwenden können, um im Rahmen des Replikationsplanprozesses eine Ressourcengruppe zu erstellen. Weitere Informationen finden Sie unter "Erstellen eines Replikationsplans" .

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

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

Schritte zum Zugriff auf diese Seite

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



Schritte zum Auswählen des Datenspeichers bzw. der Datenspeicher:

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

Weiter mit"Assistent zum Erstellen eines Replikationsplans – Schritt 3" .

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

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

Sie müssen vier primäre Arten von Informationen zuordnen:

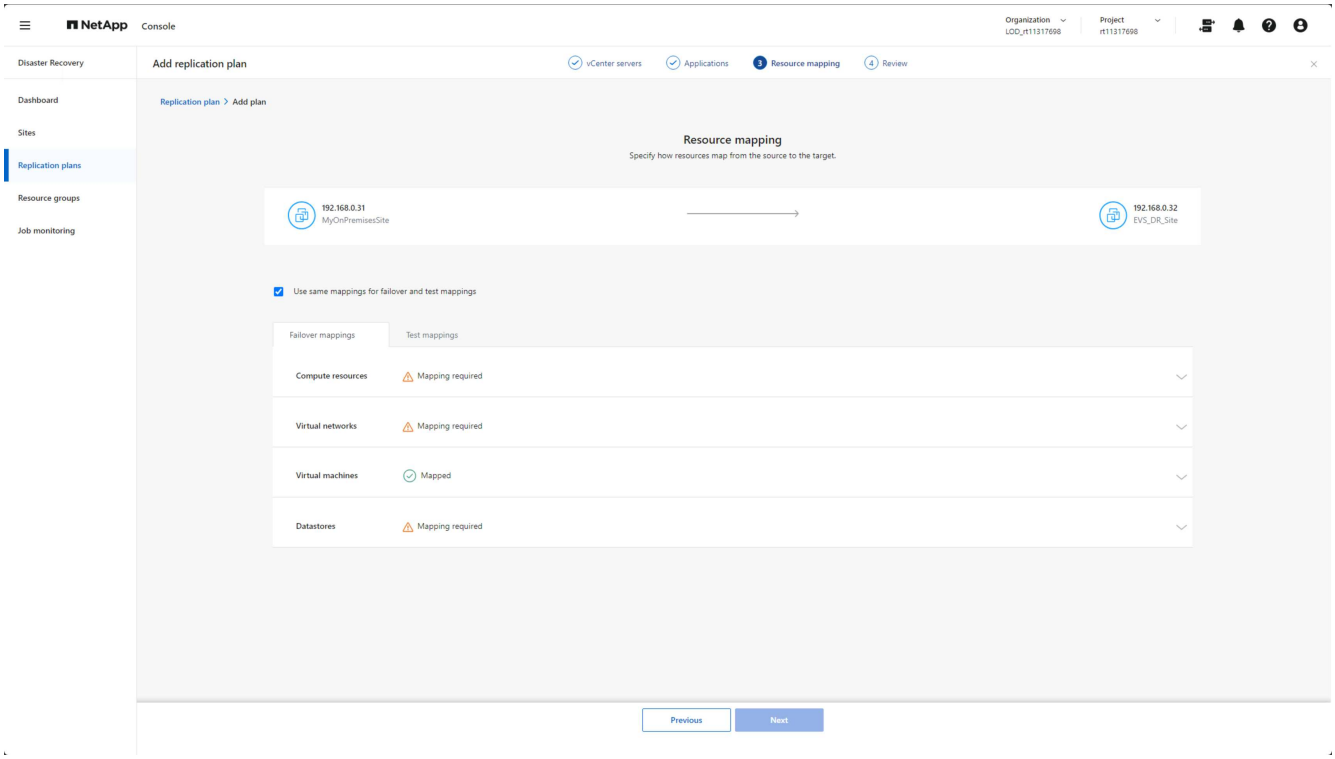
- Rechenressourcen
- Virtuelle Netzwerke
- VM-Neukonfiguration
- Datenspeicherzuordnung

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

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

Schritte zum Zugriff auf diese Seite

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



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

neben dem Abschnitt aus.

Zuordnung von Rechenressourcen

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

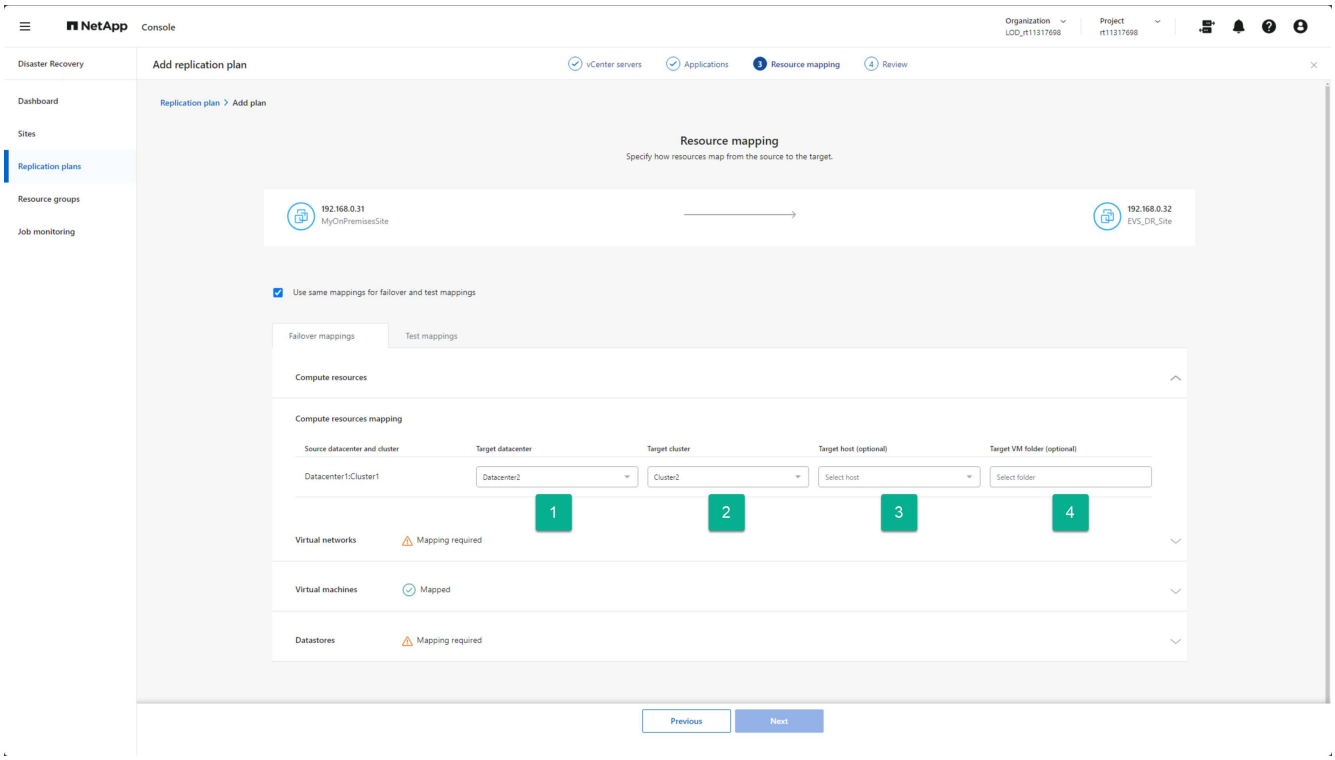
Schritte zum Zuordnen von Computeressourcen

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

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

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

   Dies dient Ihren organisatorischen Anforderungen und ist nicht erforderlich.

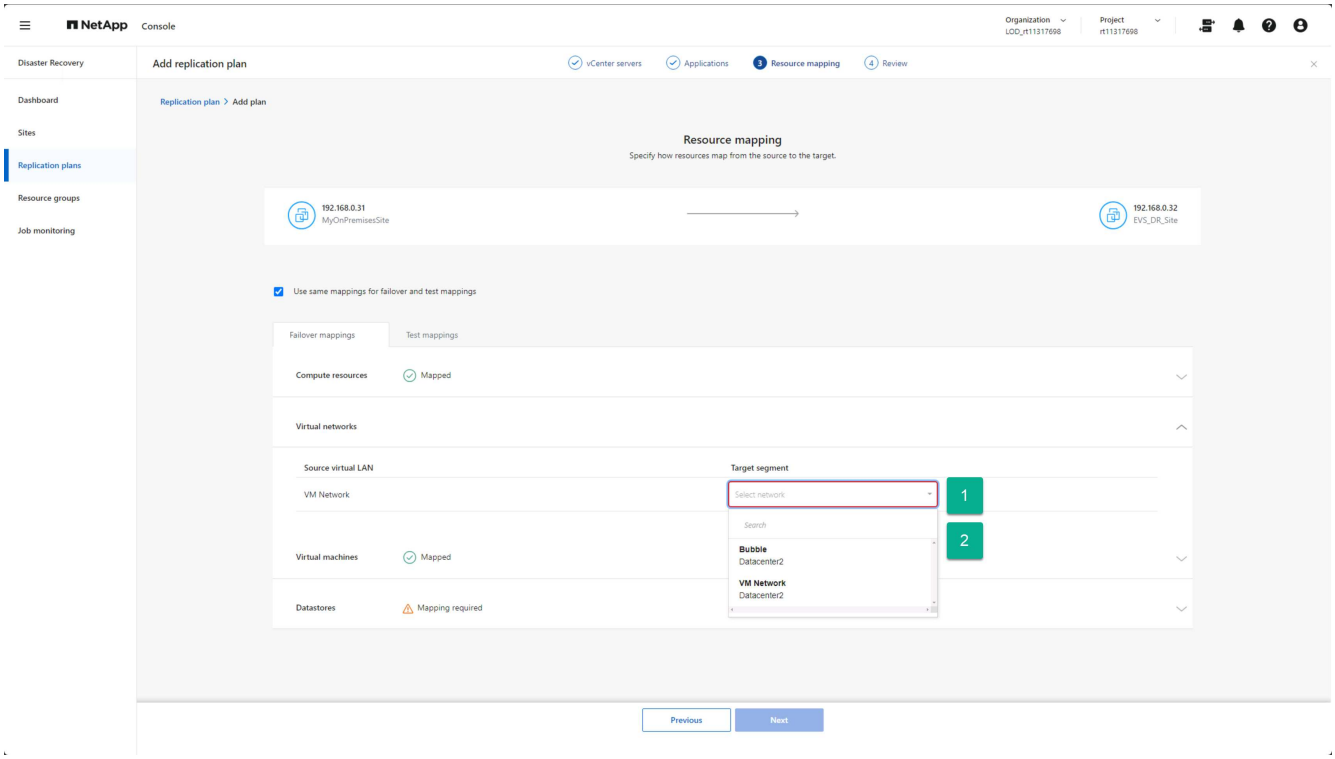


Zuordnen virtueller Netzwerkressourcen

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

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

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



Definieren Sie Optionen für die VM-Neukonfiguration während des Failovers

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

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

Netzwerkneukonfiguration

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

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

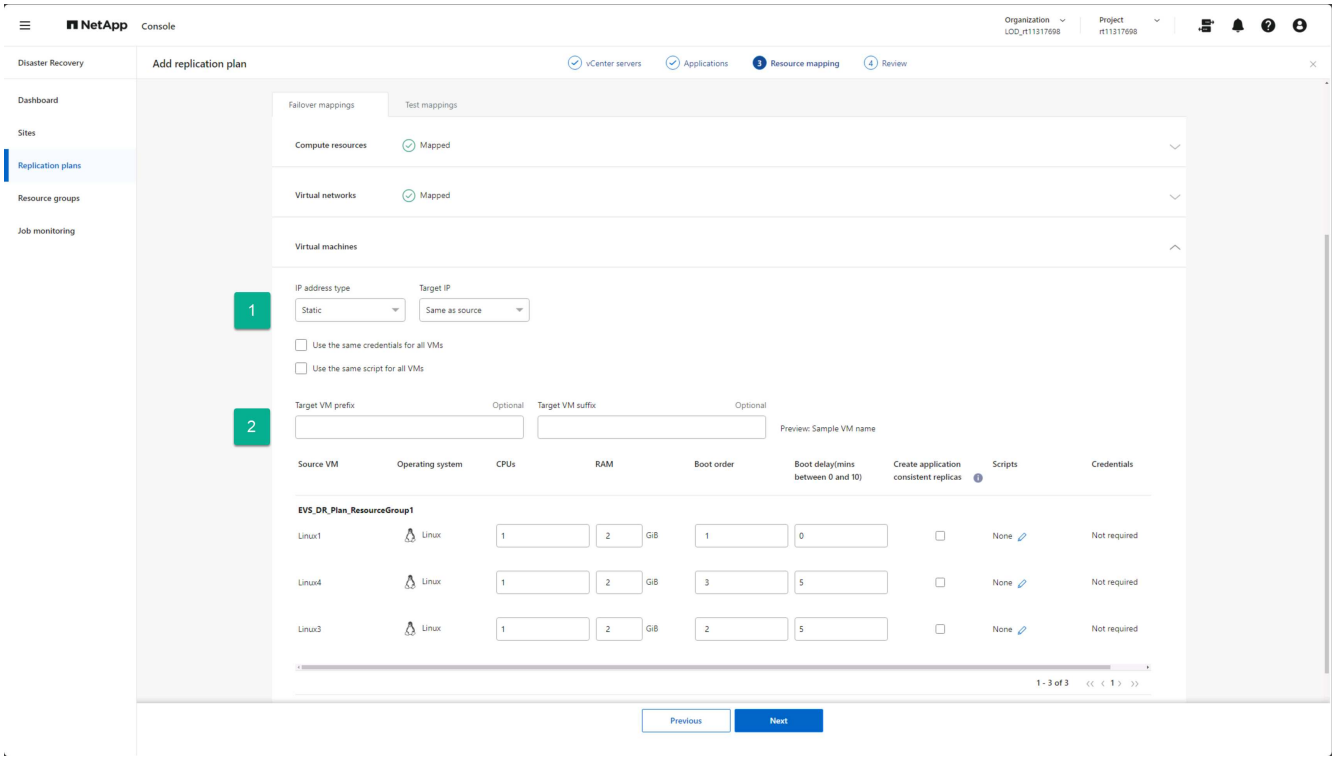
die virtuellen Netzwerke jedes vCenters über eine definierte CIDR-Einstellung innerhalb des Dienstes verfügen, wie in den vCenter-Informationen auf der Sites-Seite geändert.

