BlueXP Disaster Recovery-Dokumentation

BlueXP disaster recovery

NetApp
August 08, 2025

Inhalt

BlueXP Disaster Recovery-Dokumentation

Versionshinweise

Neuerungen bei der BlueXP Disaster Recovery

Erfahren Sie mehr über die Neuerungen bei BlueXP Disaster Recovery.

04. August 2025

Version 4.2.5P2

BlueXP disaster recovery

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 "BlueXP disaster recovery -Lizenzierung" Und "Lizenzierung für die Disaster Recovery von BlueXP einrichten" .

14 Juli 2025

Version 4.2.5

Benutzerrollen in der BlueXP disaster recovery

Die BlueXP 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 die BlueXP disaster recovery sind.

- **Notfallwiederherstellungsadministrator**: Führen Sie beliebige Aktionen in der BlueXP disaster recovery durch.
- **Disaster Recovery-Failover-Administrator**: Führen Sie Failover- und Migrationsaktionen in der BlueXP disaster recovery durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Erstellen und ändern Sie Replikationspläne und starten Sie Test-Failover.

- **Disaster Recovery Viewer**: Informationen in BlueXP disaster recovery anzeigen, aber keine Aktionen ausführen.

Wenn Sie auf den BlueXP disaster recovery klicken und ihn zum ersten Mal konfigurieren, müssen Sie über die Berechtigung **SnapCenterAdmin** verfügen oder die Rolle **Organisationsadministrator** innehaben.

Weitere Informationen finden Sie unter "Benutzerrollen und Berechtigungen in der BlueXP disaster recovery".

"Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Weitere Updates zur BlueXP 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 die BlueXP disaster recovery sie jetzt automatisch aus dem Replikationsplan.
  - Wenn ein Datenspeicher oder Netzwerk im vCenter gelöscht wird, löscht die BlueXP disaster recovery es jetzt aus dem Replikationsplan und der Ressourcengruppe.
  - Wenn ein Cluster, Host oder Rechenzentrum im vCenter gelöscht wird, löscht BlueXP disaster recovery es jetzt aus dem Replikationsplan und der Ressourcengruppe.
- Sie können jetzt im Inkognito-Modus Ihres Browsers auf die Swagger-Dokumentation zugreifen. Sie erreichen sie in BlueXP disaster recovery über die Option „Einstellungen“ > „API-Dokumentation“ oder direkt über die folgende URL im Inkognito-Modus Ihres Browsers: "Swagger-Dokumentation" .
- In manchen Fällen blieb die iGroup nach einem Failback-Vorgang bestehen. Dieses Update entfernt die iGroup, falls sie veraltet ist.
- Wenn der NFS-FQDN im Replikationsplan verwendet wurde, löst BlueXP disaster recovery ihn nun in eine IP-Adresse auf. Dieses Update ist nützlich, wenn der FQDN am Disaster Recovery-Standort 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 nun schnell bestimmte Subnetze durch die Eingabe von Suchbegriffen finden, was die Verwaltung von Subnetzzuordnungen vereinfacht.

9 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 nun Subnetzzuordnungsoptionen auswählen und die LAPS-Option aktivieren, indem Sie die Domänencontrollerdetails angeben. Mit dieser Option müssen Sie nicht für jede Ihrer virtuellen Maschinen ein Kennwort angeben.

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

13 Mai 2025

Version 4.2.3

Subnetzzuordnung

Mit diesem Release können Sie IP-Adressen bei einem Failover auf neue Weise mithilfe der Subnetzzuordnung managen, wodurch Sie Subnetze für jedes vCenter hinzufügen können. Dabei definieren Sie den IPv4 CIDR, das Standard-Gateway und den DNS für jedes virtuelle Netzwerk.

Bei einem Failover ermittelt die Disaster Recovery von BlueXP die geeignete IP-Adresse jeder vNIC, indem das für das zugeordnete virtuelle Netzwerk bereitgestellte CIDR betrachtet und es zum Ableiten der neuen IP-Adresse verwendet wird.

Beispiel:

- NetworkA = 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. NetworkA wird in den Einstellungen des Replikationsplans zu NetworkB zugeordnet.

Bei einem Failover ersetzt die Disaster Recovery von BlueXP den Teil Netzwerk der ursprünglichen IP-Adresse (10.1.1) und behält die Host-Adresse (.50) der ursprünglichen IP-Adresse (10.1.1.50) bei. Für VM1 betrachtet die BlueXP Disaster Recovery die CIDR-Einstellungen für NetworkB und verwendet den Netzwerk-B-Teil 192.168.1, während der Host-Teil (.50) beibehalten wird, um die neue IP-Adresse für VM1 zu erstellen. Die neue IP wird 192.168.1.50.

Zusammenfassend bleibt die Host-Adresse unverändert, während die Netzwerkadresse durch das ersetzt wird, was in der Subnetz-Zuordnung des Standorts konfiguriert ist. So lässt sich die IP-Adressenzuweisung beim Failover einfacher managen, insbesondere wenn Sie hunderte Netzwerke und tausende VMs managen müssen.

Weitere Informationen zum Einbeziehen der Subnetzzuordnung in Ihre Standorte finden Sie unter "Fügen Sie vCenter-Serverstandorte hinzu".

Schutz überspringen

Sie können jetzt den Schutz überspringen, damit der Dienst nach einem Failover des Replikationsplans nicht automatisch eine umgekehrte Schutzbeziehung erstellt. Dies ist nützlich, wenn Sie auf dem wiederhergestellten Standort weitere Vorgänge durchführen möchten, bevor Sie ihn in BlueXP Disaster Recovery wieder online schalten.

Wenn Sie ein Failover initiieren, erstellt der Service standardmäßig automatisch eine umgekehrte Schutzbeziehung für jedes Volume im Replizierungsplan, wenn der ursprüngliche Quellstandort online ist. Das bedeutet, dass der Service eine SnapMirror-Beziehung vom Zielstandort zurück zum Quellstandort erstellt. Der Service kehrt auch automatisch die SnapMirror-Beziehung um, wenn Sie ein Failback initiieren.

Wenn Sie ein Failover starten, können Sie jetzt eine Option **Skip Protection** wählen. Damit wird die SnapMirror-Beziehung nicht automatisch rückgängig gemacht. Stattdessen verlässt es das beschreibbare Volume auf beiden Seiten des Replizierungsplans.

Nachdem der ursprüngliche Quellstandort wieder online ist, können Sie den 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 ein Failback auf die übliche Weise initiieren.

Weitere Informationen zum Übersprungsschutz finden Sie unter "Failover von Anwendungen an einen Remote-Standort".

SnapMirror plant Updates im Replizierungsplan

BlueXP Disaster Recovery unterstützt nun die Verwendung externer Snapshot-Managementlösungen, wie z. B. der native Richtlinienplaner von ONTAP SnapMirror oder die Integration von Produkten anderer Anbieter mit ONTAP. Wenn jeder Datastore (Volume) im Replizierungsplan bereits über eine SnapMirror-Beziehung verfügt, die an anderer Stelle gemanagt wird, können Sie diese Snapshots als Wiederherstellungspunkte in der BlueXP Disaster Recovery verwenden.

Aktivieren Sie zum Konfigurieren im Abschnitt Replizierungsplan > Ressourcenzuordnung das Kontrollkästchen **Plattform-verwaltete Backups und Aufbewahrungszeitpläne verwenden**, wenn Sie die Datenspeicherzuordnung konfigurieren.

Wenn die Option ausgewählt ist, wird in BlueXP Disaster Recovery kein Backup-Zeitplan konfiguriert. Sie müssen jedoch weiterhin einen Aufbewahrungszeitplan konfigurieren, da darüber hinaus Snapshots für Test-, Failover- und Failback-Vorgänge erstellt werden können.

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

Weitere Informationen zur Verwendung externer Snapshot-Lösungen im Replikationsplan finden Sie unter "Erstellen Sie einen Replizierungsplan".

Bis 16. April 2025

Version 4.2.2

Geplante Ermittlung für VMs

Bei der Disaster Recovery von BlueXP werden alle 24 Stunden einmal erkannt. Mit dieser Version können Sie den Zeitplan zur Bestandsaufnahme nun an Ihre Anforderungen anpassen und die Performance bei Bedarf verringern. Wenn Sie beispielsweise über eine große Anzahl von VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 48 Stunden ausgeführt wird. Wenn Sie über eine geringe Anzahl von VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 12 Stunden ausgeführt wird.

Wenn Sie die Ermittlung nicht per wan planen, können Sie die Option für die geplante Ermittlung deaktivieren und die Ermittlung jederzeit manuell aktualisieren.

Weitere Informationen finden Sie unter "Fügen Sie vCenter-Serverstandorte hinzu".

Unterstützung für Ressourcengruppen-Datastore

Zuvor können Sie Ressourcengruppen nur nach VMs erstellen. Mit diesem Release können Sie eine Ressourcengruppe nach Datastores 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 von VMs verfügen und sie nach Datenspeicher gruppieren möchten.

Sie haben folgende Möglichkeiten, eine Ressourcengruppe mit einem Datastore zu erstellen:

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

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Benachrichtigungen über Ablauf der kostenlosen Testversion oder Lizenz

Diese Version enthält Benachrichtigungen, dass die kostenlose Testversion in 60 Tagen abläuft, um sicherzustellen, dass Sie Zeit haben, um eine Lizenz zu erhalten. Diese Version enthält auch Benachrichtigungen an dem Tag, an dem die Lizenz abläuft.

Benachrichtigung über Service-Updates

Mit diesem Release wird oben ein Banner angezeigt, das anzeigt, dass Services aktualisiert werden und der Service in den Wartungsmodus versetzt wird. Das Banner wird angezeigt, wenn der Dienst aktualisiert wird, und wird nach Abschluss der Aktualisierung nicht mehr angezeigt. Sie können zwar weiterhin in der Benutzeroberfläche arbeiten, während das Upgrade ausgeführt wird, Sie können jedoch keine neuen Jobs senden. Geplante Jobs werden ausgeführt, nachdem die Aktualisierung abgeschlossen ist und der Dienst in den Produktionsmodus zurückkehrt.

10 März 2025

Version 4.2.1

Intelligente Proxy-Unterstützung

Der BlueXP -Connector unterstützt den intelligenten Proxy. Ein intelligenter Proxy ist eine einfache, sichere und effiziente Möglichkeit, Ihre On-Premises-Umgebung mit dem BlueXP -Service zu verbinden. Sie stellt eine

sichere Verbindung zwischen Ihrer Umgebung und dem BlueXP -Dienst her, ohne dass ein VPN oder ein direkter Internetzugang erforderlich ist. Diese optimierte Proxy-Implementierung entlastet den API-Verkehr innerhalb des lokalen Netzwerks.

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

Für die Implementierung eines BlueXP Disaster Recovery Proxy ist eine Port 443-Kommunikation zwischen dem Connector und allen vCenter-Servern und ONTAP-Arrays über ein HTTPS-Protokoll erforderlich. Der BlueXP Disaster Recovery-Agent im Connector kommuniziert direkt mit VMware vSphere, VC oder ONTAP, wenn Aktionen durchgeführt werden.

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

Weitere Informationen über die Einrichtung eines allgemeinen Proxys in BlueXP finden Sie unter "Konfigurieren Sie einen Konnektor für die Verwendung eines Proxy-Servers".

Beenden Sie die kostenlose Testversion jederzeit

Sie können die kostenlose Testversion an jedem Zinken stoppen oder Sie können warten, bis sie abläuft.

Siehe "Beenden Sie die kostenlose Testversion".

19 Februar 2025

Version 4.2

Unterstützung von ASA r2 für VMs und Datastores auf VMFS Storage

Diese Version von BlueXP Disaster Recovery unterstützt ASA r2 für VMs und Datastores auf VMFS-Storage. Auf einem ASA r2 System unterstützt die ONTAP Software grundlegende SAN-Funktionen und beseitigt gleichzeitig Funktionen, die in SAN-Umgebungen nicht unterstützt werden.

Dieser Release unterstützt die folgenden Funktionen für ASA r2:

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

Die Unterstützung für ASA r2 für BlueXP Disaster Recovery verwendet ONTAP 9.16.1.

Während Datastores auf einem ONTAP Volume oder einer ASA r2 Storage-Einheit gemountet werden können, kann eine Ressourcengruppe in der Disaster Recovery mit BlueXP nicht sowohl einen Datenspeicher aus ONTAP als auch einen Datenspeicher aus ASA r2 umfassen. Sie können entweder einen Datenspeicher aus ONTAP oder einen Datenspeicher aus ASA r2 in einer Ressourcengruppe auswählen.

30 Oktober 2024

Berichterstellung

Sie können jetzt Berichte erstellen und herunterladen, um Ihre Umgebung zu analysieren. Vordefinierte Berichte fassen Failover und Failbacks zusammen, zeigen Replikationsdetails auf allen Standorten an und zeigen Jobdetails der letzten sieben Tage an.

Siehe "Erstellen von Disaster-Recovery-Berichten".

30 Tage kostenlos testen

Sie können sich jetzt für eine kostenlose 30-Tage-Testversion von BlueXP Disaster Recovery anmelden. Zuvor waren kostenlose Testversionen für 90 Tage.

Siehe "Lizenzierung einrichten".

Deaktivieren und aktivieren Sie Replikationspläne

Eine frühere Version beinhaltete Aktualisierungen der Planungsstruktur für Failover-Tests, die zur Unterstützung von täglichen und wöchentlichen Zeitplänen erforderlich war. Für dieses Update mussten Sie alle vorhandenen Replikationspläne deaktivieren und wieder aktivieren, damit Sie die neuen täglichen und wöchentlichen Failover-Testpläne verwenden können. Dies ist eine einmalige Anforderung.

Und so funktioniert es:

1. Wählen Sie im oberen 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 ein paar Minuten **enable**.

Ordnerzuordnung

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

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

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

Wenn ein Fehler auftritt und Sie einen Failover starten, ein Failback durchführen oder den Failover testen, können Sie jetzt die Details der VMs sehen und ermitteln, welche VMs nicht neu gestartet wurden.

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

VM-Boot-Verzögerung mit bestellter Boot-Sequenz

Wenn Sie einen Replizierungsplan erstellen, können Sie jetzt für jede VM im Plan eine Boot-Verzögerung festlegen. So können Sie eine Sequenz für die VMs festlegen, die gestartet werden soll, um sicherzustellen, dass alle Ihre Priorität 1 VMs ausgeführt werden, bevor nachfolgende VMs mit Priorität gestartet werden.

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Informationen zum VM-Betriebssystem

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

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Aliasing für VM-Namen

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

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Alte Snapshots bereinigen

Sie können alle Snapshots löschen, die nicht mehr über die angegebene Aufbewahrungszahl hinaus benötigt werden. Snapshots können sich im Laufe der Zeit ansammeln, wenn Sie die Anzahl der Snapshot-Aufbewahrung senken, und Sie können sie jetzt entfernen, um Speicherplatz freizugeben. Dies ist jederzeit nach Bedarf oder beim Löschen eines Replikationsplans möglich.

Weitere Informationen finden Sie unter "Verwalten von Standorten, Ressourcengruppen, Replikationsplänen, Datastores und Informationen zu virtuellen Maschinen".

Snapshots abgleichen

Sie können jetzt Snapshots abgleichen, die nicht synchron zwischen Quelle und Ziel sind. Dies kann vorkommen, wenn Snapshots auf einem Ziel außerhalb der Disaster Recovery von BlueXP gelöscht werden. Der Dienst löscht den Snapshot auf der Quelle automatisch alle 24 Stunden. Sie können dies jedoch nach Bedarf durchführen. Mit dieser Funktion können Sie sicherstellen, dass die Snapshots über alle Standorte hinweg konsistent sind.

Weitere Informationen finden Sie unter "Verwalten von Replikationsplänen".

20 September 2024

Unterstützung von lokalen bis lokalen VMware VMFS-Datastores

Diese Version umfasst Unterstützung für VMs, die auf VMware vSphere VMFS-Datastores (Virtual Machine File System) für iSCSI und FC gemountet sind und in lokalem Storage geschützt sind. Zuvor bot der Service eine Technologievorschau, die VMFS-Datastores für iSCSI und FC unterstützte.

Folgende Punkte sollten in Bezug auf iSCSI- und FC-Protokolle zusätzlich beachtet werden:

- FC-Unterstützung ist für Front-End-Protokolle des Clients, nicht für Replizierung.
- Die Disaster Recovery von BlueXP unterstützt nur eine einzige LUN pro ONTAP Volume. Das Volume sollte nicht über mehrere LUNs verfügen.
- Bei jedem Replizierungsplan sollte das Ziel-ONTAP-Volume die gleichen Protokolle verwenden wie das Quell-ONTAP-Volume, auf dem die geschützten VMs gehostet werden. Wenn z. B. die Quelle ein FC-Protokoll verwendet, sollte das Ziel auch FC verwenden.

2 August 2024

Unterstützung von lokalen bis lokalen VMware VMFS-Datastores für FC

Diese Version enthält eine Technologievorschau von Unterstützung für VMs, die auf VMware vSphere VMFS-Datastores (Virtual Machine File System) für FC-Schutz auf lokalem Storage gemountet sind. Zuvor wurde eine Technologievorschau bereitgestellt, die VMFS-Datastores für iSCSI unterstützt.

NetApp berechnet Ihnen keine Kosten für vorab angezeigte Workload-Kapazität.

Job wird abgebrochen

Mit diesem Release können Sie nun einen Job in der Job Monitor-Benutzeroberfläche abbrechen.

Siehe "Überwachen von Jobs".

17 Juli 2024

Zeitpläne für Failover-Tests

Diese Version enthält Updates der Zeitplanstruktur für Failover-Tests, die zur Unterstützung der täglichen und wöchentlichen Zeitpläne benötigt wurde. Für dieses Update müssen Sie alle vorhandenen Replikationspläne deaktivieren und wieder aktivieren, damit Sie die neuen täglichen und wöchentlichen Failover-Testpläne verwenden können. Dies ist eine einmalige Anforderung.

Und so funktioniert es:

1. Wählen Sie im oberen 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 ein paar Minuten **enable**.

Aktualisierungen des Replikationsplans

Diese Version enthält Aktualisierungen der Daten des Replikationsplans, wodurch das Problem „Snapshot nicht gefunden“ behoben wird. Dies erfordert, dass Sie die Aufbewahrungszahl in allen Replikationsplänen auf 1 ändern und einen On-Demand-Snapshot initiieren. Dieser Prozess erstellt ein neues Backup und entfernt alle älteren Backups.

Und so funktioniert es:

1. Wählen Sie im oberen Menü **Replikationspläne** aus.
2. Wählen Sie den Replikationsplan aus, klicken Sie auf die Registerkarte **Failover Mapping** und klicken Sie auf das Bleistiftsymbol **Bearbeiten**.
3. Klicken Sie auf den Pfeil **Datastores**, um ihn zu erweitern.
4. Notieren Sie sich den Wert der Aufbewahrungszahl im Replizierungsplan. Sie müssen diesen ursprünglichen Wert wieder aktivieren, wenn Sie mit diesen Schritten fertig sind.
5. Verringern Sie die Anzahl auf 1.
6. Initiieren Sie einen On-Demand-Snapshot. Wählen Sie dazu auf der Seite Replizierungsplan den Plan aus, klicken Sie auf das Aktionen-Symbol und wählen Sie **Snapshot jetzt 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 angegeben haben.
8. Wiederholen Sie diese Schritte für alle vorhandenen Replikationspläne.

5 Juli 2024

Diese BlueXP Disaster Recovery-Version umfasst die folgenden Updates:

Unterstützung der AFF A-Series

Dieser Release unterstützt die Hardware-Plattformen der NetApp AFF A-Series.

Unterstützung von lokalen bis lokalen VMware VMFS-Datastores

Diese Version enthält eine Technologievorschau von Unterstützung für VMs, die auf VMware vSphere VMFS-Datastores (Virtual Machine File System) gemountet sind und auf lokalem Storage geschützt sind. In dieser Version wird Disaster Recovery in einer Technologievorschau für lokale VMware-Workloads in lokale VMware-Umgebungen mit VMFS-Datastores unterstützt.

NetApp berechnet Ihnen keine Kosten für vorab angezeigte Workload-Kapazität.

Aktualisierungen des Replikationsplans

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

Bearbeiten Sie Replikationspläne

Mit dieser Version wurde die Seite Failover Mappings für eine bessere Übersichtlichkeit verbessert.

Siehe "Pläne verwalten".

Bearbeiten Sie VMs

Mit dieser Version beinhaltete der Prozess zum Bearbeiten von VMs im Plan einige kleinere Verbesserungen der Benutzeroberfläche.

Siehe "Managen von VMs".

Failover-Updates

Bevor Sie einen Failover initiieren, können Sie nun den Status der VMs ermitteln und bestimmen, ob sie ein- oder ausgeschaltet sind. Mit dem Failover-Prozess können Sie jetzt einen Snapshot erstellen oder die Snapshots auswählen.

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

Zeitpläne für Failover-Tests

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

Siehe "Pläne verwalten".

Aktualisierung der erforderlichen Informationen

Informationen zu den BlueXP Disaster Recovery-Voraussetzungen wurden aktualisiert.

Siehe "Voraussetzungen für die Disaster Recovery von BlueXP".

15 Mai 2024

Diese BlueXP Disaster Recovery-Version umfasst die folgenden Updates:

Replizierung von VMware-Workloads vor Ort

Diese Funktion wird jetzt als allgemeine Verfügbarkeitsfunktion veröffentlicht. Zuvor war es eine Technologievorschau mit eingeschränkter Funktionalität.

Lizenzierungs-Updates

Mit BlueXP Disaster Recovery können Sie sich für eine kostenlose 90-Tage-Testversion anmelden, ein PAYGO-Abonnement (Pay-as-you-go) für Amazon Marketplace erwerben oder NetApp die BYOL-Lizenz (Bring-Your-Own-License) verwenden, die Sie von Ihrem NetApp Vertriebsmitarbeiter oder der NetApp Support-Website (NSS) erhalten.

Weitere Informationen zur Einrichtung einer Lizenzierung für die Disaster Recovery von BlueXP finden Sie unter "Lizenzierung einrichten".

"Erfahren Sie mehr über die Disaster Recovery von BlueXP".

5 März 2024

Dies ist die Disaster Recovery-Version von BlueXP für die allgemeine Verfügbarkeit. Sie umfasst folgende Updates.

Lizenzierungs-Updates

Mit BlueXP Disaster Recovery können Sie sich für eine kostenlose 90-Tage-Testversion anmelden oder Ihre eigene Lizenz (BYOL, Bring Your Own License) verwenden. Hierbei handelt es sich um eine NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um das BYOL in der Digital Wallet von BlueXP zu aktivieren. Die Disaster-Recovery-Gebühren für BlueXP basieren auf der bereitgestellten Kapazität von Datastores.

Weitere Informationen zur Einrichtung einer Lizenzierung für die Disaster Recovery von BlueXP finden Sie unter "Lizenzierung einrichten".

Weitere Informationen zum Verwalten von Lizenzen für **alle** BlueXP Services finden Sie unter "Managen Sie Lizenzen für alle BlueXP Services".

Schichtpläne bearbeiten

Mit dieser Version können Sie jetzt Zeitpläne zum Testen von Compliance- und Failover-Tests einrichten, um sicherzustellen, dass diese bei Bedarf korrekt funktionieren.

Weitere Informationen finden Sie unter "Erstellen Sie den Replizierungsplan".

Februar 2024

Diese BlueXP Disaster-Recovery-Vorschau enthält die folgenden Updates:

Netzwerkoptimierung

Mit diesem Release können Sie nun die Größe der VM-CPU- und RAM-Werte ändern. Sie können nun auch ein Netzwerk-DHCP oder eine statische IP-Adresse für die VM auswählen.

- DHCP: Wenn Sie diese Option wählen, geben Sie Anmeldeinformationen für die VM an.
- Statische IP: Sie können die gleichen oder andere Informationen aus der Quell-VM auswählen. Wenn Sie dieselbe Auswahl wie die Quelle wählen, müssen Sie keine Anmeldeinformationen eingeben. Wenn Sie jedoch andere Informationen aus der Quelle verwenden möchten, können Sie Anmeldeinformationen, IP-Adresse, Subnetzmaske, DNS und Gateway-Informationen angeben.

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Benutzerdefinierte Skripts

Kann nun auch als Post Failover-Prozesse genutzt werden. Mit benutzerdefinierten Skripts kann die BlueXP Disaster Recovery Ihr Skript nach einem Failover-Prozess ausführen. Sie können beispielsweise ein benutzerdefiniertes Skript verwenden, um alle Datenbanktransaktionen nach Abschluss des Failovers wieder aufzunehmen.

Weitere Informationen finden Sie unter "Failover an einen Remote-Standort".

SnapMirror Beziehung

Sie können jetzt eine SnapMirror-Beziehung erstellen und gleichzeitig den Replizierungsplan entwickeln. Früher mussten Sie diese Beziehung außerhalb der Disaster Recovery von BlueXP aufbauen.

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Konsistenzgruppen

Bei der Erstellung eines Replizierungsplans können Sie VMs mit unterschiedlichen Volumes und unterschiedlichen SVMs einbeziehen. Die Disaster Recovery von BlueXP erstellt einen KonsistenzgruppenSnapshot, der alle Volumes enthält und alle sekundären Standorte aktualisiert.

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

VM-Verzögerungsoption beim Einschalten

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

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

Applikationskonsistente Snapshot Kopien

Sie können angeben, applikationskonsistente Snapshot Kopien zu erstellen. Der Service setzt die Applikation still und erstellt dann einen Snapshot, um einen konsistenten Status der Applikation zu erhalten.

Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

11 Januar 2024

Diese Vorschauversion des Disaster Recovery von BlueXP enthält die folgenden Updates:

Schnelleres Dashboard

Mit dieser Version können Sie schneller auf Informationen auf anderen Seiten über das Dashboard zugreifen.

"Erfahren Sie mehr über BlueXP Disaster Recovery".

20 Oktober 2023

Diese Vorschauversion des Disaster Recovery von BlueXP enthält die folgenden Updates.

Sichern Sie lokale NFS-basierte VMware Workloads

Mit der Disaster Recovery von BlueXP können Sie Ihre lokalen, NFS-basierten VMware-Workloads vor Ausfällen in eine andere lokale, NFS-basierte VMware Umgebung, zusätzlich zur Public Cloud, schützen. Mit BlueXP Disaster Recovery werden die Disaster-Recovery-Pläne orchestriert.

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

"Erfahren Sie mehr über die Disaster Recovery von BlueXP".

27 September 2023

Diese Vorschauversion des Disaster Recovery von BlueXP enthält die folgenden Updates:

Dashboard-Updates

Sie können nun auf die Optionen im Dashboard klicken, um die Informationen schneller zu prüfen. Darüber hinaus wird im Dashboard jetzt der Status von Failover und Migrationen angezeigt.

Siehe "Zeigen Sie den Zustand Ihrer Disaster-Recovery-Pläne auf dem Dashboard an".

Aktualisierungen des Replikationsplans

- **RPO**: Sie können jetzt im Abschnitt Datastores des Replikationsplans den Wiederherstellungspunkt Objective (RPO) und Retention Count eingeben. Zeigt die Datenmenge an, die nicht älter als die eingestellte Zeit sein muss. Wenn Sie beispielsweise die Einstellung auf 5 Minuten festlegen, kann das System bei einem Zwischenfall bis zu 5 Minuten an Daten verlieren, ohne dass dies geschäftskritische Anforderungen beeinträchtigt.

  Siehe "Erstellen Sie einen Replizierungsplan".

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

  Siehe "Erstellen Sie einen Replizierungsplan".

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

  Siehe "Ressourcen managen".

- **SnapMirror-Automatisierung**: Während Sie den Replizierungsplan in diesem Release erstellen, können Sie die SnapMirror Beziehung zwischen Quell- und Ziel-Volumes in einer der folgenden Konfigurationen definieren:
  - 1 zu 1
  - 1 zu vielen in einer Fanout-Architektur
  - Von vielen zu 1 als Konsistenzgruppe
  - Von vielen auf viele

  Siehe "Erstellen Sie einen Replizierungsplan".

August 2023

BlueXP Disaster Recovery-Vorschau

Die Disaster-Recovery-Vorschau von BlueXP ist ein Cloud-basierter Disaster-Recovery-Service, der Disaster-Recovery-Workflows automatisiert. Mit der BlueXP Disaster-Recovery-Vorschau können Sie zunächst Ihre lokalen NFS-basierten VMware-Workloads schützen, die NetApp Storage in VMware Cloud (VMC) auf AWS mit Amazon FSX for ONTAP ausführen.

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

"Erfahren Sie mehr über die Disaster Recovery von BlueXP".

Diese Version enthält die folgenden Updates:

Ressourcengruppen werden für die Startreihenfolge aktualisiert

Wenn Sie einen Disaster Recovery- oder Replizierungsplan erstellen, können Sie virtuelle Maschinen zu funktionalen Ressourcengruppen hinzufügen. Mit Ressourcengruppen können Sie eine Reihe abhängiger virtueller Maschinen in logische Gruppen umwandeln, die Ihren Anforderungen entsprechen. Gruppen können beispielsweise die Startreihenfolge enthalten, die bei der Wiederherstellung ausgeführt werden kann. Mit diesem Release kann jede Ressourcengruppe eine oder mehrere virtuelle Maschinen enthalten. Die Virtual Machines werden basierend auf der Reihenfolge, in der Sie sie in den Plan aufnehmen, eingeschaltet. Siehe "Wählen Sie Anwendungen aus, die Sie replizieren und Ressourcengruppen zuweisen möchten".

Replizierungsüberprüfung

Nachdem Sie den Disaster Recovery- oder Replizierungsplan erstellt haben, identifizieren Sie die Wiederholung im Assistenten und initiieren Sie eine Replikation an einem Disaster Recovery-Standort. Alle 30 Minuten überprüft die BlueXP Disaster Recovery, ob die Replikation tatsächlich gemäß dem Plan erfolgt. Sie können den Fortschritt auf der Seite Job Monitor überwachen. Siehe "Replizierung von Applikationen an einen anderen Standort".

Der Replizierungsplan zeigt die Zeitpläne für die Übertragung der Recovery Point Objective (RPO) an

Wenn Sie einen Disaster Recovery- oder Replizierungsplan erstellen, wählen Sie die VMs aus. In diesem

Release können Sie jetzt die SnapMirror anzeigen, die mit jedem der Volumes verknüpft sind, die dem Datenspeicher oder der VM zugeordnet sind. Sie können auch die mit dem SnapMirror Zeitplan verknüpften RPO-Übertragungszeitpläne anzeigen. Anhand des RPO können Sie feststellen, ob Ihr Backup-Zeitplan für die Wiederherstellung nach einem Ausfall ausreicht. Siehe "Erstellen Sie einen Replizierungsplan".

Jobüberwachung aktualisieren

Die Seite Job Monitor enthält jetzt eine Option Aktualisieren, damit Sie den aktuellen Status der Vorgänge abrufen können. Siehe "Überwachen Sie Disaster-Recovery-Jobs".

18 Mai 2023

Dies ist die erste Version der Disaster Recovery von BlueXP.

Cloud-basierter Disaster Recovery-Service

BlueXP Disaster Recovery ist ein Cloud-basierter Disaster Recovery Service, der Disaster Recovery Workflows automatisiert. Mit der BlueXP Disaster-Recovery-Vorschau können Sie zunächst Ihre lokalen NFS-basierten VMware-Workloads schützen, die NetApp Storage in VMware Cloud (VMC) auf AWS mit Amazon FSX for ONTAP ausführen.

"Erfahren Sie mehr über die Disaster Recovery von BlueXP".

Einschränkungen bei der Notfallwiederherstellung mit BlueXP

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

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

Wenn ein Failover abgeschlossen ist, starten Sie die Erkennung nicht manuell auf dem Quell-vCenter. Warten Sie, bis das Failback abgeschlossen ist, und starten Sie dann die Erkennung im Quell-vCenter.

BlueXP entdeckt möglicherweise Amazon FSX for NetApp ONTAP nicht

Manchmal erkennt BlueXP Amazon FSX for NetApp ONTAP-Cluster nicht. Dies könnte daran liegen, dass die FSX-Anmeldeinformationen nicht korrekt waren.

Workaround: Fügen Sie den Amazon FSX for NetApp ONTAP Cluster in BlueXP hinzu und aktualisieren Sie regelmäßig den Cluster, um Änderungen anzuzeigen.

Wenn Sie den ONTAP FSX-Cluster aus dem BlueXP Disaster-Recovery-Service entfernen müssen, führen Sie die folgenden Schritte aus:

1. Verwenden Sie im BlueXP Connector die Konnektivitätsoptionen Ihres Cloud-Providers, stellen Sie eine Verbindung zu der Linux VM her, auf der der Connector ausgeführt wird, und starten Sie den „occm“-Service mithilfe des neu `docker restart occm` Befehl.

   Siehe "Verwalten Sie vorhandene Anschlüsse".

2. Fügen Sie im BlueXP-Bildschirm erneut die Umgebung von Amazon FSX for ONTAP hinzu und geben Sie die FSX-Berechtigungen an.

   Siehe "Erstellen Sie ein Dateisystem von Amazon FSX für NetApp ONTAP".

3. Wählen Sie in BlueXP Disaster Recovery **sites** aus, wählen Sie in der vCenter-Zeile die Option **actions** aus  , Und wählen Sie im Menü Aktionen **Aktualisieren** aus, um die FSX-Erkennung in BlueXP Disaster Recovery zu aktualisieren.

   Dadurch werden der Datastore, seine Virtual Machines und seine Zielbeziehung neu erkannt.

Los geht’s

Erfahren Sie mehr über BlueXP Disaster Recovery für VMware

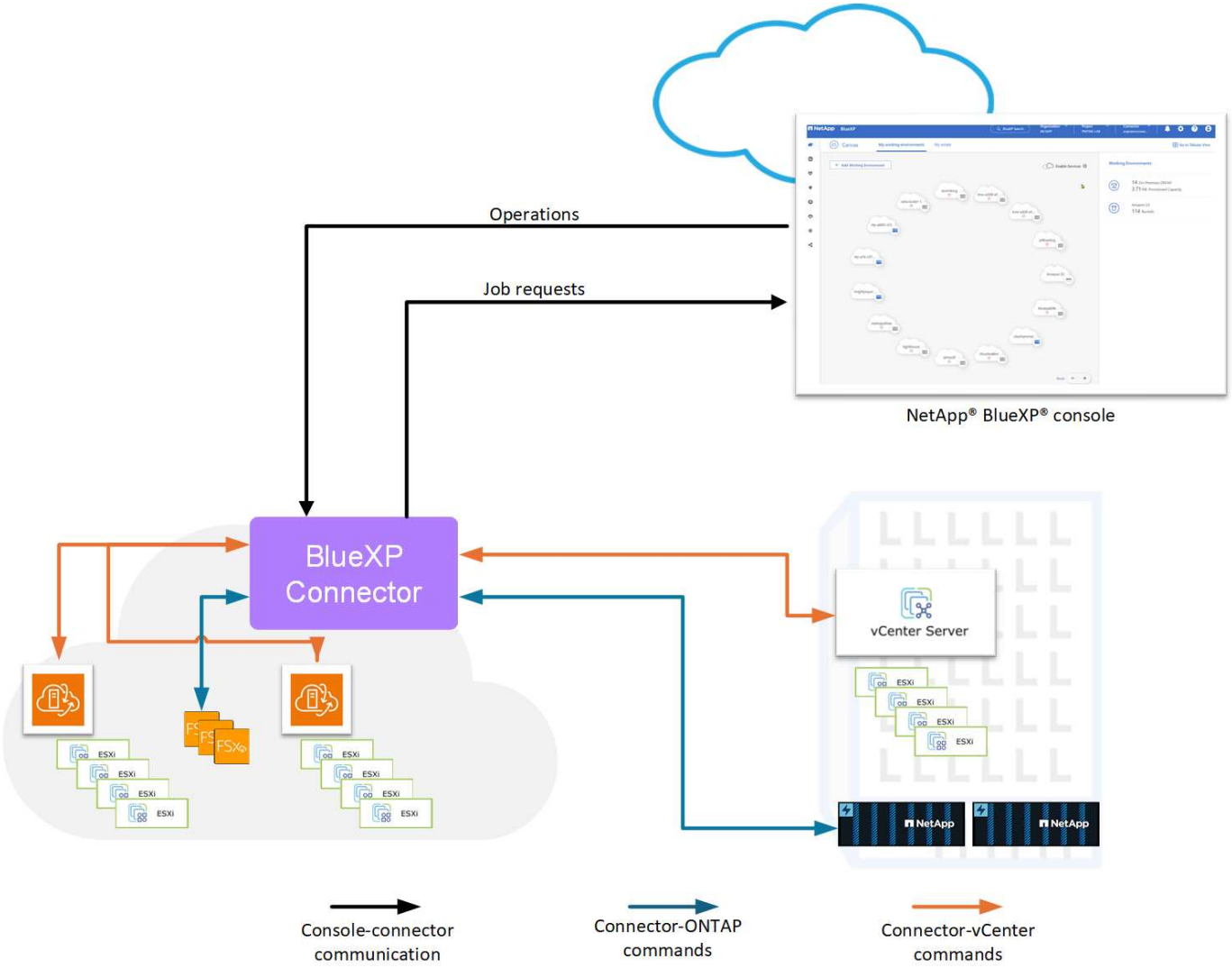
Disaster Recovery in der Cloud ist eine ausfallsichere und kostengünstige Möglichkeit zum Schutz von Workloads vor Standortausfällen und Datenbeschädigung. Mit BlueXP Disaster Recovery für VMware können Sie Ihre lokalen VMware-VMs oder Datastore-Workloads, auf denen ONTAP Storage ausgeführt wird, in ein softwaredefiniertes VMware Datacenter in einer Public Cloud mit NetApp Cloud-Storage oder in eine andere lokale VMware-Umgebung mit ONTAP Storage als Disaster-Recovery-Standort replizieren.