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

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

Nehmen Sie Änderungen an der Neukonfiguration der Netzwerkeinstellungen vor

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



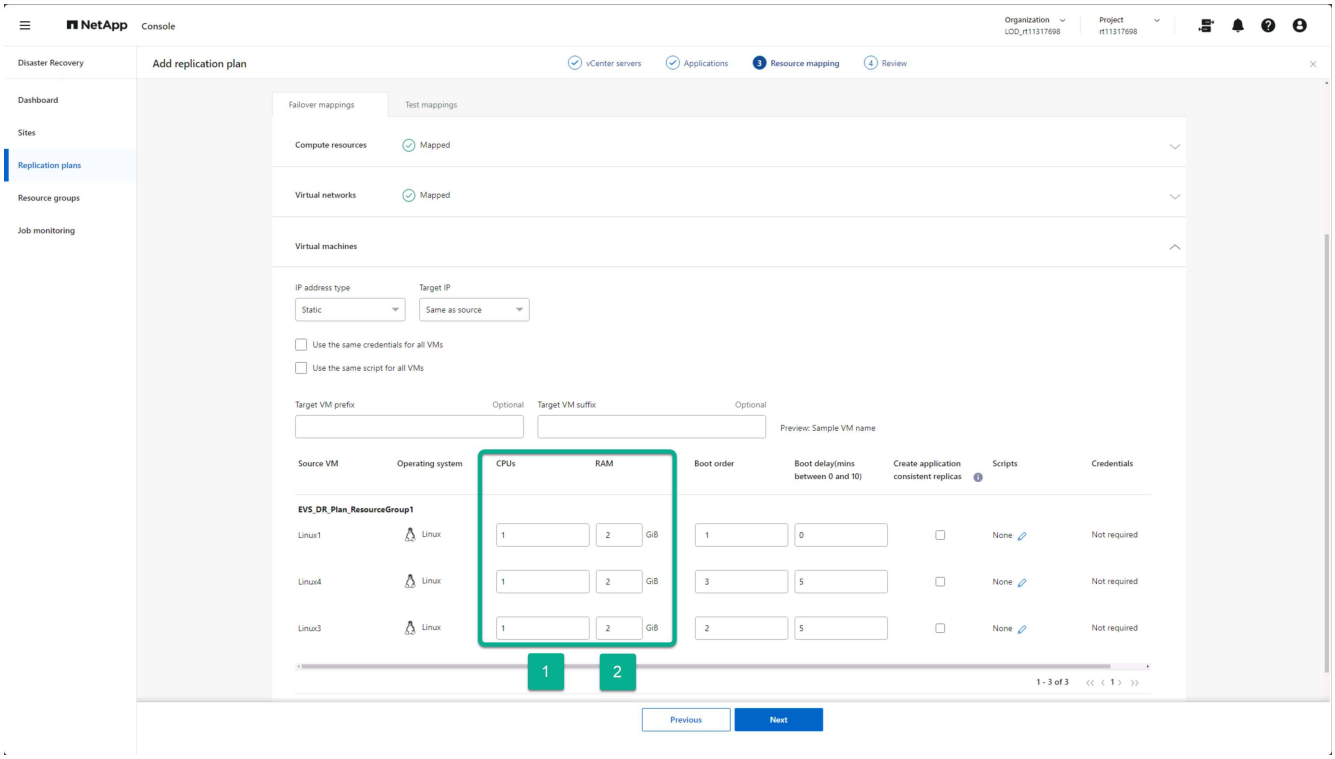
Neukonfiguration der VM-Rechenressourcen

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

Geben Sie alle VM-Konfigurationsänderungen an

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

vCenter-Cluster-Hosts.

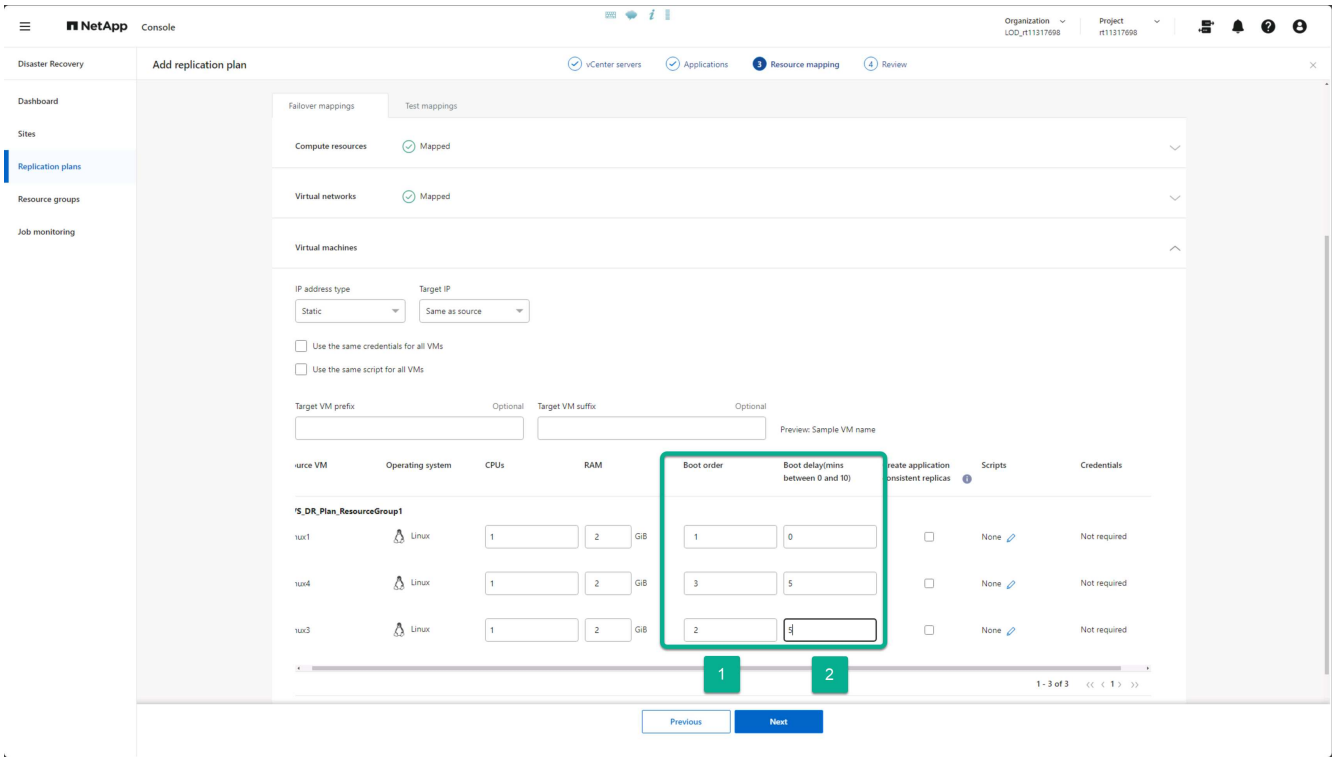


Bootreihenfolge

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

Ändern Sie die Einstellungen für die Startreihenfolge

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



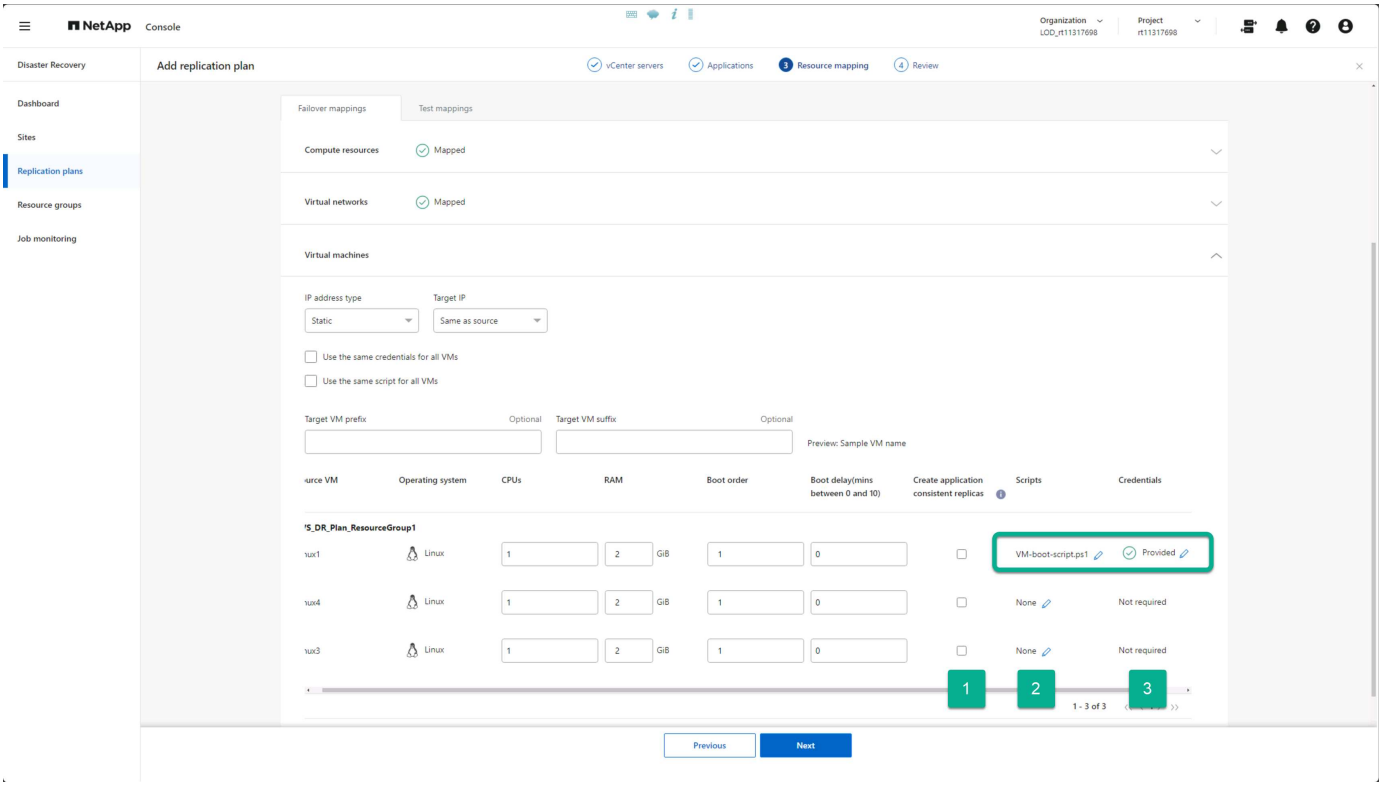
Benutzerdefinierte Gastbetriebssystemvorgänge

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

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

Ändern Sie die benutzerdefinierten Gastbetriebssystemvorgänge jeder VM

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



Kartendatenspeicher

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

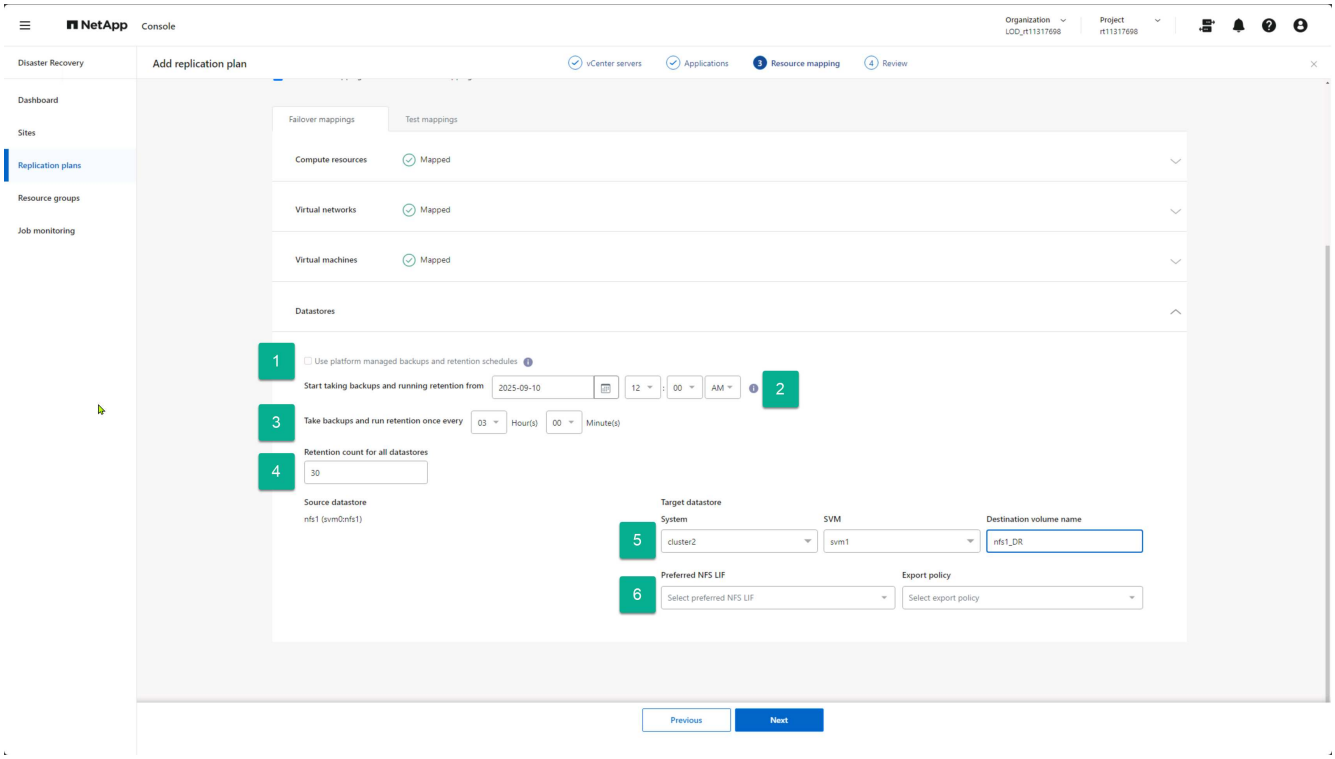
Standardmäßig verwaltet NetApp Disaster Recovery seinen eigenen Snapshot-Replikationszeitplan. Optional können Sie jedoch angeben, dass Sie den vorhandenen SnapMirror -Replikationsrichtlinienzeitplan zum Schutz des Datenspeichers verwenden möchten.

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

So konfigurieren Sie die Datenspeicherzuordnung (Volume)

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

Standardexportrichtlinie verwendet



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

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

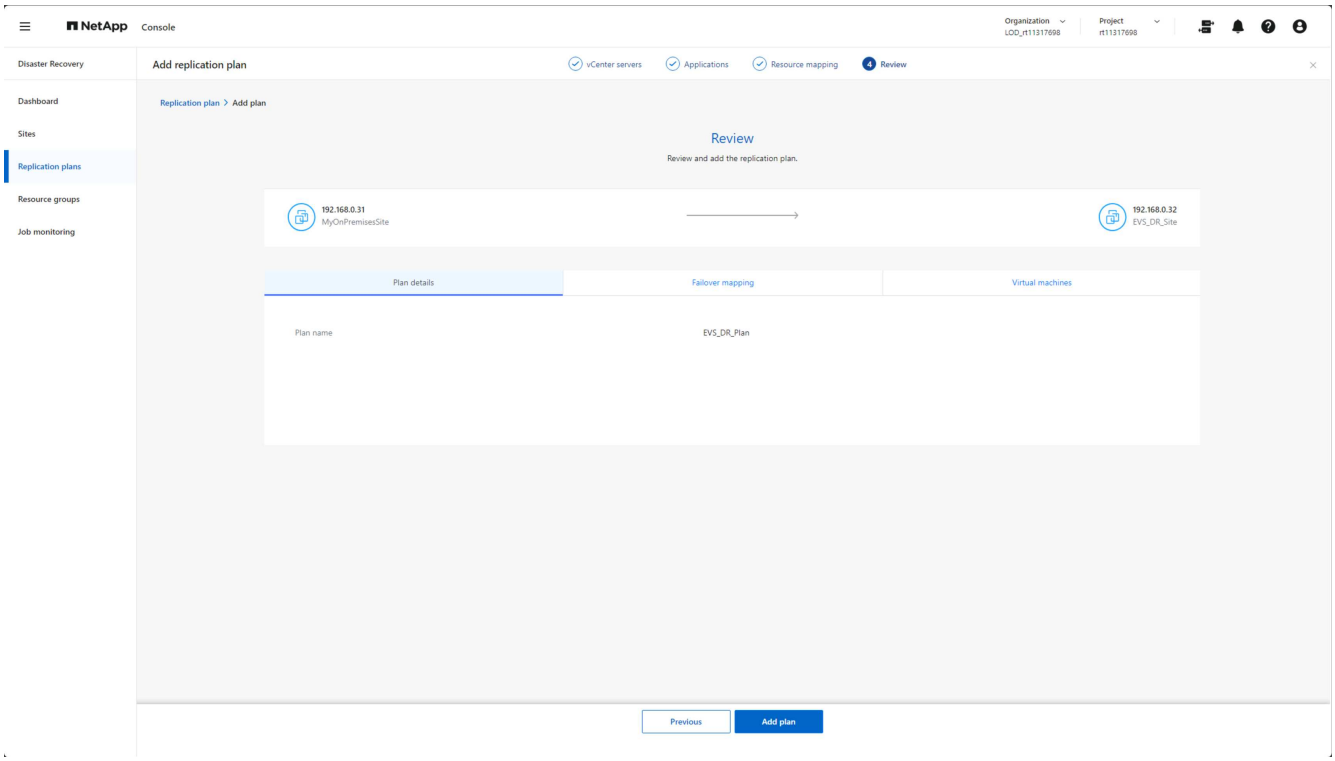
Nachdem Sie die Replikationsplaninformationen in NetApp Disaster Recovery hinzugefügt haben, überprüfen Sie, ob die eingegebenen Informationen richtig sind.

Schritte

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

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

   Überprüfung der
   Replikationsplaneinstellungen



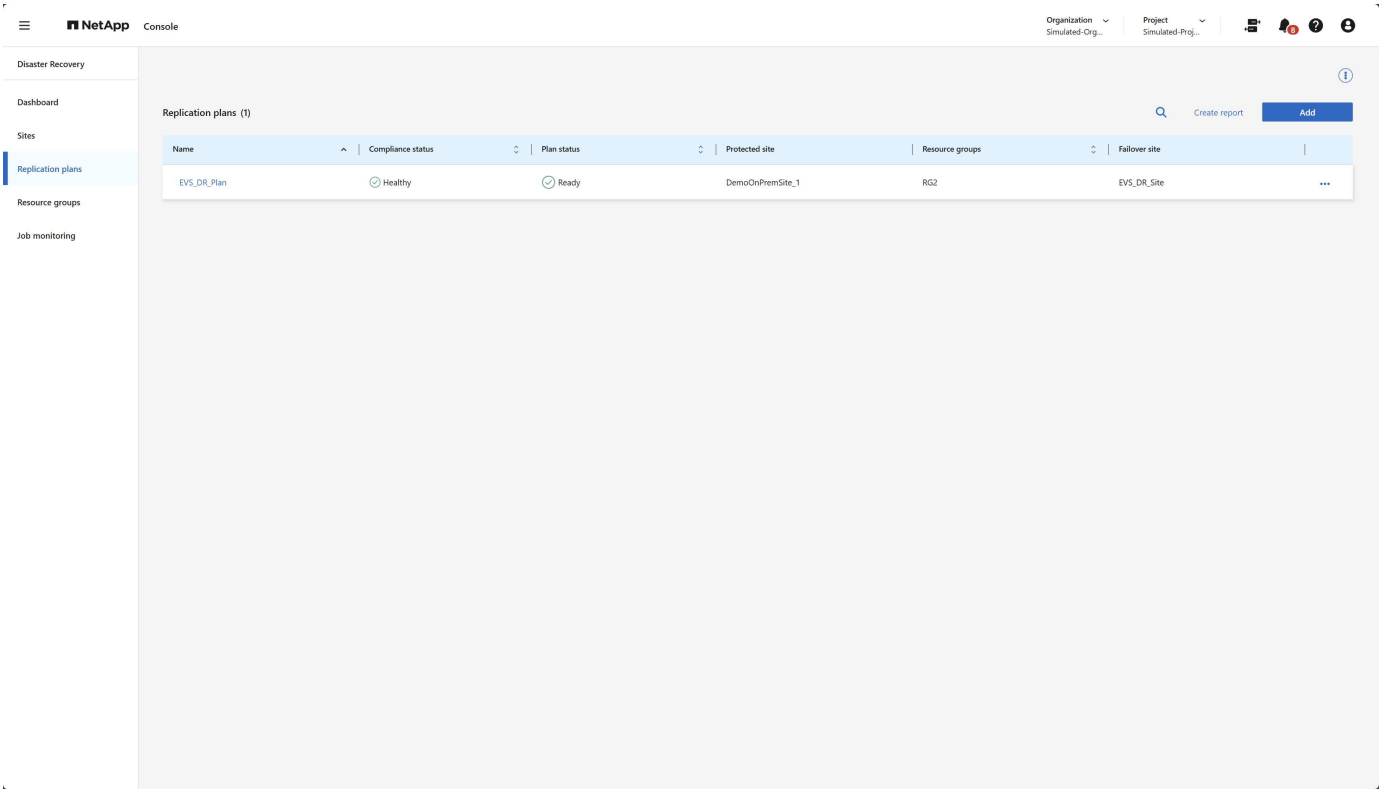
2. Wenn Sie sicher sind, dass alle Einstellungen korrekt sind, wählen Sie unten auf dem Bildschirm **Plan hinzufügen** aus.

Weiter mit"Überprüfen des Replikationsplans" .

Überprüfen Sie, ob in NetApp Disaster Recovery alles funktioniert

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

Abbildung: Seite
„Replikationspläne“



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

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

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

Ausführen von Replikationsplanvorgängen mit NetApp Disaster Recovery

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

Failover

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

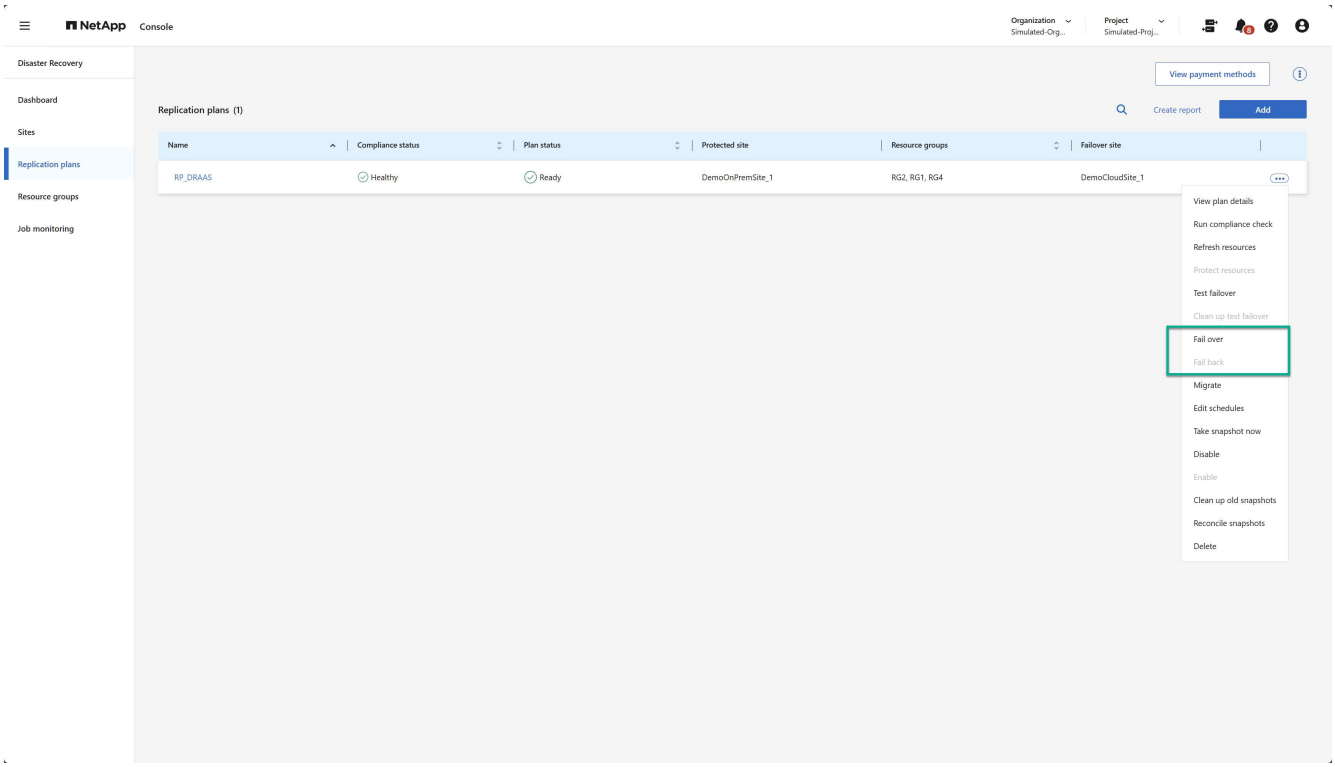
Failover ist ein manuell initiierter Prozess.

Schritte zum Zugriff auf den Failover-Vorgang

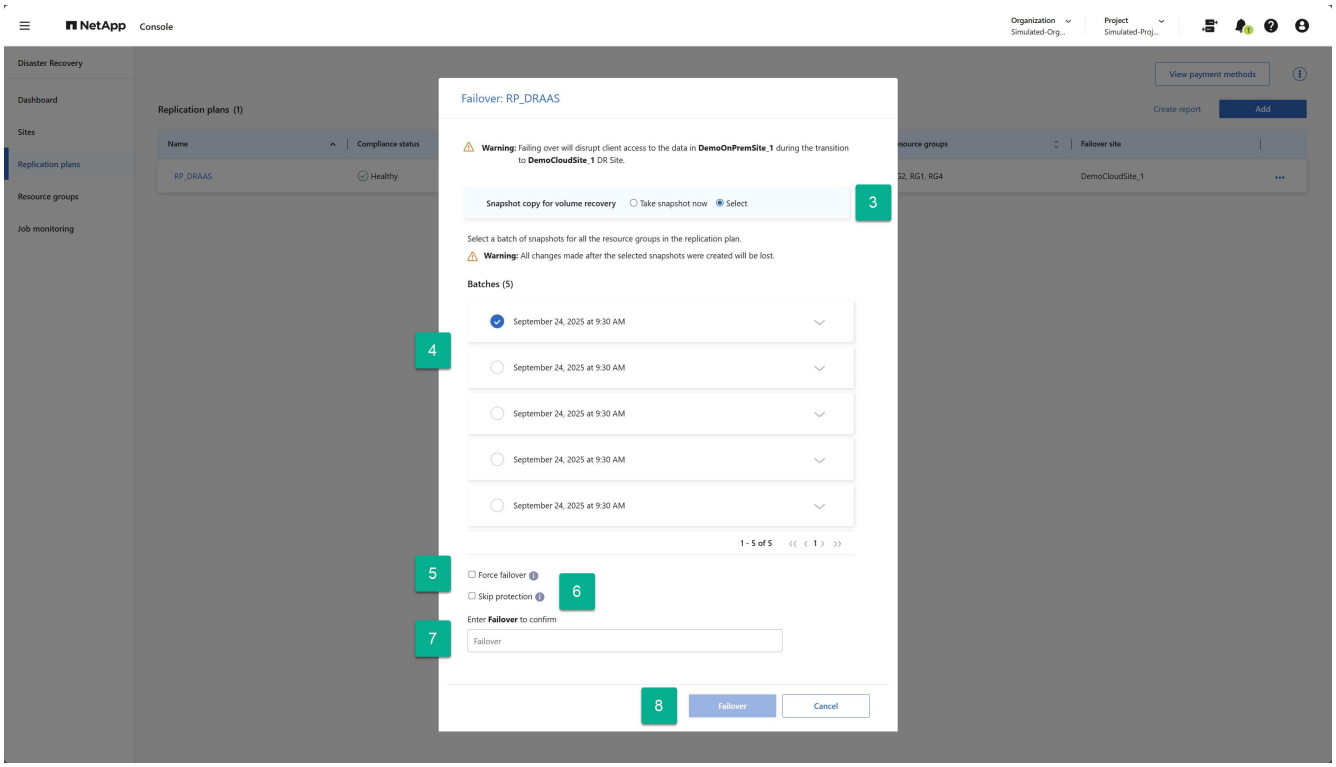
1. Wählen Sie in der linken Navigationsleiste der NetApp Console **Schutz** > **Notfallwiederherstellung**.
2. Wählen Sie im NetApp Disaster Recovery Menü **Replikationspläne** aus.

Schritte zum Durchführen eines Failovers

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



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



Testen des Failovers

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

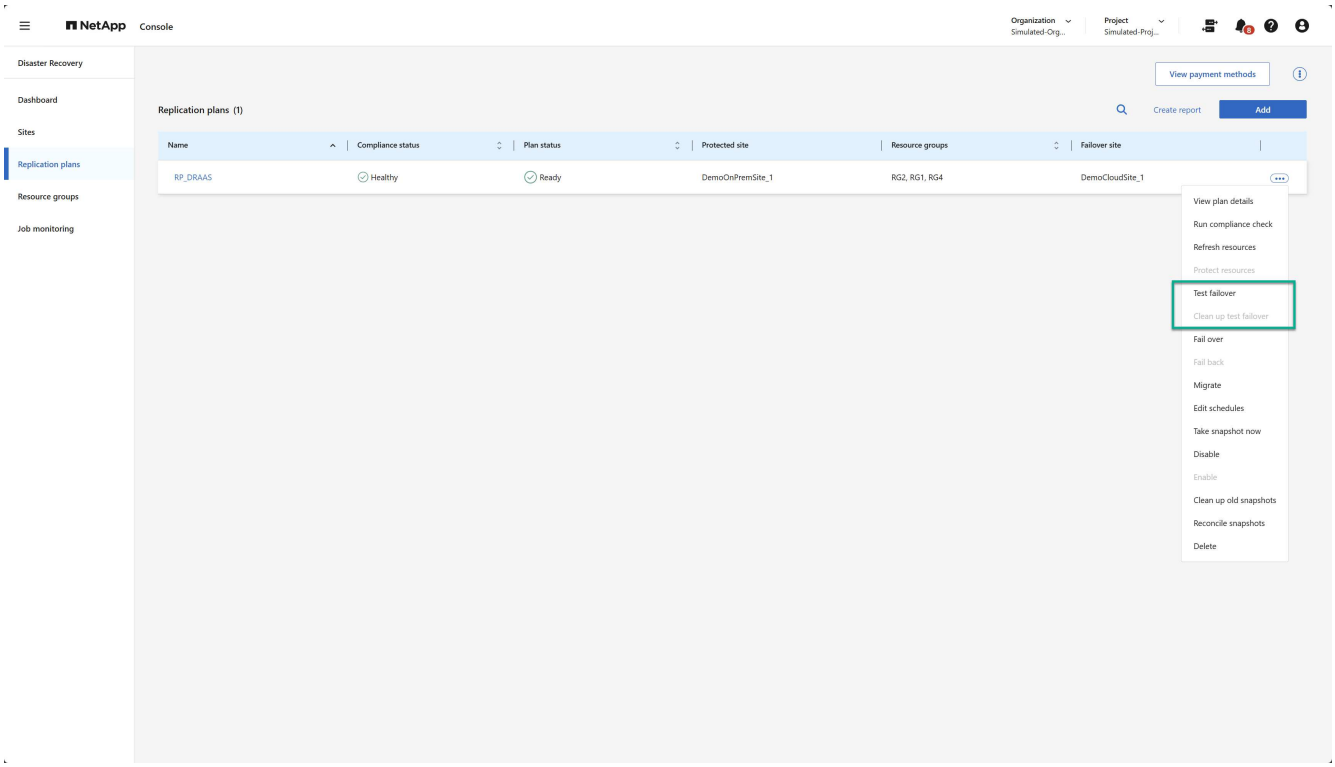
- Die Produktionssite ist weiterhin aktiv und alle VMs funktionieren weiterhin wie erwartet.
- Der NetApp Disaster Recovery Schutz der Produktions-VMs wird fortgesetzt.