BlueXP Disaster Recovery ist ein Cloud-basierter Disaster Recovery Service, der Disaster Recovery Workflows automatisiert. Mit dem Disaster Recovery-Service BlueXP können Sie Ihre lokalen, NFS-basierten Workloads und VMware vSphere Datastores des Virtual Machine File System (VMFS) für iSCSI und FC mit NetApp Storage in einer der folgenden Systeme schützen:

- VMware Cloud (VMC) auf AWS mit Amazon FSX für NetApp ONTAP oder
- Eine weitere lokale NFS-basierte VMware Umgebung mit ONTAP Storage

> DIESE DOKUMENTATION ZU AWS EVS WIRD ALS TECHNOLOGIEVORSCHAU BEREITGESTELLT. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitpläne vor der allgemeinen Verfügbarkeit zu ändern. Weitere Informationen finden Sie unter "Einführung der BlueXP-Notfallwiederherstellung mit Amazon Elastic VMware Service und Amazon FSx für NetApp ONTAP".

Bei der Disaster Recovery von BlueXP kommt die ONTAP SnapMirror Technologie als Replizierungstransport zum Disaster-Recovery-Standort zum Einsatz. Dies ermöglicht eine branchenführende Storage-Effizienz (Komprimierung und Deduplizierung) an primären und sekundären Standorten.



Vorteile des Einsatzes von BlueXP Disaster Recovery für VMware

Die Disaster Recovery von BlueXP bietet folgende Vorteile:

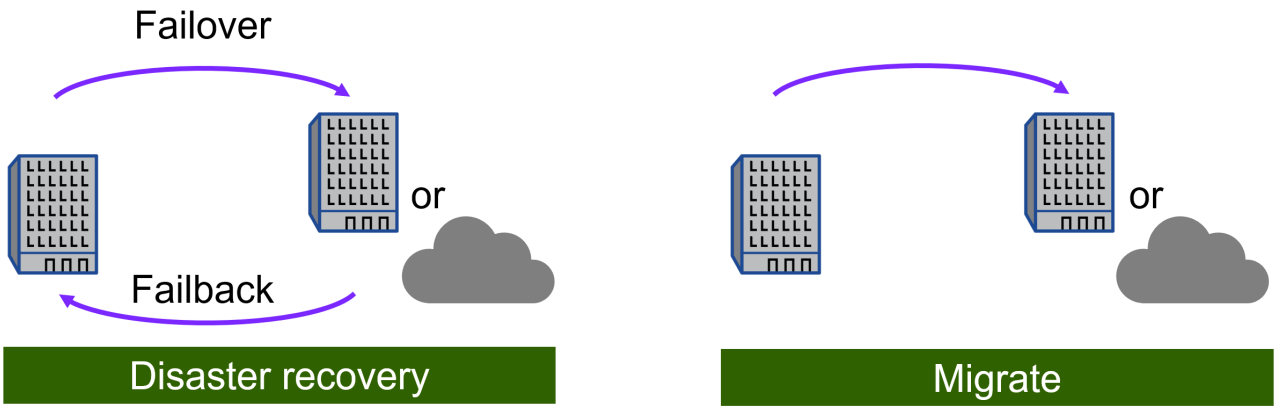
- Vereinfachte Benutzererfahrung bei der Erkennung und Wiederherstellung von Applikationen durch vCenter mit mehreren Point-in-Time-Recovery-Vorgängen
- Senken Sie Ihre TCO, dank niedrigerer Betriebskosten und der Möglichkeit, Disaster-Recovery-Pläne mit minimalen Ressourcen zu erstellen und anzupassen
- Kontinuierliche Disaster Recovery-Bereitschaft mit virtuellen Failover-Tests, die den Betrieb nicht unterbrechen
- Schnellere Amortisierung aufgrund dynamischer Änderungen in der IT-Umgebung und der Möglichkeit zur Umsetzung Ihrer Disaster Recovery-Pläne

Was Sie mit BlueXP Disaster Recovery für VMware erreichen können

Mit BlueXP Disaster Recovery profitieren Sie von der vollständigen Nutzung verschiedener NetApp Technologien, um folgende Ziele zu erreichen:

- Replizieren Sie VMware Applikationen an Ihrem lokalen Produktionsstandort an einen Disaster-Recovery-Remote-Standort in der Cloud oder vor Ort. Nutzen Sie dazu SnapMirror Replizierung.

- Migrieren Sie VMware-Workloads von Ihrem ursprünglichen Standort zu einem anderen Standort.
- Führen Sie einen Failover-Test durch, während virtuelle Maschinen vorübergehend erstellt werden. Die Disaster Recovery von BlueXP erstellt aus dem ausgewählten Snapshot ein neues FlexClone-Volume, und ein temporärer Datenspeicher für das FlexClone-Volume wird den ESXi Hosts zugeordnet. Dieser Prozess beansprucht keine zusätzliche physische Kapazität, lokal im ONTAP Storage oder auf FSX for NetApp ONTAP Storage in AWS. Das ursprüngliche Quell-Volume wird nicht geändert, und Replikatjobs können auch während der Disaster Recovery fortgesetzt werden.
- Bei einem Notfall führen Sie ein Failover Ihres primären Standorts nach Bedarf zum Disaster-Recovery-Standort durch. Dabei kann es sich um VMware Cloud on AWS mit Amazon FSX for NetApp ONTAP oder eine lokale VMware-Umgebung mit ONTAP handeln.
- Nach der Behebung des Ausfalls können Sie nach Bedarf ein Failback vom Disaster-Recovery-Standort zum primären Standort durchführen. *Gruppieren Sie VMs oder Datastores in logische Ressourcengruppen für eine effiziente Verwaltung.



Die Konfiguration des vSphere Servers erfolgt außerhalb von BlueXP Disaster Recovery in vSphere Server.

Kosten

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

Der Disaster Recovery-Service von BlueXP lässt sich entweder mit einer NetApp Lizenz oder mit einem Jahresabonnement-basierten Plan über Amazon Web Services nutzen.

Einige Versionen enthalten eine Technologievorschau. NetApp berechnet Ihnen keine Kosten für vorab angezeigte Workload-Kapazität. Weitere Informationen zu den Vorschauen der neuesten Technologie finden Sie unter "Was ist neu an BlueXP Disaster Recovery" .

Lizenzierung

Sie können die folgenden Lizenztypen verwenden:

- Melden Sie sich für eine kostenlose 30-Tage-Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) für * NetApp Intelligent Services* über den

Amazon Web Services (AWS) Marketplace und den Microsoft Azure Marketplace.

- Bring-Your-Own-License (BYOL) bei einer NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um das BYOL in der Digital Wallet von BlueXP zu aktivieren.

Das Management der Lizenzen für alle BlueXP Services erfolgt über den BlueXP Digital Wallet Service. Nachdem Sie Ihr BYOL eingerichtet haben, können Sie eine aktive Lizenz für den Service in der Digital Wallet von BlueXP sehen.

> Die Disaster Recovery-Gebühren von BlueXP basieren auf der genutzten Kapazität von Datastores am Quellstandort, wenn mindestens eine VM mit einem Replizierungsplan vorhanden ist. Die Kapazität für einen Failover-Datenspeicher ist in der zulässigen Kapazität nicht enthalten. Wenn die Daten bei einem BYOL die zulässige Kapazität überschreiten, werden die Vorgänge im Service so lange eingeschränkt, bis Sie eine zusätzliche Kapazitätslizenz erhalten oder die Lizenz in der Digital Wallet von BlueXP aktualisieren.

Weitere Informationen zur Einrichtung einer Lizenzierung für die Disaster Recovery von BlueXP finden Sie unter "Disaster-Recovery-Lizenzen für BlueXP einrichten".

30 Tage kostenlos testen

Sie können die Disaster Recovery von BlueXP mit einer kostenlosen Testversion von 30 Tagen testen.

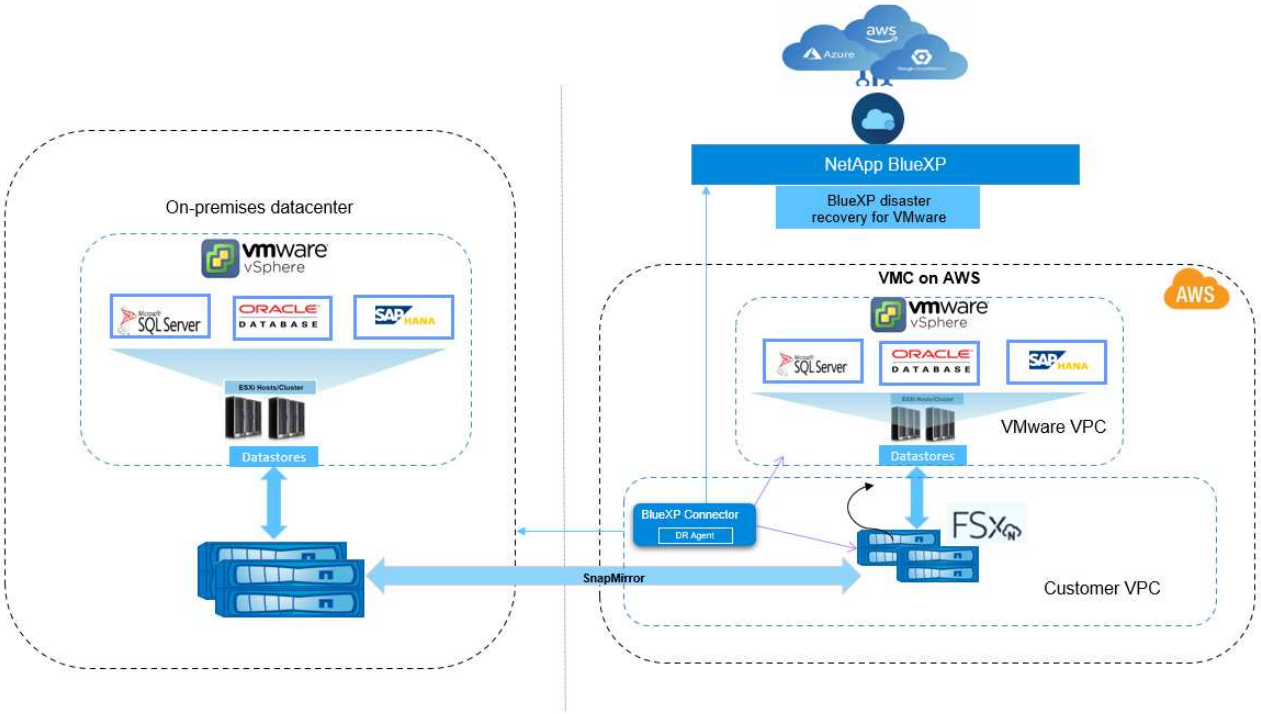
Um nach der 30-Tage-Testsoftware fortzufahren, benötigen Sie ein PAYGO-Abonnement (Pay-as-you-go) von Ihrem Cloud-Provider oder eine BYOL-Lizenz von NetApp.

Sie können jederzeit eine Lizenz erwerben und Sie werden erst nach Ablauf der 30-tägigen Testversion belastet.

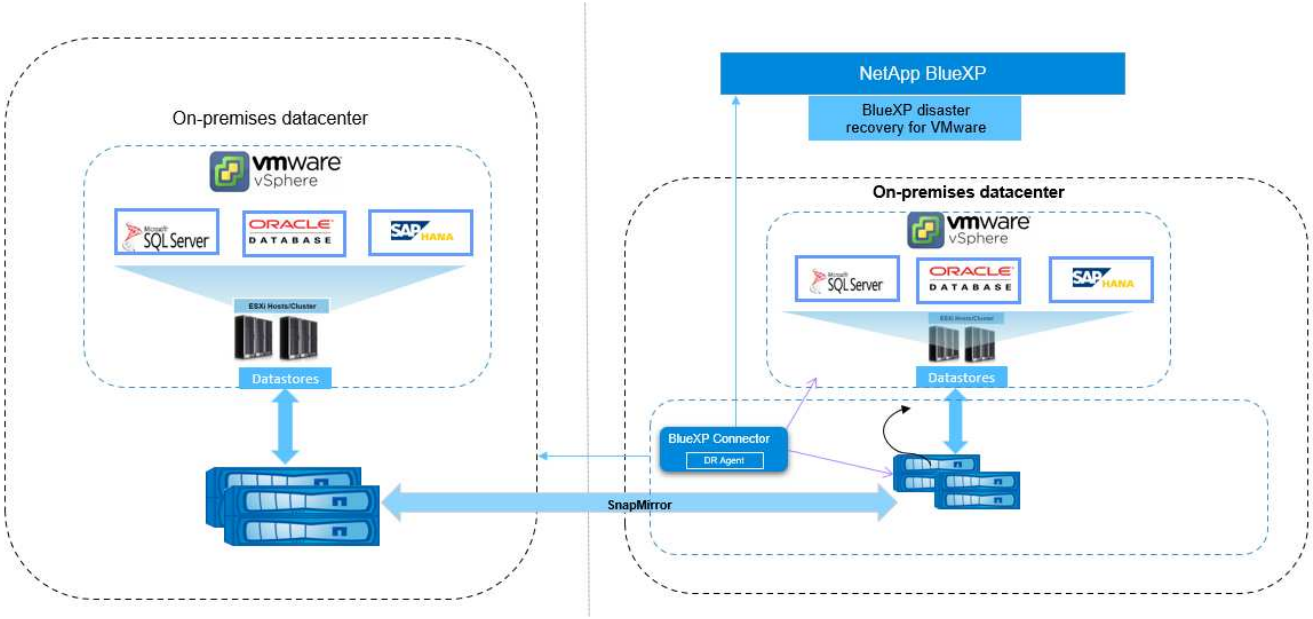
Funktionsweise der BlueXP Disaster Recovery

Mit BlueXP Disaster Recovery können Sie Workloads wiederherstellen, die von einem On-Premises-Standort zu Amazon FSX for ONTAP oder zu einem anderen On-Premises-Standort repliziert werden. Dieser Service automatisiert die Recovery von der SnapMirror Ebene durch die Registrierung der Virtual Machines in der Virtual Machine Cloud (VMC) und bis zu Netzwerkzuordnungen direkt auf der VMware Netzwerkvirtualisierungs- und Sicherheitsplattform NSX-T. Diese Funktion ist in allen Virtual Machine Cloud-Umgebungen enthalten.

Bei der Disaster Recovery in BlueXP kommt die ONTAP SnapMirror Technologie zum Einsatz, die für eine hocheffiziente Replizierung sorgt und die ONTAP fortlaufend inkrementelle Snapshot-Effizienz erhält. Die SnapMirror Replizierung stellt sicher, dass applikationskonsistente Snapshot Kopien immer synchron sind und die Daten sofort nach einem Failover nutzbar sind.



Das folgende Diagramm zeigt die Architektur von lokalen zu lokalen Disaster-Recovery-Plänen.



Bei einem Notfall unterstützt dieser Service Sie bei der Wiederherstellung von Virtual Machines in der anderen lokalen VMware Umgebung oder VMC, indem die SnapMirror Beziehungen aufgehoben und der Zielstandort aktiviert wird.

- Mit dem Service können Sie außerdem ein Failback der virtuellen Maschinen zum ursprünglichen Quellspeicherort durchführen.
- Sie können den Disaster Recovery Failover-Prozess testen, ohne die ursprünglichen Virtual Machines zu unterbrechen. Bei diesem Test werden Virtual Machines in einem isolierten Netzwerk durch die Erstellung eines FlexClone des Volume wiederhergestellt.
- Für den Failover- oder Test-Failover-Prozess können Sie den neuesten (Standard-) oder ausgewählten

Snapshot auswählen, von dem Sie Ihre virtuelle Maschine wiederherstellen möchten.

Bedingungen, die Ihnen bei der BlueXP Disaster Recovery helfen könnten

Möglicherweise profitieren Sie von der Kenntnis einiger Begriffe im Zusammenhang mit Disaster Recovery.

- **Standort**: Ein logischer Container, der normalerweise mit einem physischen Rechenzentrum oder Cloud-Provider verknüpft ist.
- **Ressourcengruppe**: Ein logischer Container, mit dem Sie mehrere VMs als eine Einheit verwalten können.
- **Replizierungsplan**: Eine Reihe von Regeln, wie häufig Backups durchgeführt werden und wie Failover-Ereignisse gehandhabt werden. Pläne werden einer oder mehreren Ressourcengruppen zugewiesen.

Voraussetzungen für die Disaster Recovery von BlueXP

Bevor Sie BlueXP Disaster Recovery nutzen, sollten Sie sicherstellen, dass Ihre Umgebung die Anforderungen von ONTAP Storage, VMware vCenter Cluster und BlueXP erfüllt.

Voraussetzungen für ONTAP Storage

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

- Quell- und Ziel-Cluster müssen über eine Peer-Beziehung verfügen.
- Die SVM, auf der die Disaster-Recovery-Volumes gehostet werden, muss sich auf dem Ziel-Cluster befinden.
- Die Quell-SVM und Ziel-SVM müssen über eine Peer-Beziehung verfügen.

> Disaster-Recovery-Volumes in der Ziel-SVM oder -SVMs sollten nicht vorab erstellt werden. Bei BlueXP Disaster Recovery werden die Ziel-Volumes je nach Bedarf für den Replizierungsplan erstellt.

- Wenn die Bereitstellung mit Amazon FSX for NetApp ONTAP erfolgt, gilt die folgende Voraussetzung:
  - In der VPC muss eine Instanz von Amazon FSX for NetApp ONTAP zum Hosten von VMware DR-Datastores vorhanden sein. Siehe Amazon FSX für ONTAP-Dokumentation auf "Erste Schritte".

Voraussetzungen für VMware vCenter-Cluster

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

- Alle VMware Cluster, die Sie für die Disaster Recovery von BlueXP benötigen, müssen auf ONTAP Volumes gehostet werden.
- Für alle VMware Datastores, die von BlueXP Disaster Recovery gemanagt werden sollen, muss eines der folgenden Protokolle verwendet werden:
  - NFS
  - VMFS mithilfe des iSCSI- oder FC-Protokolls
- VMware vSphere Version 7.0 Update 3 (7.0v3) oder höher

- Wenn Sie VMware Cloud SDDC nutzen, gelten diese Voraussetzungen.
  - Verwenden Sie in der VMware Cloud Console die Dienstrollen Administrator und NSX Cloud Administrator. Verwenden Sie auch den Organisationseigentümer für die Rolle Organisation. Siehe "Using VMware Cloud Foundations with AWS FSX for NetApp ONTAP – Dokumentation".
  - Verknüpfen Sie das VMware Cloud SDDC mit der Amazon FSX for NetApp ONTAP Instanz. Siehe "VMware Cloud on AWS lässt sich in Amazon FSX for NetApp ONTAP Implementierungsinformationen integrieren".

Voraussetzungen für BlueXP

Erste Schritte mit BlueXP

Wenn Sie dies noch nicht getan haben, "melden sie sich bei BlueXP an und erstellen Sie eine Organisation"

Sammeln Sie Anmeldeinformationen für ONTAP und VMware

- Im Rahmen des BlueXP -Projekts müssen die Zugangsdaten für Amazon FSX for ONTAP und AWS zur Arbeitsumgebung hinzugefügt werden, die für das Management der BlueXP Disaster Recovery genutzt werden.
- Für die Disaster Recovery von BlueXP sind vCenter Zugangsdaten erforderlich. Beim Hinzufügen eines Standorts in BlueXP Disaster Recovery geben Sie die vCenter Zugangsdaten ein.

  Eine Liste der erforderlichen vCenter-Berechtigungen finden Sie unter "Für die Disaster Recovery von BlueXP sind vCenter Berechtigungen erforderlich". Anweisungen zum Hinzufügen einer Site finden Sie unter "Fügen Sie eine Site hinzu".

BlueXP Connector erstellen

Es muss ein BlueXP Connector eingerichtet werden. Wenn Sie BlueXP Connector verwenden, wird dies die entsprechenden Funktionen für den Disaster Recovery Service umfassen.

- Die Disaster Recovery von BlueXP ist nur mit der Connector-Standardimplementierung möglich. Siehe "Erste Schritte mit BlueXP im Standardmodus".
- Stellen Sie sicher, dass sowohl das Quell- als auch das Ziel-vCenter denselben BlueXP Connector verwenden.
- Erforderlicher BlueXP Connector:
  - **On-Premises zu On-Premises Disaster Recovery**: Installieren Sie den lokalen BlueXP Connector am Disaster Recovery-Standort. Siehe "Installieren und Einrichten eines Connectors auf dem Gelände".
  - **On-Premises zu AWS**: Installieren Sie den BlueXP Connector für AWS in Ihrer AWS VPC. Siehe "Installationsoptionen für Konnektoren in AWS".

    On-Premises bis On-Premises: Nutzen Sie den BlueXP On-Premises Connector. Nutzen Sie lokal die AWS Connector-Lösung BlueXP, die Zugriff auf das lokale vCenter Quell- und das lokale vCenter Ziel bietet.

  - Der installierte BlueXP Connector muss auf alle VMware Cluster zugreifen können, die von der BlueXP Disaster Recovery gemanagt werden.
- Alle ONTAP Arrays, die von BlueXP Disaster Recovery gemanagt werden sollen, müssen zu jeder Arbeitsumgebung im BlueXP -Projekt hinzugefügt werden, die für das Management der BlueXP Disaster

Recovery verwendet wird.

Siehe "Erkennen von ONTAP Clustern vor Ort".

- Informationen zur Einrichtung eines intelligenten Proxys für die Disaster Recovery von BlueXP finden Sie unter "Richten Sie Ihre Infrastruktur für die Disaster Recovery von BlueXP ein".

Workload-Voraussetzungen

Um sicherzustellen, dass die Prozesse der Anwendungskonsistenz erfolgreich sind, wenden Sie die folgenden Voraussetzungen an:

- 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 ausgeführt wird, sollten die VSS-Writer für die Datenbanken aktiviert sein.
- Bei Oracle-Datenbanken, die auf einem Linux-Betriebssystem ausgeführt werden, sollte die Benutzerauthentifizierung des Betriebssystems für die Rolle „Oracle Database SYSDBA“ aktiviert sein.

Schnellstart für die Disaster Recovery von BlueXP

Hier erhalten Sie einen Überblick über die Schritte, die Sie für Ihren Einstieg in die Disaster Recovery von BlueXP benötigen. Die Links in den einzelnen Schritten führen zu einer Seite, die weitere Details enthält.

Voraussetzungen prüfen

"Stellen Sie sicher, dass Ihre Umgebung diese Anforderungen erfüllt".

Disaster-Recovery-Service von BlueXP einrichten

- "Richten Sie die Infrastruktur für den Service ein".
- "Lizenzierung einrichten".

Was kommt als Nächstes?

Nachdem Sie den Service eingerichtet haben, gehen Sie wie folgt vor.

- "Fügen Sie Ihre vCenter Sites zur Disaster Recovery von BlueXP hinzu".
- "Erstellen Sie Ihre erste Ressourcengruppe".
- "Erstellen Sie Ihren ersten Replizierungsplan".
- "Replizierung von Applikationen an einen anderen Standort".
- "Failover von Anwendungen an einen Remote-Standort".
- "Führen Sie ein Failback von Anwendungen zum ursprünglichen Quellstandort durch".
- "Verwalten von Standorten, Ressourcengruppen und Replikationsplänen".
- "Überwachen Sie Disaster-Recovery-Vorgänge".

Richten Sie Ihre Infrastruktur für die Disaster Recovery von BlueXP ein

Um das Disaster Recovery von BlueXP zu nutzen, müssen Sie es in wenigen Schritten sowohl in Amazon Web Services (AWS) als auch in BlueXP einrichten.

Prüfen "Voraussetzungen" Und stellen Sie sicher, dass Ihre Umgebung bereit ist.

Machen Sie sich bereit für die BlueXP Disaster Recovery zur Sicherung vor Ort

Vergewissern Sie sich, dass die folgenden Anforderungen erfüllt sind, bevor Sie BlueXP Disaster Recovery für On-Premises-zu-On-Premises-Sicherung einrichten:

- ONTAP-Lagerung
  - Stellen Sie sicher, dass Sie über ONTAP-Anmeldeinformationen verfügen.
  - Disaster-Recovery-Standort erstellen oder überprüfen
  - Ziel-ONTAP SVM erstellen oder überprüfen.
  - Stellen Sie sicher, dass die ONTAP SVMs Ihrer Quell- und Ziel-SVMs geeignet sind.
- VCenter-Cluster
  - Stellen Sie sicher, dass die VMs, die Sie sichern möchten, auf NFS-Datenspeichern (mit ONTAP NFS Volumes) oder VMFS-Datenspeichern (mit NetApp iSCSI LUNs) gehostet werden.
  - Prüfung "VCenter Privileges"für BlueXP DR erforderlich.
  - Erstellen Sie ein Disaster Recovery-Benutzerkonto (nicht das standardmäßige vCenter-Administratorkonto) und weisen Sie dem Konto die vCenter Privileges zu.

Intelligente Proxy-Unterstützung

Der BlueXP -Connector unterstützt den intelligenten Proxy. Ein intelligenter Proxy ist eine einfache, sichere und effiziente Möglichkeit, Ihre On-Premises-Umgebung mit dem BlueXP -Service zu verbinden. Sie stellt eine sichere Verbindung zwischen Ihrer Umgebung und dem BlueXP -Dienst her, ohne dass ein VPN oder ein direkter Internetzugang erforderlich ist. Diese optimierte Proxy-Implementierung entlastet den API-Verkehr innerhalb des lokalen Netzwerks.

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

Für die Implementierung eines BlueXP Disaster Recovery Proxy ist eine Port 443-Kommunikation zwischen dem Connector und allen vCenter-Servern und ONTAP-Arrays über ein HTTPS-Protokoll erforderlich. Der BlueXP Disaster Recovery-Agent im Connector kommuniziert direkt mit VMware vSphere, VC oder ONTAP, wenn Aktionen durchgeführt werden.

Weitere Informationen über die Einrichtung eines allgemeinen Proxys in BlueXP finden Sie unter "Konfigurieren Sie einen Konnektor für die Verwendung eines Proxy-Servers".

Machen Sie sich bereit für die BlueXP Disaster Recovery für den Schutz vor Ort in der Cloud mit AWS

Um BlueXP Disaster Recovery für den On-Premises- zu-Cloud-Schutz mit AWS einzurichten, müssen Sie

Folgendes einrichten:

- AWS FSX für NetApp ONTAP einrichten
- Richten Sie VMware Cloud on AWS SDDC ein

AWS FSX für NetApp ONTAP einrichten

- Erstellen Sie ein Dateisystem von Amazon FSX für NetApp ONTAP.
  - Bereitstellung und Konfiguration von FSX für ONTAP Amazon FSX for NetApp ONTAP ist ein vollständig gemanagter Service, der auf dem NetApp ONTAP Filesystem als Basis äußerst zuverlässigen, skalierbaren, hochperformanten und funktionsreichen File-Storage bietet.
  - Befolgen Sie die Schritte in "Technischer Bericht 4938: Amazon FSX ONTAP als NFS-Datastore mit VMware Cloud on AWS mounten" und "Schnellstart für Amazon FSX for NetApp ONTAP", um FSX für ONTAP bereitzustellen und zu konfigurieren.
- Fügen Sie Amazon FSX for ONTAP in die Arbeitsumgebung ein und fügen Sie AWS-Zugangsdaten für FSX for ONTAP hinzu.
- ONTAP-ZielSVM in AWS FSX for ONTAP-Instanz erstellen oder überprüfen.
- Konfigurieren Sie die Replizierung zwischen Ihrem lokalen Quell-ONTAP-Cluster und Ihrer FSX for ONTAP-Instanz in BlueXP .

Detaillierte Schritte finden Sie unter "So richten Sie ein FSX für ONTAP-Arbeitsumgebung ein".

Richten Sie VMware Cloud on AWS SDDC ein

"VMware Cloud auf AWS" Cloud-native Arbeitsumgebung für VMware-basierte Workloads im AWS Ecosystem Jedes VMware SDDC (softwaredefiniertes Datacenter) wird in einer Amazon Virtual Private Cloud (VPC) ausgeführt und bietet ein vollständiges VMware Stack (einschließlich vCenter Server), NSX-T Software-definiertes Networking, vSAN Software-definierten Storage und einen oder mehrere ESXi Hosts, die Computing- und Storage-Ressourcen für die Workloads zur Verfügung stellen.

Um eine VMware Cloud-Umgebung auf AWS zu konfigurieren, folgen Sie den Schritten in "Implementieren und Konfigurieren der Virtualisierungsumgebung auf AWS". Ein Pilot-Light-Cluster kann auch für Disaster-Recovery-Zwecke verwendet werden.

Zugriff auf BlueXP Disaster Recovery

Zur Anmeldung beim BlueXP Disaster Recovery Service verwenden Sie NetApp BlueXP.

Zur Anmeldung bei BlueXP können Sie Ihre Zugangsdaten für die NetApp Support Website nutzen oder sich mithilfe Ihrer E-Mail und eines Passworts für eine NetApp Cloud-Anmeldung anmelden. "Erfahren Sie mehr über die Anmeldung".

Bestimmte Aufgaben erfordern bestimmte BlueXP Benutzerrollen. "Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

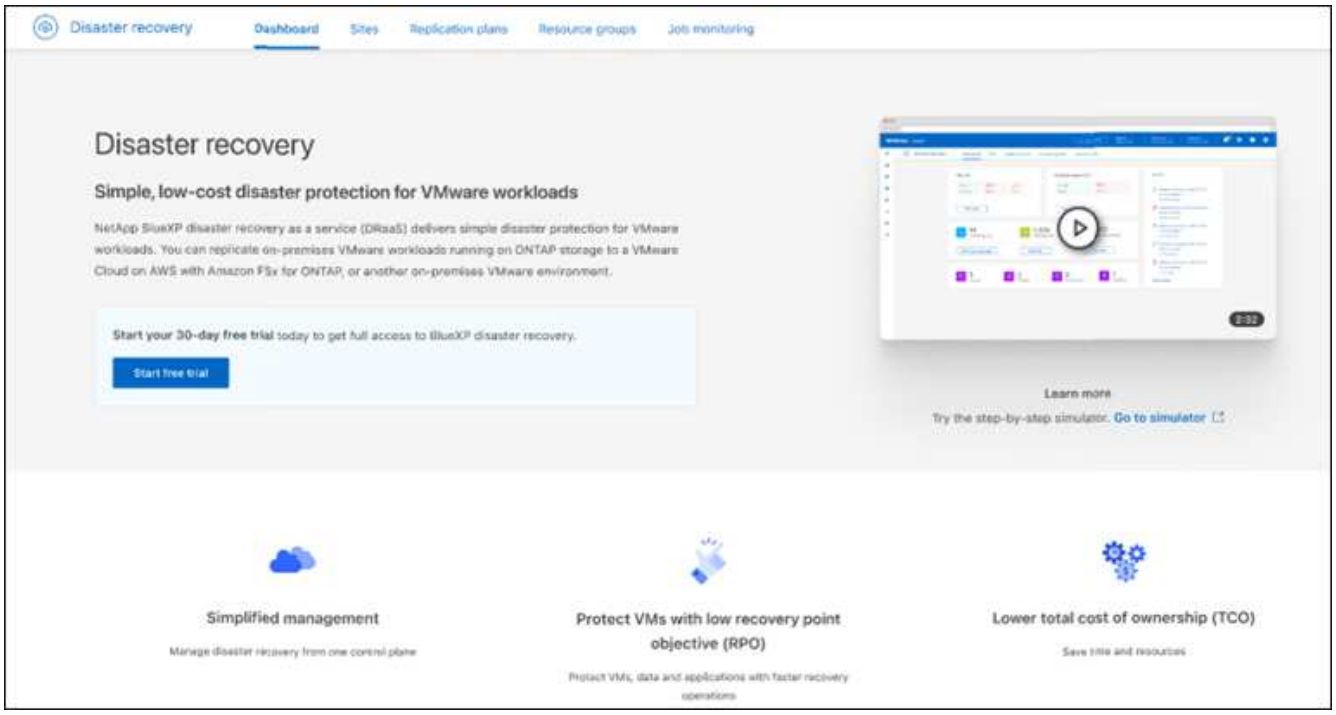
Schritte

1. Öffnen Sie einen Webbrowser, und rufen Sie den auf "BlueXP-Konsole".

   Die Anmeldeseite für NetApp BlueXP wird angezeigt.

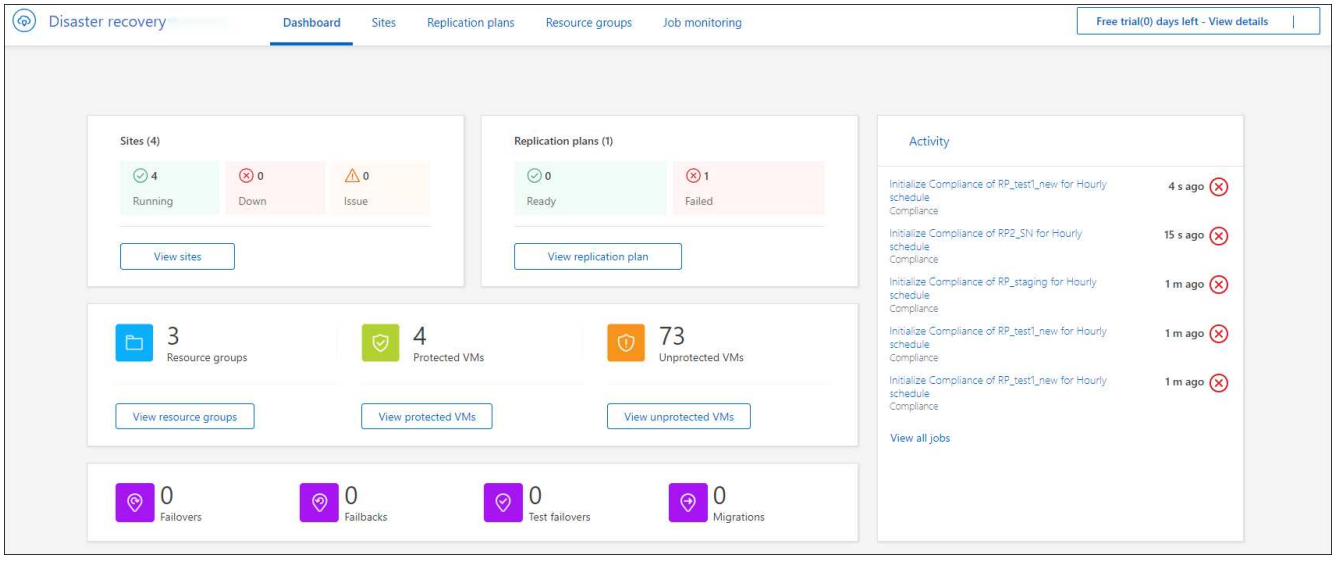
2. Melden Sie sich bei BlueXP an.
3. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.

   Wenn Sie sich zum ersten Mal bei diesem Service anmelden, wird die Landing Page angezeigt, und Sie können sich für eine kostenlose Testversion anmelden.



Andernfalls wird das BlueXP Disaster Recovery Dashboard angezeigt.