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

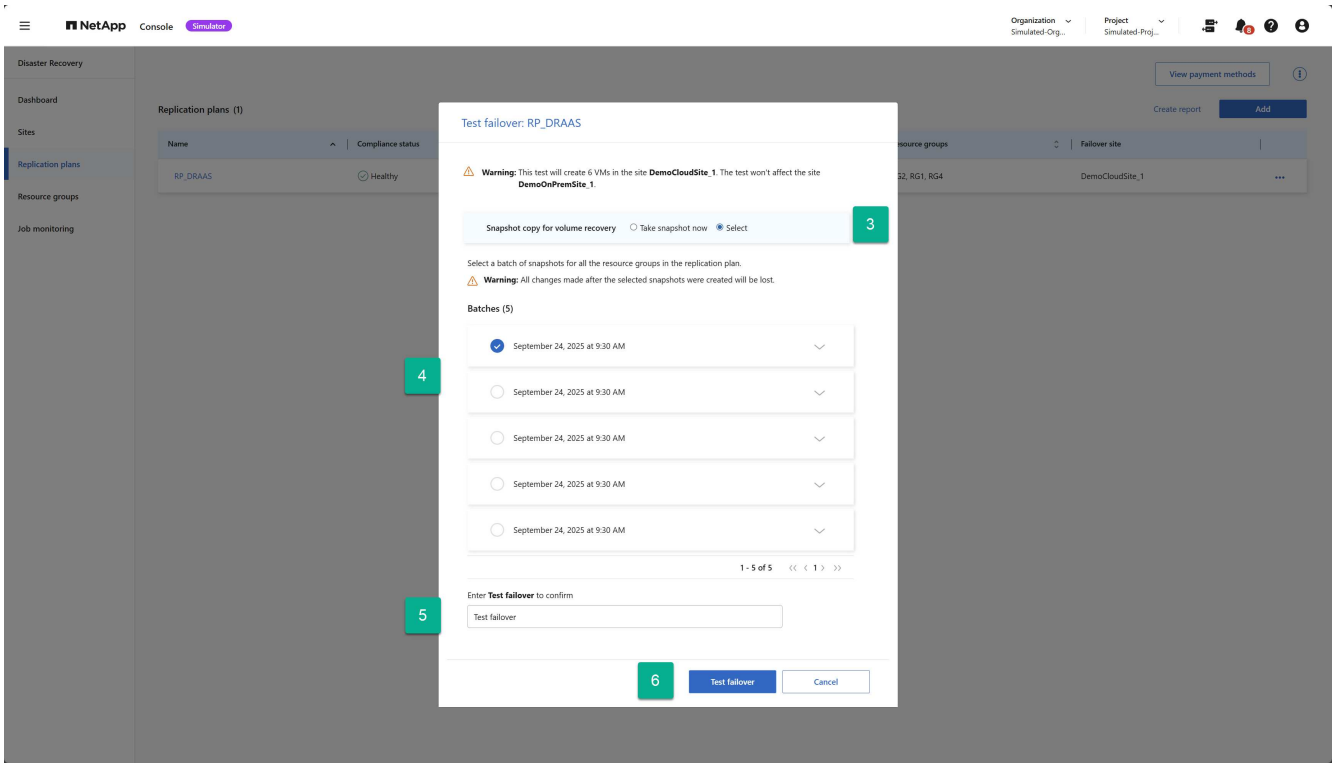
Die Schritte zum Ausführen eines Test-Failovers sind mit denen zum Ausführen eines echten Failovers identisch, mit der Ausnahme, dass Sie den Vorgang „Test-Failover“ im Kontextmenü des Replikationsplans verwenden.

Schritte

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



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

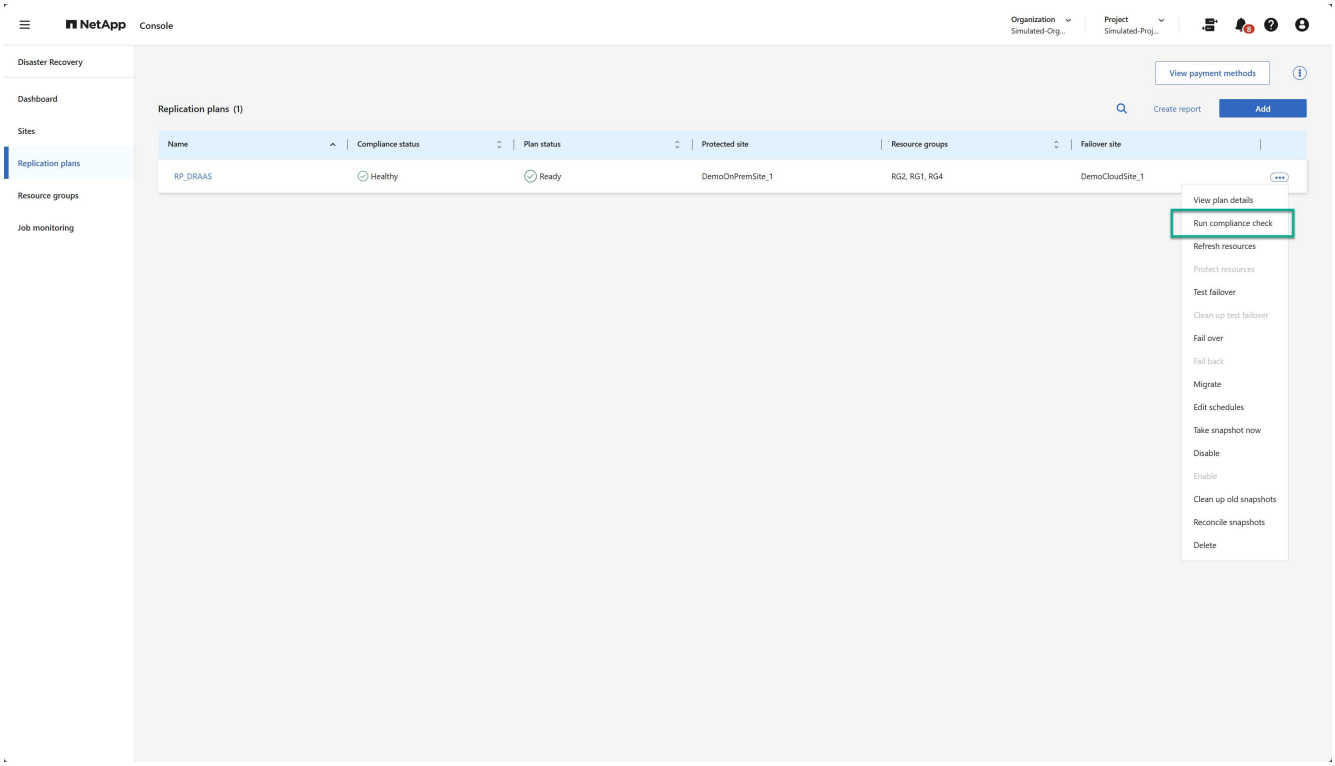


Führen Sie eine Konformitätsprüfung durch

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

Schritte

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



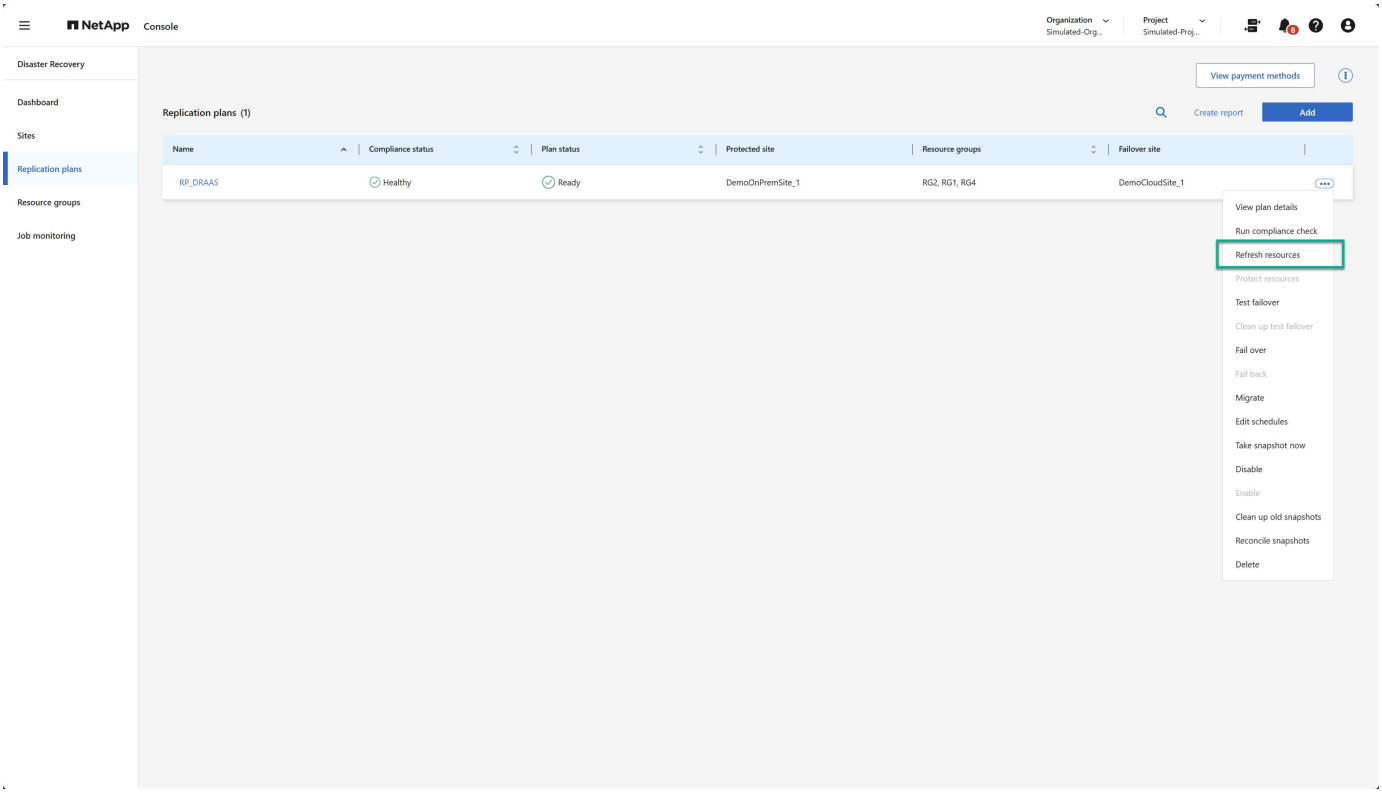
3. Um zu ändern, wie oft NetApp Disaster Recovery automatisch Konformitätsprüfungen durchführt, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Zeitpläne bearbeiten“ aus.

Ressourcen aktualisieren

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

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

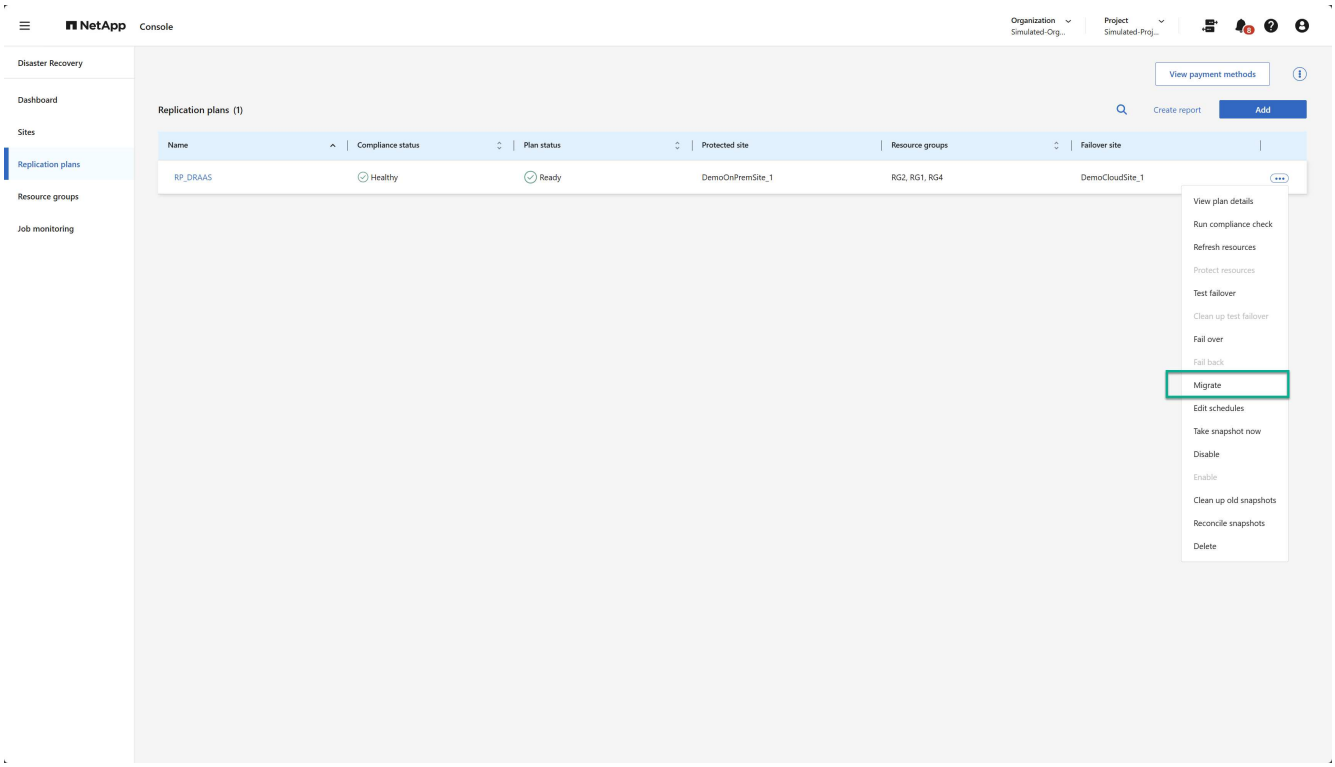
- vCenter-Aktualisierung: Führen Sie eine vCenter-Aktualisierung durch, wenn VMs zu einem vCenter-Cluster hinzugefügt, daraus gelöscht oder aus diesem verschoben werden:
- Aktualisierung des Replikationsplans: Führen Sie jedes Mal eine Aktualisierung des Replikationsplans durch, wenn eine VM zwischen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