- Wenn Sie noch keinen BlueXP Connector hinzugefügt haben, müssen Sie einen Connector hinzufügen. Informationen zum Hinzufügen eines Connectors finden Sie unter "Erfahren Sie mehr über Steckverbinder".
- Wenn Sie ein BlueXP Benutzer mit einem vorhandenen Connector sind, wird bei Auswahl von „Disaster Recovery“ eine Meldung über Ihre Anmeldung angezeigt.
- Wenn Sie den Dienst bereits verwenden, wird bei Auswahl von „Disaster Recovery“ das Dashboard angezeigt.



Lizenzierung für die Disaster Recovery von BlueXP einrichten

Mit BlueXP Disaster Recovery können Sie verschiedene Lizenzierungsmodelle verwenden, darunter eine kostenlose Testversion, ein Pay-as-you-go-Abonnement oder eine eigene Lizenz.

Erforderliche BlueXP Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Administratorrolle für Notfallwiederherstellungsanwendungen.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Lizenzierungsoptionen Sie können die folgenden Lizenzierungsoptionen nutzen:

- Melden Sie sich für eine kostenlose 30-Tage-Testversion an.
- Erwerben Sie ein Pay-as-you-go-Abonnement (PAYGO) für * NetApp Intelligent Services* über den Amazon Web Services (AWS) Marketplace oder den Microsoft Azure Marketplace.
- Bring-Your-Own-License (BYOL) bei einer NetApp Lizenzdatei (NLF), die Sie von Ihrem NetApp Vertriebsmitarbeiter erhalten. Sie können die Seriennummer der Lizenz verwenden, um das BYOL in der Digital Wallet von BlueXP zu aktivieren.

> Die Disaster Recovery-Gebühren von BlueXP basieren auf der genutzten Kapazität von Datastores am Quellstandort, wenn mindestens eine VM mit einem Replizierungsplan vorhanden ist. Die Kapazität für einen Failover-Datenspeicher ist in der zulässigen Kapazität nicht enthalten. Wenn die Daten bei einem BYOL die zulässige Kapazität überschreiten, werden die Vorgänge im Service so lange eingeschränkt, bis Sie eine zusätzliche Kapazitätslizenz erhalten oder die Lizenz in der Digital Wallet von BlueXP aktualisieren.

"Erfahren Sie mehr über Digital Wallet".

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

- Zeigen Sie alle Ressourcen an, z. B. einen Workload oder einen Replizierungsplan.
- Löschen Sie alle Ressourcen, z. B. einen Workload oder einen Replizierungsplan.
- Führen Sie alle geplanten Vorgänge aus, die während des Testzeitraums oder unter der Lizenz erstellt wurden.

Testen Sie es mit einer kostenlosen 30-Tage-Testversion

BlueXP Disaster Recovery können Sie kostenlos testen, indem Sie 30 Tage testen.

> Während der Testphase werden keine Kapazitätsgrenzen durchgesetzt.

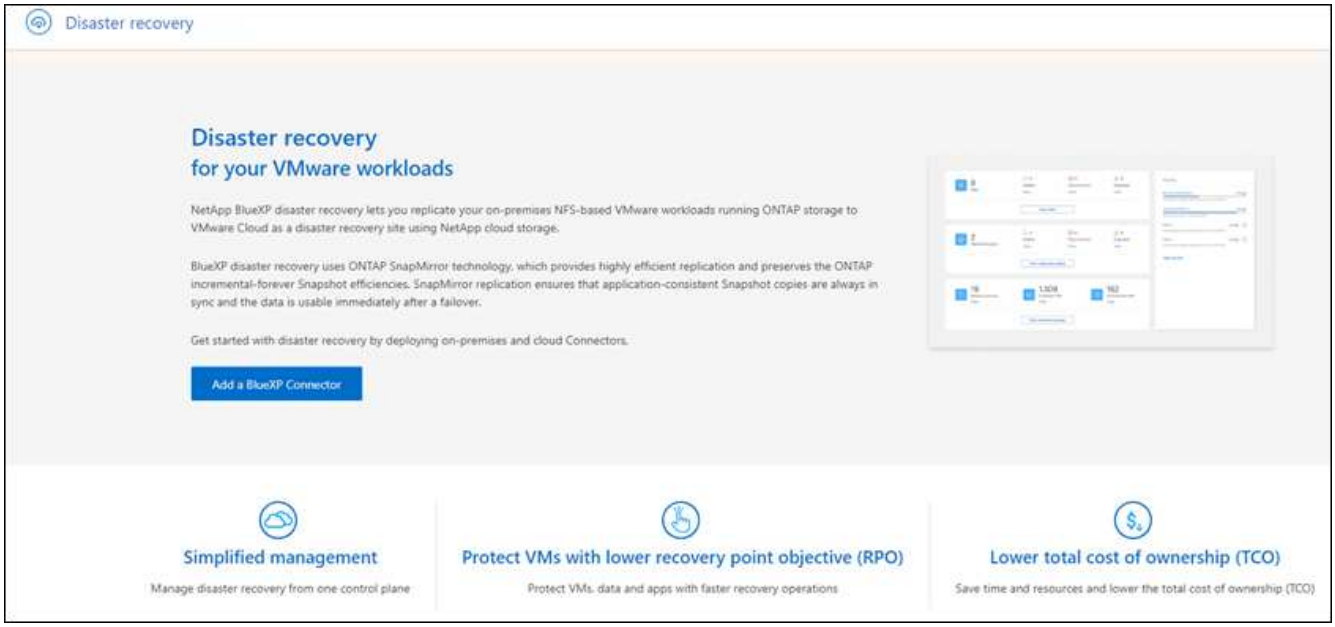
Um nach der Testphase fortzufahren, müssen Sie eine BYOL-Lizenz oder ein PAYGO AWS-Abonnement erwerben. Sie können jederzeit eine Lizenz erhalten und Sie werden erst belastet, wenn die Testversion endet.

Während der Testphase haben Sie volle Funktionalität.

Schritte

1. Auf das zugreifen "BlueXP-Konsole".
2. Melden Sie sich bei BlueXP an.
3. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.

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



4. Wenn Sie noch keinen Connector für andere Dienste hinzugefügt haben, fügen Sie einen hinzu.

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

5. Nach der Einrichtung eines Connectors wird auf der Startseite von BlueXP Disaster Recovery die Schaltfläche zum Hinzufügen eines Connectors zu einer Schaltfläche geändert, um eine kostenlose Testversion zu starten. Wählen Sie **Kostenlose Testversion starten**.
6. Fügen Sie zunächst vCenter hinzu.

   Weitere Informationen finden Sie unter "Fügen Sie vCenter Sites hinzu".

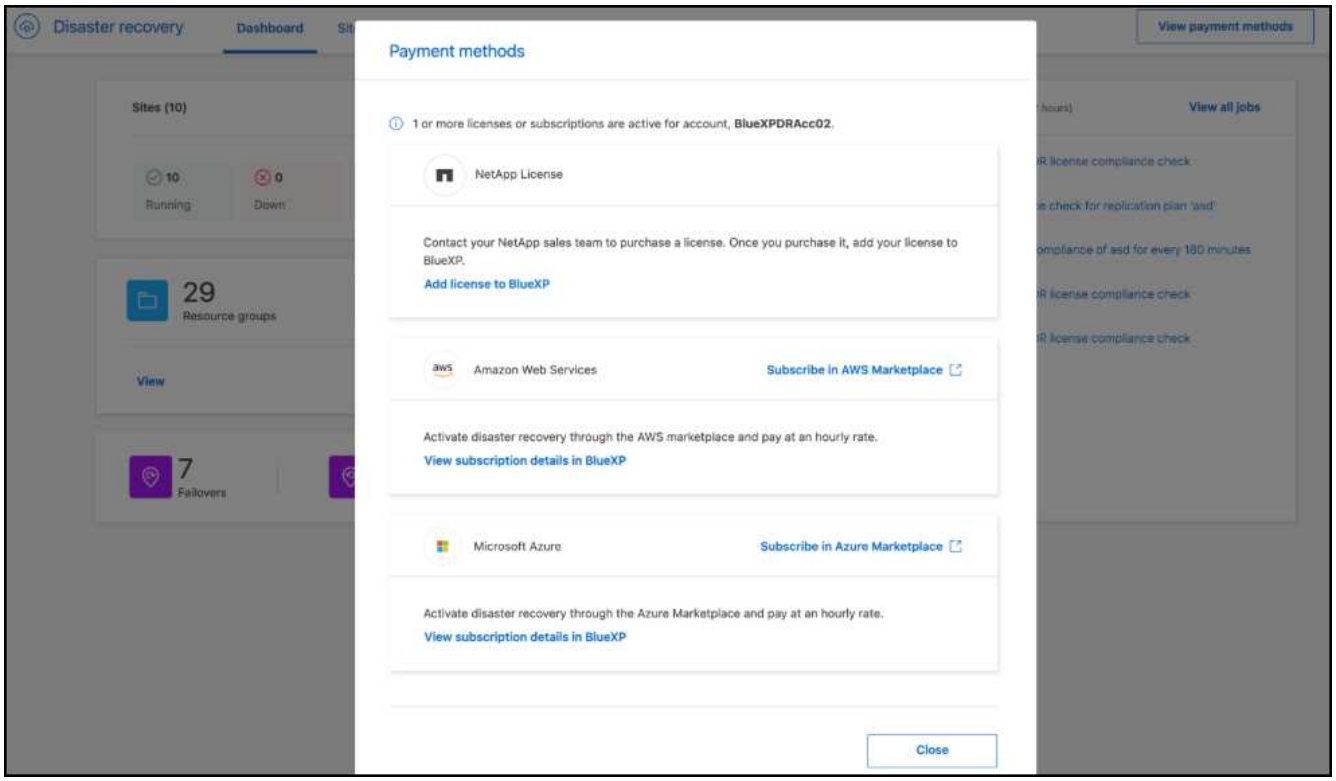
Nach Ablauf der Testphase abonnieren Sie über einen der Marketplaces

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

Schritte

1. Bei der Disaster Recovery von BlueXP wird deutlich, dass die kostenlose Testversion ausläuft. Wählen Sie in der Nachricht **Abonnieren oder eine Lizenz erwerben**.

   Oder wählen Sie oben rechts **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 Intelligent Services* und * BlueXP disaster recovery* zu abonnieren.
4. Wenn Sie zur Disaster Recovery von BlueXP zurückkehren, wird in einer Meldung angezeigt, dass Sie abonniert sind.

   Die Abonnementdetails finden Sie in der BlueXP Digital Wallet. "Weitere Informationen Management von Abonnements mit Digital Wallet".

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

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

Wenn Sie Ihre eigene Lizenz (BYOL, Bring-Your-Own-License) verwenden, umfasst die Einrichtung den Erwerb der Lizenz, das Abrufen der NetApp Lizenzdatei (NLF) und das Hinzufügen der Lizenz zum digitalen Wallet von BlueXP.

Lizenz zur BlueXP Digital Wallet hinzufügen* Nachdem Sie Ihre BlueXP Disaster Recovery Lizenz von Ihrem NetApp Vertriebsmitarbeiter erworben haben, können Sie die Lizenz in Digital Wallet verwalten.

"Informieren Sie sich über das Hinzufügen von Lizenzen mit Digital Wallet".

Aktualisieren Sie Ihre BlueXP Lizenz, wenn sie abläuft

Wenn die Lizenzlaufzeit kurz vor dem Ablaufdatum steht oder die lizenzierte Kapazität das Limit erreicht, werden Sie über die Benutzeroberfläche von BlueXP für Disaster Recovery benachrichtigt. Sie können Ihre BlueXP Disaster-Recovery-Lizenz aktualisieren, bevor sie abläuft, damit der Zugriff auf die gescannten Daten nicht unterbrochen wird.

Diese Meldung wird auch in der Digital Wallet von BlueXP und in angezeigt "Benachrichtigungen".

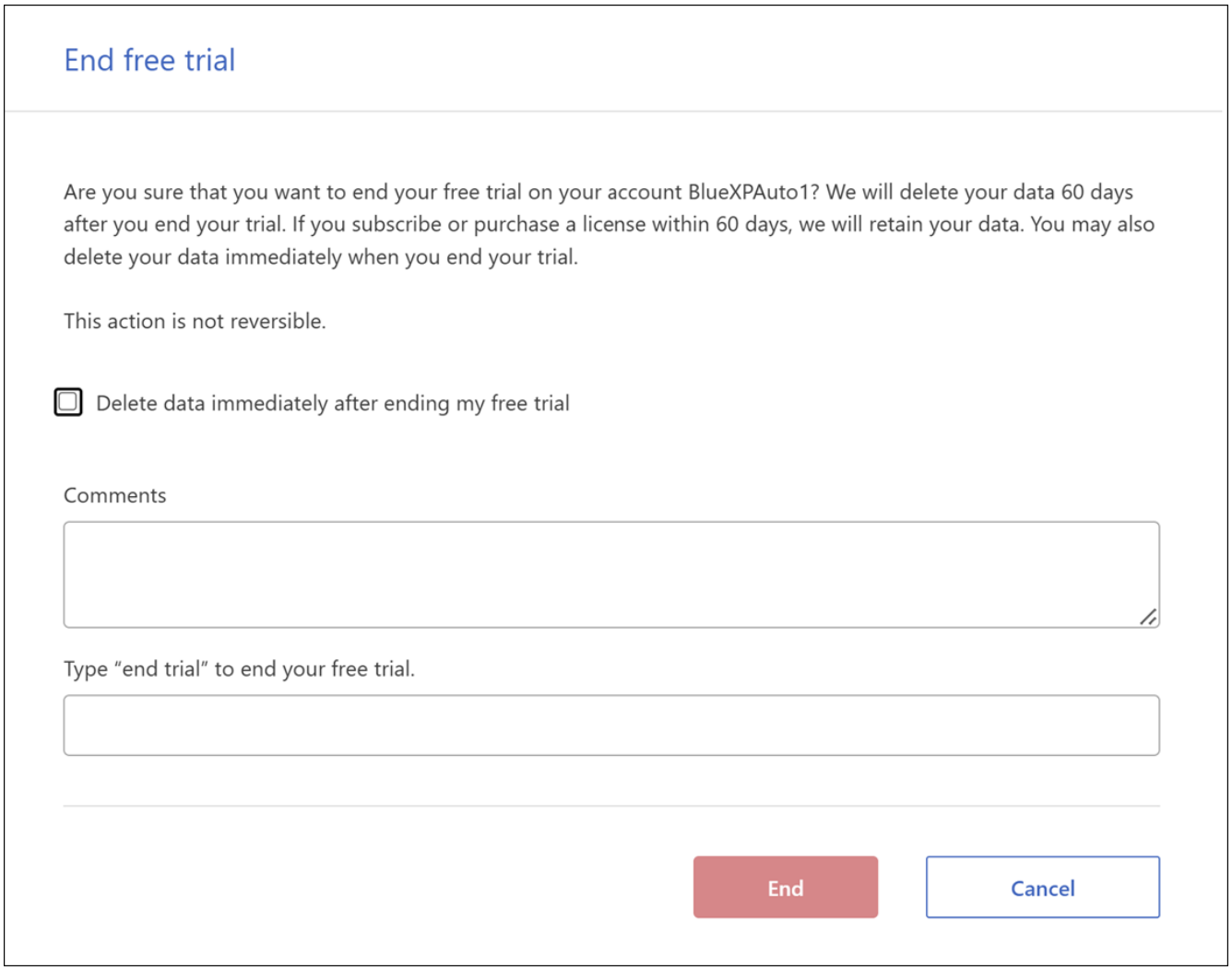
"Informieren Sie sich über die Aktualisierung von Lizenzen mit Digital Wallet".

Beenden Sie die kostenlose Testversion

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

Schritte

1. Wählen Sie in BlueXP Disaster Recovery oben rechts **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 dem Beenden meiner kostenlosen Testversion löschen**.

   Dadurch werden alle Zeitpläne, Replikationspläne, Ressourcengruppen, vCenter und Standorte gelöscht. Audit-Daten, Betriebsprotokolle und Jobverlauf werden bis zum Ende der Lebensdauer des Produkts aufbewahrt.

Wenn Sie die kostenlose Testversion beenden, keine Daten löschen möchten und keine Lizenz oder kein Abonnement erwerben, löscht BlueXP Disaster Recovery 60 Tage nach Ablauf der kostenlosen Testversion alle Ihre Daten.

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

Häufig gestellte Fragen zur Disaster Recovery von BlueXP

Diese FAQ kann Ihnen helfen, wenn Sie nur nach einer schnellen Antwort auf eine Frage suchen.

Wie sieht die Disaster-Recovery-URL von BlueXP aus?
Geben Sie für die URL in einem Browser Folgendes ein: "https://console.bluexp.netapp.com/" Um auf die BlueXP Konsole zuzugreifen.

Benötigen Sie eine Lizenz für die Nutzung von BlueXP Disaster Recovery?
Für vollständigen Zugriff ist eine Disaster-Recovery-Lizenz von BlueXP erforderlich. Sie können es jedoch mit der kostenlosen Testversion ausprobieren.

Weitere Informationen zur Einrichtung einer Lizenzierung für die Disaster Recovery von BlueXP finden Sie unter "Disaster-Recovery-Lizenzen für BlueXP einrichten".

Wie greifen Sie auf Disaster Recovery von BlueXP zu? Für die Disaster Recovery von BlueXP ist keine Aktivierung erforderlich. Die Disaster-Recovery-Option wird automatisch in der linken Navigation von BlueXP angezeigt.

Nutzen Sie BlueXP Disaster Recovery

Nutzen Sie die Disaster Recovery-Übersicht von BlueXP

Mit der Disaster Recovery von BlueXP können Sie folgende Ziele erreichen:

- "Zeigen Sie den Zustand Ihrer Disaster-Recovery-Pläne an".
- "Fügen Sie vCenter Sites hinzu".
- "Erstellen Sie Ressourcengruppen, um VMs zusammen zu organisieren"
- "Disaster-Recovery-Plan erstellen".
- "Replizierung von VMware Applikationen" Sie erfolgt an Ihrem primären Standort an einem Disaster-Recovery-Remote-Standort in der Cloud mithilfe von SnapMirror Replizierung.
- "Migrieren Sie VMware-Applikationen" Am primären Standort zu einem anderen Standort wechseln.
- "Testen Sie das Failover" Ohne eine Unterbrechung der ursprünglichen Virtual Machines.
- Im Notfall, "Failover an Ihrem primären Standort" Zu VMware Cloud on AWS mit FSX for NetApp ONTAP
- Nachdem die Katastrophe behoben ist, "Failback" Von einem Disaster-Recovery-Standort zum primären Standort.
- "Überwachen Sie Disaster-Recovery-Vorgänge" Auf der Seite Jobüberwachung.

Sehen Sie sich den Zustand Ihrer BlueXP-Notfallwiederherstellungspläne auf dem Dashboard an

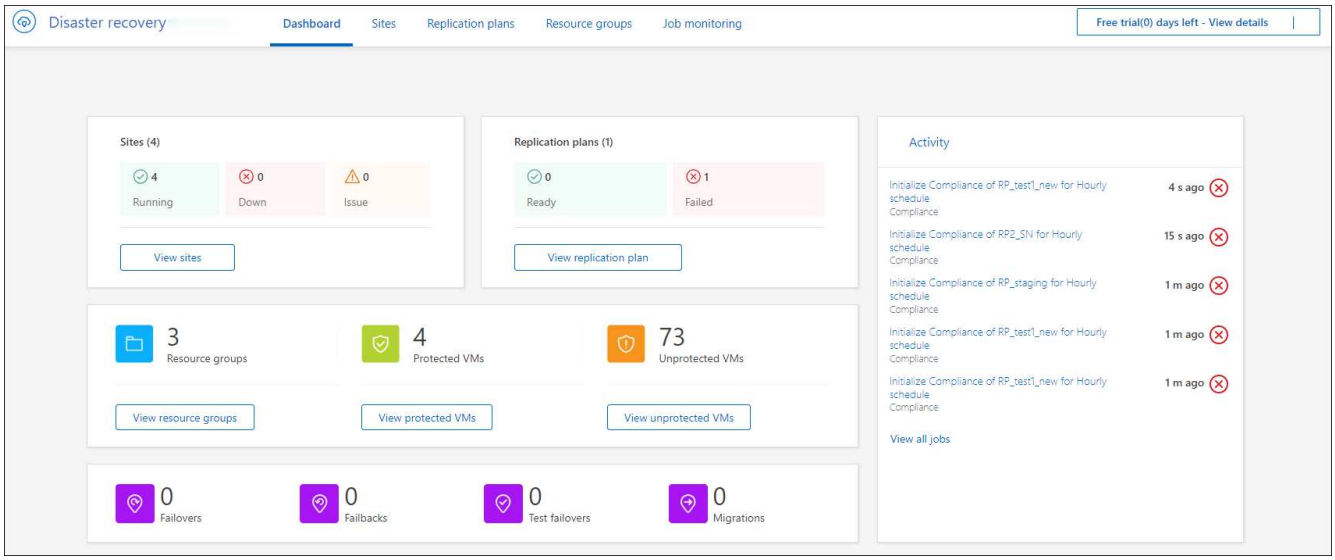
Mit dem BlueXP Disaster Recovery-Dashboard können Sie den Zustand Ihrer Disaster-Recovery-Standorte und Replizierungspläne bestimmen. Sie können schnell feststellen, welche Standorte und Pläne gesund, getrennt oder degradiert sind.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungsanwendungsadministrator oder Notfallwiederherstellungsbetrachterrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie aus dem BlueXP Disaster Recovery-Hauptmenü **Dashboard** aus.



3. Überprüfen Sie die folgenden Informationen auf dem Dashboard:
   - **Sites**: Sehen Sie die Gesundheit Ihrer Sites. Ein Standort kann einen der folgenden Status haben:
     - **Running**: VCenter ist verbunden, funktionsfähig und läuft.
     - **Down**: VCenter ist nicht erreichbar oder hat Verbindungsprobleme.
     - **Problem**: VCenter ist nicht erreichbar oder hat Verbindungsprobleme.

       Um die Standortdetails anzuzeigen, wählen Sie **Alle anzeigen** für einen Status oder **Sites anzeigen**, um 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 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 Details zu überprüfen, wählen Sie den Link **Ansicht** unter jedem.
   - Die Anzahl der Failover, Test-Failover und Migrationen. Wenn Sie beispielsweise zwei Pläne erstellt und zu den Zielen migriert haben, wird die Migrationszahl als „2“ angezeigt.
4. Überprüfen Sie alle Vorgänge im Bereich „Aktivität“. Um alle Vorgänge auf dem Job Monitor anzuzeigen, wählen Sie **Alle Jobs anzeigen**.

vCenters zu einem Standort in BlueXP Disaster Recovery hinzufügen

Bevor Sie einen Disaster Recovery-Plan erstellen können, müssen Sie einem Standort einen primären vCenter Server und einen vCenter Ziel-Disaster-Recovery-Standort in BlueXP hinzufügen.

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

Nach dem Hinzufügen von vCenters führt BlueXP Disaster Recovery eine umfassende Erkennung der vCenter-Umgebungen durch, einschließlich vCenter-Cluster, ESXi-Hosts, Datastores, Storage-Platzbedarf, Details zu virtuellen Maschinen, SnapMirror-Replikaten und Virtual-Machine-Netzwerken.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator oder Notfallwiederherstellungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

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

Bei der Disaster Recovery von BlueXP werden alle 24 Stunden einmal erkannt. Nach der Einrichtung eines Standorts können Sie später das vCenter bearbeiten, um den Ermittlungsplan an Ihre Anforderungen anzupassen. Wenn Sie beispielsweise über eine große Anzahl an VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 23 Stunden und 59 Minuten ausgeführt wird. Wenn Sie über eine geringe Anzahl von VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 12 Stunden ausgeführt wird. Das Mindestintervall beträgt 30 Minuten und das Maximum 24 Stunden.

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

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

VMs können nur gesichert werden, wenn der Replizierungsplan einen der folgenden Status hat:

- Bereit
- Failback durchgeführt
- Failover-Test festgelegt

Schritte

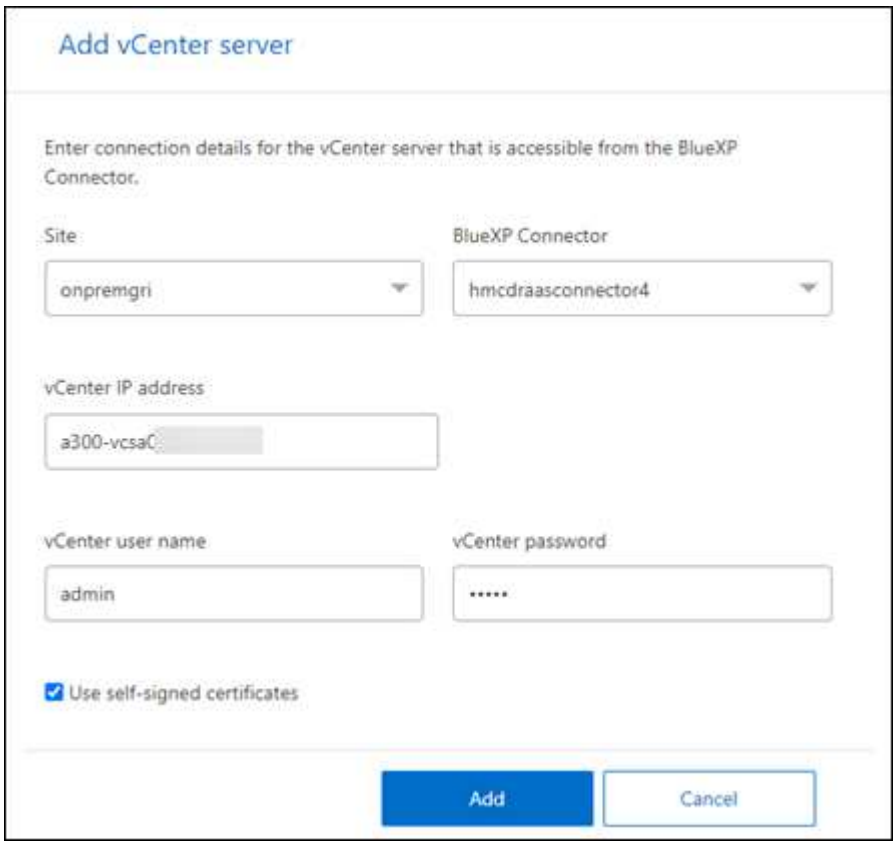
1. Melden Sie sich bei BlueXP an und wählen Sie im linken Navigationsmenü **Schutz** > **Notfallwiederherstellung**.

   Sie finden die Seite zum Disaster Recovery Dashboard von BlueXP. Wenn Sie mit dem Service beginnen, müssen Sie vCenter-Informationen hinzufügen. Später werden im Dashboard Daten zu Ihren Standorten und Replikationsplänen angezeigt.

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

2. **Quelle**: Wählen Sie **Discover vCenter Server**, um Informationen über den vCenter-Quellstandort einzugeben.

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



- Fügen Sie eine Site hinzu, wählen Sie den BlueXP Connector aus und geben Sie vCenter Zugangsdaten an.
- (Gilt nur für On-Premises-Standorte) um selbstsignierte Zertifikate für das Quell-vCenter zu akzeptieren, aktivieren Sie das Kontrollkästchen.

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

3. Wählen Sie **Hinzufügen**.

Als Nächstes fügen Sie ein Ziel-vCenter hinzu.

4. **Ziel**:

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

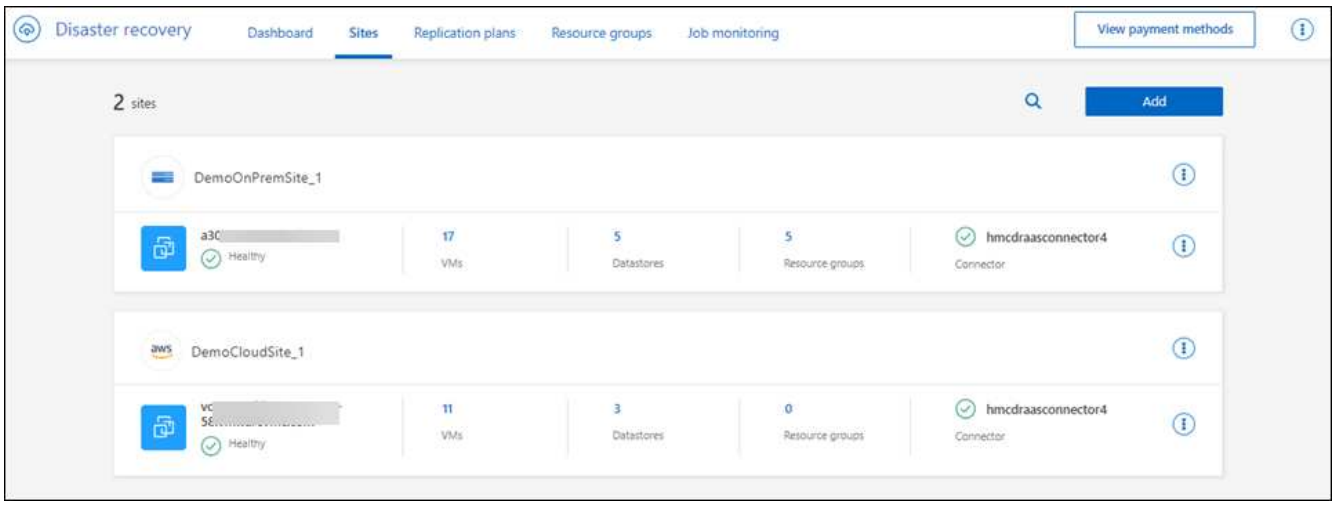
- (Gilt nur für Cloud-Sites) **API-Token**: Geben Sie das API-Token ein, um den Dienstzugriff für Ihre Organisation zu autorisieren. Erstellen des API-Tokens durch Angabe bestimmter Unternehmens-

und Servicerollen

- (Gilt nur für Cloud-Standorte) **lange Organisations-ID**: Geben Sie die eindeutige ID für die Organisation ein. Sie können diese ID identifizieren, indem Sie auf den Benutzernamen im Abschnitt „Konto“ der BlueXP -Konsole klicken.

b. Wählen Sie **Hinzufügen**.

Die Quell- und Ziel-vCenter werden in der Liste der Standorte angezeigt.



5. Um den Fortschritt des Vorgangs anzuzeigen, wählen Sie im oberen Menü **Job-Überwachung**.

Fügen Sie die Subnetzzuordnung für einen vCenter-Standort hinzu

Managen Sie IP-Adressen beim Failover auf neue Weise mithilfe der Subnetzzuordnung, wodurch Sie Subnetze für jedes vCenter hinzufügen können. Dabei definieren Sie den IPv4 CIDR, das Standard-Gateway und den DNS für jedes virtuelle Netzwerk.

Bei einem Failover ermittelt die Disaster Recovery von BlueXP die geeignete IP-Adresse jeder vNIC, indem das für das zugeordnete virtuelle Netzwerk bereitgestellte CIDR betrachtet und es zum Ableiten der neuen IP-Adresse verwendet wird.

Beispiel:

- NetworkA = 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. NetworkA wird in den Einstellungen des Replikationsplans zu NetworkB zugeordnet.

Bei einem Failover ersetzt die Disaster Recovery von BlueXP den Teil Netzwerk der ursprünglichen IP-Adresse (10.1.1) und behält die Host-Adresse (.50) der ursprünglichen IP-Adresse (10.1.1.50) bei. Für VM1 betrachtet die BlueXP Disaster Recovery die CIDR-Einstellungen für NetworkB und verwendet den Netzwerk-B-Teil 192.168.1, während der Host-Teil (.50) beibehalten wird, um die neue IP-Adresse für VM1 zu erstellen. Die neue IP wird 192.168.1.50.

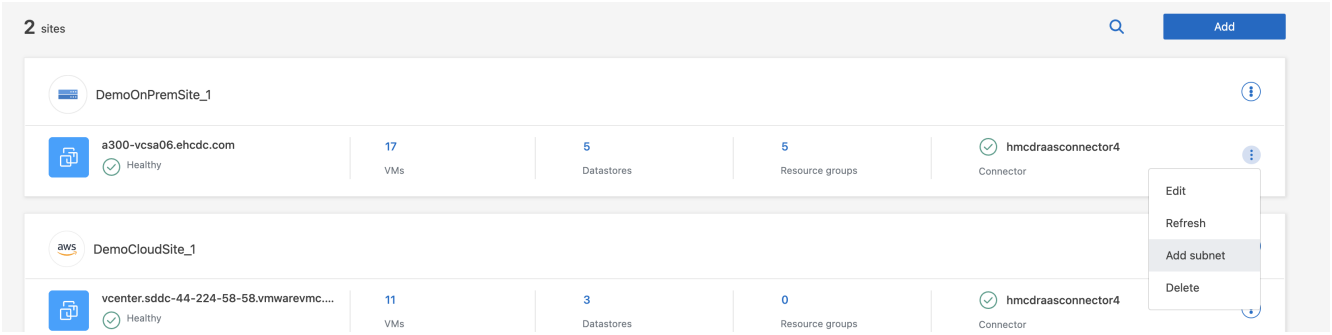
Zusammenfassend bleibt die Host-Adresse unverändert, während die Netzwerkadresse durch das ersetzt wird, was in der Subnetz-Zuordnung des Standorts konfiguriert ist. So lässt sich die IP-Adressenzuweisung beim Failover einfacher managen, insbesondere wenn Sie hunderte Netzwerke und tausende VMs managen müssen.

Die Verwendung der Subnetzzuordnung ist ein optionaler Prozess in zwei Schritten:

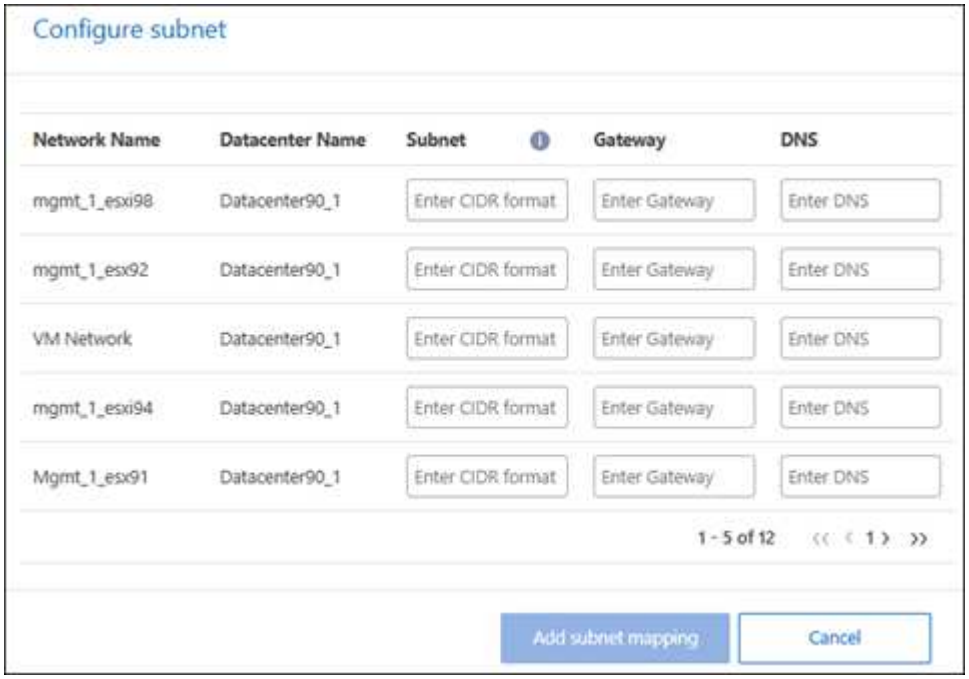
- Fügen Sie zunächst die Subnetzzuordnung für jeden vCenter-Standort hinzu.
- Geben Sie anschließend im Replikationsplan an, dass Sie die Subnetzzuordnung verwenden möchten.

Schritte

1. Wählen Sie im oberen BlueXP -Disaster-Recovery-Menü **Sites** aus.
2. Wählen Sie aus dem Aktionen- Symbol auf der rechten Seite **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 zur Angabe von IP-Adressen und deren Netzwerkmasken. /24 bezeichnet die Netzmaske. Die Nummer besteht aus einer IP-Adresse mit der Zahl nach dem „/“, die angibt, wie viele Bits der IP-Adresse das Netzwerk kennzeichnen. Beispiel: 192.168.0.50/24, die IP-Adresse ist 192.168.0.50 und die Gesamtzahl der Bits in der Netzwerkadresse ist 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**.

Wählen Sie die Subnetzzuordnung für einen Replikationsplan aus

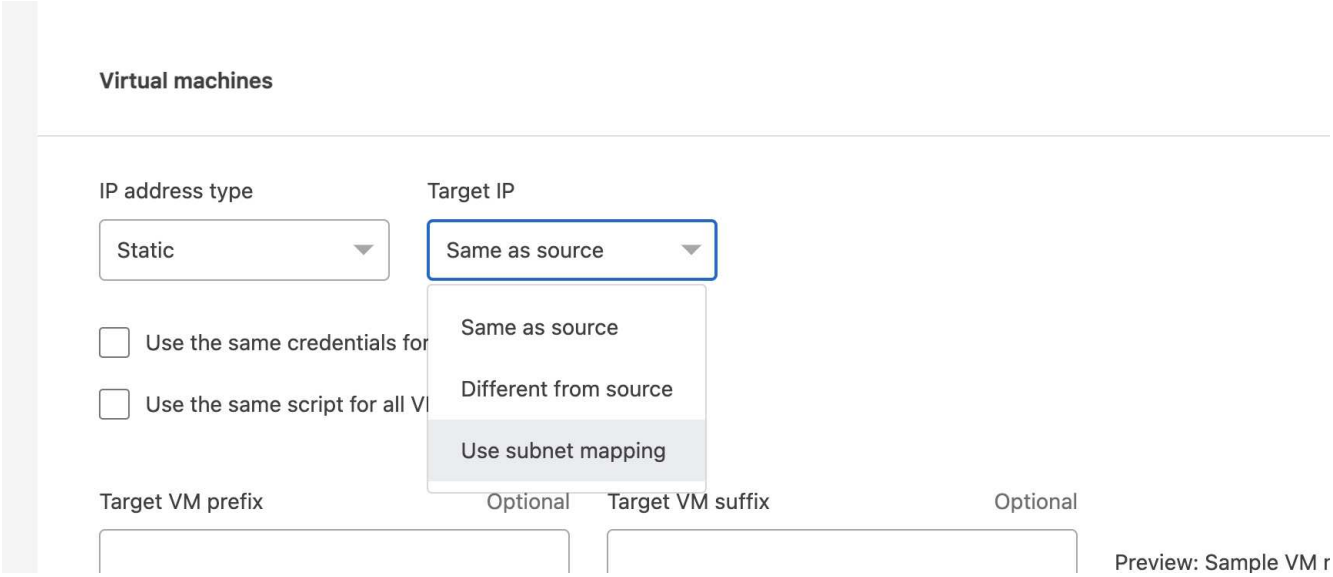
Wenn Sie einen Replikationsplan erstellen, können Sie die Subnetzzuordnung für den Replikationsplan auswählen.

Die Verwendung der Subnetzzuordnung ist ein optionaler Prozess in zwei Schritten:

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

Schritte

1. Wählen Sie im oberen Menü der BlueXP Disaster Recovery die Option **Replication Plans** aus.
2. Wählen Sie **Add**, 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 abschließen.
4. Wählen Sie auf der Seite Replizierungsplan > Ressourcenzuordnung den Abschnitt **Virtuelle Maschinen** aus.



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

> Wenn zwei VMs vorhanden sind (z. B. Linux und Windows), werden nur Anmeldeinformationen für Windows benötigt.

6. Fahren Sie mit dem Erstellen des Replikationsplans fort.

Bearbeiten Sie den vCenter Server-Standort und passen Sie den Ermittlungsplan an

Sie können den vCenter Server-Standort bearbeiten, um den Ermittlungsplan anzupassen. Wenn Sie

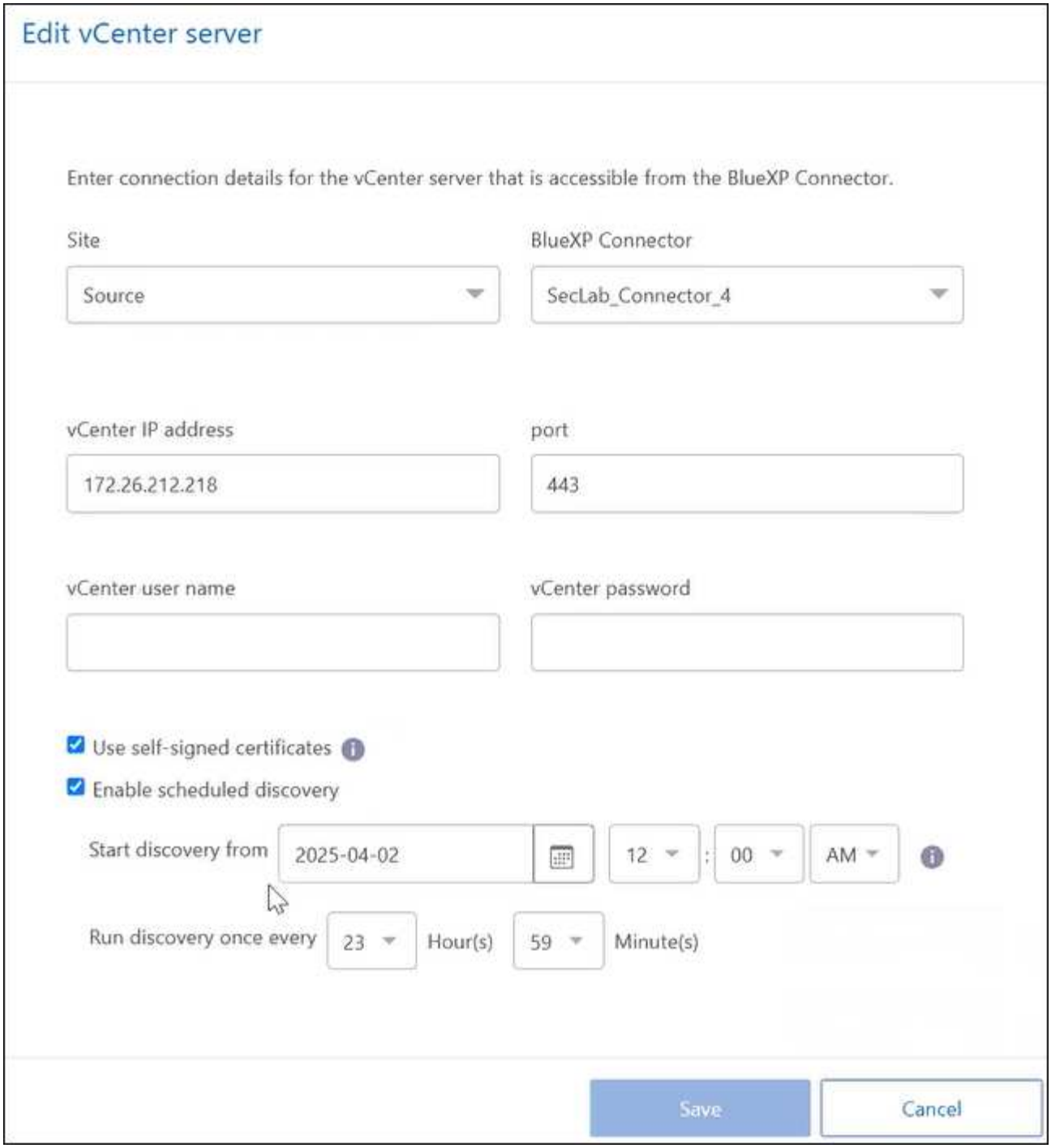
beispielsweise über eine große Anzahl an VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 23 Stunden und 59 Minuten ausgeführt wird. Wenn Sie über eine geringe Anzahl von VMs verfügen, können Sie den Erkennungszeitplan so einstellen, dass er alle 12 Stunden ausgeführt wird.

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

Wenn Sie die Ermittlung nicht planen möchten, können Sie die Option für die geplante Ermittlung deaktivieren und die Ermittlung jederzeit manuell aktualisieren.

Schritte

1. Wählen Sie im BlueXP Disaster Recovery-Menü **Sites** aus.
2. Wählen Sie die Site aus, die Sie bearbeiten möchten.
3. Wählen Sie das Aktionen-  Symbol auf der rechten Seite und wählen Sie **Bearbeiten**.
4. Bearbeiten Sie die Felder auf der Seite vCenter-Server bearbeiten nach Bedarf.
5. Um den Ermittlungszeitplan anzupassen, aktivieren Sie das Kontrollkästchen **geplante Ermittlung aktivieren**, und wählen Sie das gewünschte Datum und das gewünschte Zeitintervall aus.



6. Wählen Sie **Speichern**.

Erkennung manuell aktualisieren

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

Schritte

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

Wählen Sie das Aktionen-  Symbol auf der rechten Seite und wählen Sie **Aktualisieren**.

Erstellen Sie eine Ressourcengruppe, um VMs gemeinsam in der BlueXP-Notfallwiederherstellung zu organisieren

Nachdem Sie vCenter Sites hinzugefügt haben, möchten Sie möglicherweise Ressourcengruppen erstellen, die VMs durch VMs oder Datastores gruppieren. Ressourcengruppen ermöglichen es Ihnen, eine Reihe abhängiger VMs in logischen Gruppen zu organisieren, die Ihren Anforderungen entsprechen. Beispielsweise können Sie VMs einer Applikation gruppieren oder Applikationen mit ähnlichen Tiers gruppieren. Als weiteres Beispiel könnten Gruppen verzögerte Startaufträge enthalten, die bei der Wiederherstellung ausgeführt werden können.

Erforderliche BlueXP Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Administratorrolle für Notfallwiederherstellungsanwendungen.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Sie können VMs selbst oder VMs in Datastores gruppieren.

Sie können Ressourcengruppen mithilfe der folgenden Methoden erstellen:

- Auf der Registerkarte Ressourcengruppen
- Während Sie einen Disaster Recovery- oder Replizierungsplan erstellen. Wenn viele VMs von einem vCenter Quell-Cluster gehostet werden, ist es möglicherweise einfacher für Sie, die Ressourcengruppen beim Erstellen des Replikationsplans zu erstellen. Anweisungen zum Erstellen von Ressourcengruppen während des Erstellens eines Replikationsplans finden Sie unter "Erstellen Sie einen Replizierungsplan".

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

Informationen zu Ressourcengruppen

Mit Ressourcengruppen können Sie VMs oder Datastores kombinieren, die VMs umfassen, die operativ verbunden sind und als ein einziges System geschützt werden müssen.

Eine Point-of-Sale-Applikation kann beispielsweise aus mehreren VMs bestehen, die Datenbanken hosten, mehreren VMs, die Management von Geschäftslogikregeln hosten, und mehreren VMs, die als Webserver-basierte Storefront fungieren. Es kann sich vorteilhaft auswirken, die Verfügbarkeit der gesamten Applikation mit einem einzigen Sicherungsprozess zu managen, indem diese VMs in einer einzelnen Ressourcengruppe platziert werden.

Wenn Ressourcengruppen eingerichtet sind, können Sie die Regeln des Replikationsplans für eine ordnungsgemäße VM-Startreihenfolge, Netzwerkverbindung und mehr anwenden, um eine ordnungsgemäße Wiederherstellung aller für die Anwendung erforderlichen VMs sicherzustellen.

Wie funktioniert das?

BlueXP Disaster Recovery sichert VMs, indem die zugrunde liegenden ONTAP Volumes und LUNs repliziert

werden, die die VMs in der Ressourcengruppe hosten. Dazu fragt das System vCenter nach dem Namen jedes Datenspeichers ab, der VMs in einer Ressourcengruppe hostet. BlueXP Disaster Recovery identifiziert dann das ONTAP Quell-Volume oder die LUN, die diesen Datenspeicher hostet. Sämtliche Sicherung wird mithilfe der SnapMirror Replizierung auf ONTAP Volume-Ebene durchgeführt.

Wenn VMs in der Ressourcengruppe auf verschiedenen Datenspeichern gehostet werden, verwendet die Disaster Recovery von BlueXP eine der folgenden Methoden, um einen Daten-konsistenten Snapshot der ONTAP Volumes oder LUNs zu erstellen.

Relative Position von FlexVol Volumes	**Snapshot-Replikatprozess**
Mehrere Datenspeicher - FlexVol Volumes in der **gleichen SVM**	• Die ONTAP Konsistenzgruppe wurde erstellt • Snapshots der erstellten Konsistenzgruppe • Die SnapMirror-Replizierung im Volume wurde durchgeführt
Mehrere Datenspeicher – FlexVol Volumes in **mehreren SVMs**	• ONTAP-API: `cg_start`. Stellt alle Volumes nach, damit Snapshots erstellt werden können, und initiiert Volume-bezogene Snapshots aller Ressourcengruppen-Volumes. • ONTAP-API: `cg_end`. Setzt den I/O-Vorgang auf allen Volumes fort und ermöglicht die SnapMirror-Replizierung mit Volume-Umfang, nachdem Snapshots erstellt wurden.

Wenn Sie Ressourcengruppen erstellen, beachten Sie die folgenden Probleme:

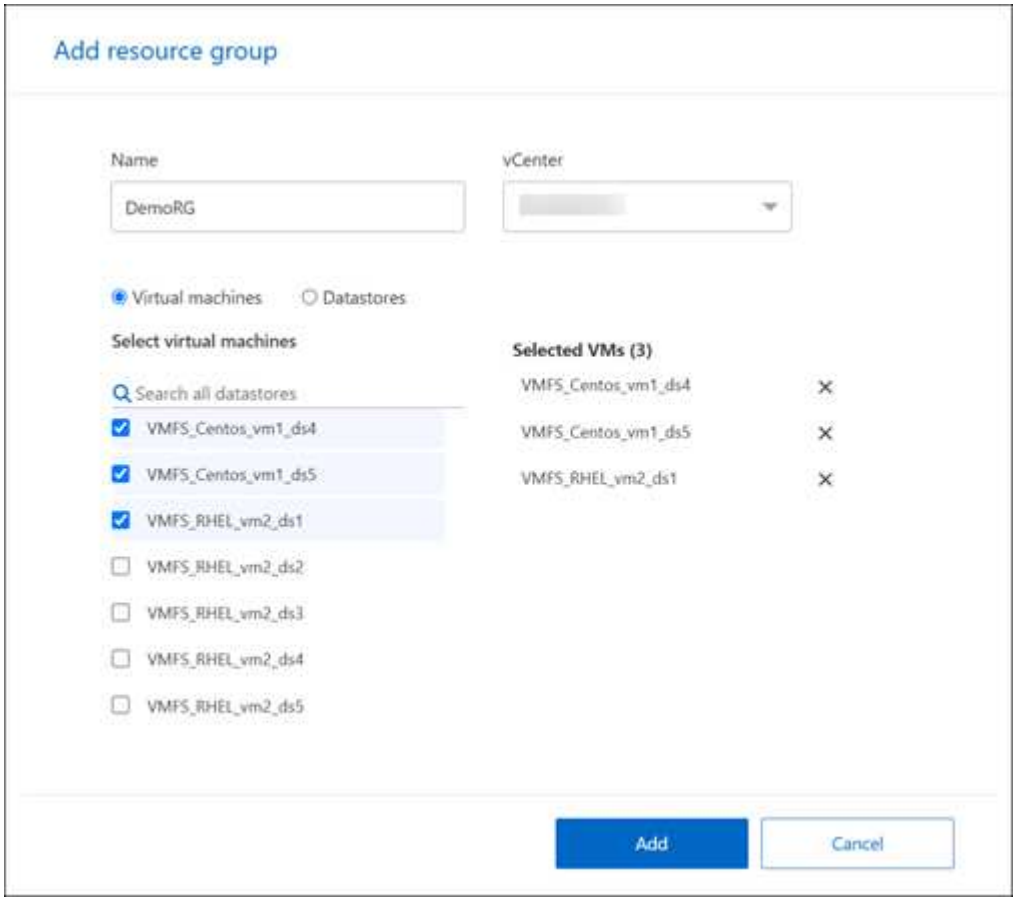
- Bevor Sie Datastores zu Ressourcengruppen hinzufügen, starten Sie zunächst eine manuelle Ermittlung oder eine geplante Ermittlung der VMs. Dadurch wird sichergestellt, dass die VMs erkannt und in der Ressourcengruppe aufgelistet werden. Wenn Sie keine manuelle Ermittlung auslösen, werden die VMs möglicherweise nicht in der Ressourcengruppe aufgeführt.
- Stellen Sie sicher, dass sich mindestens eine VM im Datastore befindet. Wenn sich keine VMs im Datastore befinden, wird der Datastore nicht erkannt.
- Ein einzelner Datenspeicher sollte keine VMs hosten, die durch mehr als einen Replizierungsplan geschützt sind.
- Hosten Sie keine geschützten und ungesicherten VMs auf demselben Datenspeicher. Wenn geschützte und ungesicherte VMs auf demselben Datenspeicher gehostet werden, können folgende Probleme auftreten:
  - Da bei der Disaster Recovery von BlueXP SnapMirror verwendet und das System ganze ONTAP Volumes repliziert, wird die genutzte Kapazität dieses Volumes zu Lizenzierungsüberlegungen verwendet. In diesem Fall wird der von geschützten und ungeschützten VMs verbrauchte Volume-Speicherplatz in diese Berechnung einbezogen.
  - Wenn für die Ressourcengruppe und die zugehörigen Datastores ein Failover am Disaster Recovery-Standort erforderlich ist, sind alle ungesicherten VMs (VMs, die nicht zur Ressourcengruppe gehören, aber auf dem ONTAP Volume gehostet werden) vom Failover-Prozess nicht mehr am Quellstandort vorhanden. Dies führt zu einem Ausfall ungeschützter VMs am Quellstandort. Darüber hinaus startet die Disaster Recovery von BlueXP diese ungeschützten VMs nicht am vCenter Failover-Standort.
- Damit eine VM geschützt ist, muss sie in eine Ressourcengruppe aufgenommen werden.

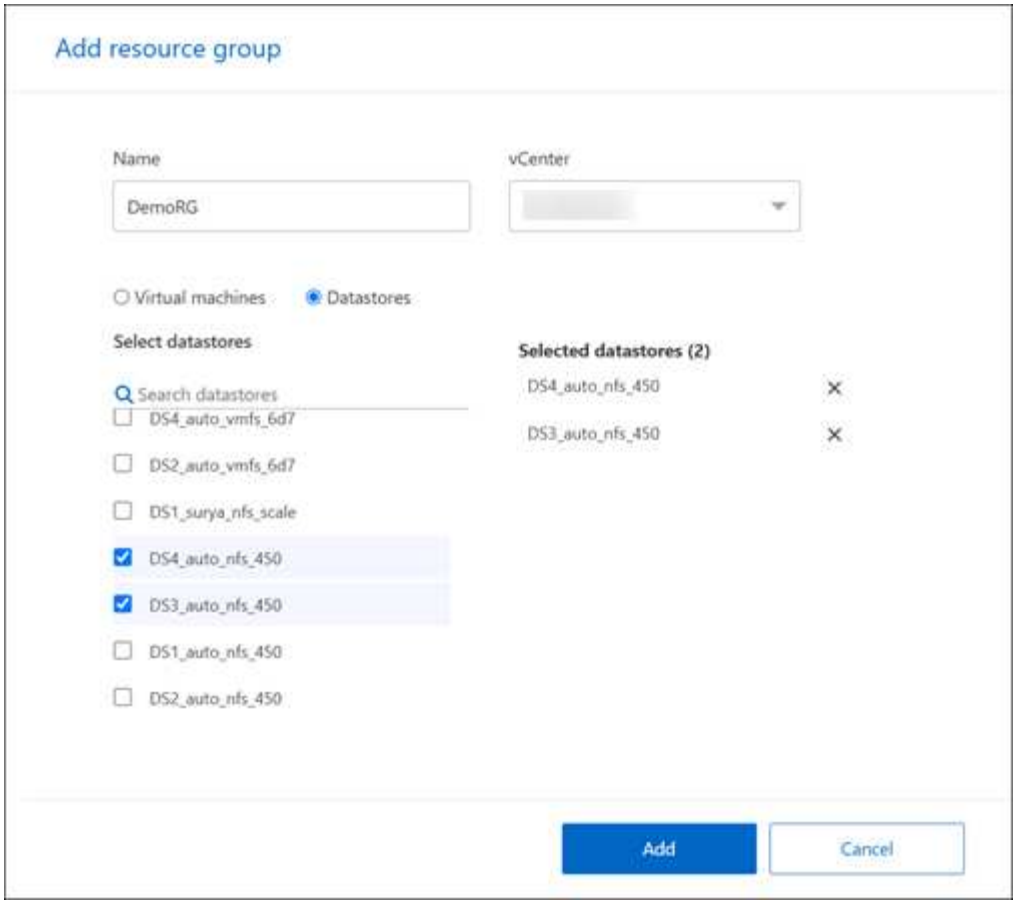
BEST PRACTICE: Organisieren Sie Ihre VMs vor der Bereitstellung der Disaster Recovery von BlueXP , um die Ausbreitung von Datastores zu minimieren. Platzieren Sie VMs, die eine Sicherung auf einer Teilmenge

von Datenspeichern benötigen, und platzieren Sie VMs, die nicht in einer anderen Teilmenge von Datenspeichern gesichert werden sollen. Stellen Sie sicher, dass die VMs auf einem beliebigen Datastore nicht durch unterschiedliche Replikationspläne geschützt sind.

Schritte

1. Wählen Sie im BlueXP Disaster Recovery-Menü **Ressourcengruppen** aus.
2. Wählen Sie **Hinzufügen**.
3. Geben Sie einen Namen für die Ressourcengruppe ein.
4. Wählen Sie das vCenter-Quellcluster aus, in dem sich die VMs befinden.
5. Wählen Sie entweder **Virtual Machines** oder **Datastores** je nachdem, wie Sie suchen möchten.
6. Wählen Sie die Registerkarte **Ressourcengruppen hinzufügen**. Das System listet alle Datastores oder VMs im ausgewählten vCenter-Cluster auf. Wenn Sie **Datastores** ausgewählt haben, listet das System alle Datastores im ausgewählten vCenter Cluster auf. Wenn Sie **Virtual Machines** ausgewählt haben, listet das System alle VMs im ausgewählten vCenter-Cluster auf.
7. Wählen Sie auf der linken Seite der Seite Ressourcengruppen hinzufügen die VMs aus, die Sie schützen möchten.





8. Sie können optional die Reihenfolge der VMs auf der rechten Seite ändern, indem Sie die einzelnen VMs nach oben oder unten in der Liste ziehen. Die VMs werden basierend auf der Reihenfolge, in der Sie sie einschließen, eingeschaltet.
9. Wählen Sie **Hinzufügen**.

Erstellen Sie einen Replikationsplan in der BlueXP-Notfallwiederherstellung

Nachdem Sie vCenter Standorte hinzugefügt haben, sind Sie bereit, einen Disaster Recovery- oder Replizierungsplan zu erstellen. Wählen Sie die Quell- und Ziel-vCenter aus, wählen Sie die Ressourcengruppen aus und gruppieren Sie, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen. Beispielsweise könnten Sie Virtual Machines (VMs) gruppieren, die einer Applikation zugeordnet sind, oder Sie könnten Applikationen mit ähnlichen Tiers gruppieren.

Solche Pläne werden manchmal *Blueprints* genannt.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungs-Failover-Administrator oder Notfallwiederherstellungsanwendungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Sie können einen Replizierungsplan erstellen und darüber hinaus Zeitpläne für Compliance und Tests

bearbeiten.

Sie können mehrere VMs auf mehreren Datenspeichern sichern. Die Disaster Recovery von BlueXP erstellt ONTAP-Konsistenzgruppen für alle ONTAP-Volumes, die geschützte VM-Datastores hosten.

VMs können nur gesichert werden, wenn der Replizierungsplan einen der folgenden Status hat:

- Bereit
- Failback durchgeführt
- Failover-Test festgelegt

Erstellen Sie den Plan

Ein Assistent führt Sie durch die folgenden Schritte:

- Wählen Sie vCenter-Server aus.
- Wählen Sie die VMs oder Datastores aus, die Sie replizieren möchten, und weisen Sie Ressourcengruppen zu.
- Zuordnen der Ressourcen aus der Quellumgebung zum Ziel
- Identifizieren Sie die Wiederholung, führen Sie ein vom Gast gehostetes Skript aus, legen Sie die Startreihenfolge fest, und wählen Sie das Ziel für den Wiederherstellungspunkt aus.
- Überprüfen Sie den Plan.

Wenn Sie den Plan erstellen, sollten Sie folgende Richtlinien befolgen:

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

Bevor Sie beginnen

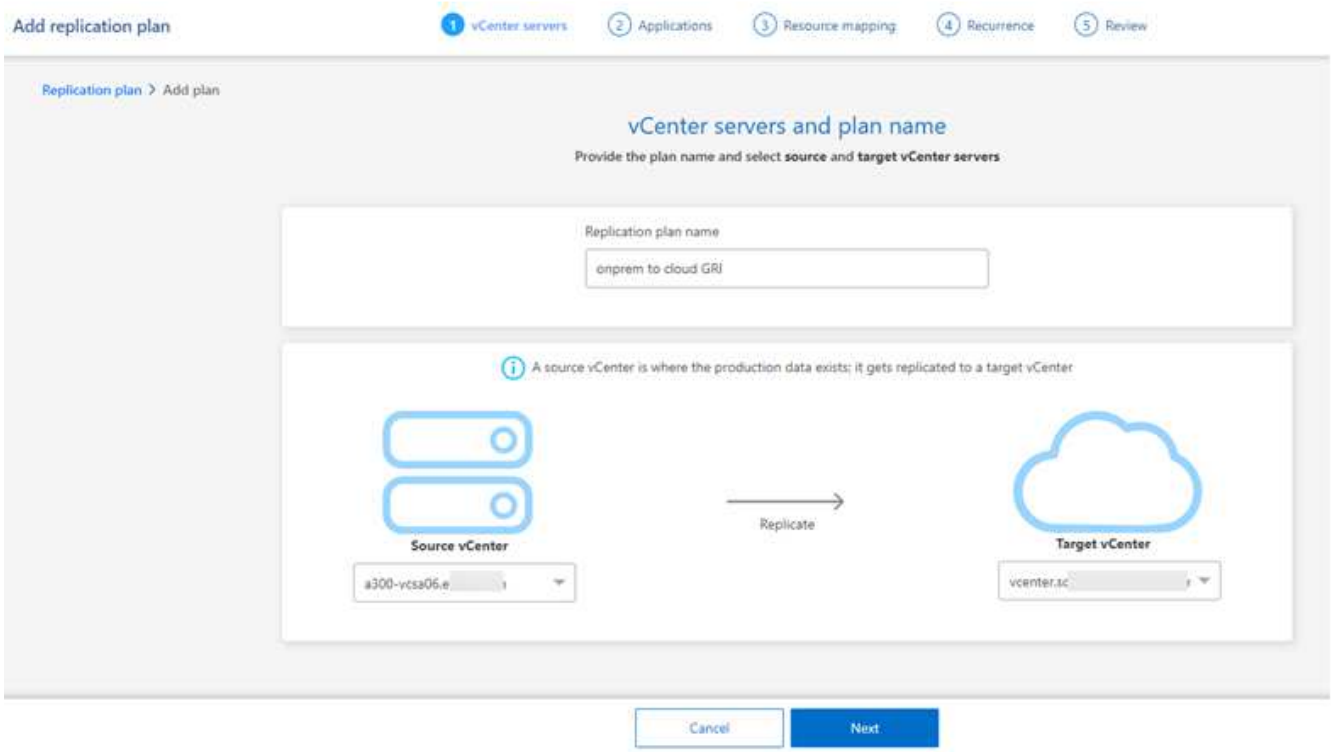
Wenn Sie in diesem Service eine SnapMirror Beziehung erstellen möchten, hätten Sie den Cluster und dessen SVM-Peering bereits außerhalb der Disaster Recovery von BlueXP eingerichtet haben müssen.

Wählen Sie vCenter-Server aus

Zuerst wählen Sie das Quell-vCenter aus und dann das Ziel-vCenter aus.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü der BlueXP Disaster Recovery **Replikationspläne** und dann **Hinzufügen** aus. Wenn Sie den Dienst gerade erst nutzen, wählen Sie im Dashboard **Replizierungsplan hinzufügen** aus.



3. Erstellen Sie einen Namen für den Replikationsplan.
4. Wählen Sie die Quell- und Ziel-vCenter aus den Listen Source und Target vCenter aus.
5. Wählen Sie **Weiter**.

Wählen Sie Anwendungen aus, die Sie replizieren und Ressourcengruppen zuweisen möchten

Im nächsten Schritt werden die erforderlichen VMs oder Datastores in funktionale Ressourcengruppen gruppiert. Mit Ressourcengruppen können Sie eine Reihe von VMs oder Datastores mit einem gemeinsamen Snapshot schützen.

Wenn Sie Anwendungen im Replizierungsplan auswählen, wird das Betriebssystem für jede VM oder jeden Datastore im Plan angezeigt. Dies ist hilfreich bei der Entscheidung, wie VMs oder Datastores in einer Ressourcengruppe gruppiert werden.

Jede Ressourcengruppe kann eine oder mehrere VMs oder Datenspeicher enthalten.

Wenn Sie Ressourcengruppen erstellen, beachten Sie die folgenden Probleme:

- Bevor Sie Datastores zu Ressourcengruppen hinzufügen, starten Sie zunächst eine manuelle Ermittlung oder eine geplante Ermittlung der VMs. Dadurch wird sichergestellt, dass die VMs erkannt und in der Ressourcengruppe aufgelistet werden. Wenn Sie keine manuelle Ermittlung auslösen, werden die VMs möglicherweise nicht in der Ressourcengruppe aufgeführt.
- Stellen Sie sicher, dass sich mindestens eine VM im Datastore befindet. Wenn sich keine VMs im Datastore befinden, wird der Datastore nicht erkannt.
- Ein einzelner Datenspeicher sollte keine VMs hosten, die durch mehr als einen Replizierungsplan geschützt sind.
- Hosten Sie keine geschützten und ungesicherten VMs auf demselben Datenspeicher. Wenn geschützte und ungesicherte VMs auf demselben Datenspeicher gehostet werden, können folgende Probleme auftreten:

- Da bei der Disaster Recovery von BlueXP SnapMirror verwendet und das System ganze ONTAP Volumes repliziert, wird die genutzte Kapazität dieses Volumes zu Lizenzierungsüberlegungen verwendet. In diesem Fall wird der von geschützten und ungeschützten VMs verbrauchte Volume-Speicherplatz in diese Berechnung einbezogen.
- Wenn für die Ressourcengruppe und die zugehörigen Datastores ein Failover am Disaster Recovery-Standort erforderlich ist, sind alle ungesicherten VMs (VMs, die nicht zur Ressourcengruppe gehören, aber auf dem ONTAP Volume gehostet werden) vom Failover-Prozess nicht mehr am Quellstandort vorhanden. Dies führt zu einem Ausfall ungeschützter VMs am Quellstandort. Darüber hinaus startet die Disaster Recovery von BlueXP diese ungeschützten VMs nicht am vCenter Failover-Standort.

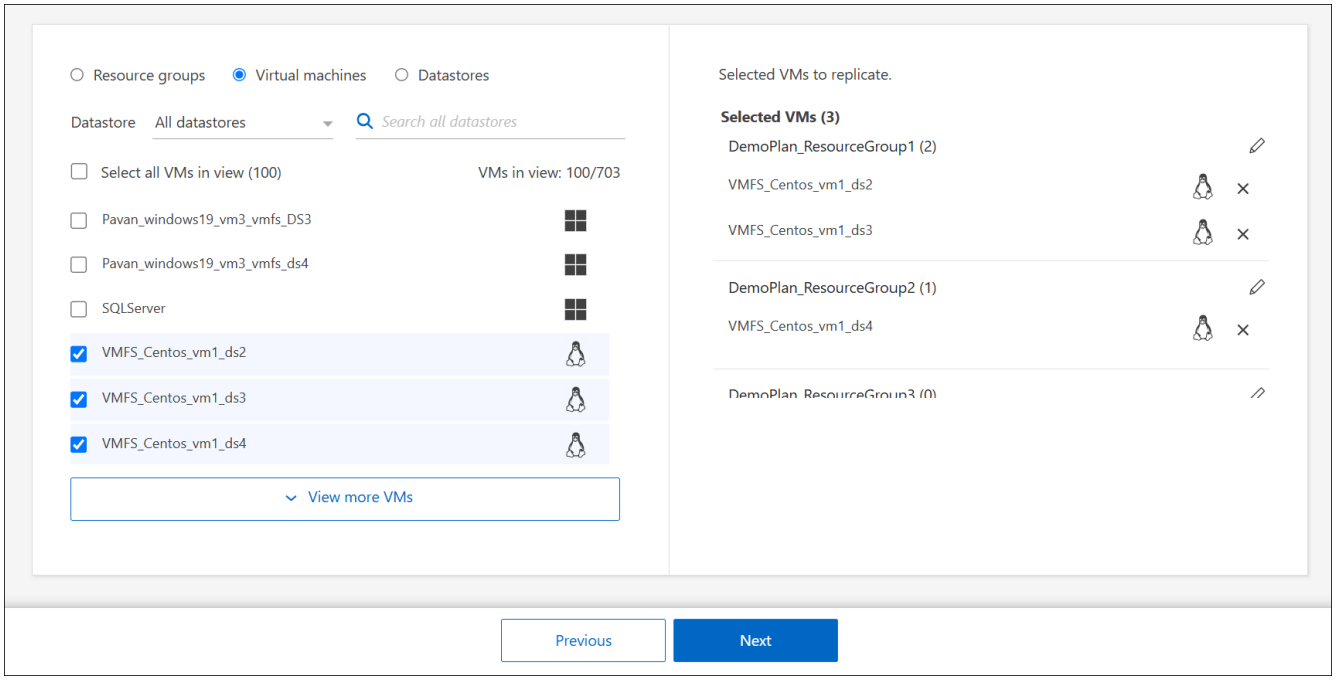
- Damit eine VM geschützt ist, muss sie in eine Ressourcengruppe aufgenommen werden.

BEST PRACTICE: Organisieren Sie Ihre VMs vor der Bereitstellung der Disaster Recovery von BlueXP , um die Ausbreitung von Datastores zu minimieren. Platzieren Sie VMs, die eine Sicherung auf einer Teilmenge von Datenspeichern benötigen, und platzieren Sie VMs, die nicht in einer anderen Teilmenge von Datenspeichern gesichert werden sollen. Mit Datastore-basiertem Schutz können Sie sicherstellen, dass die VMs auf jedem gegebenen Datastore gesichert sind.

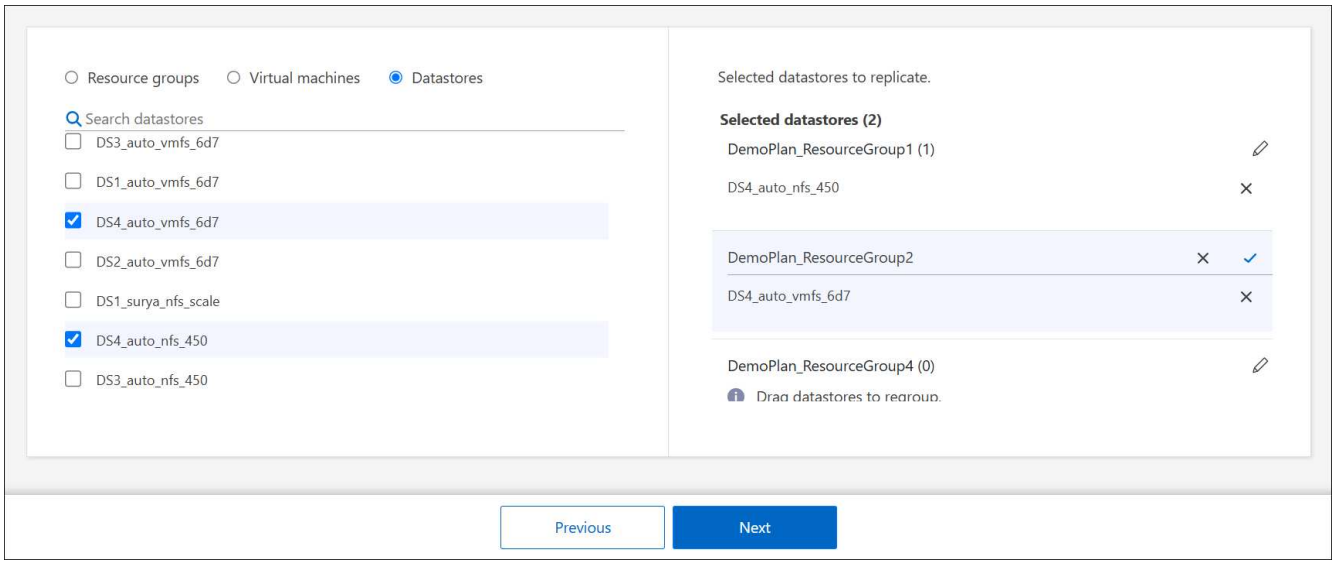
Schritte

1. Wählen Sie **Virtual Machines** oder **Datastores** aus.
2. Optional können Sie nach bestimmten VMs oder Datastores anhand des Namens suchen.
3. Wählen Sie auf der linken Seite der Seite Anwendungen die VMs oder Datastores aus, die Sie schützen möchten, und weisen Sie sie der ausgewählten Gruppe zu.