Wandern

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

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

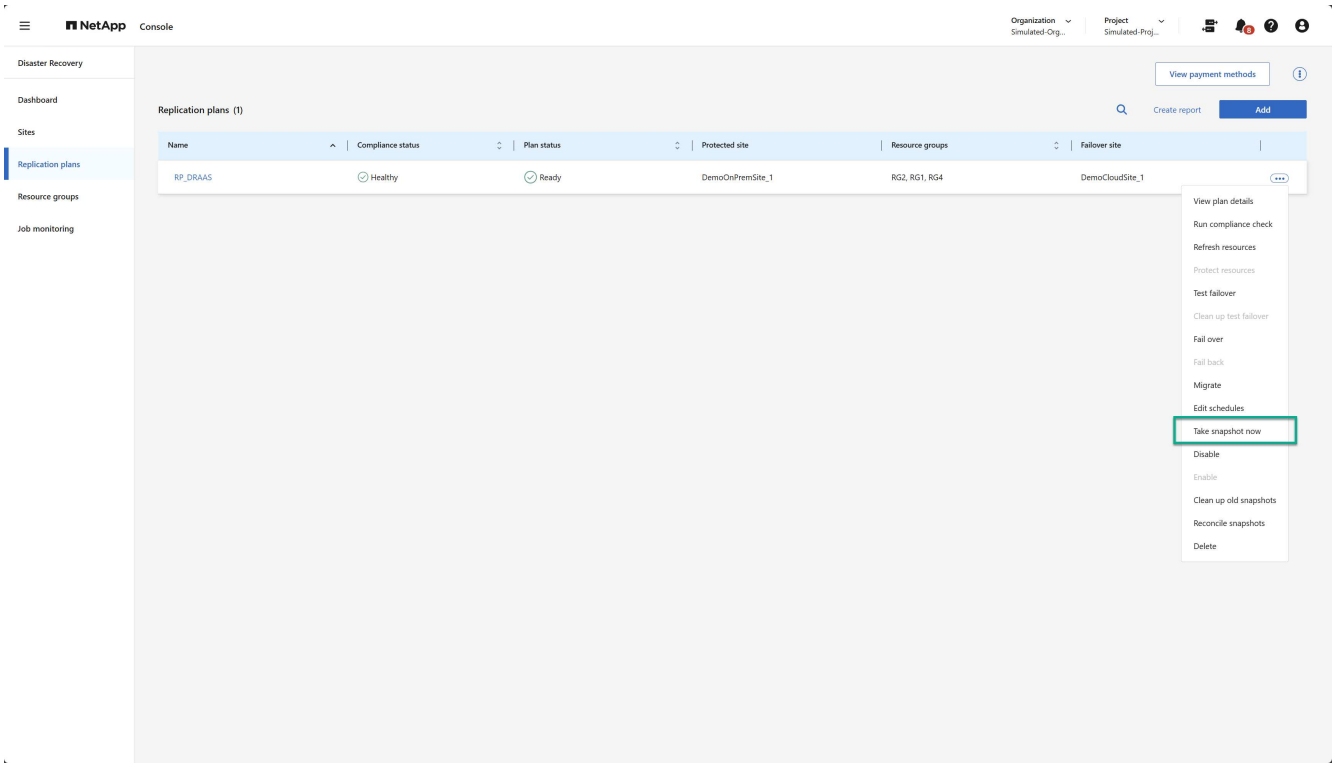


3. Geben Sie Informationen in das Dialogfeld „Migrieren“ ein.

Jetzt Schnappschuss machen

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

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

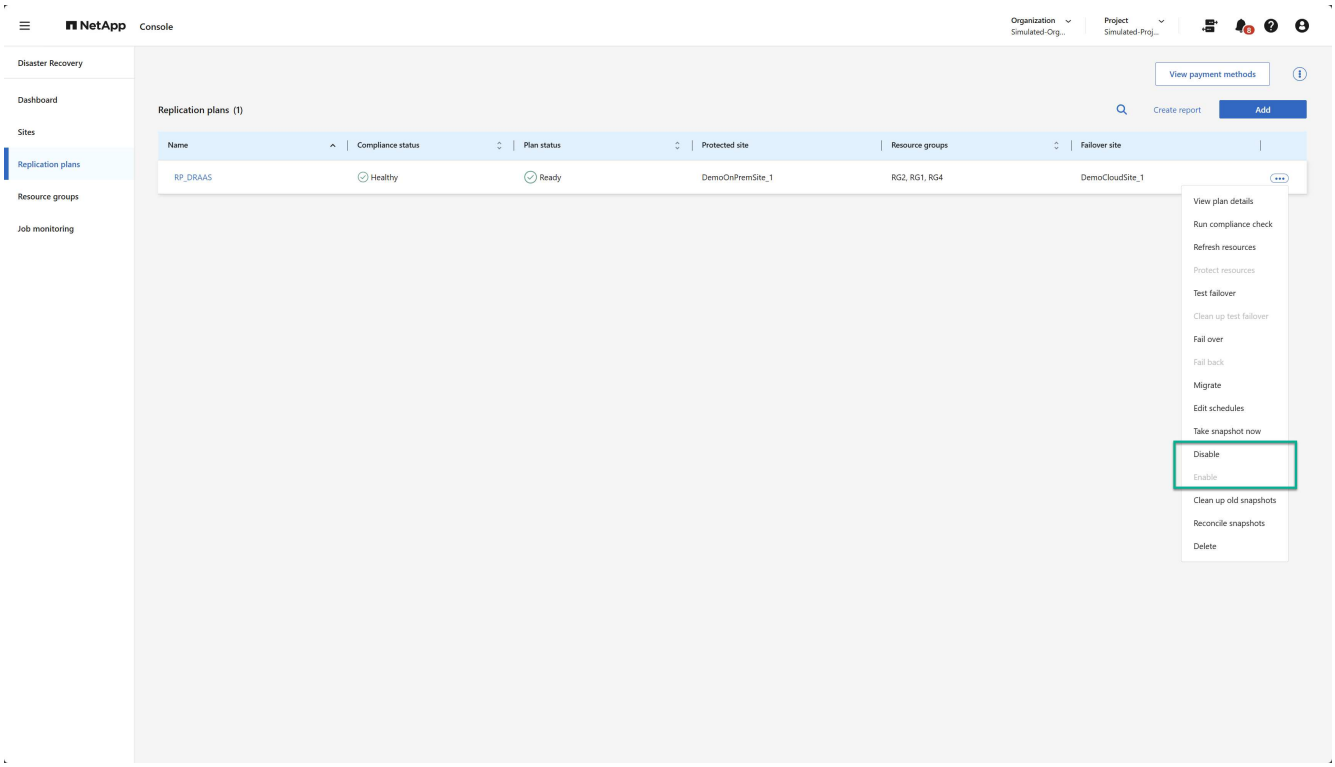


Replikationsplan deaktivieren oder aktivieren

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

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

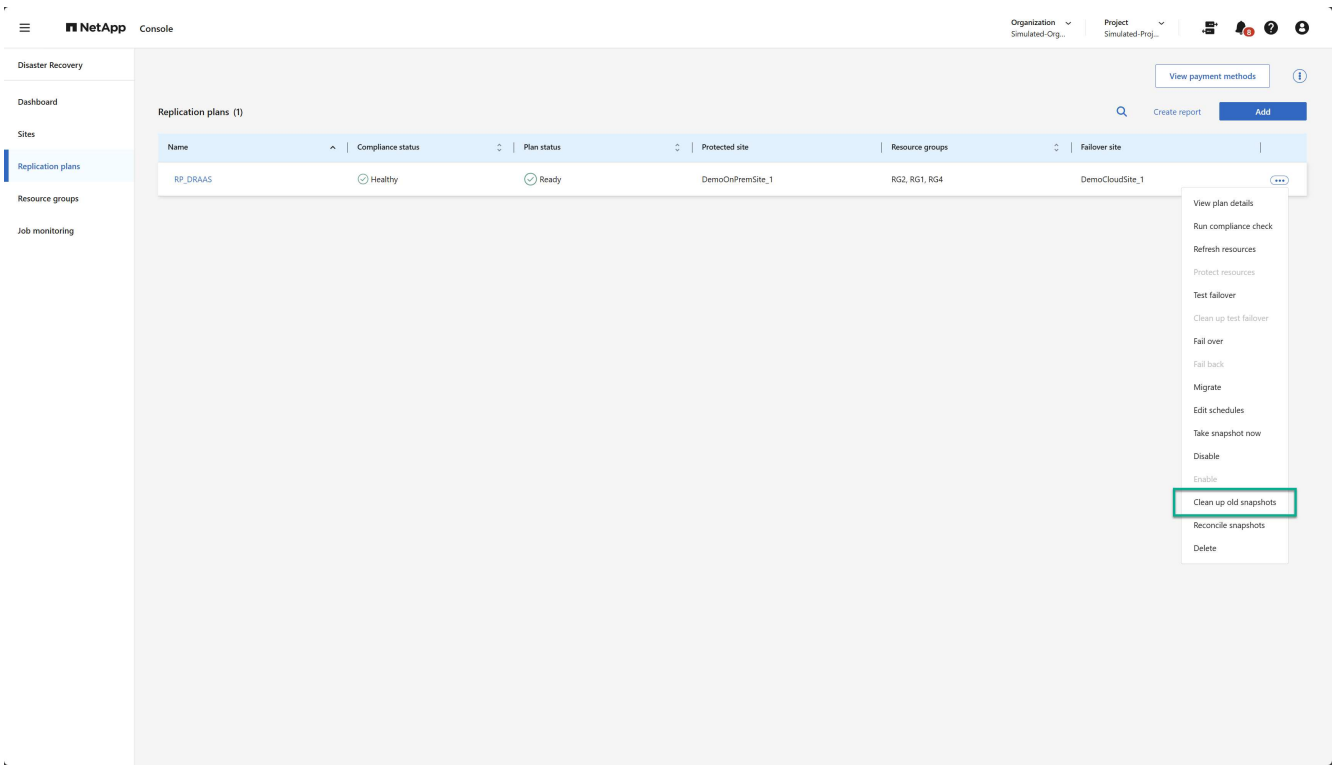
   Wenn der Replikationsplan aktiv ist, ist der Befehl **Aktivieren** ausgegraut. Wenn der Replikationsplan deaktiviert ist, ist der Befehl **Deaktivieren** ausgegraut.



Bereinigen Sie alte Snapshots

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

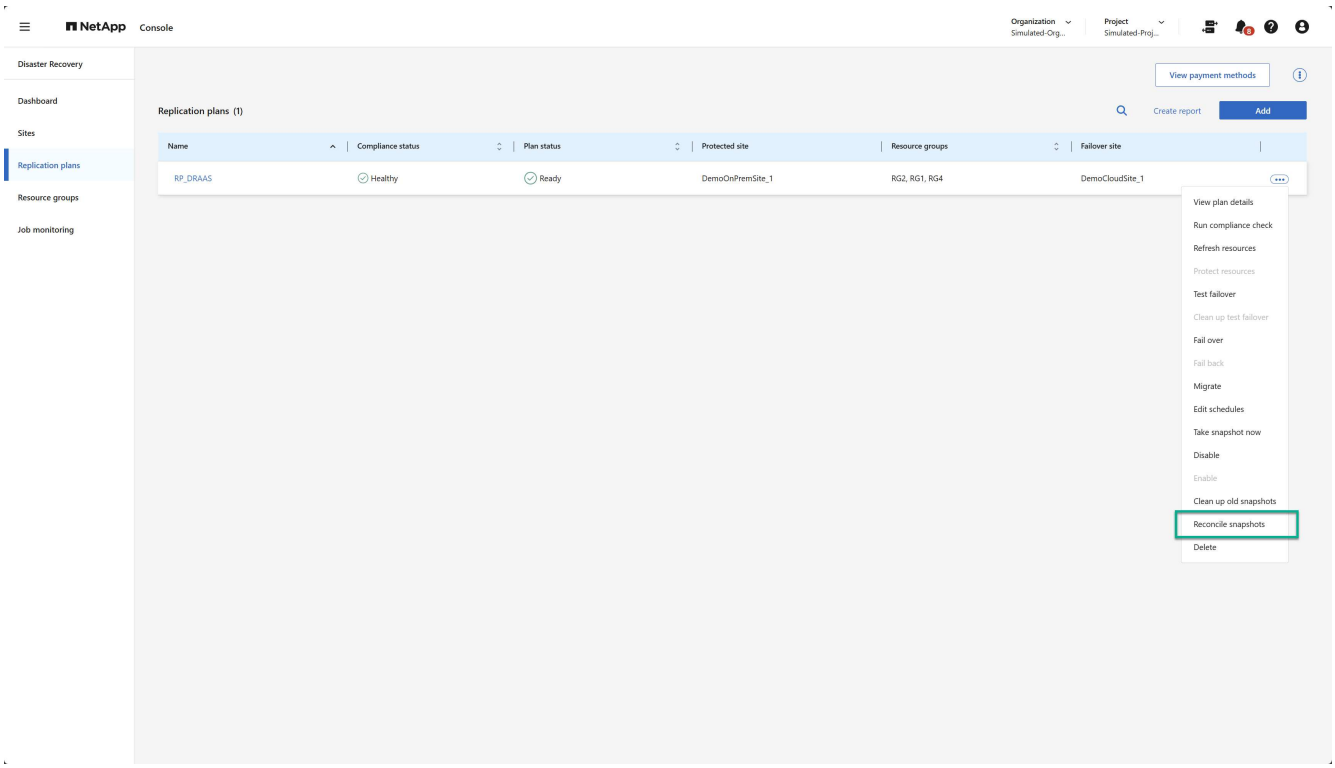
1. Wählen Sie die Option *Aktionen* ••• neben dem Replikationsplan.
2. Um diese älteren Snapshots manuell zu entfernen, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Alte Snapshots bereinigen“ aus.