   Die ausgewählte Ressource wird automatisch zu 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 Datastores:



4. Führen Sie optional einen der folgenden Schritte aus:
   - Um den Gruppennamen zu ändern, klicken Sie auf das Gruppensymbol *Bearbeiten* .
   - 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 in die neue Gruppe.

   Um einen Datastore in eine andere Ressourcengruppe zu verschieben, heben Sie die Auswahl des unerwünschten Datastore auf und senden Sie den Replikationsplan ab. Erstellen oder bearbeiten Sie dann den anderen Replizierungsplan und wählen Sie den Datenspeicher erneut aus.

5. Wählen Sie **Weiter**.

Ordnen Sie dem Ziel Quellressourcen zu

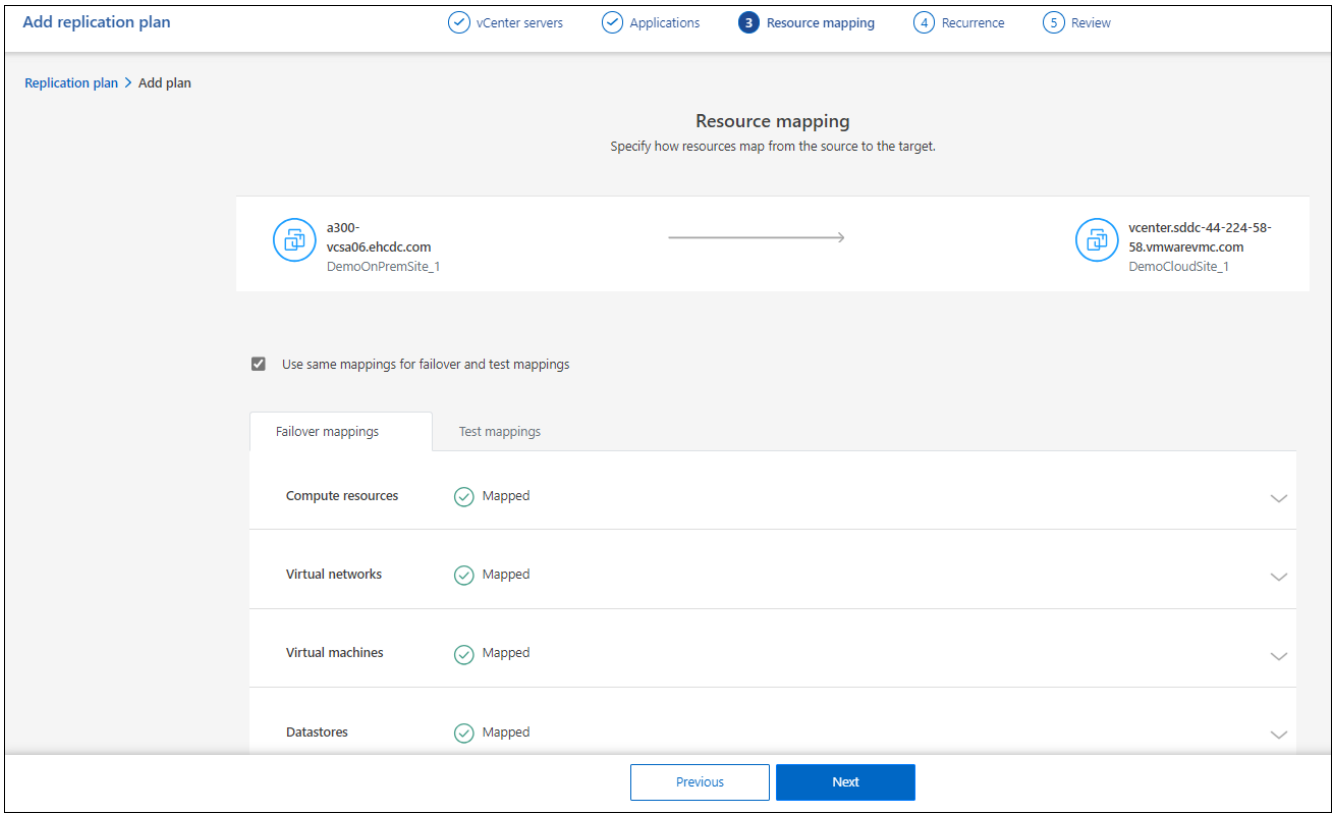
Geben Sie im Schritt „Ressourcenzuordnung“ an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden sollen. Beim Erstellen eines Replikationsplans können Sie eine Boot-Verzögerung festlegen und für jede VM im Plan bestellen. Dadurch können Sie eine Sequenz für den Start der VMs festlegen.

Bevor Sie beginnen

Wenn Sie in diesem Service eine SnapMirror Beziehung erstellen möchten, hätten Sie den Cluster und dessen SVM-Peering bereits außerhalb der Disaster Recovery von BlueXP eingerichtet haben müssen.

Schritte

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



2. Wählen Sie auf der Registerkarte Failover Mappings den Abwärtspfeil rechts neben jeder Ressource aus, und ordnen Sie die jeweiligen Ressourcen zu.

Ressourcen zuordnen > Abschnitt „Computing-Ressourcen“

Wählen Sie den Abwärtspfeil neben **Compute Resources**.

- **Quell- und Ziel-Rechenzentren**
- **Zielcluster**
- **Target Host** (optional): Nachdem Sie den Cluster ausgewählt haben, können Sie diese Information einstellen.

> Wenn ein vCenter über einen Distributed Resource Scheduler (DRS) verfügt, der für das Management mehrerer Hosts in einem Cluster konfiguriert ist, müssen Sie keinen Host auswählen. Wenn Sie einen Host auswählen, werden alle VMs von BlueXP Disaster Recovery auf dem ausgewählten Host platziert. * **Ziel-VM-Ordner** (optional): Erstellen Sie einen neuen Stammordner, um die ausgewählten VMs zu speichern.

Ressourcen zuordnen > Abschnitt Virtuelle Netzwerke

Wählen Sie auf der Registerkarte Failover Mappings 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 werden. Wählen Sie daher das entsprechende virtuelle LAN für die Zuordnung der VM aus.

Ressourcen zuordnen > Abschnitt Virtuelle Maschinen

Wählen Sie auf der Registerkarte Failover Mappings den Abwärtspfeil neben **Virtual Machines** aus.

Der Standard für die VMs ist zugeordnet. Bei der Standardzuordnung werden dieselben Einstellungen verwendet, die die VMs in der Produktionsumgebung verwenden (gleiche IP-Adresse, Subnetzmaske und Gateway).

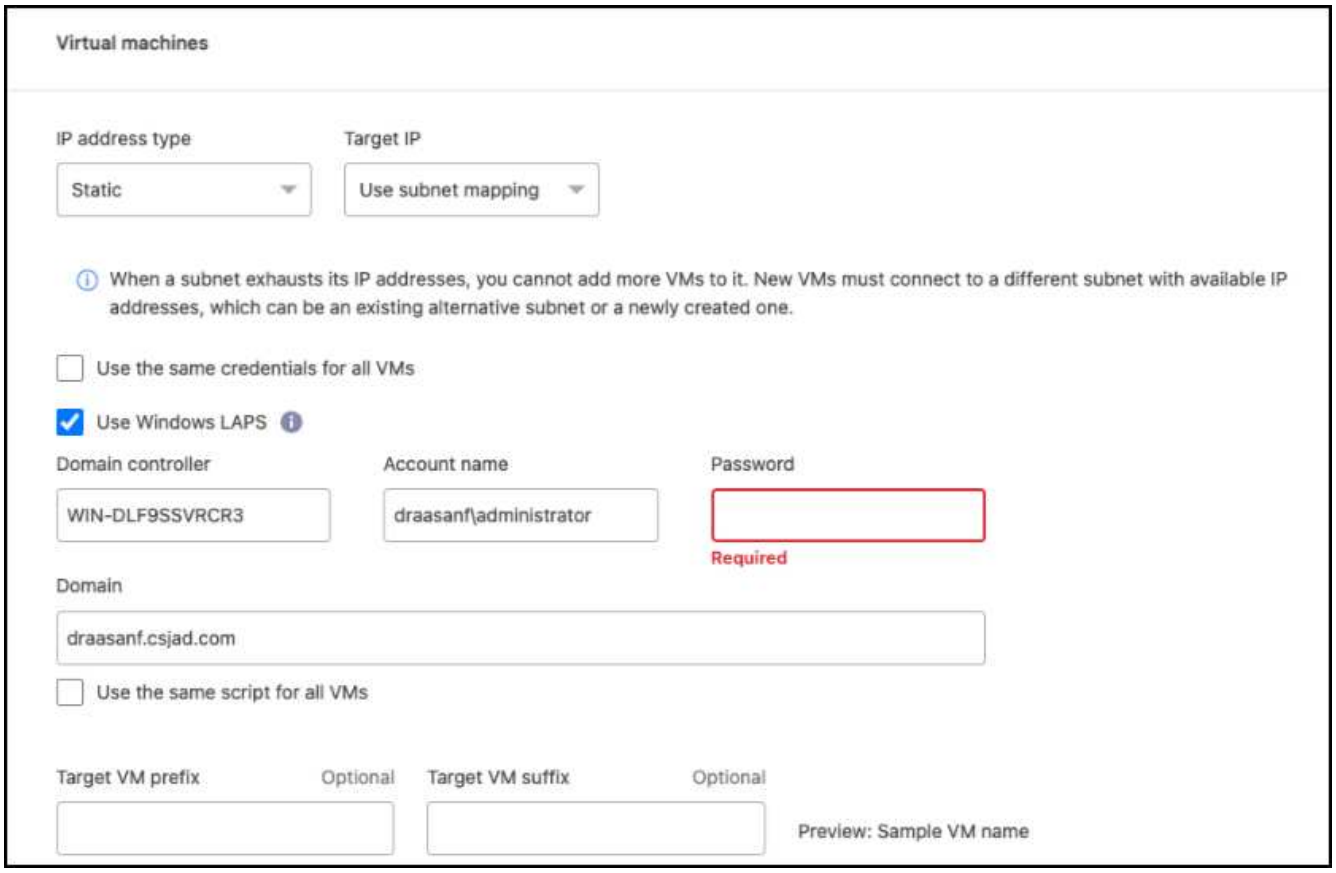
Wenn Sie Änderungen an den Standardeinstellungen vornehmen, müssen Sie das Feld Ziel-IP in „anders als die Quelle“ ändern.

> Wenn Sie Einstellungen in „anders als von der Quelle“ ändern, müssen Sie die Anmeldeinformationen für das VM-Gastbetriebssystem angeben.

In diesem Abschnitt können je nach Auswahl verschiedene Felder angezeigt werden.

- **IP-Adress-Typ**: Konfigurieren Sie die VM-Konfiguration so, dass sie den Anforderungen des virtuellen Zielnetzwerks entspricht. BlueXP Disaster Recovery bietet zwei Optionen: DHCP oder statische IP. Konfigurieren Sie für statische IPs die Subnetzmaske, das Gateway und die DNS-Server. Geben Sie darüber hinaus Anmeldedaten für VMs ein.
  - **DHCP**: Wählen Sie diese Einstellung, wenn Ihre VMs Netzwerkkonfigurationsinformationen von einem DHCP-Server beziehen sollen. Wenn Sie sich für diese Option entscheiden, geben Sie nur die Anmeldeinformationen für die VM an.
  - **Statische IP**: Wählen Sie diese Einstellung, wenn Sie IP-Konfigurationsinformationen manuell angeben möchten. Sie können eine der folgenden Optionen auswählen: Wie die Quelle, anders als die Quelle oder die Subnetzzuordnung. Wenn Sie dieselbe Auswahl wie die Quelle wählen, müssen Sie keine Anmeldeinformationen eingeben. Wenn Sie jedoch andere Informationen aus der Quelle verwenden möchten, können Sie die Anmeldeinformationen, die IP-Adresse der VM, die Subnetzmaske, das DNS und die Gateway-Informationen angeben. Die Anmeldedaten für das VM-Gastbetriebssystem sollten entweder auf globaler Ebene oder auf jeder VM-Ebene bereitgestellt werden.

    Dies ist vor allem bei der Wiederherstellung großer Umgebungen zu kleineren Ziel-Clustern oder bei Disaster-Recovery-Tests hilfreich, ohne eine 1:1-physische VMware-Infrastruktur bereitstellen zu müssen.



- Wählen Sie im Feld **Ziel-IP** eine der folgenden Optionen aus:
  - **Gleich wie Quelle**
  - **Abweichend von der Quelle**
  - **Subnetzzuordnung**: Wählen Sie diese Option, wenn Sie das Quellsubnetz einem anderen Zielsubnetz zuordnen möchten. Sie können das Quellsubnetz und anschließend das Zielsubnetz auswählen. Dies ist nützlich, wenn Sie die IP-Adresse der VM in der Zielumgebung ändern möchten.

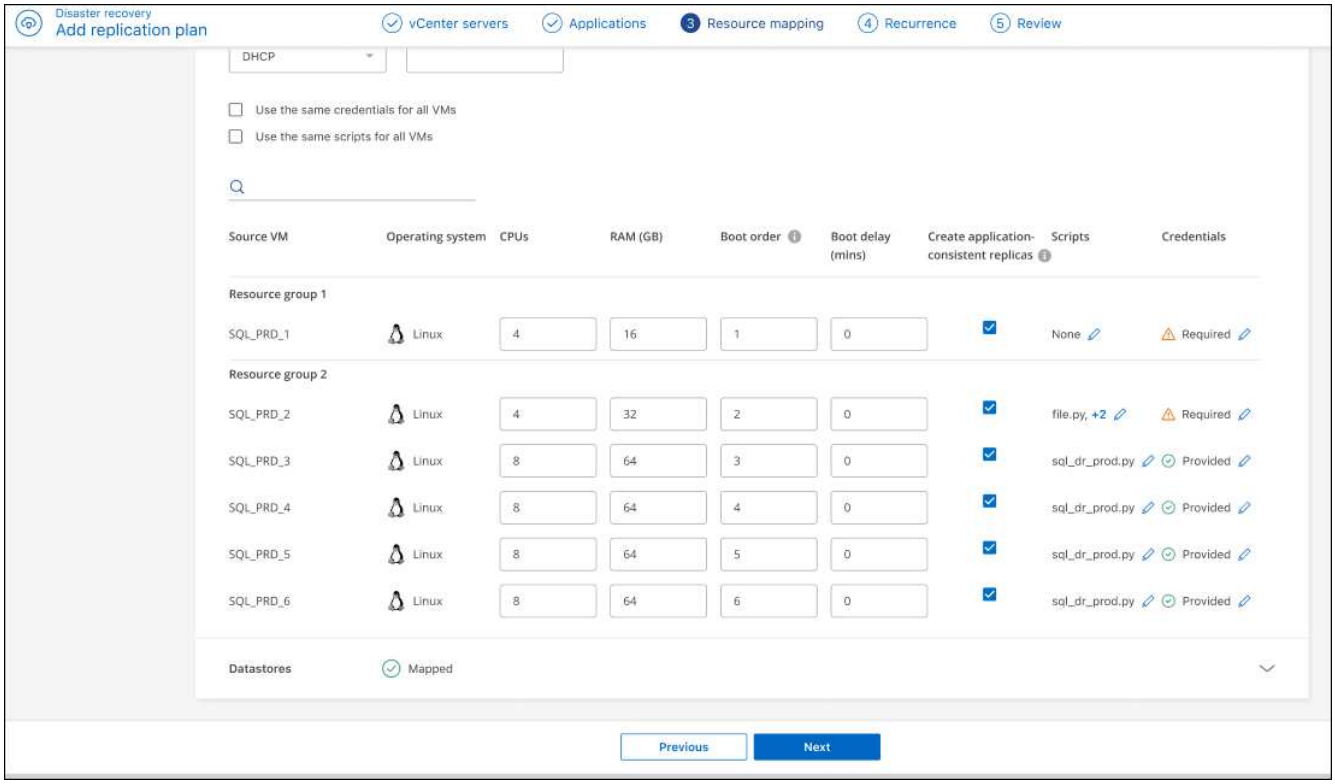
> Die Verwendung der Subnetzzuordnung ist ein optionaler zweistufiger Prozess: Fügen Sie zunächst die Subnetzzuordnung für jeden vCenter-Standort auf der Registerkarte „Standorte“ hinzu. Geben Sie anschließend im Replikationsplan an, dass Sie die Subnetzzuordnung verwenden möchten.

> Wenn zwei VMs vorhanden sind (z. B. Linux und Windows), werden nur Anmeldeinformationen für Windows benötigt.

- **Windows LAPS verwenden**: Aktivieren Sie dieses Kontrollkästchen, wenn Sie die Windows Local Administrator Password Solution (Windows LAPS) verwenden. 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 Domänencontroller-Details 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.

- **Scripts**: Sie können benutzerdefinierte Skripte im .sh-, .bat- oder .ps1-Format als Post-Failover-Prozesse einfügen. Mit benutzerdefinierten Skripts kann die BlueXP Disaster Recovery Ihr Skript nach einem Failover-Prozess ausführen. Sie können beispielsweise ein benutzerdefiniertes Skript verwenden, um alle Datenbanktransaktionen nach Abschluss des Failovers wieder aufzunehmen.
- **Ziel-VM-Präfix und Suffix**: Unter den Details der virtuellen Maschinen können Sie optional dem VM-Namen ein Präfix und Suffix hinzufügen.
- **Source VM CPU und RAM**: Unter den Details der virtuellen Maschinen können Sie optional die VM CPU und RAM Parameter anpassen.



- **Startreihenfolge**: Sie können die Startreihenfolge nach einem Failover für alle ausgewählten virtuellen Maschinen über die Ressourcengruppen hinweg ändern. Standardmäßig werden alle VMs parallel gebootet. Sie können jedoch zu diesem Zeitpunkt Änderungen vornehmen. So können Sie sicherstellen, dass alle VMs mit Ihrer Priorität ausgeführt werden, bevor VMs mit der folgenden Priorität gestartet werden.

  Alle VMs mit derselben Startauftragsnummer werden parallel gestartet.

  - Sequenzieller Start: Weisen Sie jeder VM eine eindeutige Nummer zu, um den in der zugewiesenen Reihenfolge zu booten, z. B. 1,2,3,4,5.
  - Gleichzeitiges Booten: Weisen Sie jeder VM dieselbe Zahl zu, um sie gleichzeitig zu booten, z. B. 1,1,4,2,2,3,4,1,1.
- **Boot Delay**: Passen Sie die Verzögerung in Minuten der Boot-Aktion an.

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

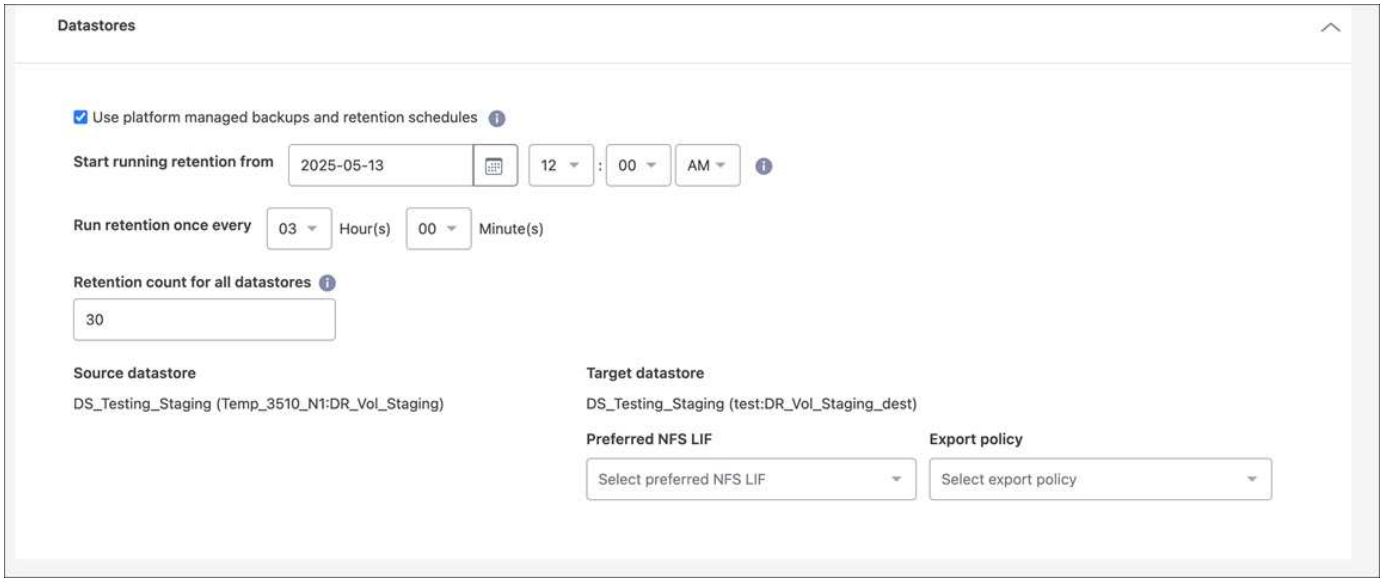
- **Erstellen Sie anwendungskonsistente Replikate**: Geben Sie an, ob anwendungskonsistente Snapshot-Kopien erstellt werden sollen. Der Service stellt die Anwendung still und erstellt dann einen Snapshot, um

einen konsistenten Status der Anwendung zu erhalten. Diese Funktion wird von Oracle unter Windows sowie von Linux und SQL Server unter Windows unterstützt.

Ressourcen zuordnen > Abschnitt Datastores

Wählen Sie den Abwärtspfeil neben **Datastores**. Je nach Auswahl der VMs werden automatisch Datastore-Zuordnungen ausgewählt.

Dieser Abschnitt kann je nach Auswahl aktiviert oder deaktiviert sein.



- **Plattform-verwaltete Backups und Aufbewahrungszeitpläne verwenden**: Wenn Sie eine externe Snapshot-Managementlösung verwenden, aktivieren Sie dieses Kontrollkästchen. BlueXP Disaster Recovery unterstützt die Verwendung externer Snapshot-Managementlösungen, wie z. B. der native Richtlinienplaner von ONTAP SnapMirror oder Integrationen durch Drittanbieter. Wenn jeder Datastore (Volume) im Replizierungsplan bereits über eine SnapMirror-Beziehung verfügt, die an anderer Stelle gemanagt wird, können Sie diese Snapshots als Wiederherstellungspunkte in der BlueXP Disaster Recovery verwenden.

  Wenn diese Option ausgewählt ist, wird für BlueXP Disaster Recovery kein Backup-Zeitplan konfiguriert. Sie müssen jedoch weiterhin einen Aufbewahrungszeitplan konfigurieren, da darüber hinaus Snapshots für Test-, Failover- und Failback-Vorgänge erstellt werden können.

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

- **Startzeit**: Geben Sie das Datum und die Uhrzeit ein, zu der Backups und die Aufbewahrung ausgeführt werden sollen.
- **Run interval**: Geben Sie das Zeitintervall in Stunden und Minuten ein. Wenn Sie beispielsweise eine Stunde eingeben, erstellt der Dienst stündlich einen Snapshot.
- **Retention count**: Geben Sie die Anzahl der Snapshots ein, die Sie behalten möchten.
- **Quell- und Zieldatenspeicher**: Wenn mehrere (Fan-out) SnapMirror-Beziehungen existieren, können Sie das zu verwendende Ziel auswählen. Wenn ein Volume bereits eine SnapMirror-Beziehung aufgebaut hat, werden die entsprechenden Quell- und Ziel-Datastores angezeigt. Wenn ein Volume nicht über eine SnapMirror-Beziehung verfügt, können Sie es jetzt erstellen. Dazu wählen Sie ein Ziel-Cluster aus, wählen eine Ziel-SVM aus und geben einen Volume-Namen an. Der Service erstellt die Volume- und SnapMirror-Beziehung.

Wenn Sie in diesem Service eine SnapMirror Beziehung erstellen möchten, hätten Sie den Cluster und dessen SVM-Peering bereits außerhalb der Disaster Recovery von BlueXP eingerichtet haben müssen.

- Wenn die VMs vom gleichen Volume und derselben SVM stammen, führt der Service einen standardmäßigen ONTAP-Snapshot durch und aktualisiert die sekundären Ziele.
- Wenn die VMs aus unterschiedlichen Volumes und derselben SVM stammen, erstellt der Service einen KonsistenzgruppenSnapshot, in dem alle Volumes eingeschlossen werden und die sekundären Ziele aktualisiert werden.
- Wenn die VMs aus verschiedenen Volumes und unterschiedlichen SVMs stammen, führt der Service eine Startphase für die Konsistenzgruppe und einen Snapshot der Commit-Phase durch, indem alle Volumes im selben oder unterschiedlichen Cluster eingeschlossen werden und die sekundären Ziele aktualisiert werden.
- Während des Failovers können Sie einen beliebigen Snapshot auswählen. Wenn Sie den neuesten Snapshot auswählen, erstellt der Service On-Demand-Backups, aktualisiert das Ziel und verwendet diesen Snapshot für das Failover.

Fügen Sie Test-Failover-Zuordnungen hinzu

Schritte

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

   Auf der Registerkarte Testzuordnungen sind die Zuordnungen für virtuelle Maschinen und Datenspeicher deaktiviert.

Sie können den gesamten Plan später testen. Derzeit richten Sie die Zuordnungen für die Testumgebung ein.

Überprüfen Sie den Replizierungsplan

Nehmen Sie sich zum Schluss einen Moment Zeit, um den Replizierungsplan zu prüfen.

Sie können den Replikationsplan später deaktivieren oder löschen.

Schritte

1. Überprüfen Sie die Informationen auf den einzelnen Registerkarten: Plandetails, Failover Mapping und VMs.
2. Wählen Sie **Plan hinzufügen**.

   Der Plan wird zur Liste der Pläne hinzugefügt.

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

Möglicherweise möchten Sie Zeitpläne zum Testen von Compliance- und Failover-Tests einrichten, um bei Bedarf sicherzustellen, dass diese korrekt funktionieren.

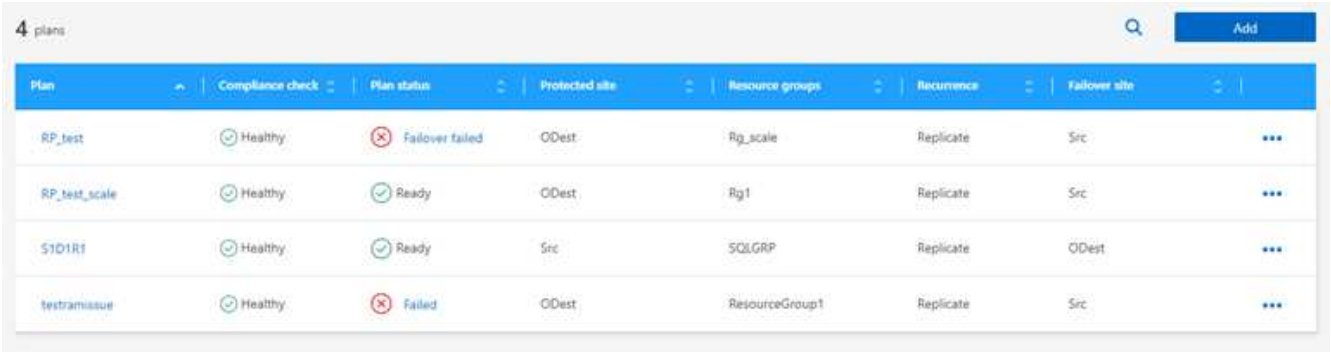
- **Auswirkungen auf die Compliance-Zeit**: Wenn ein Replikationsplan erstellt wird, erstellt der Dienst standardmäßig einen Compliance-Zeitplan. Die Standard-Compliance-Zeit beträgt 30 Minuten. Um diese Zeit zu ändern, können Sie den Zeitplan im Replikationsplan bearbeiten verwenden.
- **Auswirkungen auf Failover-Test**: Sie können einen Failover-Prozess nach Bedarf oder nach einem Zeitplan testen. Damit können Sie den Failover von virtuellen Maschinen zu einem Ziel testen, das in einem Replikationsplan angegeben ist.

  Ein Test-Failover erstellt ein FlexClone Volume, mountet den Datastore und verschiebt den Workload auf diesen Datastore. Ein Test-Failover-Vorgang wirkt sich auf Produktions-Workloads, die auf dem Teststandort verwendete SnapMirror Beziehung und geschützte Workloads aus, die weiterhin ordnungsgemäß ausgeführt werden müssen.

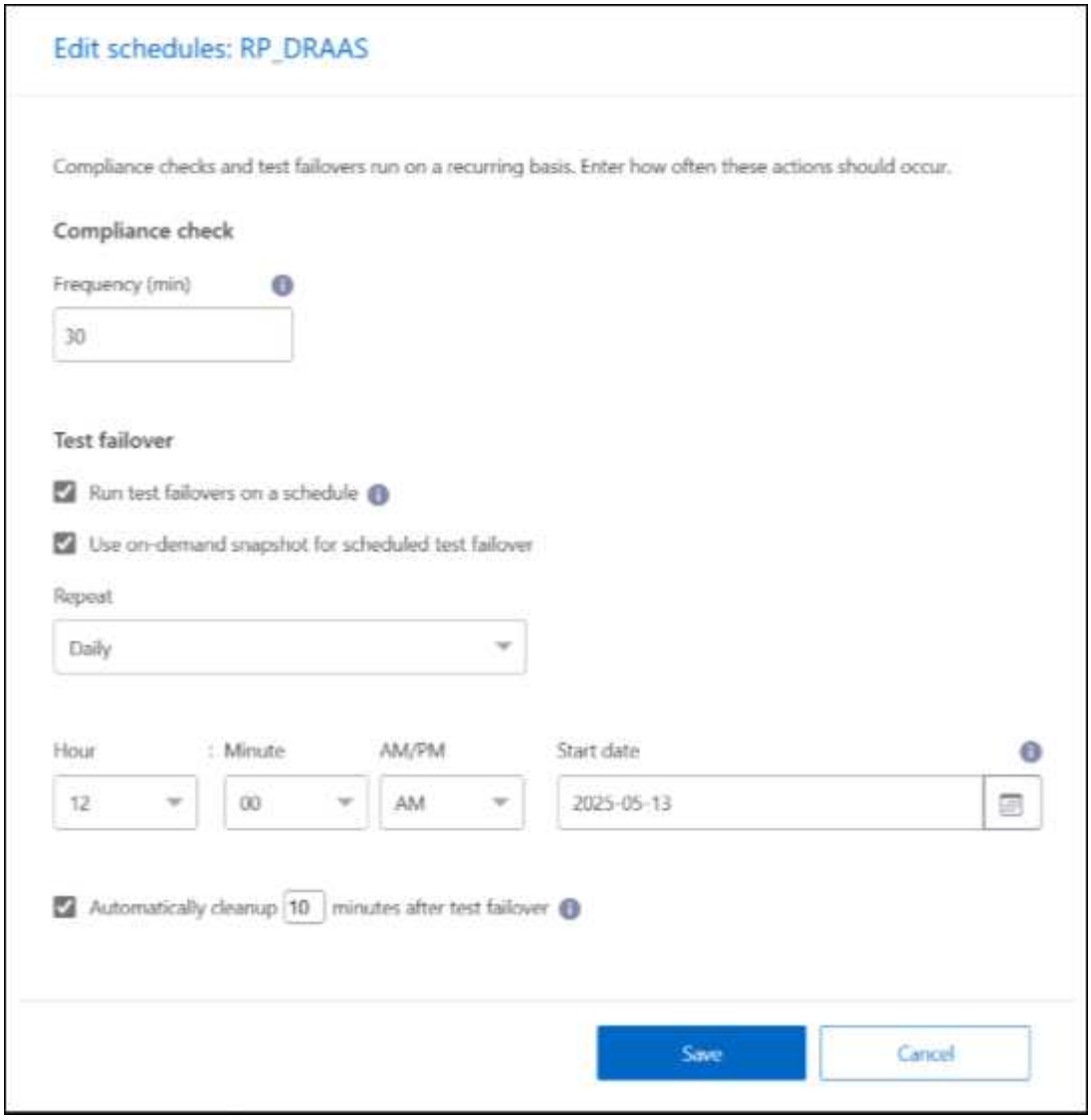
Basierend auf dem Zeitplan wird der Failover-Test ausgeführt und stellt sicher, dass Workloads an das vom Replizierungsplan angegebene Ziel verschoben werden.

Schritte

1. Wählen Sie im oberen Menü der BlueXP Disaster Recovery die Option **Replication Plans** aus.



2. Wählen Sie die Option **actions** ••• Und wählen Sie **Schichtpläne bearbeiten**.
3. Geben Sie ein, wie oft Sie in wenigen Minuten BlueXP Disaster Recovery verwenden möchten, um die Compliance von Tests zu überprüfen.
4. Um zu überprüfen, ob Ihre Failover-Tests ordnungsgemäß sind, überprüfen Sie **Failover nach einem monatlichen Zeitplan ausführen**.
   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, wenn der Test gestartet werden soll.



5. **On-Demand-Snapshot für geplanten Test-Failover verwenden**: Um einen neuen Snapshot vor dem Initiieren des automatischen Test-Failovers zu erstellen, aktivieren Sie dieses Kontrollkästchen.
6. Um die Testumgebung nach Abschluss des Failover-Tests zu bereinigen, aktivieren Sie **Automatically clean up after Test Failover** und geben Sie die Anzahl der Minuten ein, die Sie warten möchten, bevor die Bereinigung beginnt.

> Durch diesen Prozess werden die temporären VMs vom Teststandort entfernt, das erstellte FlexClone Volume gelöscht und die temporären Datenspeicher abgehängt.

7. Wählen Sie **Speichern**.

Replizieren Sie Anwendungen an einen anderen Standort mit BlueXP Disaster Recovery

Mit der Disaster Recovery von BlueXP können Sie VMware Applikationen an Ihrem Quellstandort mithilfe von SnapMirror Replizierung an einen Remote-Standort zur Disaster Recovery in der Cloud replizieren.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Notfallwiederherstellungs-Failover-Administratorrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Nachdem Sie den Disaster-Recovery-Plan erstellt haben, identifizieren Sie im Assistenten die Wiederholung und initiieren Sie eine Replizierung zu einem Disaster-Recovery-Standort. Die BlueXP Disaster Recovery überprüft alle 30 Minuten, ob die Replizierung tatsächlich gemäß dem Plan stattfindet. Sie können den Fortschritt auf der Seite Job Monitor überwachen.

Bevor Sie beginnen

Bevor Sie die Replikation starten, sollten Sie einen Replizierungsplan erstellt und zum Replizieren der Apps ausgewählt haben. Im Menü Aktionen erscheint dann die Option **replicate**.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü **Replikationspläne** aus.
3. Wählen Sie den Replikationsplan aus.
4. Wählen Sie rechts die Option **actions** aus ••• Und wählen Sie **replicate**.

Migrieren Sie Anwendungen mit BlueXP Disaster Recovery an einen anderen Standort

Mit der Disaster Recovery von BlueXP können Sie VMware Applikationen von Ihrem Quellstandort zu einem anderen Standort migrieren.

Nachdem Sie den Replizierungsplan erstellt, das erneute Auftreten im Assistenten identifiziert und die Migration initiiert haben, überprüft die BlueXP Disaster Recovery alle 30 Minuten, ob die Migration tatsächlich gemäß dem Plan erfolgt. Sie können den Fortschritt auf der Seite Job Monitor überwachen.

Bevor Sie beginnen

Bevor Sie die Migration starten, sollten Sie einen Replizierungsplan erstellt und für die Migration der Apps ausgewählt haben. Im Menü Aktionen erscheint dann die Option **Migrate**.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü **Replikationspläne** aus.
3. Wählen Sie den Replikationsplan aus.
4. Wählen Sie rechts die Option **actions** aus ••• Und wählen Sie **Migrate**.