Snapshots abgleichen

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

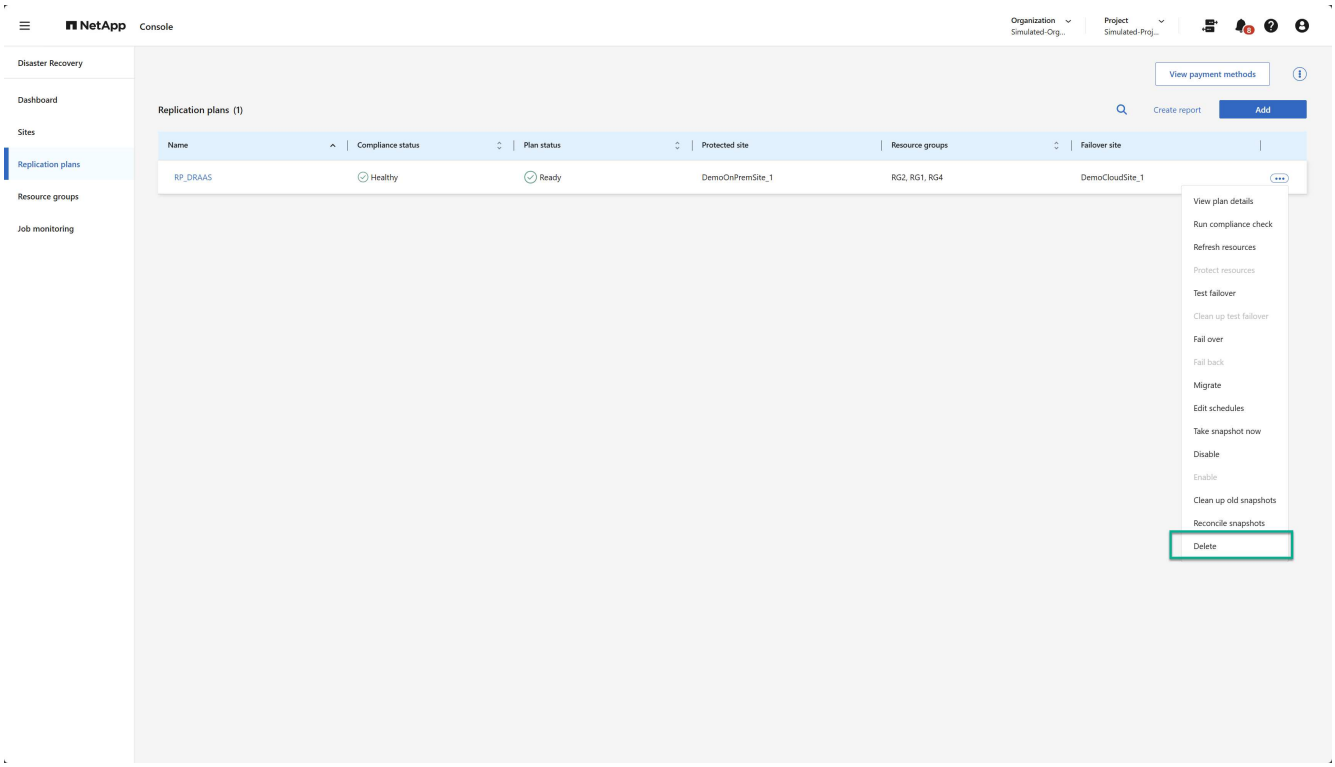
1. Wählen Sie die Option *Aktionen* ••• neben dem Replikationsplan.
2. Um Snapshots aus dem Quellcluster zu löschen, die im Zielcluster nicht vorhanden sind, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Snapshots abgleichen“ aus.



Replikationsplan löschen

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

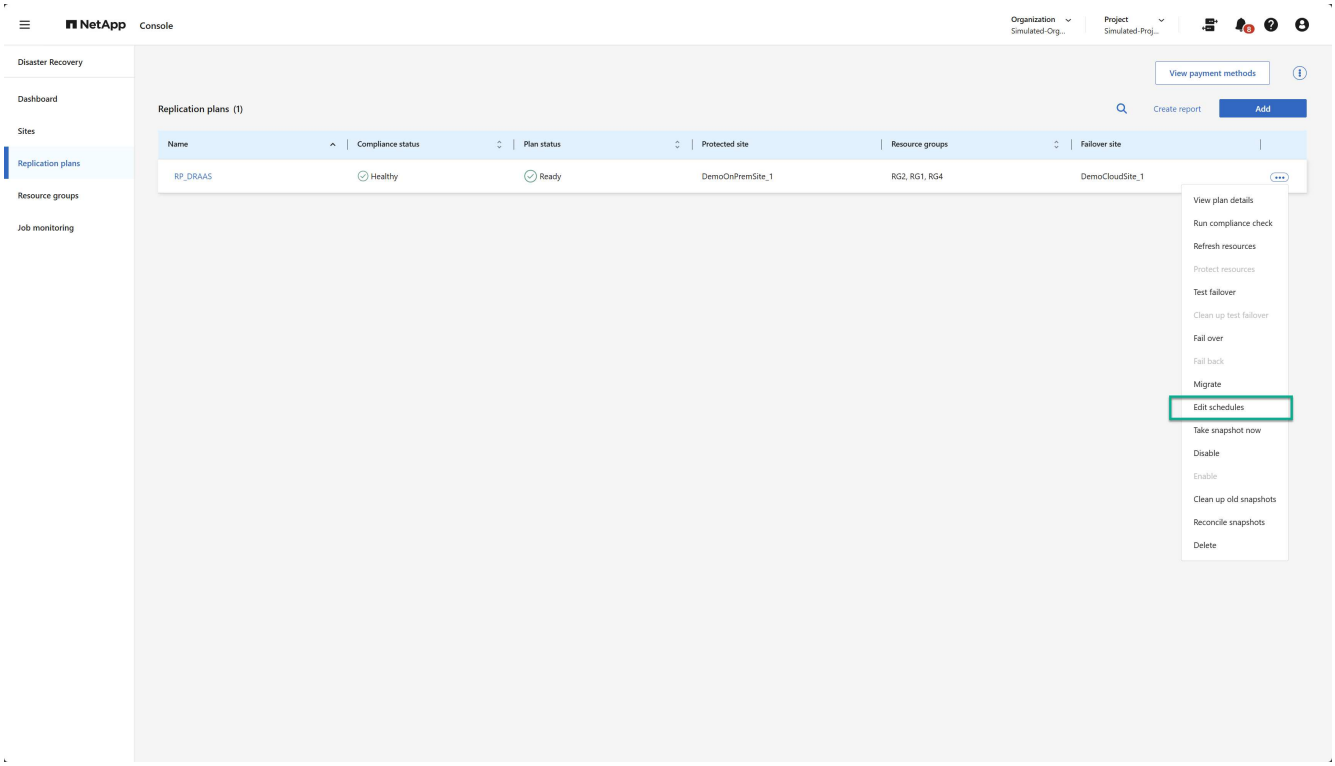
1. Wählen Sie die Option *Aktionen* ••• neben dem Replikationsplan.
2. Um den Replikationsplan zu löschen, wählen Sie **Löschen** aus dem Kontextmenü des Replikationsplans.



Zeitpläne bearbeiten

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

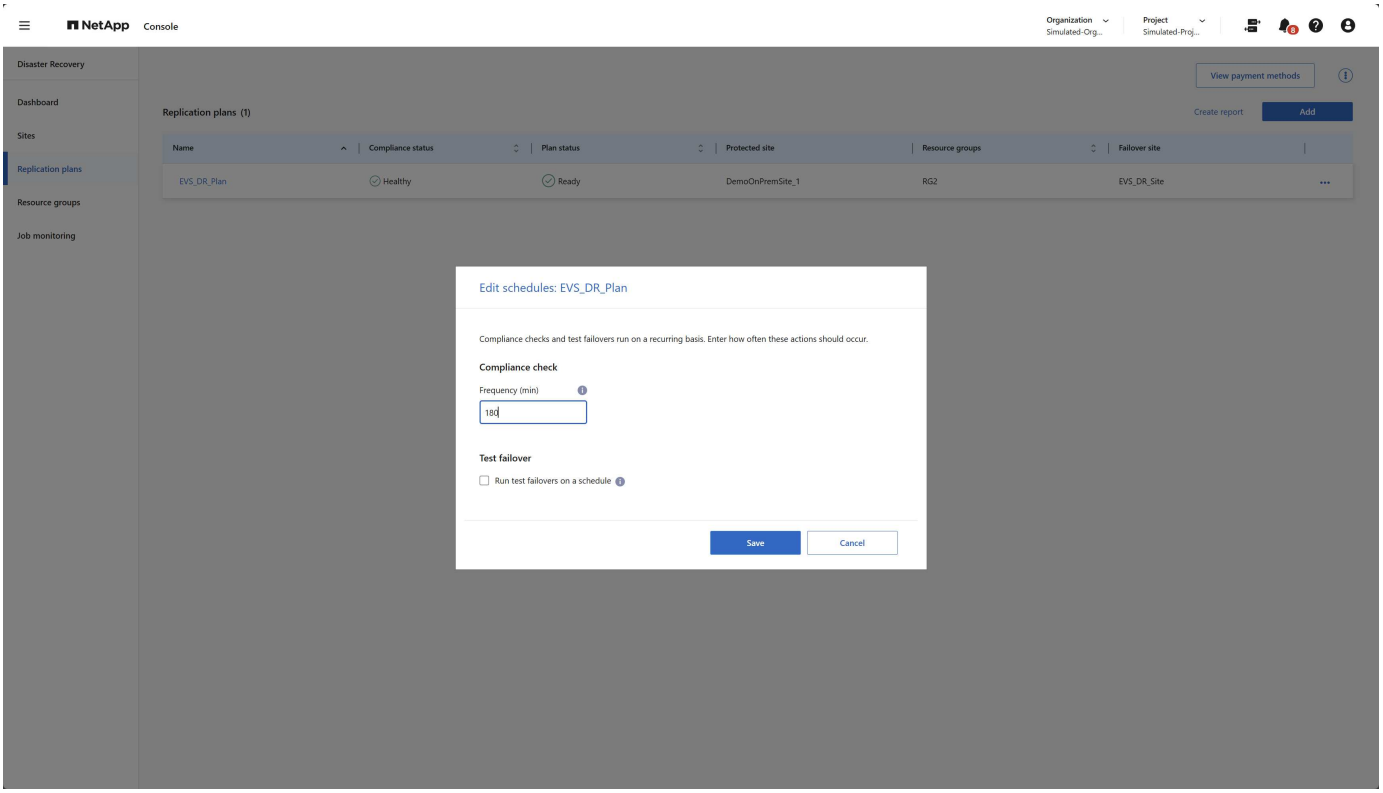
1. Wählen Sie die Option *Aktionen* ••• neben dem Replikationsplan.
2. Um diese Zeitpläne für einen dieser beiden Vorgänge zu ändern, wählen Sie **Zeitpläne bearbeiten** für den Replikationsplan aus.



Intervall für die Konformitätsprüfung ändern

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

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



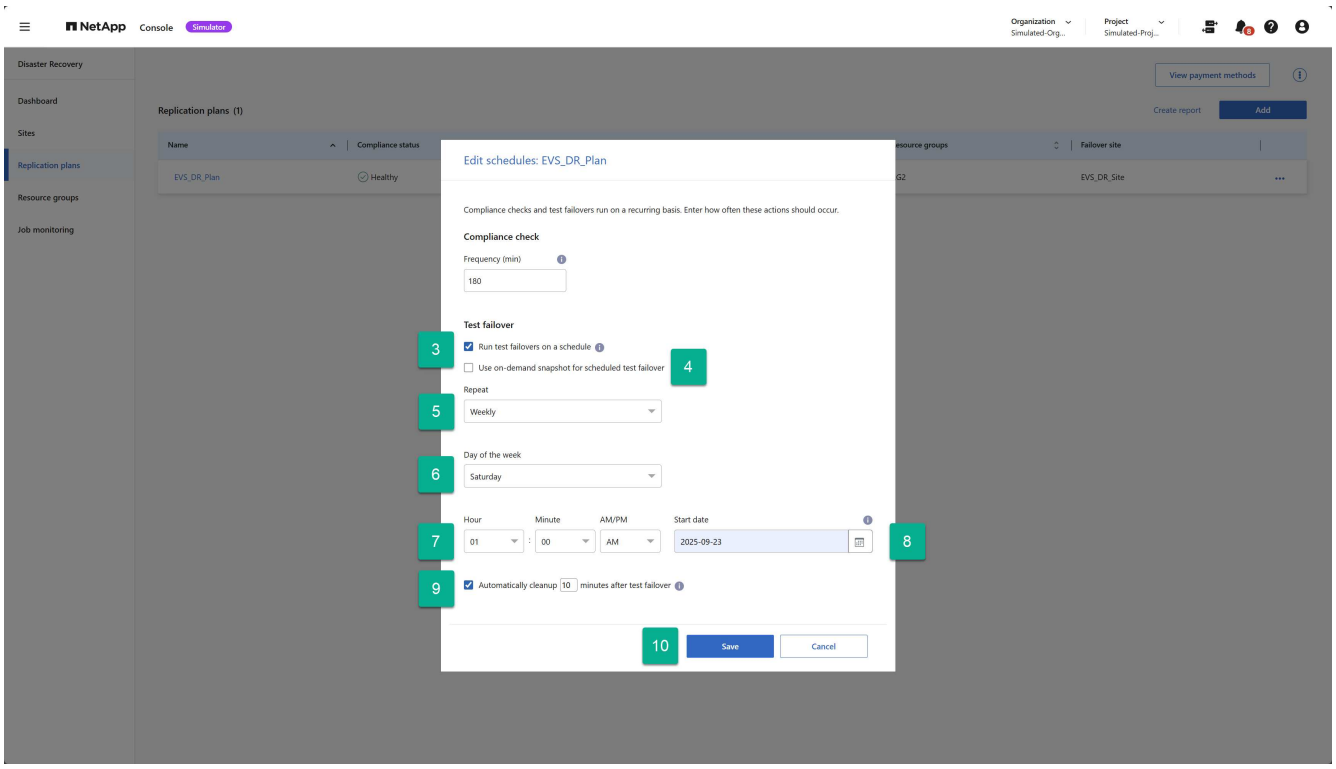
Planen Sie automatisierte Test-Failover

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

Schritte zum Planen von Test-Failovern

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

10. Wählen Sie **Speichern**.



Häufig gestellte Fragen zu NetApp Disaster Recovery

Diese FAQ können hilfreich sein, wenn Sie nur schnell eine Antwort auf eine Frage suchen.

Wie lautet die URL für NetApp Disaster Recovery ? Geben Sie als URL in einem Browser Folgendes ein: "https://console.netapp.com/" um auf die NetApp Konsole zuzugreifen.

Benötigen Sie eine Lizenz, um NetApp Disaster Recovery zu verwenden? Für den vollständigen Zugriff ist eine NetApp Disaster Recovery -Lizenz erforderlich. Sie können es jedoch mit der kostenlosen Testversion ausprobieren.

Einzelheiten zum Einrichten der Lizenzierung für NetApp Disaster Recovery finden Sie unter"Einrichten der NetApp Disaster Recovery -Lizenzierung" .

Wie greifen Sie auf NetApp Disaster Recovery zu? Für NetApp Disaster Recovery ist keine Aktivierung erforderlich. Die Option zur Notfallwiederherstellung wird automatisch in der linken Navigation der NetApp Console angezeigt.

Wissen und Unterstützung

Für Support registrieren

Um technischen Support speziell für BlueXP und seine Speicherlösungen und -dienste zu erhalten, ist eine Support-Registrierung erforderlich. Eine Support-Registrierung ist auch erforderlich, um wichtige Workflows für Cloud Volumes ONTAP Systeme zu aktivieren.

Durch die Registrierung für den Support wird kein NetApp Support für den Dateidienst eines Cloud-Anbieters aktiviert. Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der BlueXP -Dokumentation für das jeweilige Produkt.

- "Amazon FSx für ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Übersicht zur Support-Registrierung

Zur Aktivierung des Supportanspruchs stehen zwei Registrierungsformen zur Verfügung:

- Registrieren Sie die Seriennummer Ihres BlueXP Kontos (Ihre 20-stellige Seriennummer 960xxxxxxxx, die Sie auf der Support-Ressourcenseite in BlueXP finden).

  Dies dient als Ihre einzige Support-Abonnement-ID für alle Dienste innerhalb von BlueXP. Jedes Support-Abonnement auf BlueXP -Kontoebene muss registriert werden.