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

Bei einem Ausfall sollte ein Failover Ihres primären lokalen VMware-Standorts auf einen anderen VMware-Standort vor Ort oder auf VMware Cloud on AWS erfolgen. Sie können

den Failover-Prozess testen, um sicherzustellen, dass er bei Bedarf erfolgreich ist.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Notfallwiederherstellungs-Failover-Administratorrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Während eines Failover wird die aktuellste SnapMirror Snapshot Kopie verwendet. Sie können auch einen bestimmten Snapshot aus einem zeitpunktgenauen Snapshot auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann hilfreich sein, wenn Sie vor einem Korruptionsereignis wie Ransomware stehen, wo die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. Die Disaster Recovery von BlueXP zeigt alle verfügbaren Zeitpunkte an.

Dieser Prozess unterscheidet sich, je nachdem, ob der Produktionsstandort in einem ordnungsgemäßen Zustand ist und Sie aus anderen Gründen als zum Ausfall der Infrastruktur ein Failover auf den Disaster-Recovery-Standort durchführen:

- Ausfall eines kritischen Produktionsstandorts, auf den kein Zugriff auf das Quell-vCenter- oder ONTAP-Cluster möglich ist: Mit BlueXP Disaster Recovery können Sie einen beliebigen verfügbaren Snapshot auswählen, der wiederhergestellt werden soll.
- Produktionsumgebung ist in gutem Zustand: Sie können entweder „jetzt einen Snapshot erstellen“ oder einen zuvor erstellten Snapshot auswählen.

Bei diesem Verfahren wird die Replikationsbeziehung unterbrochen, die vCenter Quell-VMs offline gestellt, die Volumes als Datastores im Disaster Recovery vCenter registriert, die geschützten VMs anhand der Failover-Regeln im Plan neu gestartet und das Lesen/Schreiben auf dem Zielstandort ermöglicht.

Testen Sie den Failover-Prozess

Bevor Sie das Failover starten, können Sie den Prozess testen. Durch den Test werden die Virtual Machines nicht offline geschaltet.

Während eines Failover-Tests werden vorübergehend virtuelle Maschinen erstellt. Bei der Disaster Recovery von BlueXP wird das Ziel-Volume nicht zugeordnet. Stattdessen wird ein neues FlexClone Volume aus dem ausgewählten Snapshot erstellt und ein temporärer Datenspeicher, der das FlexClone Volume sichert, den ESXi Hosts zugeordnet.

Dieser Prozess beansprucht keine zusätzliche physische Kapazität, lokal im ONTAP Storage oder auf FSX for NetApp ONTAP Storage in AWS. Das ursprüngliche Quell-Volume wird nicht geändert, und Replikatjobs können auch während der Disaster Recovery fortgesetzt werden.

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

Ein Test-Failover-Vorgang wirkt sich auf Produktions-Workloads, die auf dem Teststandort verwendete SnapMirror Beziehung und geschützte Workloads aus, die weiterhin ordnungsgemäß ausgeführt werden müssen.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü der BlueXP Disaster Recovery die Option **Replication Plans** aus.
3. Wählen Sie den Replikationsplan aus.

4. Wählen Sie rechts die Option **actions** aus ••• Und wählen Sie **Failover testen**.
5. Geben Sie auf der Seite Test Failover „Test Failover“ ein und wählen Sie **Test Failover**.
6. Nach Abschluss des Tests die Testumgebung bereinigen.

Reinigen Sie die Testumgebung nach einem Failover-Test

Nach Abschluss des Failover-Tests sollten Sie die Testumgebung bereinigen. Durch diesen Prozess werden die temporären VMs vom Teststandort, den FlexClones und die temporären Datenspeicher entfernt.

Schritte

1. Wählen Sie im oberen Menü der BlueXP Disaster Recovery die Option **Replication Plans** aus.
2. Wählen Sie den Replikationsplan aus.
3. Wählen Sie rechts die Option **actions** aus ••• Und wählen Sie **Clean Up Failover Test**.
4. Geben Sie auf der Seite Failover testen „Clean Up Failover“ ein und wählen Sie **Clean Up Failover Test**.

Führen Sie ein Failover über den Quellstandort an einen Disaster-Recovery-Standort durch

Bei einem Ausfall sollte ein Failover Ihres primären lokalen VMware-Standorts nach Bedarf zu einem anderen lokalen VMware-Standort oder zu VMware Cloud on AWS mit FSX for NetApp ONTAP erfolgen.

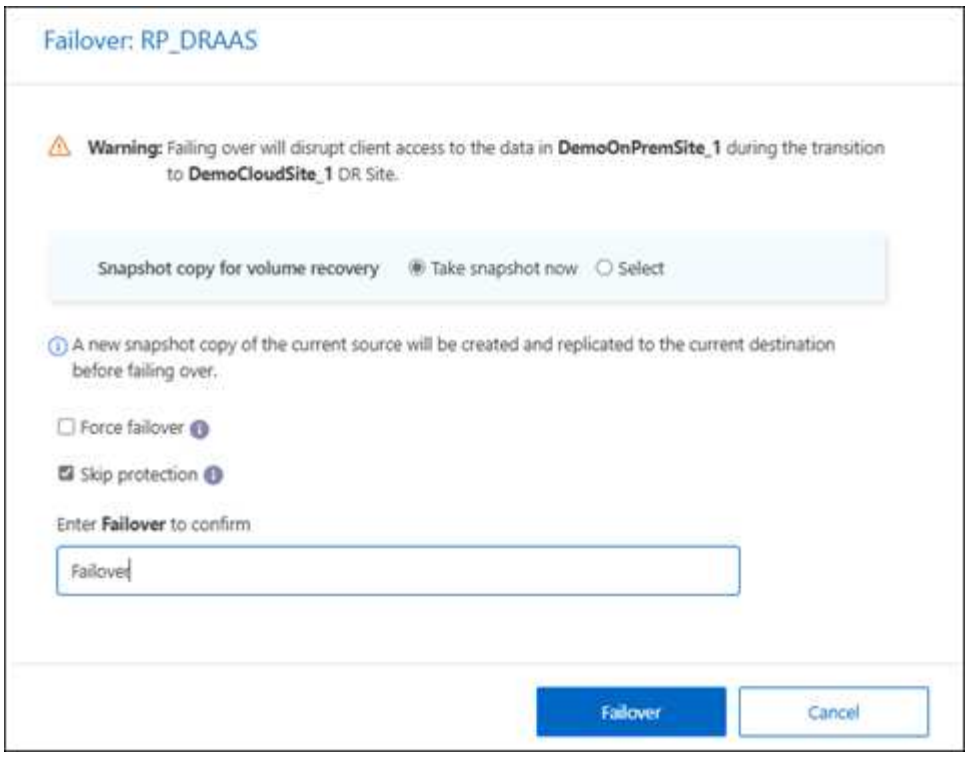
Der Failover-Prozess umfasst die folgenden Vorgänge:

- Wenn Sie den letzten Snapshot ausgewählt haben, wird die SnapMirror-Aktualisierung ausgeführt, um die letzten Änderungen zu replizieren.
- Die virtuellen Quellmaschinen sind heruntergefahren.
- Die SnapMirror Beziehung ist unterbrochen und das Zielvolume wird Lese-/Schreibzugriff gemacht.
- Basierend auf der Auswahl des Snapshots wird das aktive Dateisystem auf dem angegebenen Snapshot wiederhergestellt (zuletzt oder ausgewählt)
- Datastores werden basierend auf den im Replikationsplan erfassten Informationen erstellt und auf dem VMware- oder VMC-Cluster oder -Host gemountet.
- Die virtuellen Zielmaschinen werden registriert und basierend auf der auf der Seite Ressourcengruppen erfassten Reihenfolge betrieben.
- Die SnapMirror Beziehung wird vom Ziel zur Quell-Virtual Machine umgekehrt.

Nach dem Start des Failovers sind die wiederhergestellten VMs im vCenter des Disaster-Recovery-Standorts (Virtual Machines, Netzwerke und Datastores) zu sehen. Standardmäßig werden die virtuellen Maschinen im Ordner Workload wiederhergestellt.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü der BlueXP Disaster Recovery die Option **Replication Plans** aus.
3. Wählen Sie den Replikationsplan aus.
4. Wählen Sie rechts die Option **actions** aus ••• Und wählen Sie **Failover**.



5. Starten Sie auf der Seite Failover entweder jetzt einen Snapshot, oder wählen Sie den Snapshot für den Datastore aus, von dem aus wiederhergestellt werden soll. Die Standardeinstellung ist die neueste.

   Vor dem Failover wird ein Snapshot der aktuellen Quelle erstellt und auf das aktuelle Ziel repliziert.

6. Wählen Sie optional **Force Failover** aus, wenn das Failover auch dann erfolgen soll, wenn ein Fehler erkannt wird, der normalerweise das Failover verhindert.
7. 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 auf dem wiederhergestellten Standort weitere Vorgänge durchführen möchten, bevor Sie ihn in BlueXP Disaster Recovery wieder online schalten.

   Sie können den 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 ein Failback auf die übliche Weise initiieren.

8. Geben Sie „Failover“ in die Box ein.
9. Wählen Sie **Failover**.
10. Um den Fortschritt zu überprüfen, wählen Sie im oberen Menü **Job-Überwachung**.

Failback von Anwendungen auf die ursprüngliche Quelle mit BlueXP Disaster Recovery

Nachdem ein Notfall behoben wurde, können Sie ein Failback vom Disaster-Recovery-Standort zum Quellstandort durchführen, um den normalen Betrieb wiederherzustellen. Sie können den Snapshot auswählen, von dem Sie wiederherstellen möchten.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Notfallwiederherstellungs-Failover-Administratorrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

In diesem Workflow repliziert (synchronisiert) die Disaster Recovery von BlueXP alle Änderungen zurück auf die ursprüngliche Quell-Virtual Machine, bevor die Replizierungsrichtung umgekehrt wird. Dieser Prozess beginnt mit einer Beziehung, die das Failover zu einem Ziel abgeschlossen hat, und umfasst die folgenden Schritte:

- Am Zielstandort werden die virtuellen Maschinen ausgeschaltet und nicht registriert, und die Volumes werden nicht gemountet.
- Die SnapMirror Beziehung auf der ursprünglichen Quelle ist beschädigt, um sie lesen/schreiben zu lassen.
- Die SnapMirror Beziehung wird neu synchronisiert, um die Replizierung rückgängig zu machen.
- Die virtuellen Quellmaschinen werden eingeschaltet und registriert, und Volumes werden auf der Quelle gemountet.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü der BlueXP Disaster Recovery die Option **Replication Plans** aus.
3. Wählen Sie den Replikationsplan aus.
4. Wählen Sie rechts die Option **actions** aus ••• Und wählen Sie **Failback**.
5. Geben Sie den Namen des Replikationsplans ein, um das Failback zu bestätigen und zu starten.
6. Wählen Sie den Snapshot für den Datastore aus, von dem aus wiederhergestellt werden soll. Die Standardeinstellung ist die neueste.
7. Um den Fortschritt zu überprüfen, wählen Sie im oberen Menü **Job-Überwachung**.

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

Sie können einen schnellen Überblick über alle Ihre BlueXP-Ressourcen zur Notfallwiederherstellung erhalten oder sich jede im Detail ansehen:

- Standorte
- Ressourcengruppen
- Replizierungspläne
- Datenspeicher
- Virtual Machines

die einzelnen Aufgaben sind unterschiedliche BlueXP -Rollen erforderlich. Weitere Informationen finden Sie im Abschnitt „Erforderliche BlueXP -Rolle“ der jeweiligen Aufgabe.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

VCenter-Sites verwalten

Sie können den vCenter-Standortnamen und den Standorttyp (On-Premises oder AWS) bearbeiten.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator oder Notfallwiederherstellungsadministratorrolle.

Schritte

1. Wählen Sie im oberen Menü **Sites** aus.
2. Wählen Sie die Option **actions** Rechts neben dem vCenter-Namen und wählen Sie **Bearbeiten**.
3. Bearbeiten Sie den Namen und den Speicherort des vCenter-Standorts.

Verwalten von Ressourcengruppen

Sie können zwar eine Ressourcengruppe als Teil des Erstellens eines Replikationsplans hinzufügen, jedoch ist es möglicherweise bequemer, die Gruppen separat hinzuzufügen und später diese Gruppen im Plan zu verwenden. Sie erstellen Ressourcengruppen nach VMs oder Datastores.

Erforderliche BlueXP Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator oder Administratorrolle für Notfallwiederherstellungsanwendungen.

Sie haben folgende Möglichkeiten, eine Ressourcengruppe nach Datastores zu erstellen:

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

Sie können auch Ressourcengruppen bearbeiten und löschen.

Schritte

1. Wählen Sie im oberen Menü **Ressourcengruppen** aus.
2. Um eine Ressourcengruppe hinzuzufügen, wählen Sie **Gruppe hinzufügen**.
3. Um Aktionen mit der Ressourcengruppe durchzuführen, wählen Sie die Option **actions** aus Wählen Sie rechts eine der Optionen aus, wie z.B. **Ressourcengruppe bearbeiten** oder **Ressourcengruppe löschen**.

Verwalten von Replikationsplänen

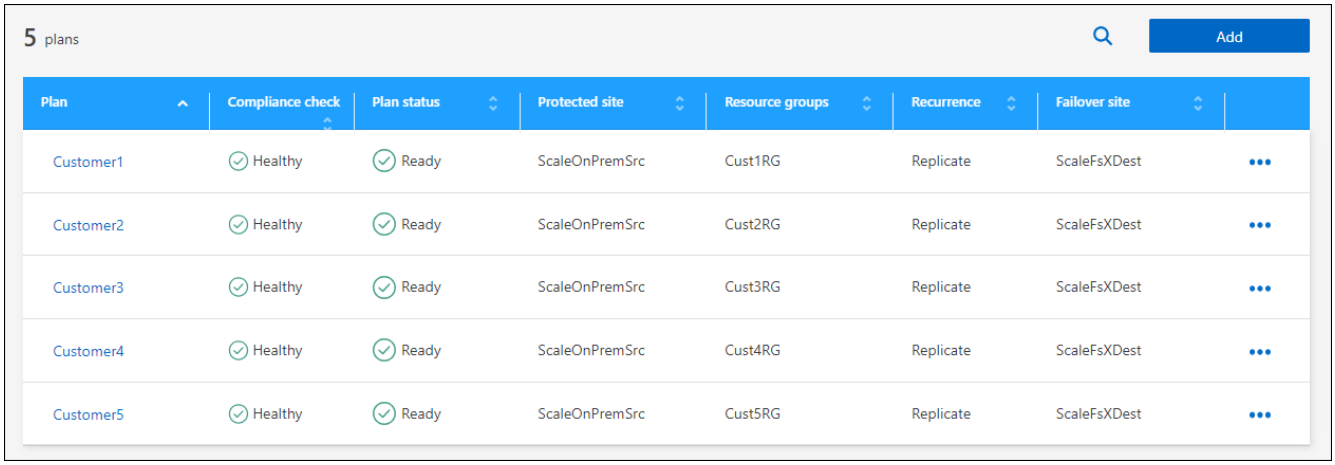
Sie können Replikationspläne deaktivieren, aktivieren und löschen. Sie können Zeitpläne ändern.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungs-Failover-Administrator oder Notfallwiederherstellungsanwendungsadministrator.

- 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 oberen Menü **Replikationspläne** aus.



2. Um die Plandetails anzuzeigen, wählen Sie die Option **actions** ••• Und wählen Sie **Plandetails anzeigen**.
3. Führen Sie einen der folgenden Schritte aus:
   - Um die Plandetails zu bearbeiten (Wiederholung ändern), wählen Sie die Registerkarte **Plandetails** und wählen Sie das Symbol **Bearbeiten** rechts.
   - Um die Ressourcenzuordnungen zu bearbeiten, wählen Sie die Registerkarte **Failover Mapping** und wählen Sie 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 den Semmelbröseln oben links „Replikationspläne“ auswählen.
5. Um Aktionen mit dem Plan auszuführen, wählen Sie aus der Liste der Replikationspläne die Option **actions** rechts neben dem Plan aus und wählen Sie eine der Optionen aus •••, wie z.B. **Edit Schedules**, **Test Failover**, **Failover**, **Failback**, **Migrate**, **Take Snapshot now**, **clean up old Snapshots**, **Disable**, **enable** oder **Delete**.
6. Um einen Test-Failover-Zeitplan festzulegen oder zu ändern oder die Prüfung der Compliance-Häufigkeit festzulegen, wählen Sie die Option **actions** ••• rechts neben dem Plan aus und wählen **Edit Schedules** aus.
   a. Geben Sie auf der Seite Zeitpläne bearbeiten ein, wie oft in Minuten die Failover-Compliance-Prüfung erfolgen soll.
   b. Prüfen Sie **Run-Test-Failovers nach einem Zeitplan**.
   c. Wählen Sie in der Option Wiederholen den täglichen, wöchentlichen oder monatlichen Zeitplan aus.
   d. Wählen Sie **Speichern**.

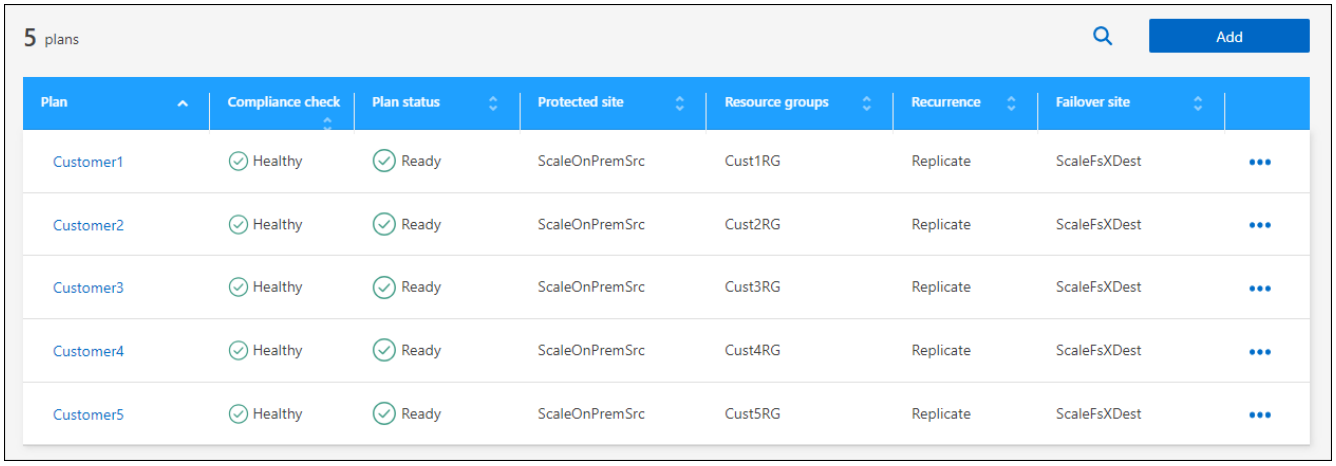
Snapshots nach Bedarf abgleichen

Sie können Snapshots abgleichen, die nicht synchron zwischen Quelle und Ziel sind. Dies kann vorkommen, wenn Snapshots auf einem Ziel außerhalb der Disaster Recovery von BlueXP gelöscht werden. Der Dienst löscht automatisch den Snapshot auf der Quelle alle 24 Stunden. Sie können dies jedoch nach Bedarf durchführen. Mit dieser Funktion können Sie sicherstellen, dass die Snapshots über alle Standorte hinweg konsistent sind.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungs-Failover-Administrator oder Notfallwiederherstellungsanwendungsadministrator.

Schritte

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



2. Wählen Sie aus der Liste der Replikationspläne rechts neben dem Plan die Option **actions** aus und wählen Sie **Snapshots abgleichen** aus •••.
3. Überprüfen Sie die Abgleichinformationen.
4. Wählen Sie **Abgleichen**.

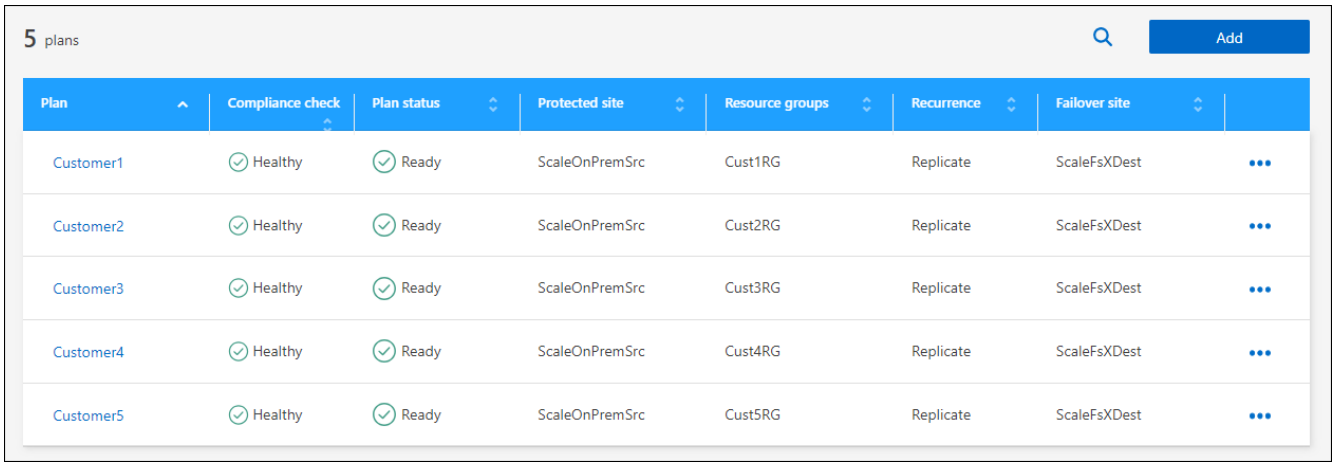
Löschen Sie einen Replikationsplan

Sie können einen Replikationsplan löschen, wenn Sie ihn nicht mehr benötigen. Wenn Sie einen Replizierungsplan löschen, können Sie auch die vom Plan erstellten primären und sekundären Snapshots löschen.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungs-Failover-Administrator oder Notfallwiederherstellungsanwendungsadministrator.

Schritte

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



2. Wählen Sie die Option **actions** ••• rechts neben dem Plan aus und wählen Sie **Delete**.
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**.

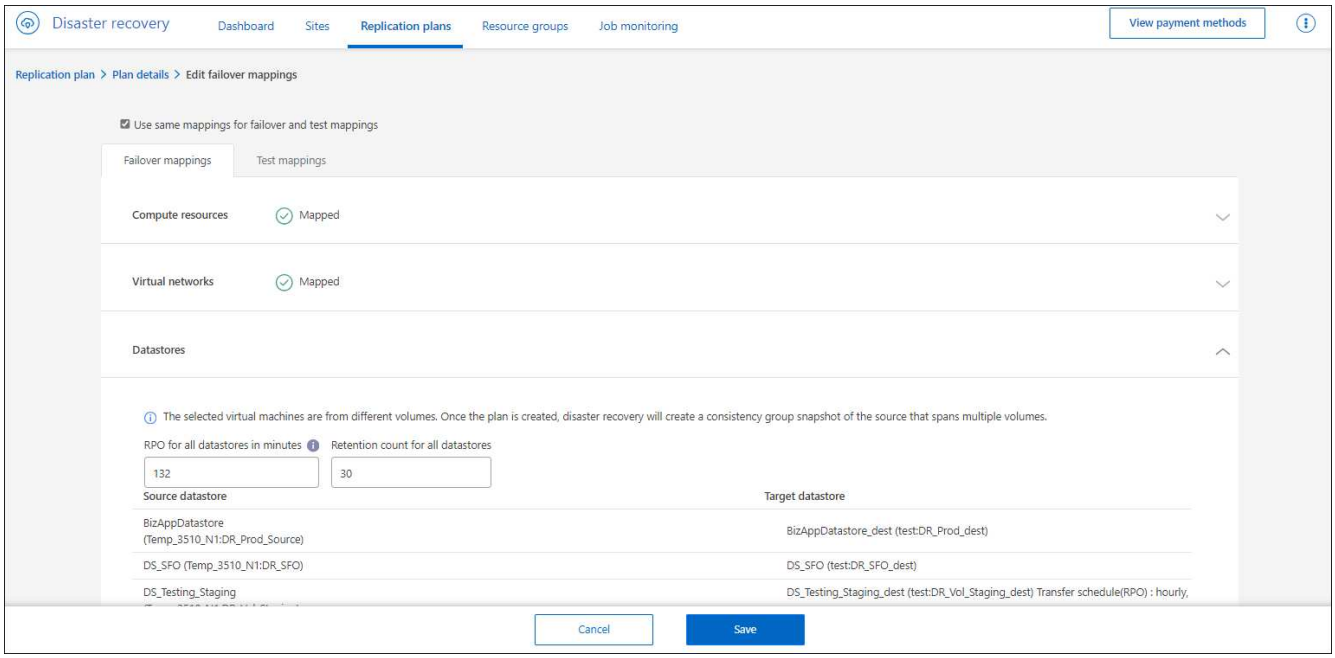
Anzahl der Aufbewahrungsfristen für Failover-Zeitpläne ändern

Sie können ändern, wie viele Datastores beibehalten werden.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungs-Failover-Administrator oder Notfallwiederherstellungsanwendungsadministrator.

Schritte

1. Wählen Sie im oberen Menü **Replikationspläne** aus.
2. Wählen Sie den Replikationsplan aus, klicken Sie auf die Registerkarte **Failover Mapping** und klicken Sie auf das Bleistiftsymbol **Bearbeiten**.
3. Klicken Sie auf den Pfeil **Datastores**, um ihn zu erweitern.



4. Ändern Sie den Wert der Aufbewahrungszahl im Replikationsplan.
5. Wenn der Replikationsplan ausgewählt ist, wählen Sie das Menü Aktionen aus, wählen Sie *alte Snapshots bereinigen“ aus, um alte Snapshots auf dem Ziel zu entfernen, die der neuen Aufbewahrungszahl entsprechen.

Anzeigen von Datenspeicherinformationen

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

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Disaster

Recovery-Administrator, Disaster Recovery-Failover-Administrator, Disaster Recovery-Anwendungsadministrator oder Disaster Recovery-Viewer-Rolle.

Schritte

1. Wählen Sie im oberen Menü **Dashboard**.
2. Wählen Sie das vCenter in der Standortzeile aus.
3. Wählen Sie **Datastores**.
4. Anzeigen der Datenspeicherinformationen.

Zeigen Sie Informationen zu virtuellen Maschinen an

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

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Disaster Recovery-Administrator, Disaster Recovery-Failover-Administrator, Disaster Recovery-Anwendungsadministrator oder Disaster Recovery-Viewer-Rolle.

Schritte

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

Überwachen Sie BlueXP-Notfallwiederherstellungsjobs

Sie können alle BlueXP-Notfallwiederherstellungsjobs überwachen und ihren Fortschritt bestimmen.

Jobs anzeigen

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungsanwendungsadministrator oder Notfallwiederherstellungsbetrachterrolle.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü **Job-Überwachung**.
3. Untersuchen Sie alle Jobs im Zusammenhang mit Operationen und überprüfen Sie deren Zeitstempel und Status.
4. Um Details zu einem bestimmten Job anzuzeigen, wählen Sie diese Zeile aus.
5. Um Informationen zu aktualisieren, wählen Sie **Aktualisieren**.

Abbrechen eines Jobs

Wenn ein Job in Bearbeitung ist oder sich in der Warteschlange befindet und Sie nicht möchten, dass er fortgesetzt wird, können Sie ihn abbrechen. Sie können einen Job abbrechen, wenn er im gleichen Status bleibt und Sie den nächsten Vorgang in der Warteschlange freigeben möchten. Sie können einen Job abbrechen, bevor es zu einer Zeitabsage kommt.

Erforderliche BlueXP -Rolle Organisationsadministrator, Ordner- oder Projektadministrator, Notfallwiederherstellungsadministrator, Notfallwiederherstellungs-Failover-Administrator oder Notfallwiederherstellungsanwendungsadministrator.

"Erfahren Sie mehr über Benutzerrollen und Berechtigungen bei der BlueXP disaster recovery". "Erfahren Sie mehr über BlueXP-Zugriffsrollen für alle Dienste".

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Protection** > **Disaster Recovery** aus.
2. Wählen Sie im oberen Menü **Job-Überwachung**.
3. Notieren Sie sich auf der Seite Job Monitor die ID des Jobs, den Sie abbrechen möchten.

   Der Job muss sich im Status „in Bearbeitung“ oder „in Warteschlange“ befinden.
4. Wählen Sie in der Spalte Aktionen die Option **Auftrag abbrechen** aus.

Erstellen Sie BlueXP-Notfallwiederherstellungsberichte

Durch die Überprüfung der BlueXP-Notfallwiederherstellungsberichte können Sie Ihre Notfallwiederherstellungsvorbereitung analysieren. Vordefinierte Berichte enthalten eine Zusammenfassung der Failover-Tests, Details zum Replizierungsplan und Jobdetails für alle Standorte innerhalb eines Kontos der letzten sieben Tage.

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

Der Download-Link ist sechs Stunden gültig.

Schritte

1. Wählen Sie in der linken Navigationsleiste von BlueXP **Schutz** > **Disaster Recovery** > **Replikationspläne** aus.
2. Wählen Sie oben auf der Seite **Bericht erstellen** aus.
3. Wählen Sie das Dateiformat und den Zeitraum innerhalb der letzten 7 Tage aus.
4. Wählen Sie **Erstellen**.

   Die Anzeige des Berichts kann einige Minuten dauern.
5. Um einen Bericht herunterzuladen, wählen Sie **Download Report** aus und wählen ihn im Download-Ordner des Administrators aus.

Referenz

Für die Disaster Recovery von BlueXP sind vCenter Berechtigungen erforderlich

Das vCenter Konto muss über mindestens einen Satz vCenter Berechtigungen verfügen, damit die Disaster Recovery von BlueXP ihre Services ausführen kann, wie zum Beispiel das Registrieren und Deregistrieren von Datastores, das Starten und Stoppen von VMs sowie das Neukonfigurieren von Virtual Machines (VMs). Die folgende Tabelle führt alle erforderlichen Berechtigungen für das BlueXP Disaster Recovery und Schnittstellen zu einem vCenter Cluster auf.

Typ	Berechtigungsname	Beschreibung
* Datastore*	Datastore: Datastore konfigurieren	Verwenden Sie, um einen Datastore zu konfigurieren.
	Datastore: Datastore entfernen	Verwenden Sie, um einen Datastore zu entfernen.
Virtuelle Maschine	Virtuelle Maschine.Konfiguration.Einstellungen ändern	Verwenden Sie, um allgemeine VM-Einstellungen zu ändern.
	Virtuelle Maschine.Konfiguration.Ändern Sie die Geräteeinstellungen	Mit können Sie die Eigenschaften eines vorhandenen Geräts ändern.
	Virtuelle Maschine.Konfiguration.Neu laden vom Pfad	Dient zum Ändern eines VM-Konfigurationspatches unter Beibehaltung der Identität der VM. Lösungen wie VMware vCenter Site Recovery Manager verwenden diesen Vorgang, um die Identifikation von VMs während Failover und Failback aufrecht zu erhalten.
	Virtuelle Maschine.Konfiguration.Umbenennen	Verwenden Sie, um eine VM umzubenennen oder die zugeordneten Nodes einer VM zu ändern.
	Virtuelle Maschine.Konfiguration.Zurücksetzen der Gastinformationen	Verwenden Sie diese Option, um die Informationen zum Gastbetriebssystem für eine VM zu bearbeiten.
	Virtuelle Maschine.Konfiguration.Speicher ändern	Verwenden Sie diese Funktion, um die der VM zugewiesene Speichermenge zu ändern.

Typ	Berechtigungsname	Beschreibung
	Virtual Machine.Configuration.Ändern der CPU-Anzahl	Mit können Sie die Anzahl der virtuellen CPUs ändern.
Virtual Machine Guest	Virtual Machine: Gastbetrieb. Änderungen Des Gastbetriebs	Aktiviert VM-Gastvorgänge, die Änderungen an einem Gastbetriebssystem in einer VM umfassen, wie beispielsweise das Übertragen einer Datei an die VM.
Interaktion Mit Virtuellen Maschinen	Virtuelle Maschine.Interaktion.Ausschalten	Zum Ausschalten einer eingeschalteten VM. Mit diesem Vorgang wird das Gastbetriebssystem heruntergefahren.
	Virtuelle Maschine.Interaktion.Einschalten	Verwenden Sie, um eine ausgeschalteten VM einzuschalten und eine angehaltene VM wieder aufzunehmen.
	Virtual Machine.Interaction.VMware Tools installieren	Verwenden Sie zum Mounten und Unmounten des CD-Installationsprogramms für VMware Tools als CD-ROM für das Gastbetriebssystem.
Virtuelle Maschineninventar	Virtuelle Maschine.Inventar.Neue erstellen	Dient zum Erstellen einer VM und Zuweisen von Ressourcen für deren Ausführung.
	Virtuelle Maschine.Bestandsaufnahme.Registrieren	Verwenden Sie diese Anwendung, um eine vorhandene VM zu einem vCenter-Server- oder Hostbestand hinzuzufügen.
	Virtuelle Maschine.Bestandsaufnahme.Registrierung aufheben	Verwenden Sie diese Anwendung, um die Registrierung einer VM von einem vCenter-Server oder Host-Inventar aufzuheben.
Status Der Virtuellen Maschine	Virtual Machine: Snapshot-Management: Erstellen Sie einen	Dient zum Erstellen eines Snapshots aus dem aktuellen Status der VM.
	Virtual Machine: Snapshot-Management: Snapshot Entfernen	Verwenden Sie, um einen Snapshot aus dem Snapshot-Verlauf zu entfernen.
	Virtual Machine: Snapshot-Management: Auf Snapshot zurücksetzen	Verwenden Sie, um die VM in den Zustand zu versetzen, in dem sie bei einem bestimmten Snapshot war.

Rollenbasierter Zugriff auf Funktionen der BlueXP disaster recovery

Die BlueXP 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 die BlueXP disaster recovery sind.

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

Diese Rollen sind spezifisch für die BlueXP disaster recovery und sind nicht dieselben wie die Plattformrollen, die in BlueXP verwendet werden. Weitere Informationen zu allen Rollen der BlueXP -Plattform finden Sie unter "Die BlueXP -Installations- und Administrationsdokumentation".

In der folgenden Tabelle sind die Aktionen aufgeführt, die jede BlueXP disaster recovery 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.
Kostenlos testen	Ja.	Nein	Nein	Nein
Beginnen Sie mit der Erkennung von Workloads	Ja.	Nein	Nein	Nein
Lizenzinformationen anzeigen	Ja.	Ja.	Ja.	Ja.
Lizenz aktivieren	Ja.	Nein	Ja.	Nein
Auf der Registerkarte „Sites“:				
Websites anzeigen	Ja.	Ja.	Ja.	Ja.
Websites hinzufügen, ändern oder löschen	Ja.	Nein	Nein	Nein
Auf der Registerkarte Replikationspläne:				
Anzeigen von Replikationsplänen	Ja.	Ja.	Ja.	Ja.

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
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 Failovern	Ja.	Ja.	Nein	Nein
Durchführen von Failbacks	Ja.	Ja.	Nein	Nein
Migrationen durchführen	Ja.	Ja.	Nein	Nein
Auf der Registerkarte „Ressourcengruppen“:				
Anzeigen von Ressourcengruppen	Ja.	Ja.	Ja.	Ja.
Erstellen, Ändern oder Löschen von Ressourcengruppen	Ja.	Nein	Ja.	Nein
Auf der Registerkarte „Jobüberwachung“:				
Jobs anzeigen	Ja.	Nein	Ja.	Ja.
Aufträge abbrechen	Ja.	Ja.	Ja.	Nein

Verwenden Sie BlueXP Disaster Recovery mit Amazon EVS

Einführung der BlueXP-Notfallwiederherstellung mit Amazon Elastic VMware Service und Amazon FSx für NetApp ONTAP

Kunden setzen für ihre Produktions-Rechenlasten zunehmend auf virtualisierte Infrastrukturen, beispielsweise auf VMware vSphere. Da diese virtuellen Maschinen (VMs) für ihre Unternehmen immer wichtiger werden, müssen sie vor den gleichen Katastrophen geschützt werden wie ihre physischen Rechenressourcen. Die derzeit angebotenen Disaster-Recovery-Lösungen (DR) sind komplex, teuer und ressourcenintensiv. NetApp, der größte Storage-Anbieter für virtualisierte Infrastrukturen, hat ein großes Interesse daran, die VMs seiner Kunden genauso zu schützen wie

ONTAP-Storage-Daten aller Art. Um dieses Ziel zu erreichen, hat NetApp den Disaster-Recovery-Service BlueXP entwickelt.