- Registrieren Sie die mit einem Abonnement verknüpften Cloud Volumes ONTAP Seriennummern im Marktplatz Ihres Cloud-Anbieters (dies sind 20-stellige 909201xxxxxxxx-Seriennummern).

  Diese Seriennummern werden allgemein als *PAYGO-Seriennummern* bezeichnet und von BlueXP zum Zeitpunkt der Bereitstellung von Cloud Volumes ONTAP generiert.

Durch die Registrierung beider Seriennummerntypen werden Funktionen wie das Öffnen von Support-Tickets und die automatische Fallgenerierung ermöglicht. Die Registrierung wird abgeschlossen, indem Sie wie unten beschrieben NetApp Support Site (NSS)-Konten zu BlueXP hinzufügen.

Registrieren Sie BlueXP für NetApp Support

Um sich für den Support zu registrieren und den Supportanspruch zu aktivieren, muss ein Benutzer in Ihrer BlueXP -Organisation (oder Ihrem Konto) ein NetApp Support Site-Konto mit seinem BlueXP Login verknüpfen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über ein NetApp Support Site (NSS)-Konto verfügen.

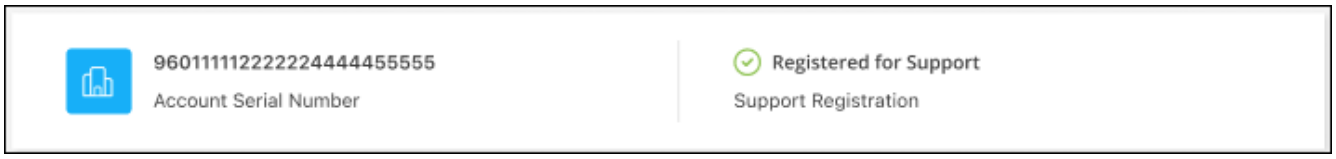
Bestandskunde mit NSS-Konto

Wenn Sie NetApp -Kunde mit einem NSS-Konto sind, müssen Sie sich lediglich für den Support über BlueXP registrieren.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Symbol „Einstellungen“ und dann „Anmeldeinformationen“ aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Authentifizierungsaufforderung der NetApp Support Site (NSS).
4. Um zu bestätigen, dass der Registrierungsvorgang erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

   Auf der Seite **Ressourcen** sollte angezeigt werden, dass Ihre BlueXP -Organisation für den Support registriert ist.

   Beachten Sie, dass anderen BlueXP Benutzern dieser Support-Registrierungsstatus nicht angezeigt wird, wenn sie ihrem BlueXP Login kein NetApp -Support-Site-Konto zugeordnet haben. Dies bedeutet jedoch nicht, dass Ihre BlueXP -Organisation nicht für den Support registriert ist. Sofern ein Benutzer in der Organisation diese Schritte befolgt hat, ist Ihre Organisation registriert.

Bestandskunde, aber kein NSS-Konto

Wenn Sie bereits NetApp -Kunde mit vorhandenen Lizenzen und Seriennummern, aber *keinem* NSS-Konto sind, müssen Sie ein NSS-Konto erstellen und es mit Ihrem BlueXP Login verknüpfen.

Schritte

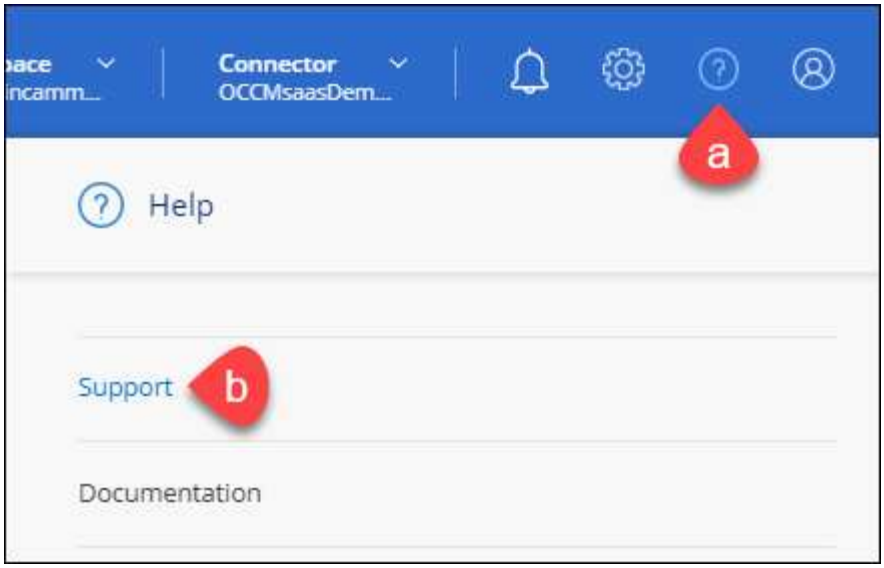
1. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die Seriennummer des BlueXP -Kontos (960xxxx) zu kopieren, die oben für das Feld „Seriennummer“ verwendet wurde. Dies beschleunigt die Kontobearbeitung.
2. Verknüpfen Sie Ihr neues NSS-Konto mit Ihrem BlueXP -Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

Ganz neu bei NetApp

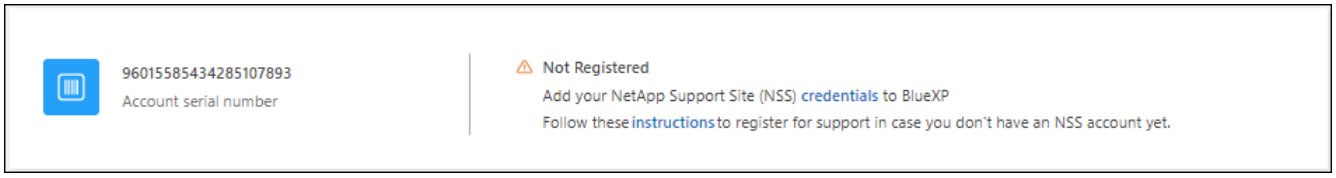
Wenn Sie NetApp noch nicht kennen und kein NSS-Konto haben, befolgen Sie die nachstehenden Schritte.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol und dann **Support** aus.



2. Suchen Sie auf der Support-Registrierungsseite nach der Seriennummer Ihrer Konto-ID.



3. Navigieren Sie zu "Support-Registrierungssite von NetApp" und wählen Sie **Ich bin kein registrierter NetApp -Kunde**.
4. Füllen Sie die Pflichtfelder (mit roten Sternchen gekennzeichnet) aus.
5. Wählen Sie im Feld **Produktlinie Cloud Manager** und dann Ihren entsprechenden Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer Ihres Kontos aus Schritt 2 oben, schließen Sie die Sicherheitsüberprüfung ab und bestätigen Sie anschließend, dass Sie die globale Datenschutzrichtlinie von NetApp gelesen haben.

   Um diese sichere Transaktion abzuschließen, wird umgehend eine E-Mail an das angegebene Postfach gesendet. Überprüfen Sie unbedingt Ihren Spam-Ordner, wenn die Bestätigungs-E-Mail nicht innerhalb weniger Minuten eintrifft.

7. Bestätigen Sie die Aktion in der E-Mail.

   Durch die Bestätigung wird Ihre Anfrage an NetApp übermittelt und es wird empfohlen, dass Sie ein NetApp Support Site-Konto erstellen.

8. Erstellen Sie ein NetApp Support Site-Konto, indem Sie das "Registrierungsformular für Benutzer der NetApp Support-Site"
   a. Achten Sie darauf, die entsprechende Benutzerebene auszuwählen, in der Regel „NetApp -Kunde/Endbenutzer“.
   b. Denken Sie daran, die oben für das Seriennummernfeld verwendete Kontoseriennummer (960xxxx) zu kopieren. Dadurch wird die Bearbeitung beschleunigt.

Nach Abschluss

NetApp sollte sich während dieses Vorgangs mit Ihnen in Verbindung setzen. Dies ist eine einmalige

Onboarding-Übung für neue Benutzer.

Sobald Sie über Ihr NetApp Support Site-Konto verfügen, verknüpfen Sie das Konto mit Ihrem BlueXP -Login, indem Sie die folgenden Schritte ausführenBestandskunde mit NSS-Konto .

NSS-Anmeldeinformationen für Cloud Volumes ONTAP Support zuordnen

Die Verknüpfung der Anmeldeinformationen der NetApp Support Site mit Ihrer BlueXP -Organisation ist erforderlich, um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu aktivieren:

- Registrieren von Pay-as-you-go Cloud Volumes ONTAP Systemen für den Support

  Die Angabe Ihres NSS-Kontos ist erforderlich, um den Support für Ihr System zu aktivieren und Zugriff auf die technischen Supportressourcen von NetApp zu erhalten.

- Bereitstellen von Cloud Volumes ONTAP mit eigener Lizenz (BYOL)

  Die Angabe Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für die von Ihnen erworbene Laufzeit aktivieren kann. Hierzu gehören automatische Updates bei Laufzeitverlängerungen.

- Aktualisieren der Cloud Volumes ONTAP -Software auf die neueste Version

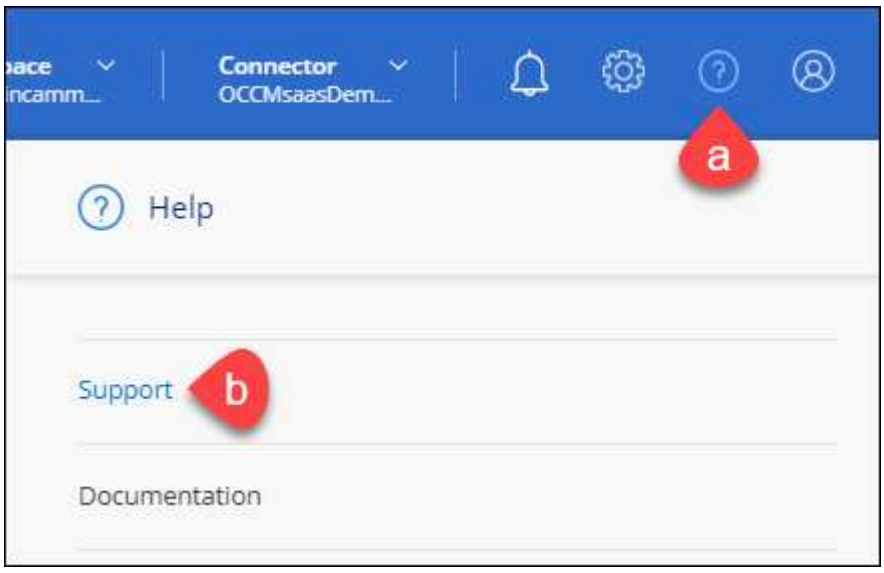
Das Verknüpfen von NSS-Anmeldeinformationen mit Ihrer BlueXP Organisation unterscheidet sich vom Verknüpfen des NSS-Kontos mit einer BlueXP Benutzeranmeldung.

Diese NSS-Anmeldeinformationen sind mit Ihrer spezifischen BlueXP -Organisations-ID verknüpft. Benutzer, die zur BlueXP -Organisation gehören, können über **Support > NSS-Verwaltung** auf diese Anmeldeinformationen zugreifen.

- Wenn Sie über ein Konto auf Kundenebene verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen.
- Wenn Sie über ein Partner- oder Reseller-Konto verfügen, können Sie ein oder mehrere NSS-Konten hinzufügen, diese können jedoch nicht zusammen mit Konten auf Kundenebene hinzugefügt werden.

Schritte

1. Wählen Sie oben rechts in der BlueXP Konsole das Hilfesymbol und dann **Support** aus.



2. Wählen Sie **NSS-Verwaltung > NSS-Konto hinzufügen**.
3. Wenn Sie dazu aufgefordert werden, wählen Sie **Weiter**, um zu einer Microsoft-Anmeldeseite weitergeleitet zu werden.

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsdienste speziell für Support und Lizenzierung.

4. Geben Sie auf der Anmeldeseite Ihre bei der NetApp Support Site registrierte E-Mail-Adresse und Ihr Kennwort ein, um den Authentifizierungsprozess durchzuführen.

   Diese Aktionen ermöglichen BlueXP , Ihr NSS-Konto für Dinge wie Lizenzdownloads, Überprüfung von Software-Upgrades und zukünftige Support-Registrierungen zu verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder temporäres Konto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto geben, wenn es sich bei diesem Konto um ein Konto auf Partnerebene handelt. Wenn Sie versuchen, NSS-Konten auf Kundenebene hinzuzufügen und ein Konto auf Partnerebene vorhanden ist, erhalten Sie die folgende Fehlermeldung:

     „Der NSS-Kundentyp ist für dieses Konto nicht zulässig, da bereits NSS-Benutzer eines anderen Typs vorhanden sind.“

   Dasselbe gilt, wenn Sie bereits über NSS-Konten auf Kundenebene verfügen und versuchen, ein Konto auf Partnerebene hinzuzufügen.

   - Nach erfolgreicher Anmeldung speichert NetApp den NSS-Benutzernamen.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail-Adresse zugeordnet ist. Auf der Seite **NSS-Verwaltung** können Sie Ihre E-Mail-Adresse aus dem ••• Speisekarte.

   - Wenn Sie Ihre Anmeldeinformationen aktualisieren müssen, gibt es auch die Option **Anmeldeinformationen aktualisieren** im ••• Speisekarte.

     Bei Verwendung dieser Option werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Sie werden durch eine entsprechende Benachrichtigung darauf aufmerksam gemacht.

Hilfe erhalten

NetApp bietet Support für BlueXP und seine Cloud-Services auf vielfältige Weise. Umfangreiche kostenlose Self-Support-Optionen stehen Ihnen rund um die Uhr zur Verfügung, darunter Knowledgebase-Artikel und ein Community-Forum. Ihre Support-Registrierung beinhaltet technischen Remote-Support per Web-Ticketing.

Erhalten Sie Unterstützung für den Dateidienst eines Cloud-Anbieters

Technischen Support für den Dateidienst eines Cloud-Anbieters, seine Infrastruktur oder eine Lösung, die den Dienst nutzt, erhalten Sie unter „Hilfe erhalten“ in der BlueXP -Dokumentation für das jeweilige Produkt.

- "Amazon FSx für ONTAP"

- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Um technischen Support speziell für BlueXP und seine Speicherlösungen und -dienste zu erhalten, verwenden Sie die unten beschriebenen Supportoptionen.

Nutzen Sie Möglichkeiten zur Selbsthilfe

Diese Optionen stehen Ihnen 24 Stunden am Tag, 7 Tage die Woche kostenlos zur Verfügung:

- Dokumentation

  Die BlueXP -Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Durchsuchen Sie die BlueXP Wissensdatenbank nach hilfreichen Artikeln zur Problembehebung.

- "Gemeinschaften"

  Treten Sie der BlueXP Community bei, um laufende Diskussionen zu verfolgen oder neue zu starten.

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie nach der Aktivierung des Supports mit einem NetApp -Support-Spezialisten zusammenarbeiten, um alle Probleme zu lösen.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** zu verwenden, müssen Sie zunächst Ihre Anmeldeinformationen für die NetApp -Support-Site mit Ihrem BlueXP Login verknüpfen. "Erfahren Sie, wie Sie die mit Ihrem BlueXP Login verknüpften Anmeldeinformationen verwalten" .
- Wenn Sie einen Fall für ein ONTAP -System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer für dieses System verknüpft sein.