DIESE DOKUMENTATION ZU AMAZON EVS DIENT ALS TECHNOLOGIEVORSCHAU. Mit diesem Vorschauangebot behält sich NetApp das Recht vor, Angebotsdetails, Inhalte und Zeitpläne vor der allgemeinen Verfügbarkeit zu ändern.

Eine der größten Herausforderungen bei jeder DR-Lösung besteht darin, die zusätzlichen Kosten für Anschaffung, Konfiguration und Wartung zusätzlicher Rechen-, Netzwerk- und Speicherressourcen allein für die Bereitstellung einer DR-Replikations- und Wiederherstellungsinfrastruktur zu bewältigen. Eine beliebte Option zum Schutz kritischer virtueller Ressourcen vor Ort ist die Nutzung von in der Cloud gehosteten virtuellen Ressourcen als DR-Replikations- und Wiederherstellungsinfrastruktur. Amazon ist ein Beispiel für eine solche Lösung, die kostengünstige Ressourcen bereitstellt, die mit 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 sowie die vertraute VMware-Software und -Tools. Dadurch können Amazon EVS vCenter als Erweiterung Ihrer virtuellen Infrastruktur vor Ort integriert werden.

Amazon EVS bietet zwar integrierte Speicherressourcen, die Nutzung nativer Speicherlösungen kann jedoch die Effektivität für Unternehmen mit hohen Speicherlasten beeinträchtigen. In diesen Fällen bietet die Kombination von Amazon EVS mit Amazon FSx für NetApp ONTAP-Speicher (Amazon FSxN) eine flexiblere Speicherlösung. Wenn Sie NetApp ONTAP-Speicherlösungen vor Ort zum Hosten Ihrer VMware-Infrastruktur nutzen, profitieren Sie durch die Verwendung von Amazon EVS mit FSx für ONTAP zudem von erstklassigen Dateninteroperabilitäts- und Sicherheitsfunktionen zwischen Ihren lokalen und Cloud-Infrastrukturen.

Weitere Informationen zu Amazon FSX for NetApp ONTAP finden Sie unter "Erste Schritte mit Amazon FSX für NetApp ONTAP".

Lösungsübersicht zur BlueXP-Notfallwiederherstellung mit Amazon EVS und Amazon FSs für NetApp ONTAP

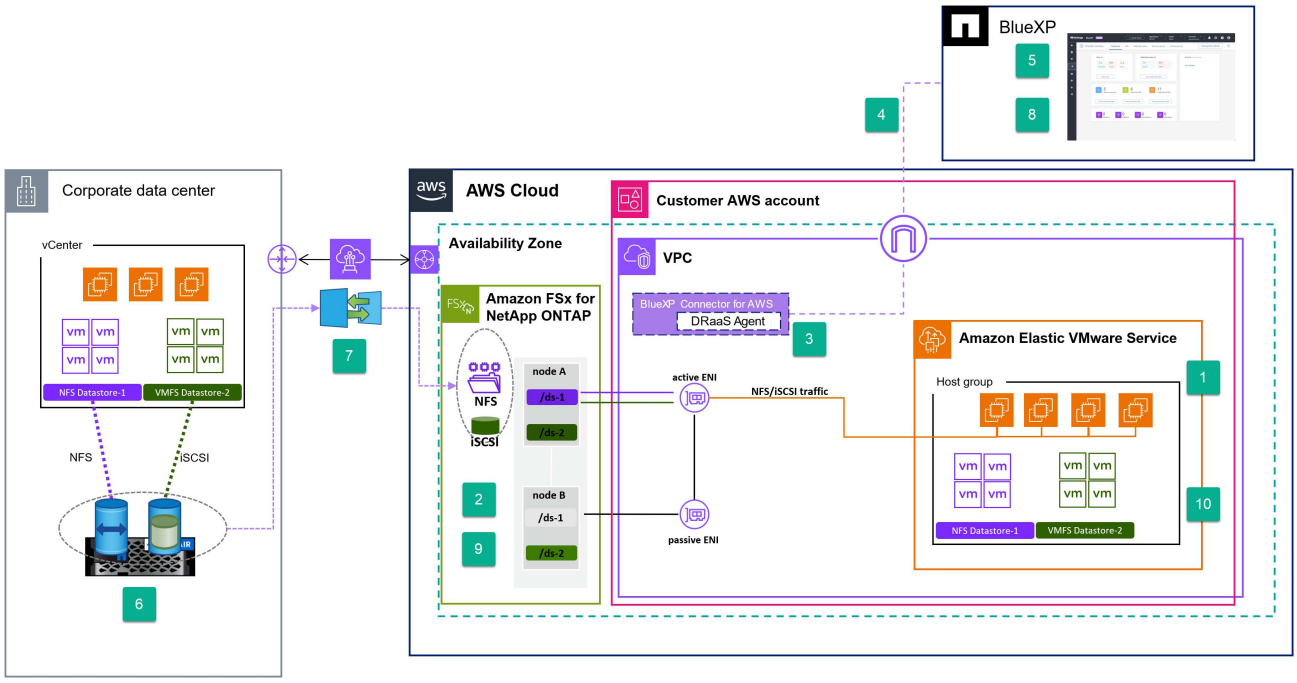
BlueXP Disaster Recovery ist ein Mehrwertdienst, der in der BlueXP Software-as-a-Service-Umgebung gehostet wird und auf der BlueXP-Kernarchitektur basiert. Mehrere Hauptkomponenten bilden den DR-Dienst für den VMware-Schutz innerhalb von BlueXP.

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

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

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

Übersicht über die Notfallwiederherstellung von BlueXP 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 for ONTAP-Dateisystem wird in derselben AZ wie die Amazon EVS-Bereitstellung bereitgestellt. Die Verbindung des Dateisystems mit Amazon EVS erfolgt entweder direkt über eine Elastic Network Interface (ENI), eine VPC-Peer-Verbindung oder ein AmazonTransit Gateway.
3. Der NetApp BlueXP Connector ist in Ihrer VPC installiert. Der BlueXP Connector hostet mehrere Datenverwaltungsdienste (Agenten), darunter den BlueXP Disaster Recovery Agent, der die Notfallwiederherstellung (DR) der VMware-Infrastruktur sowohl in Ihren lokalen physischen Rechenzentren als auch auf Ihren von Amazon AWS gehosteten Ressourcen verwaltet.
4. Der BlueXP-Disaster-Recovery-Agent kommuniziert sicher mit dem in der BlueXP-Cloud gehosteten Dienst, um Aufgaben zu empfangen, und verteilt diese Aufgaben an die entsprechenden lokalen und von AWS gehosteten vCenter- und ONTAP-Speicherinstanzen.
5. Sie erstellen einen Replikationsplan mithilfe der in der Cloud gehosteten BlueXP-UI-Konsole und geben dabei die zu schützenden VMs, die Häufigkeit des Schutzes dieser VMs und die Verfahren an, die ausgeführt werden müssen, um diese VMs im Falle eines Failovers vom lokalen Standort neu zu starten.
6. Der Replikationsplan bestimmt, welche vCenter-Datenspeicher die geschützten VMs hosten und welche ONTAP-Volumes diese Datenspeicher hosten. Falls im FSx for ONTAP-Cluster noch keine Volumes vorhanden sind, werden diese von BlueXP Disaster Recovery automatisch erstellt.
7. Für jedes identifizierte Quell-ONTAP-Volume wird eine SnapMirror-Beziehung zu jedem von FSx für ONTAP gehosteten Ziel-ONTAP-Volume erstellt und ein Replikationszeitplan wird basierend auf dem vom Benutzer im Replikationsplan bereitgestellten RPO erstellt.
8. Im Falle eines Ausfalls der primären Site leitet ein Administrator einen manuellen Failover-Prozess innerhalb der BlueXP-Konsole ein und wählt ein Backup aus, das als Wiederherstellungspunkt verwendet werden soll.
9. Der BlueXP Disaster Recovery Agent aktiviert die von FSx für ONTAP gehosteten Datenschutzvolumes.
10. Der Agent registriert jedes aktivierte FSx für ONTAP-Volume beim Amazon EVS vCenter, registriert jede geschützte VM beim Amazon EVS vCenter und startet jede gemäß den im Replikationsplan enthaltenen vordefinierten Regeln.

Installieren Sie den BlueXP Connector für die BlueXP-Notfallwiederherstellung

Ein BlueXP Connector ist eine NetApp-Software, die in Ihrer Cloud oder Ihrem lokalen Netzwerk ausgeführt wird. Er führt die Aktionen aus, die BlueXP zur Verwaltung Ihrer Dateninfrastruktur benötigt. Der Connector fragt die BlueXP Disaster Recovery-Software als Serviceebene ständig nach den erforderlichen Aktionen ab.

Für den BlueXP Disaster Recovery Service orchestrieren die ausgeführten Aktionen VMware vCenter-Cluster und ONTAP-Speicherinstanzen mithilfe nativer APIs für den jeweiligen Dienst, um den Schutz von Produktions-VMs vor Ort zu gewährleisten. Der Connector kann zwar an jedem Ihrer Netzwerkstandorte installiert werden, für die BlueXP Disaster Recovery empfehlen wir jedoch die Installation am DR-Standort. Dadurch wird sichergestellt, dass die cloudbasierte BlueXP-Konsolenoberfläche im Falle eines Ausfalls des primären Standorts weiterhin Kontakt zum Connector hat und den Wiederherstellungsprozess innerhalb dieses DR-Standorts orchestrieren kann.

Um den Dienst zu nutzen, installieren Sie den Connector im Standardmodus. Weitere Informationen zu den verschiedenen Connector-Installationsarten finden Sie unter "Erfahren Sie mehr über die Bereitstellungsmodi von BlueXP | NetApp Dokumentation" .

Obwohl der Connector für die Nutzung des Dienstes unerlässlich ist, hängen die Installationsschritte von Ihren Anforderungen und Ihrer Netzwerkkonfiguration ab. Spezifische Installationsanweisungen gehen über den Rahmen dieser Informationen hinaus.

Die einfachste Methode zur Installation eines Connectors mit Amazon AWS ist die Verwendung des AWS Marketplace. Weitere Informationen zur Connector-Installation über den AWS Marketplace finden Sie unter "Erstellen eines Connectors aus dem AWS Marketplace | NetApp-Dokumentation" .

Konfigurieren Sie die BlueXP-Notfallwiederherstellung für Amazon EVS

Übersicht: BlueXP-Notfallwiederherstellung für Amazon EVS konfigurieren

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

- "Voraussetzungen für Amazon EVS mit BlueXP Disaster Recovery"
- "Fügen Sie ONTAP-Speicher-Arrays zur BlueXP-Notfallwiederherstellung hinzu"
- "Aktivieren Sie die BlueXP-Notfallwiederherstellung für Amazon EVS"
- "Fügen Sie vCenter-Sites zur BlueXP-Notfallwiederherstellung hinzu"
- "Fügen Sie vCenter-Cluster zur BlueXP-Notfallwiederherstellung hinzu"

Voraussetzungen für Amazon EVS mit BlueXP Disaster Recovery

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

Gehen Sie insbesondere wie folgt vor:

- Erstellen Sie ein vCenter-Benutzerkonto mit den spezifischen VMware-Berechtigungen, die für die Notfallwiederherstellung von BlueXP 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 BlueXP-Disaster-Recovery-spezifisches Benutzerkonto erstellen. Eine Liste der erforderlichen Berechtigungen finden Sie unter "Für die Disaster Recovery von BlueXP sind vCenter Berechtigungen erforderlich" .

- Stellen Sie sicher, dass sich alle vCenter-Datenspeicher, die durch die Notfallwiederherstellung von BlueXP 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 für NetApp ONTAP nicht der Fall.

- Stellen Sie sicher, dass Ihr Amazon EVS vCenter mit einem Amazon FSx für 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 die Verwendung von AWS Direct Connect, AWS Private Link oder einem AWS Site-to-Site VPN.

Fügen Sie der BlueXP-Arbeitsumgebung für Amazon EVS mit BlueXP Disaster Recovery lokale Arrays hinzu

Bevor Sie die Notfallwiederherstellung von BlueXP verwenden, müssen Sie der BlueXP-Arbeitsumgebung lokale und in der Cloud gehostete Speicherinstanzen hinzufügen.

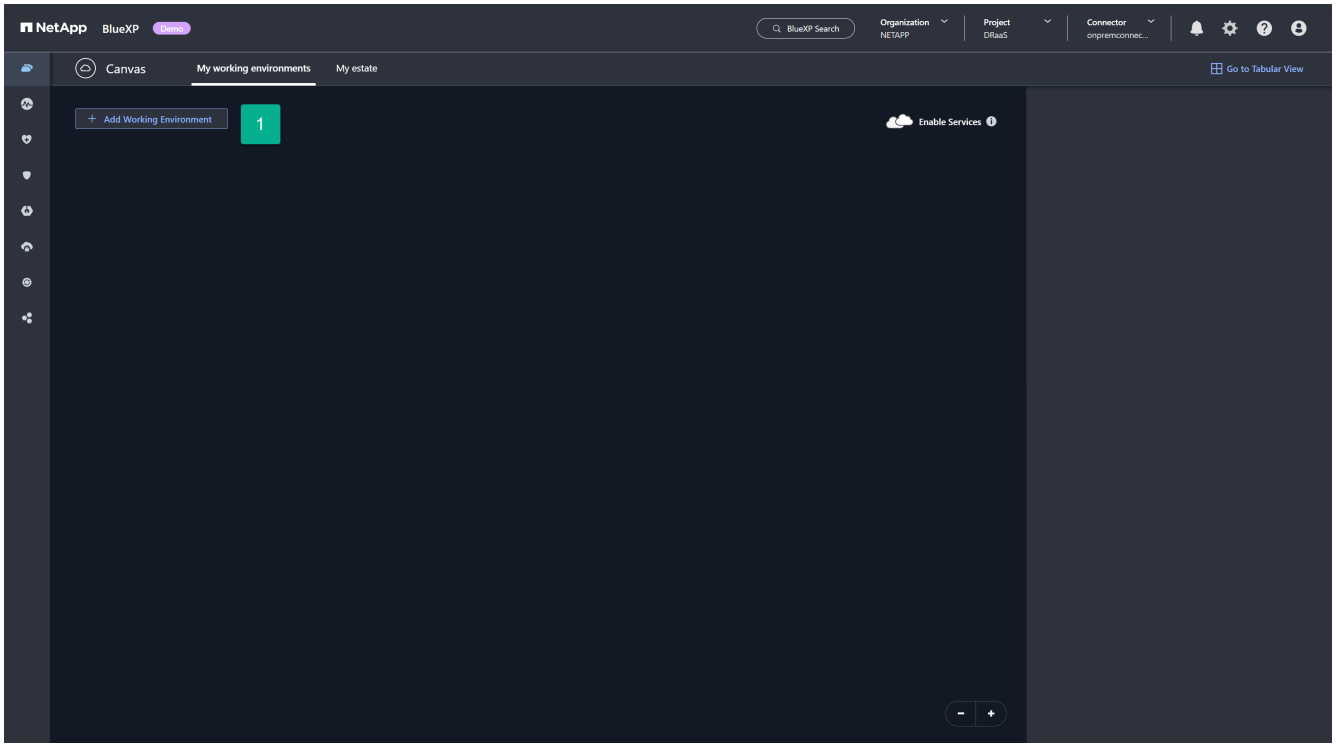
Sie müssen Folgendes tun:

- Fügen Sie Ihrer BlueXP-Arbeitsumgebung lokale Arrays hinzu.
- Fügen Sie Ihrer BlueXP-Arbeitsumgebung Amazon FSx für NetApp ONTAP (FSx für ONTAP)-Instanzen hinzu.

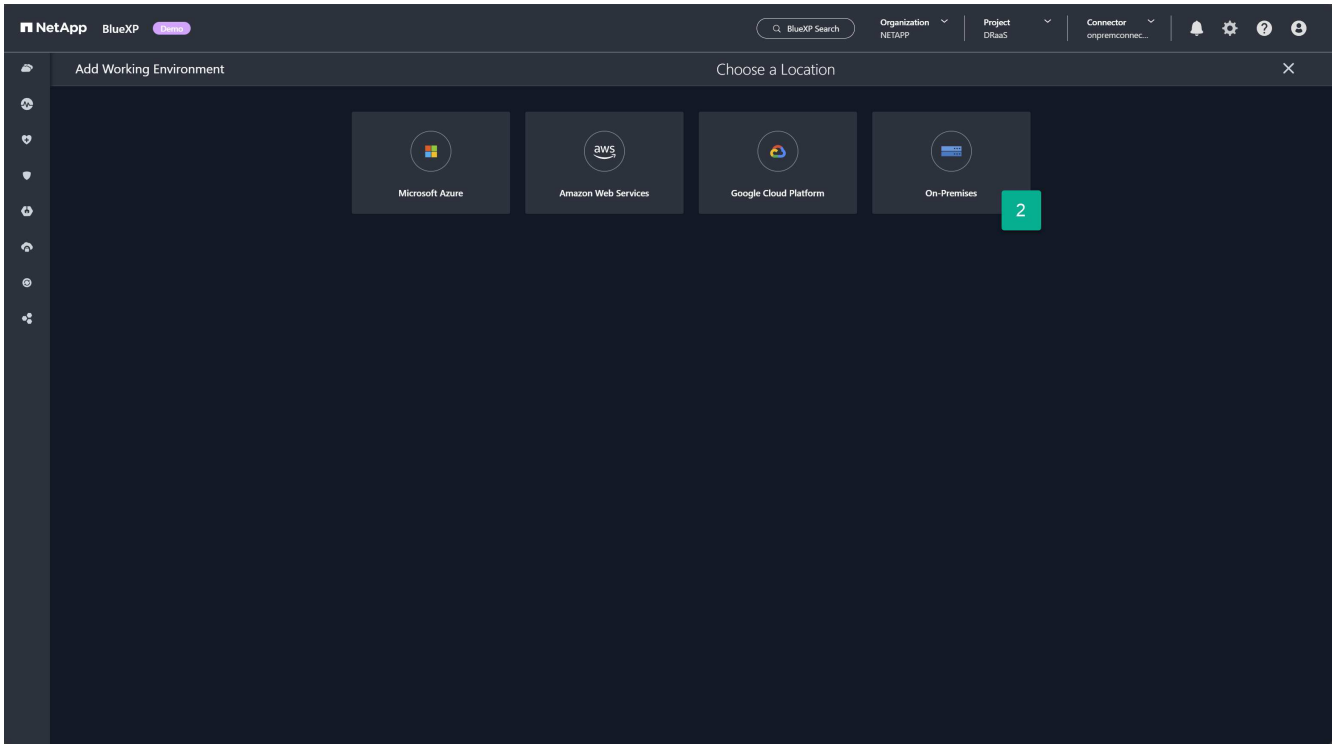
Fügen Sie der BlueXP-Arbeitsumgebung lokale Speicher-Arrays hinzu

Fügen Sie Ihrer BlueXP-Arbeitsumgebung lokale ONTAP-Speicherressourcen hinzu.

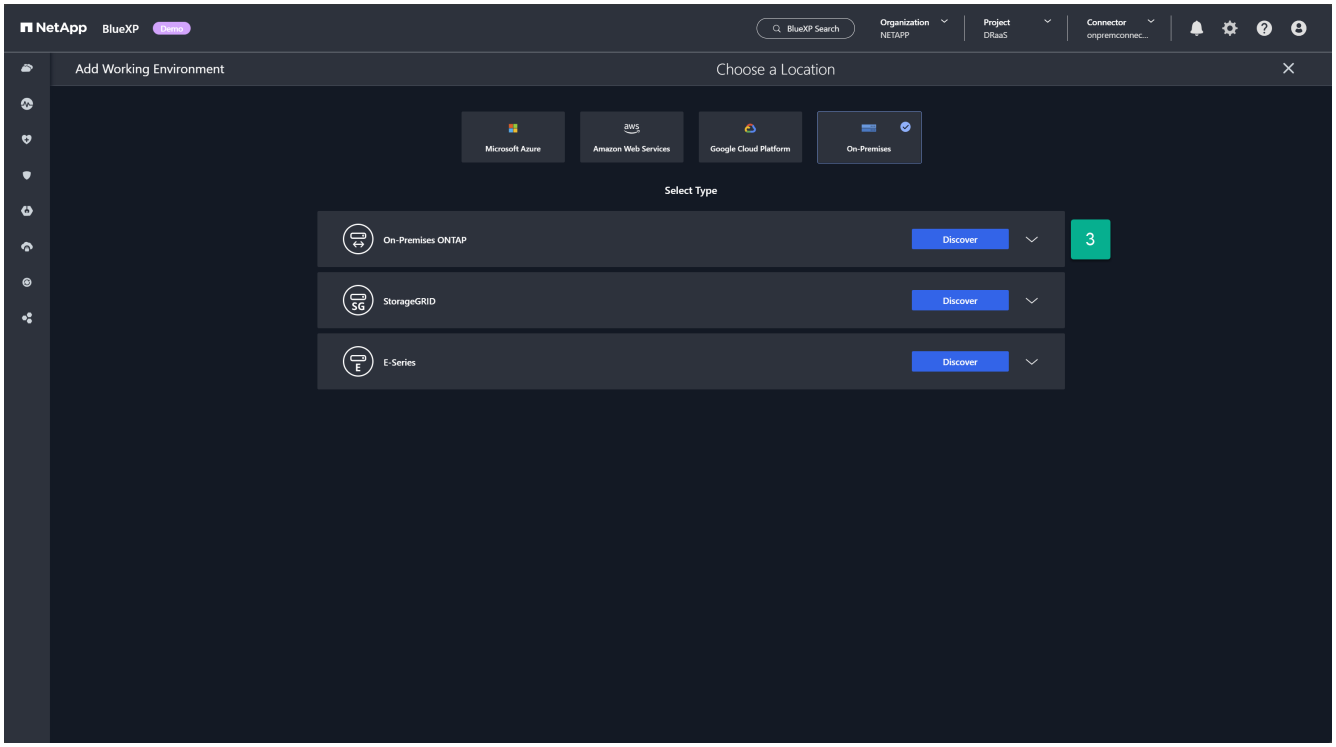
1. Wählen Sie im BlueXP Canvas **Arbeitsumgebung hinzufügen** aus.



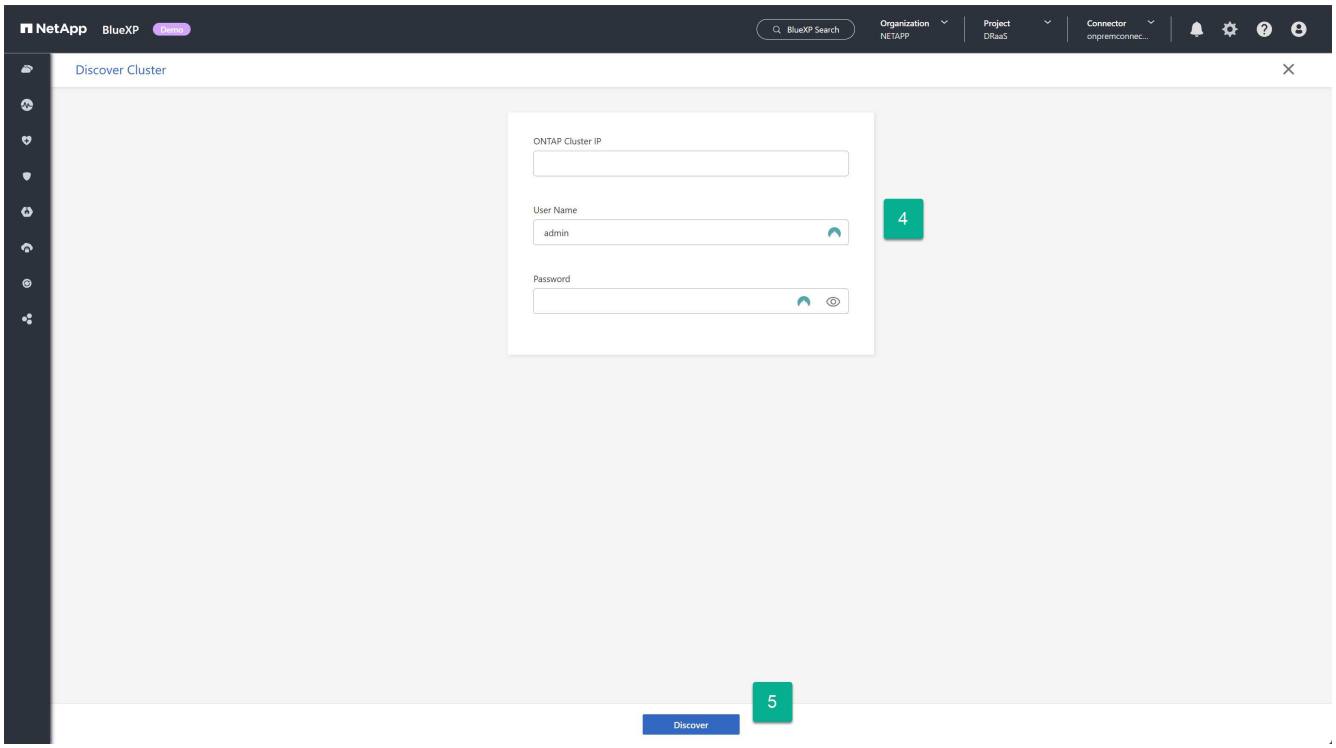
2. Wählen Sie auf der Seite „Arbeitsumgebung hinzufügen“ die Karte **On-Premises** aus.



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.

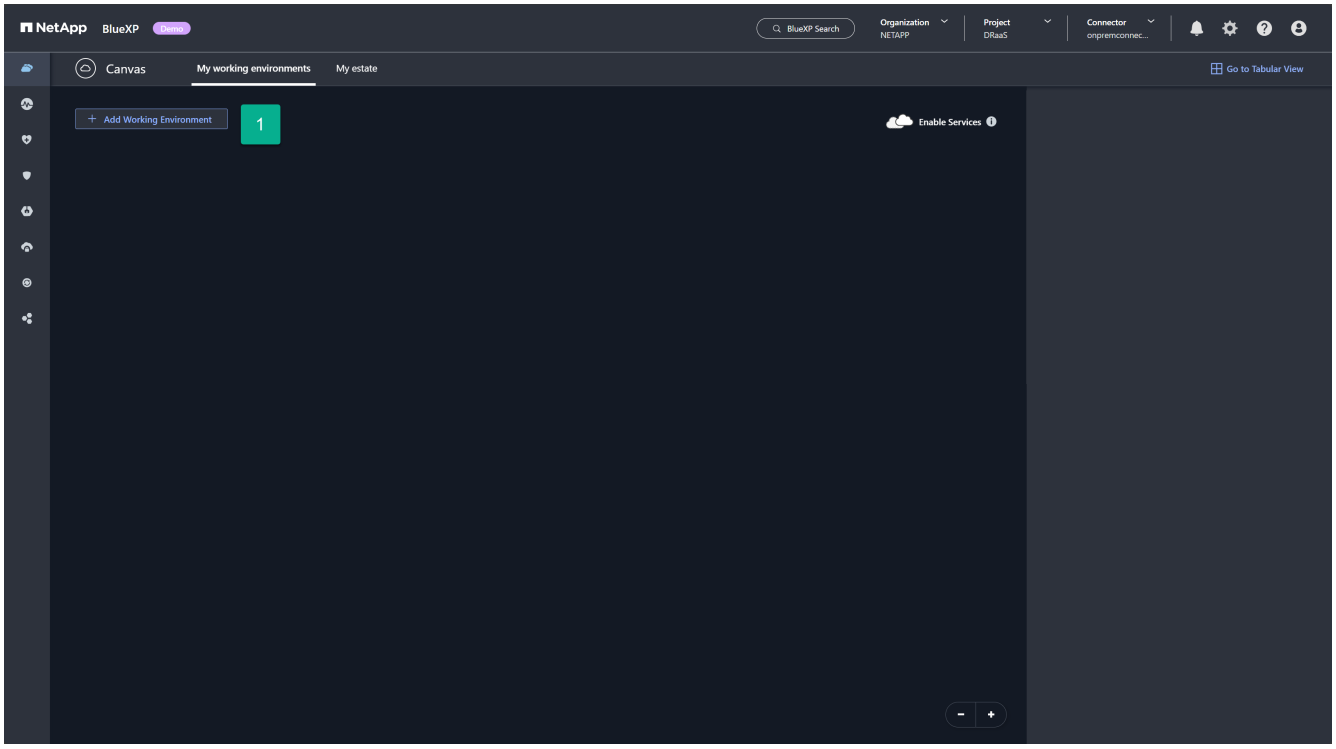


6. Wiederholen Sie die Schritte 1 bis 5 für jedes ONTAP-Array, das vCenter-Datenspeicher hosten wird.

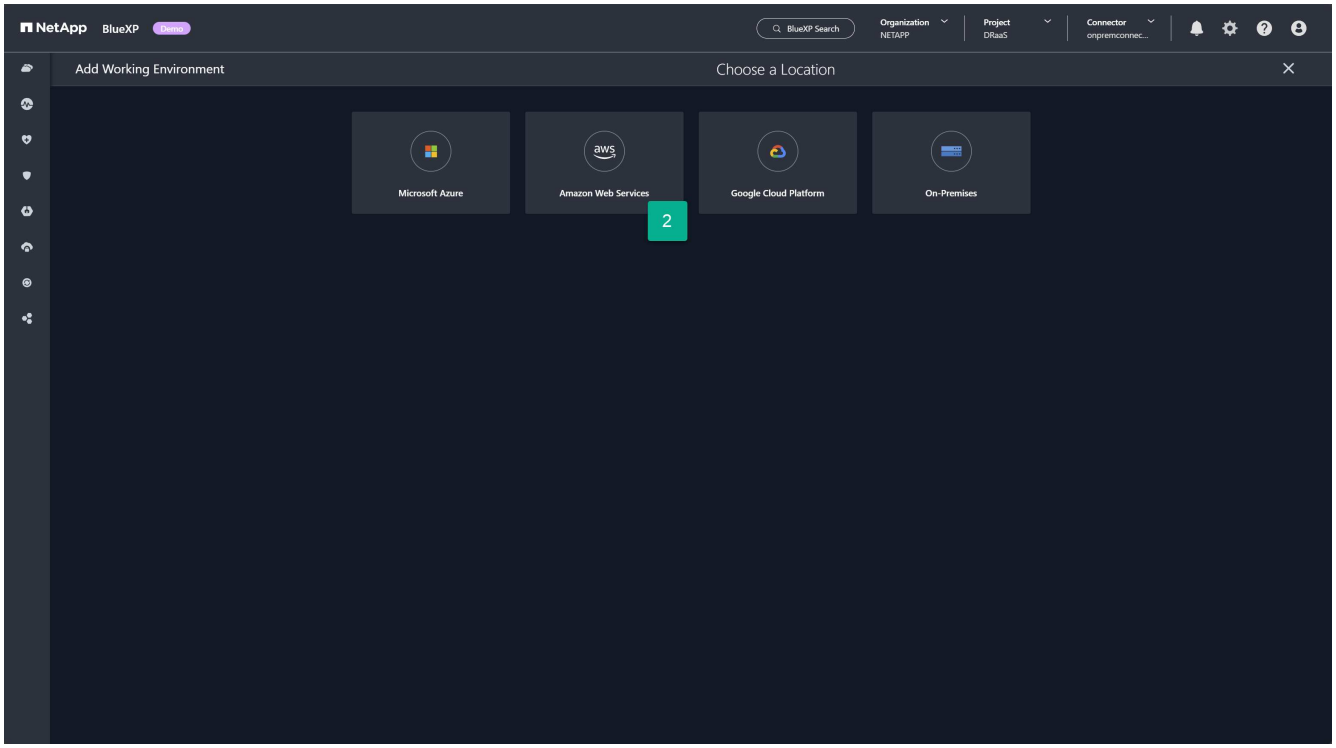
Fügen Sie Amazon FSx für NetApp ONTAP-Speicherinstanzen zur BlueXP-Arbeitsumgebung hinzu

Fügen Sie als Nächstes Ihrer BlueXP-Arbeitsumgebung ein Amazon FSx für NetApp ONTAP-Speicherressourcen hinzu.

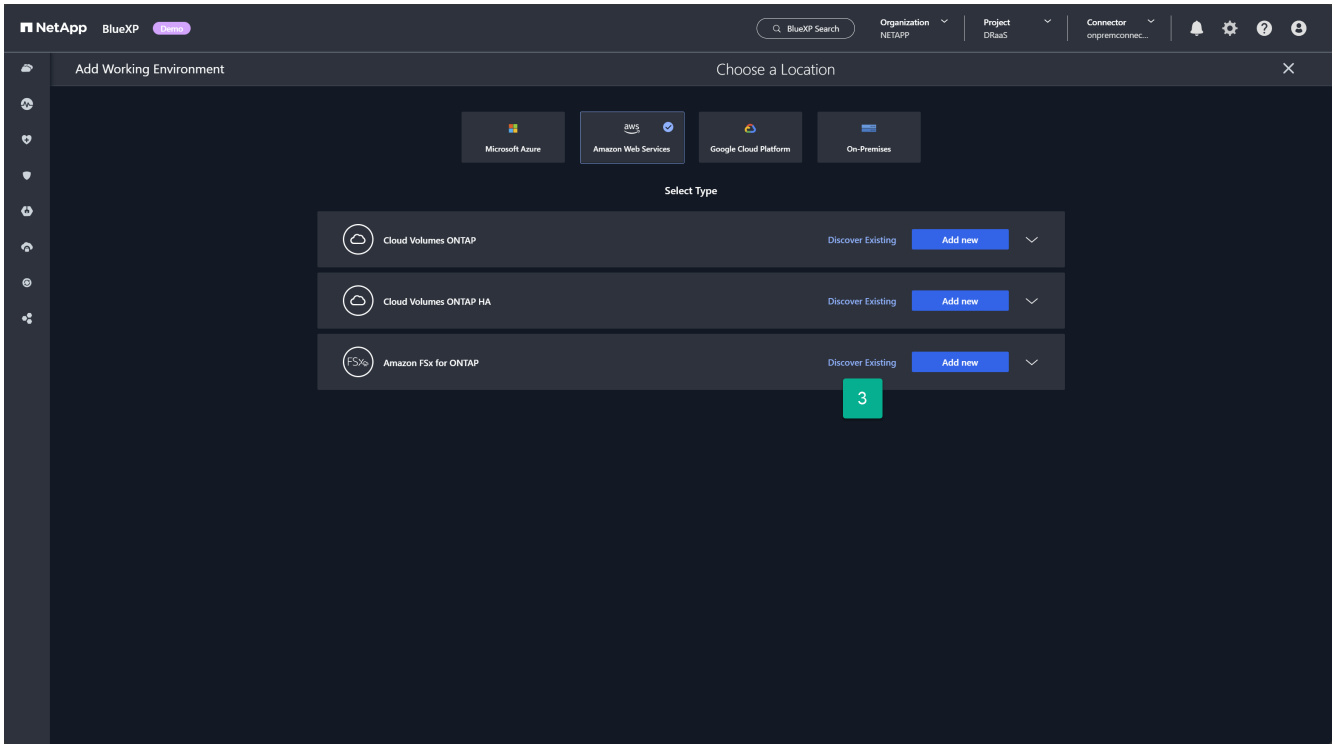
1. Wählen Sie im BlueXP Canvas **Arbeitsumgebung hinzufügen** aus.