Schritte

1. Wählen Sie in BlueXP*Hilfe > Support*.
2. Wählen Sie auf der Seite **Ressourcen** unter „Technischer Support“ eine der verfügbaren Optionen aus:

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem telefonieren möchten. Sie werden zu einer Seite auf netapp.com weitergeleitet, auf der die Telefonnummern aufgeführt sind, die Sie anrufen können.

   b. Wählen Sie **Fall erstellen**, um ein Ticket bei einem NetApp -Support-Spezialisten zu öffnen:

      - **Dienst**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispielsweise BlueXP , wenn es sich um ein spezielles technisches Supportproblem mit Arbeitsabläufen oder Funktionen innerhalb des Dienstes handelt.
      - **Arbeitsumgebung**: Wählen Sie, falls für den Speicher zutreffend, * Cloud Volumes ONTAP* oder **On-Prem** und dann die zugehörige Arbeitsumgebung aus.

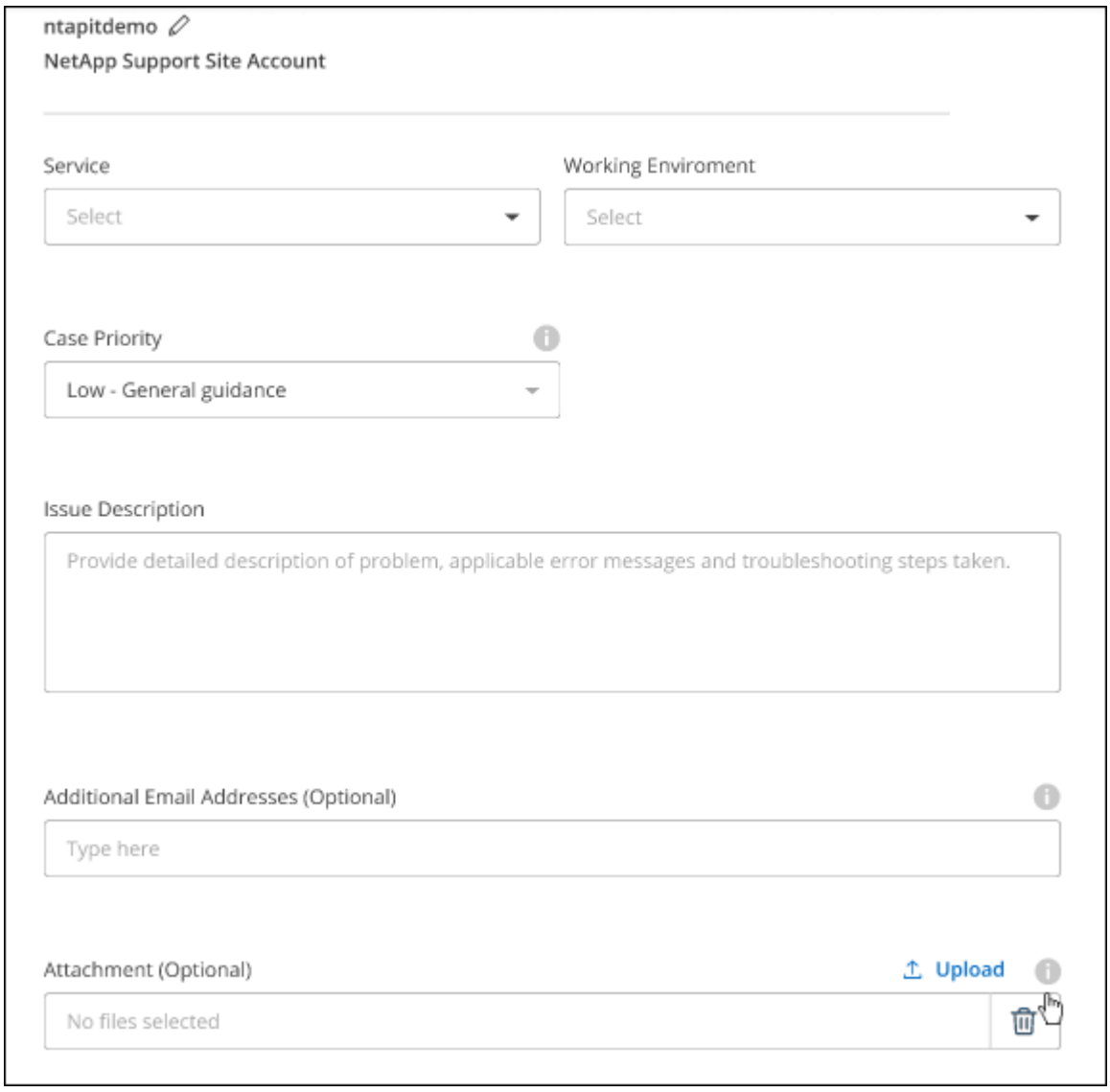
        Die Liste der Arbeitsumgebungen liegt im Rahmen der BlueXP -Organisation (oder des Kontos), des Projekts (oder Arbeitsbereichs) und des Connectors, den Sie im oberen Banner des Dienstes ausgewählt haben.

- **Fallpriorität**: Wählen Sie die Priorität für den Fall. Sie kann „Niedrig“, „Mittel“, „Hoch“ oder „Kritisch“ sein.

  Um weitere Einzelheiten zu diesen Prioritäten zu erfahren, bewegen Sie die Maus über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller zutreffenden Fehlermeldungen oder Schritte zur Fehlerbehebung, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderen auf dieses Problem aufmerksam machen möchten.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge hoch, einen nach dem anderen.

  Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.



Nach Abschluss

Es erscheint ein Popup mit Ihrer Support-Fallnummer. Ein NetApp -Support-Spezialist wird Ihren Fall prüfen und sich in Kürze bei Ihnen melden.

Um einen Verlauf Ihrer Supportfälle anzuzeigen, können Sie **Einstellungen > Zeitleiste** auswählen und nach Aktionen mit der Bezeichnung „Supportfall erstellen“ suchen. Über eine Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Beim Versuch, einen Fall zu erstellen, kann es sein, dass die folgende Fehlermeldung angezeigt wird:

„Sie sind nicht berechtigt, einen Fall für den ausgewählten Dienst zu erstellen.“

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das damit verknüpfte Unternehmen nicht dasselbe Unternehmen sind, für das die Seriennummer des BlueXP Kontos gilt (d. h. 960xxxx) oder die Seriennummer der Arbeitsumgebung. Sie können auf eine der folgenden Arten Hilfe anfordern:

- Verwenden Sie den Chat im Produkt
- Senden Sie einen nicht-technischen Fall an https://mysupport.netapp.com/site/help

Verwalten Sie Ihre Supportfälle (Vorschau)

Sie können aktive und gelöste Supportfälle direkt von BlueXP aus anzeigen und verwalten. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verknüpften Fälle verwalten.

Das Fallmanagement ist als Vorschau verfügbar. Wir planen, dieses Erlebnis zu verfeinern und in kommenden Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Feedback über den Chat im Produkt.

Beachten Sie Folgendes:

- Das Fallmanagement-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht links zeigt die Gesamtzahl der Fälle, die in den letzten drei Monaten von dem von Ihnen angegebenen NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht rechts zeigt die Gesamtzahl der in den letzten drei Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto.

  Die Ergebnisse in der Tabelle spiegeln die Fälle wider, die mit der von Ihnen ausgewählten Ansicht in Zusammenhang stehen.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie „Priorität“ und „Status“ filtern. Andere Spalten bieten lediglich Sortierfunktionen.

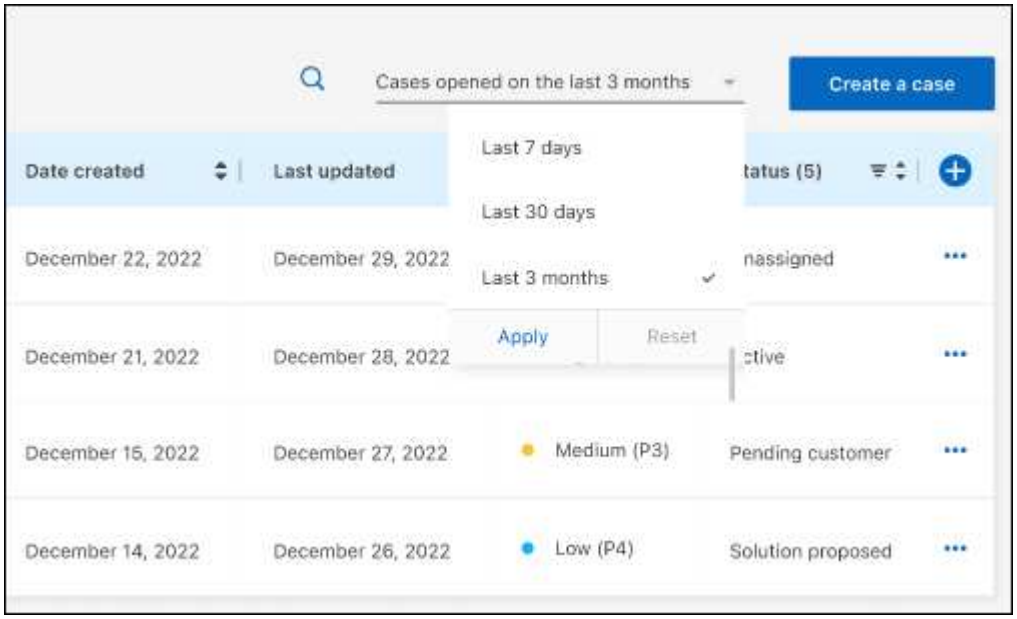
  Weitere Einzelheiten finden Sie in den folgenden Schritten.
- Auf Einzelfallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Abgeschlossen“ oder „Ausstehend abgeschlossen“ befindet.

Schritte

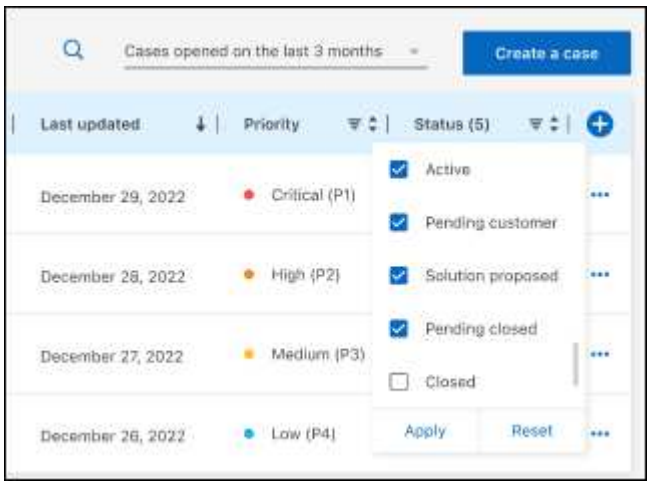
1. Wählen Sie in BlueXP*Hilfe > Support*.
2. Wählen Sie **Fallmanagement** und fügen Sie Ihr NSS-Konto zu BlueXP hinzu, wenn Sie dazu aufgefordert werden.

   Auf der Seite **Fallverwaltung** werden offene Fälle angezeigt, die sich auf das NSS-Konto beziehen, das mit Ihrem BlueXP -Benutzerkonto verknüpft ist. Dies ist dasselbe NSS-Konto, das oben auf der **NSS-Verwaltungsseite** angezeigt wird.
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:

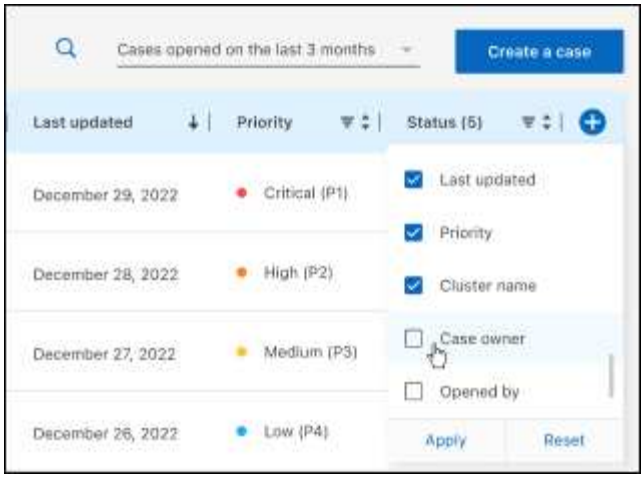
- Wählen Sie unter **Fälle der Organisation** die Option **Anzeigen** aus, um alle mit Ihrem Unternehmen verknüpften Fälle anzuzeigen.
- Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.



- Filtern Sie den Inhalt der Spalten.



- Ändern Sie die in der Tabelle angezeigten Spalten, indem Sie und wählen Sie dann die Spalten aus, die Sie anzeigen möchten.

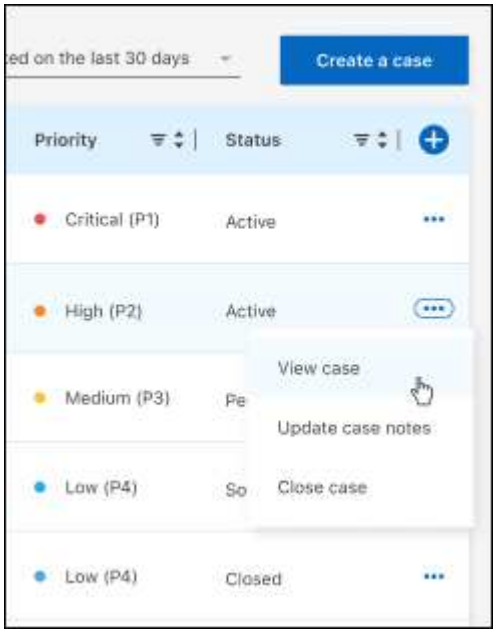


4. Verwalten Sie einen vorhandenen Fall, indem Sie ••• und wählen Sie eine der verfügbaren Optionen aus:

   - **Fall anzeigen**: Alle Details zu einem bestimmten Fall anzeigen.
   - **Fallnotizen aktualisieren**: Geben Sie zusätzliche Details zu Ihrem Problem an oder wählen Sie **Dateien hochladen**, um bis zu fünf Dateien anzuhängen.

     Anhänge sind auf 25 MB pro Datei begrenzt. Die folgenden Dateierweiterungen werden unterstützt: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx und csv.

   - **Fall schließen**: Geben Sie Details zum Grund für das Schließen des Falls an und wählen Sie **Fall schließen** aus.



Rechtliche Hinweise

Rechtliche Hinweise bieten Zugriff auf Urheberrechtserklärungen, Marken, Patente und mehr.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marken

NETAPP, das NETAPP-Logo und die auf der NetApp -Markenseite aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen- und Produktnamen können Marken ihrer jeweiligen Eigentümer sein.

"https://www.netapp.com/company/legal/trademarks/"

Patente

Eine aktuelle Liste der Patente im Besitz von NetApp finden Sie unter:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Datenschutzrichtlinie

"https://www.netapp.com/company/legal/privacy-policy/"

Open Source

Hinweisdateien enthalten Informationen zu Urheberrechten und Lizenzen Dritter, die in der NetApp -Software verwendet werden.

"Hinweis zur NetApp Disaster Recovery"