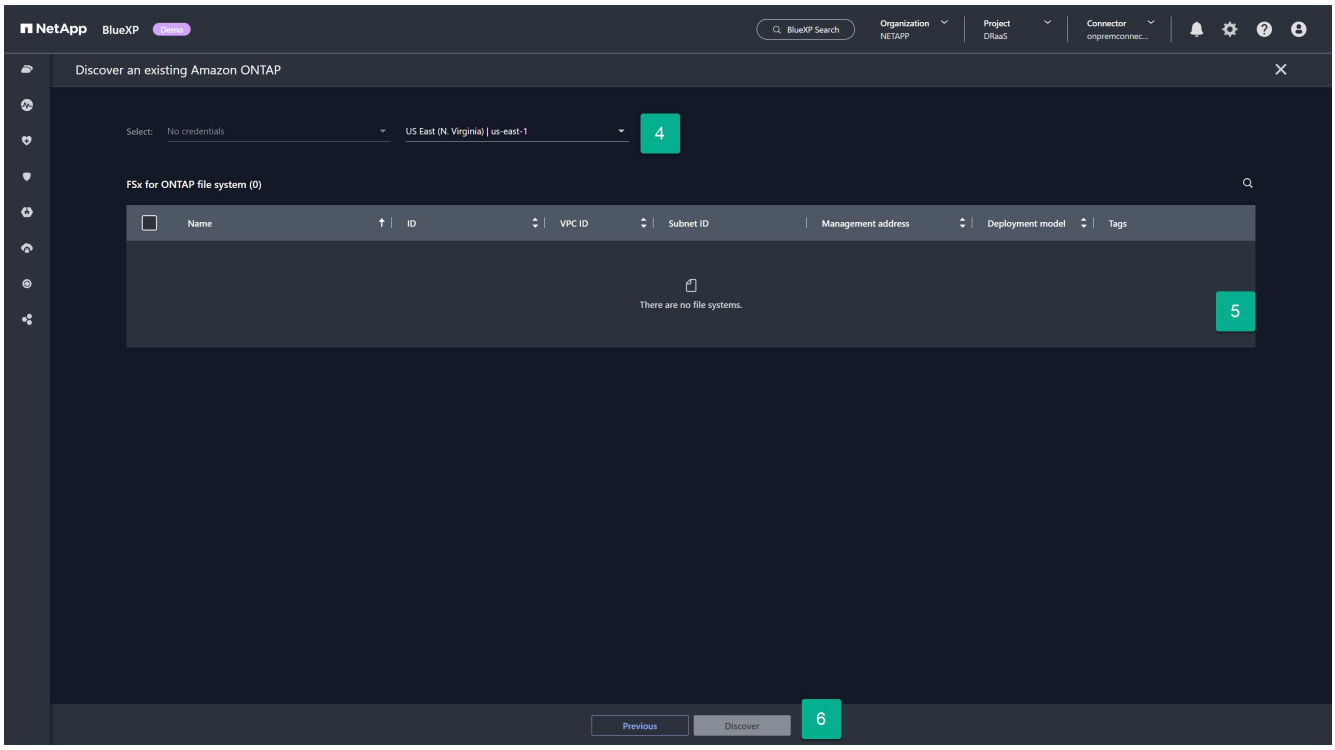
2. Wählen Sie auf der Seite „Arbeitsumgebung hinzufügen“ die Karte **Amazon Web Services** aus.



3. Wählen Sie den Link **Vorhandenes erkennen** 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 BlueXP-Konto für Amazon EVS den BlueXP-Notfallwiederherstellungsdienst hinzu

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

Weitere Informationen zu BlueXP Disaster Recovery-Lizenzen finden Sie unter "Lizenzierung für die Disaster Recovery von BlueXP einrichten" .

Lizenztypen

Es gibt zwei primäre Lizenztypen:

- NetApp bietet eine "30-Tage-Testlizenz" Damit können Sie BlueXP Disaster Recovery mit Ihren ONTAP- und VMware-Ressourcen evaluieren. Diese Lizenz ermöglicht eine 30-tägige Nutzung einer unbegrenzten Menge geschützter Kapazität.
- Erwerben Sie eine Produktionslizenz, wenn Sie DR-Schutz über die 30-tägige Testphase hinaus wünschen. Diese Lizenz ist über die Marktplätze aller NetApp Cloud-Partner erhältlich. Für diesen Leitfaden empfehlen wir jedoch den Erwerb Ihrer **NetApp Intelligent Services**-Lizenz für BlueXP Disaster Recovery über den Amazon AWS Marketplace. Weitere Informationen zum Erwerb einer Lizenz über den Amazon Marketplace finden Sie unter "Abonnieren Sie ihn 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 von NetApp ONTAP Storage ist die hohe Effizienz, mit der NetApp Ihre Daten speichert. Alle in einem ONTAP-Volume gespeicherten Daten – wie z. B. VMware-Datenspeicher mit VMs – werden hocheffizient gespeichert. ONTAP nutzt standardmäßig drei Arten der Speichereffizienz beim Schreiben von Daten in physische Speicher: Komprimierung, Deduplizierung und Kompression. Das Ergebnis sind Speichereffizienzen zwischen 1,5:1 und 4:1, abhängig von den gespeicherten Datentypen. NetApp bietet eine "Speichereffizienzgarantie" für bestimmte Arbeitslasten.

Dies ist ein Vorteil für Sie, da BlueXP Disaster Recovery die Kapazität für die Lizenzierung berechnet, nachdem alle ONTAP-Speichereffizienzen berücksichtigt wurden. Nehmen wir beispielsweise an, Sie haben einen 100 Terabyte (TiB) großen NFS-Datenspeicher in vCenter bereitgestellt, um 100 VMs zu hosten, die Sie mit dem Service schützen möchten. Nehmen wir außerdem an, dass beim Schreiben der Daten auf das ONTAP-Volume automatisch angewandte Speichereffizienztechniken dazu führen, dass diese VMs nur 33 TiB belegen (Speichereffizienz 3:1). BlueXP Disaster Recovery benötigt nur eine Lizenz für 33 TiB, nicht für 100 TiB. Dies kann die Gesamtbetriebskosten Ihrer DR-Lösung im Vergleich zu anderen DR-Lösungen deutlich senken.

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 BlueXP Disaster Recovery schützen muss. Anhand dieses Werts bestimmen Sie, wie viel Kapazität Sie lizenzieren müssen.

Sites in BlueXP Disaster Recovery für Amazon EVS hinzufügen

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, einen Standort zu erstellen, der die Quell- und Zielrechenzentren repräsentiert. Ein Standort ist eine Fehlerdomäne oder eine Wiederherstellungsdomäne.

Sie müssen Folgendes erstellen:

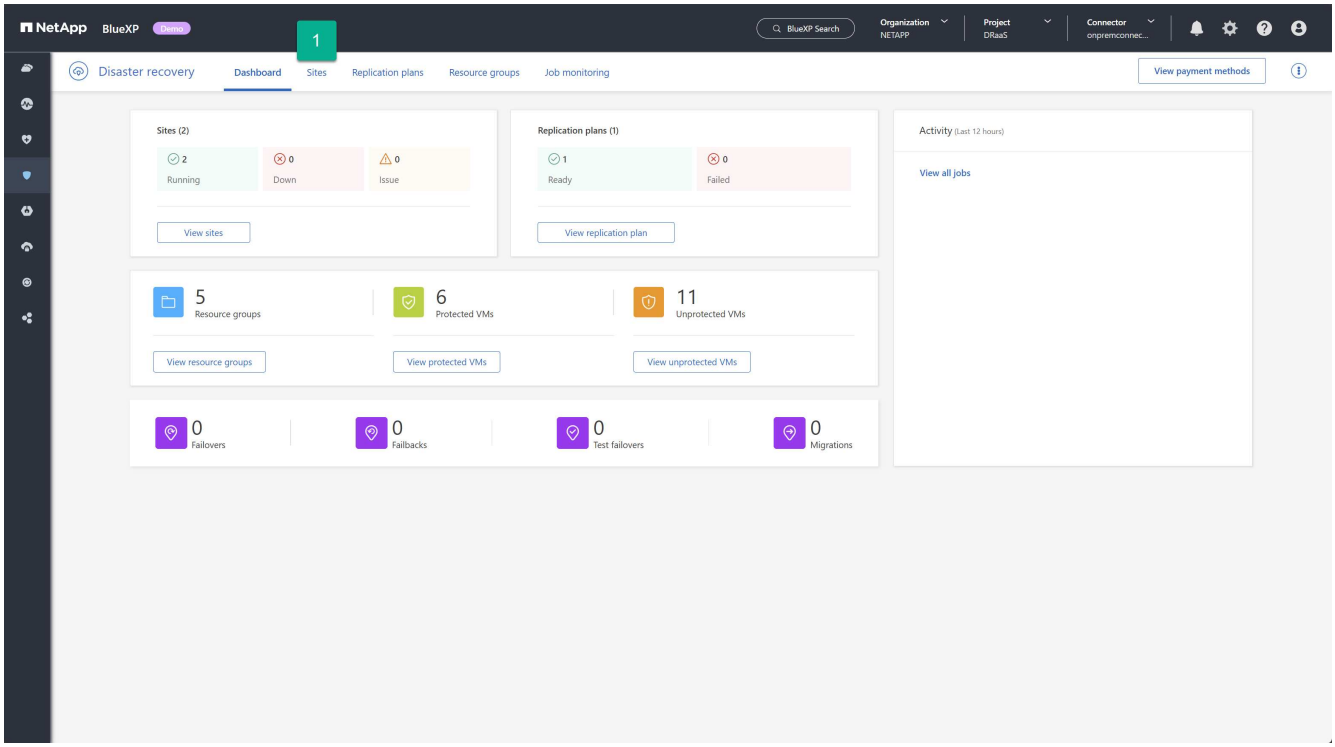
- Eine Site, die jedes Produktionsrechenzentrum darstellt, in dem sich Ihre Produktions-vCenter-Cluster befinden
- Eine Site für Ihr Amazon EVS/Amazon FSx für NetApp ONTAP Cloud-Rechenzentrum

Erstellen lokaler Websites

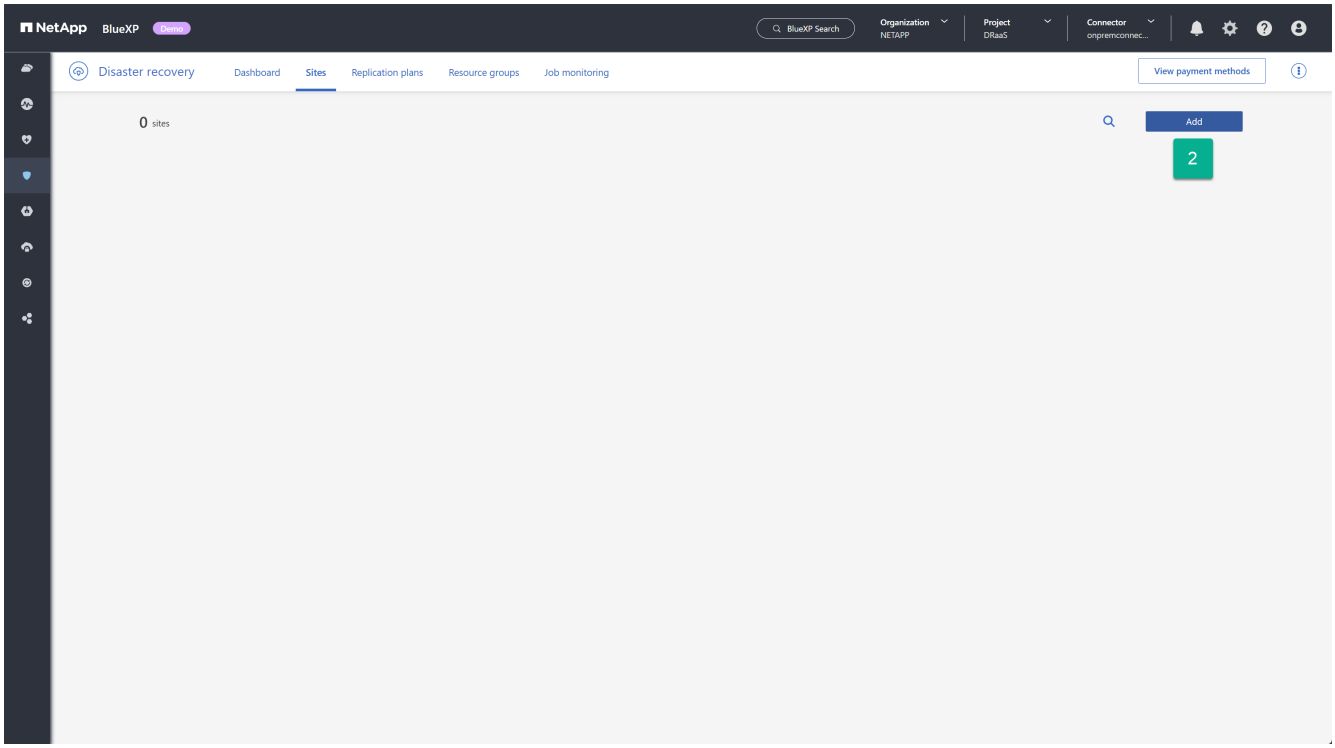
Erstellen Sie eine vCenter-Produktionssite.

Schritte

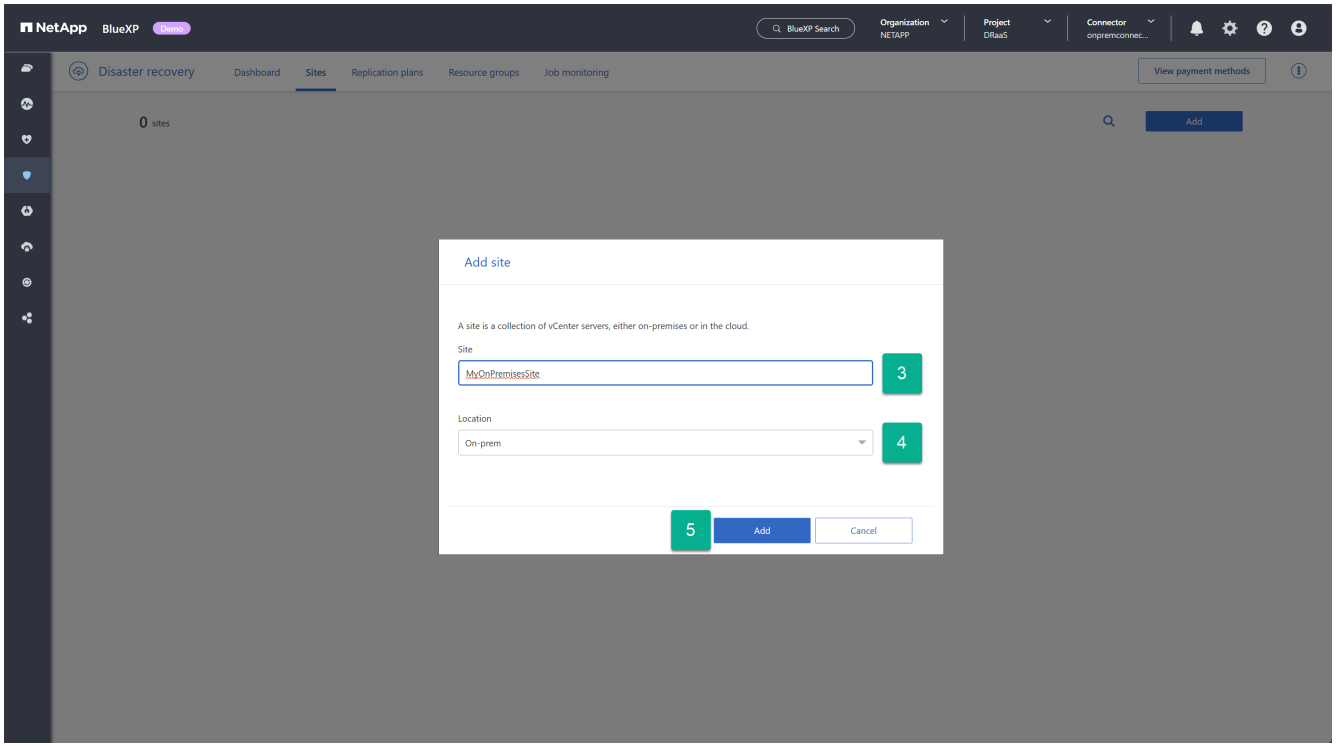
1. Wählen Sie in der linken Navigation von BlueXP **Schutz** > **Notfallwiederherstellung**.
2. Wählen Sie auf einer beliebigen Seite der BlueXP-Notfallwiederherstellung die Registerkarte **Sites** aus.



3. Wählen Sie auf der Registerkarte „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**.

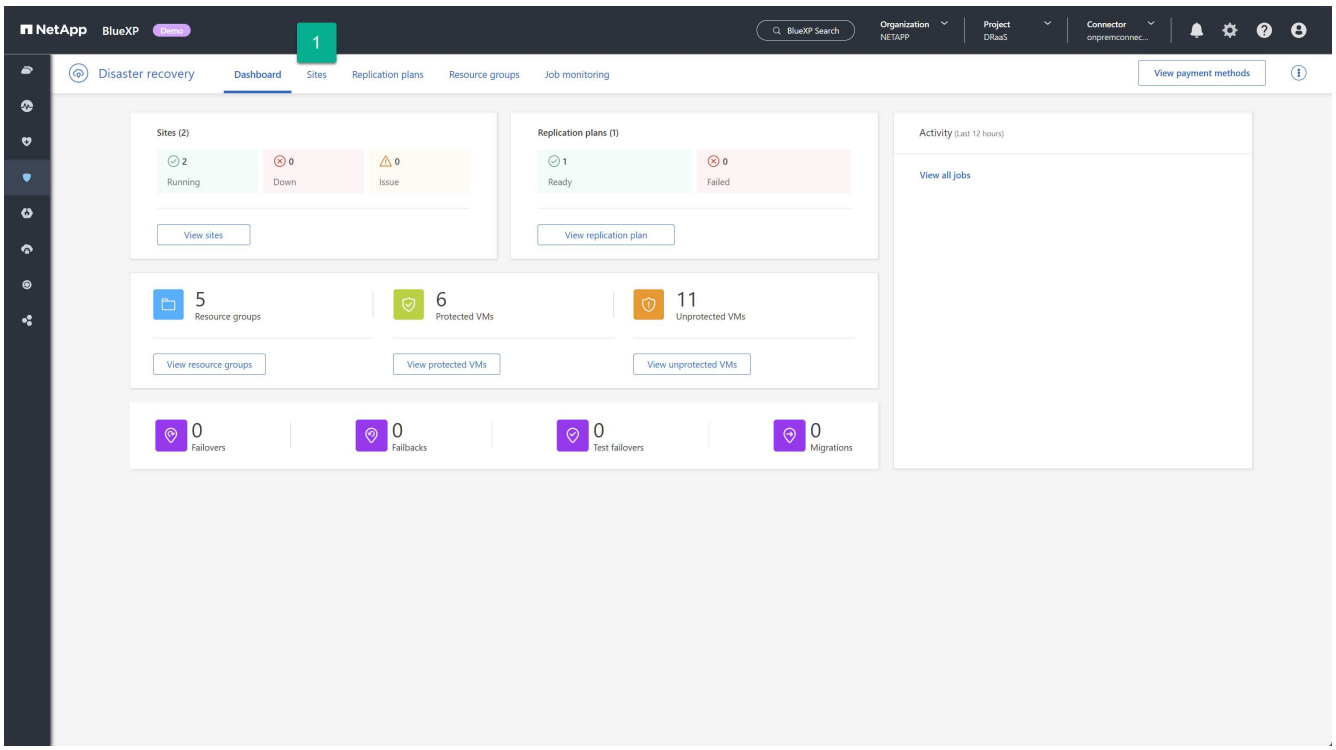


Wenn Sie über andere vCenter-Produktionssites verfügen, können Sie diese mit denselben Schritten hinzufügen.

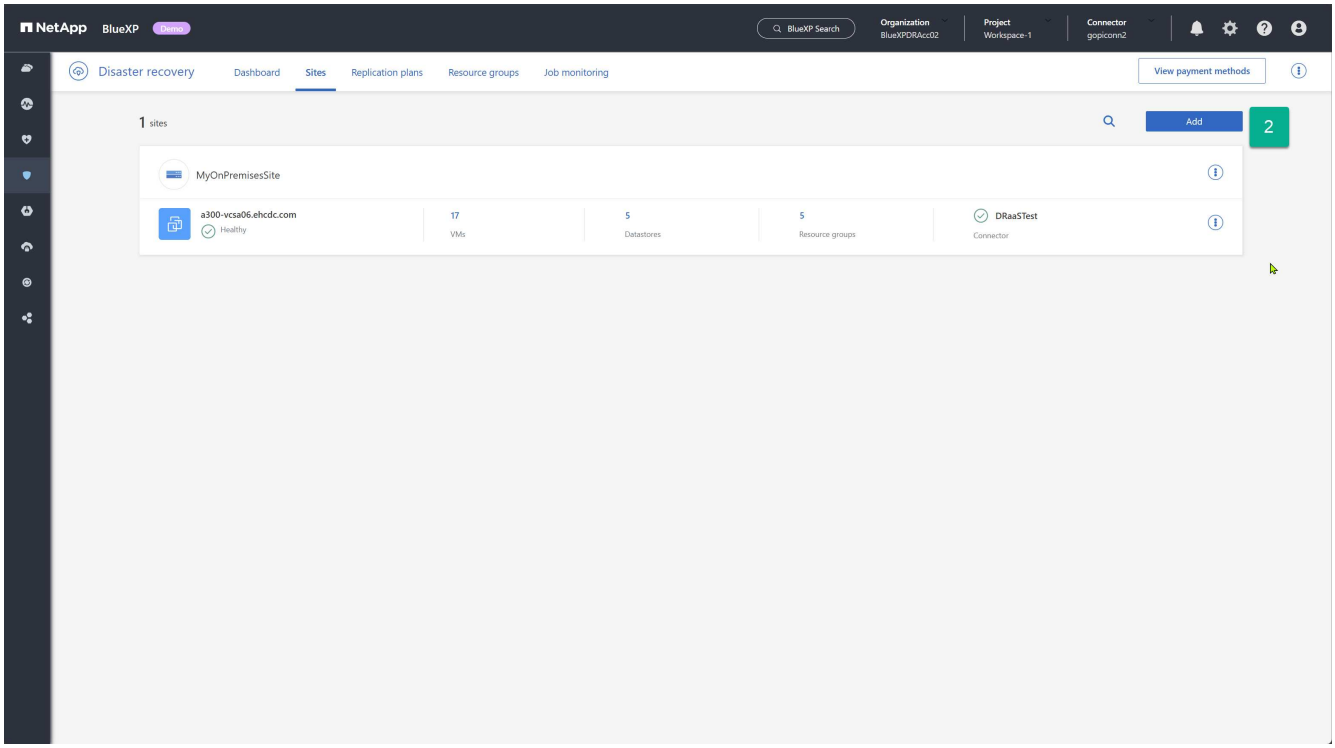
Erstellen Sie Amazon Cloud-Sites

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

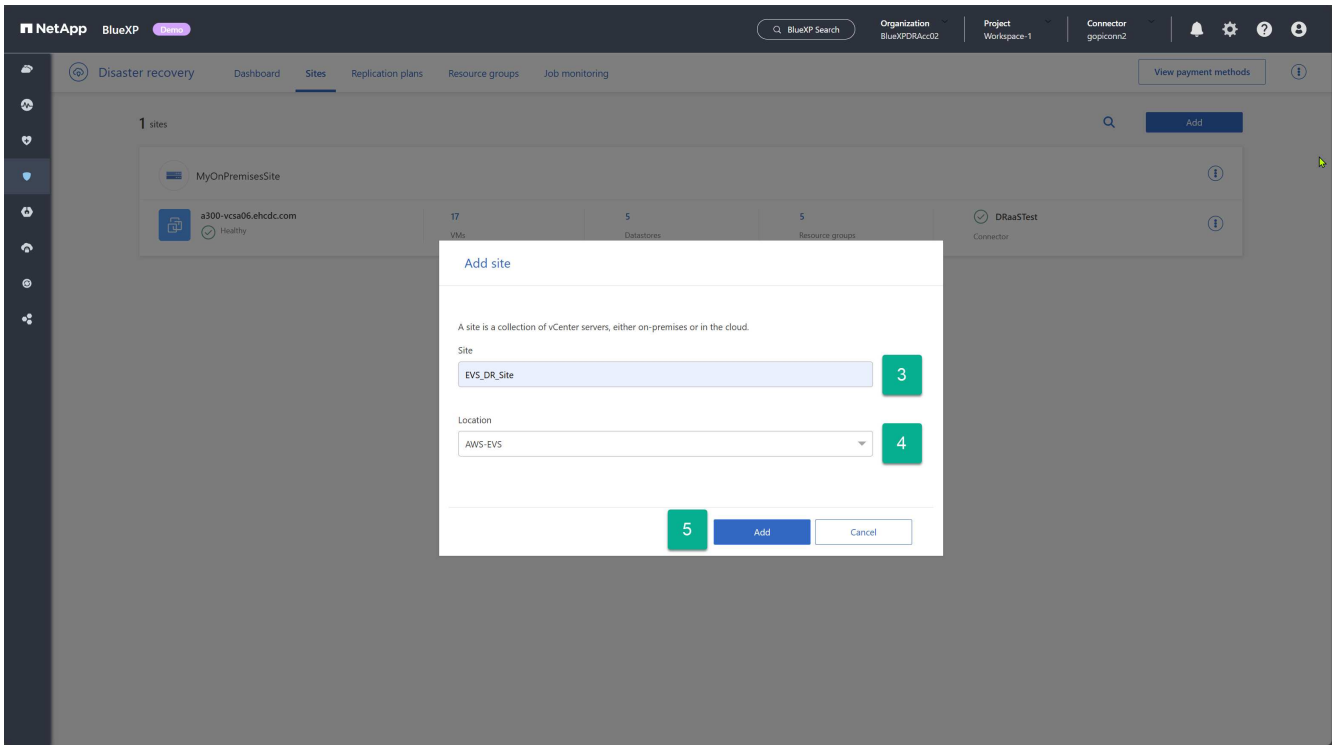
1. Wählen Sie auf einer beliebigen Seite der BlueXP-Notfallwiederherstellung die Registerkarte **Sites** aus.



2. Wählen Sie auf der Registerkarte „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

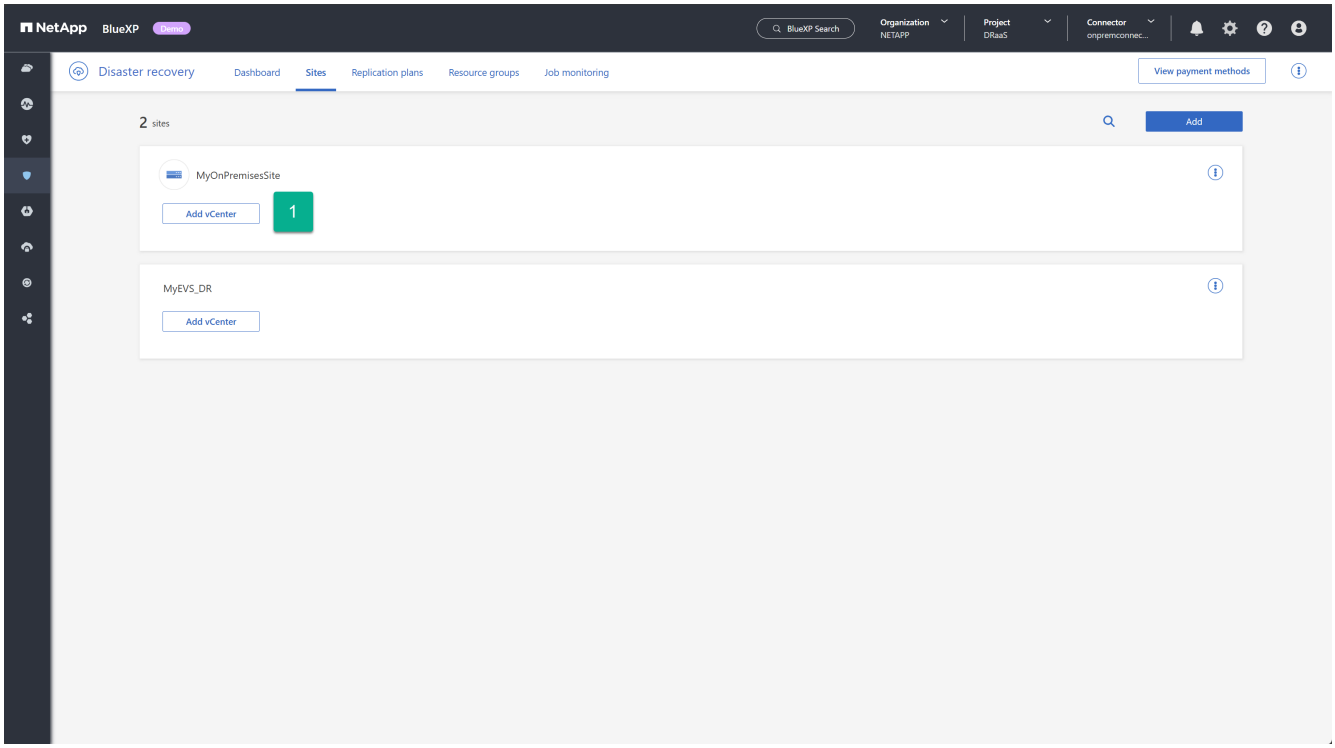
Sie haben jetzt einen Produktionsstandort (Quellstandort) und einen DR-Standort (Zielstandort) erstellt.

Fügen Sie lokale und Amazon EVS vCenter-Cluster in der BlueXP-Notfallwiederherstellung hinzu

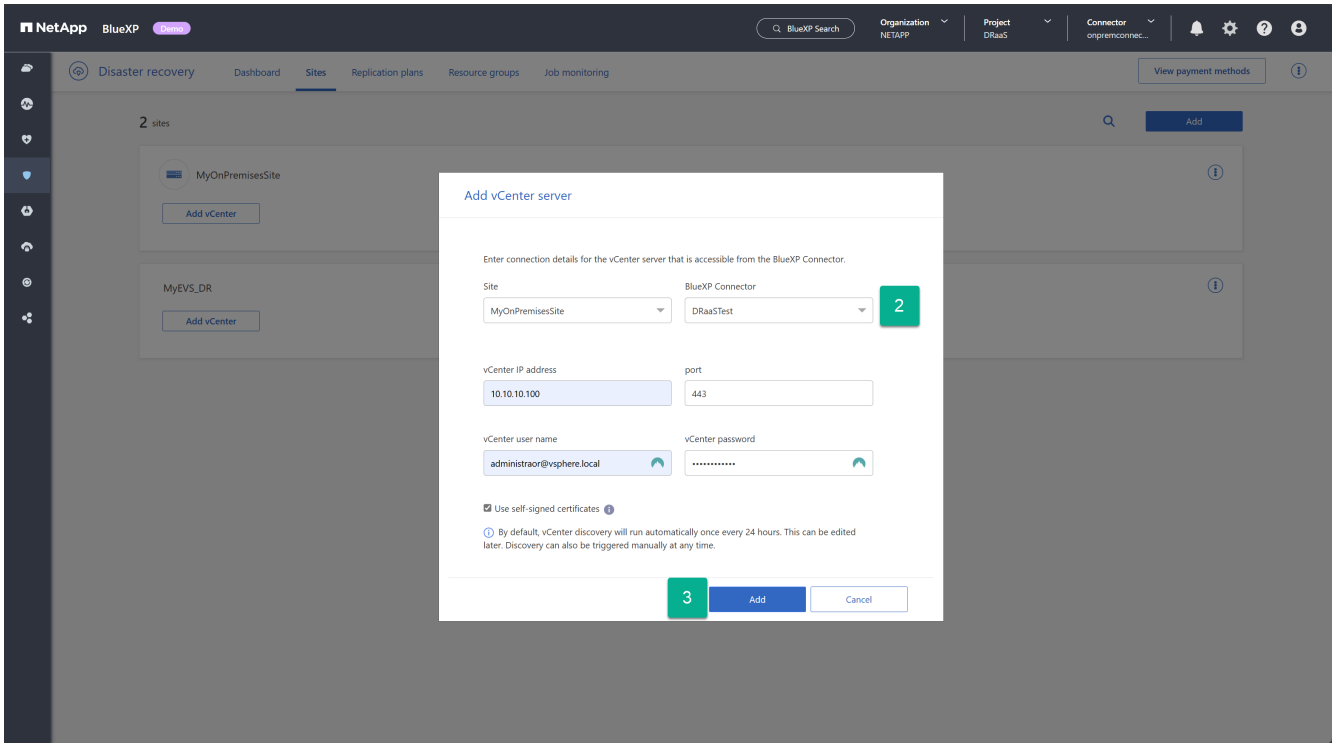
Nachdem Sie die Sites erstellt haben, fügen Sie Ihre vCenter-Cluster nun den einzelnen Sites in BlueXP Disaster Recovery hinzu. Bei der Erstellung der Sites haben wir die jeweiligen Site-Typen angegeben. Dadurch weiß BlueXP Disaster Recovery, welcher Zugriff für die dort gehosteten vCenter erforderlich ist. Ein Vorteil von Amazon EVS besteht darin, dass es keinen wirklichen Unterschied zwischen einem Amazon EVS vCenter und einem lokalen vCenter gibt. Beide benötigen dieselben Verbindungs- und Authentifizierungsinformationen.

Schritte zum Hinzufügen eines vCenters zu jeder Site

1. Wählen Sie auf der Registerkarte **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 BlueXP-Connector wird in Ihrem AWS VPC gehostet.
   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 BlueXP 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 für den Zugriff auf Ihre vCenter verwendet, deaktivieren Sie das Kontrollkästchen **Selbstsignierte Zertifikate verwenden**. Andernfalls lassen Sie das Kontrollkästchen aktiviert.
3. Wählen Sie **Hinzufügen**.



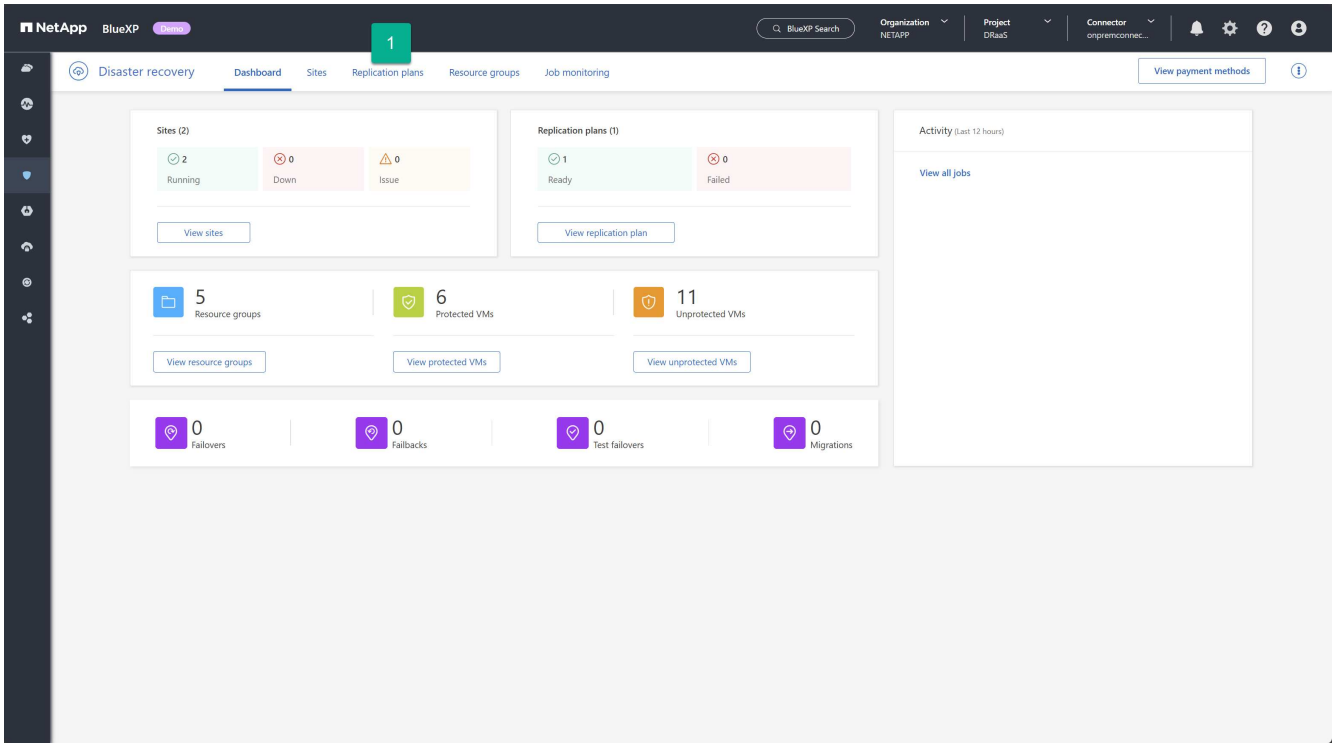
Erstellen von Replikationsplänen für Amazon EVS

Erstellen von Replikationsplänen in der BlueXP-Übersicht zur Notfallwiederherstellung

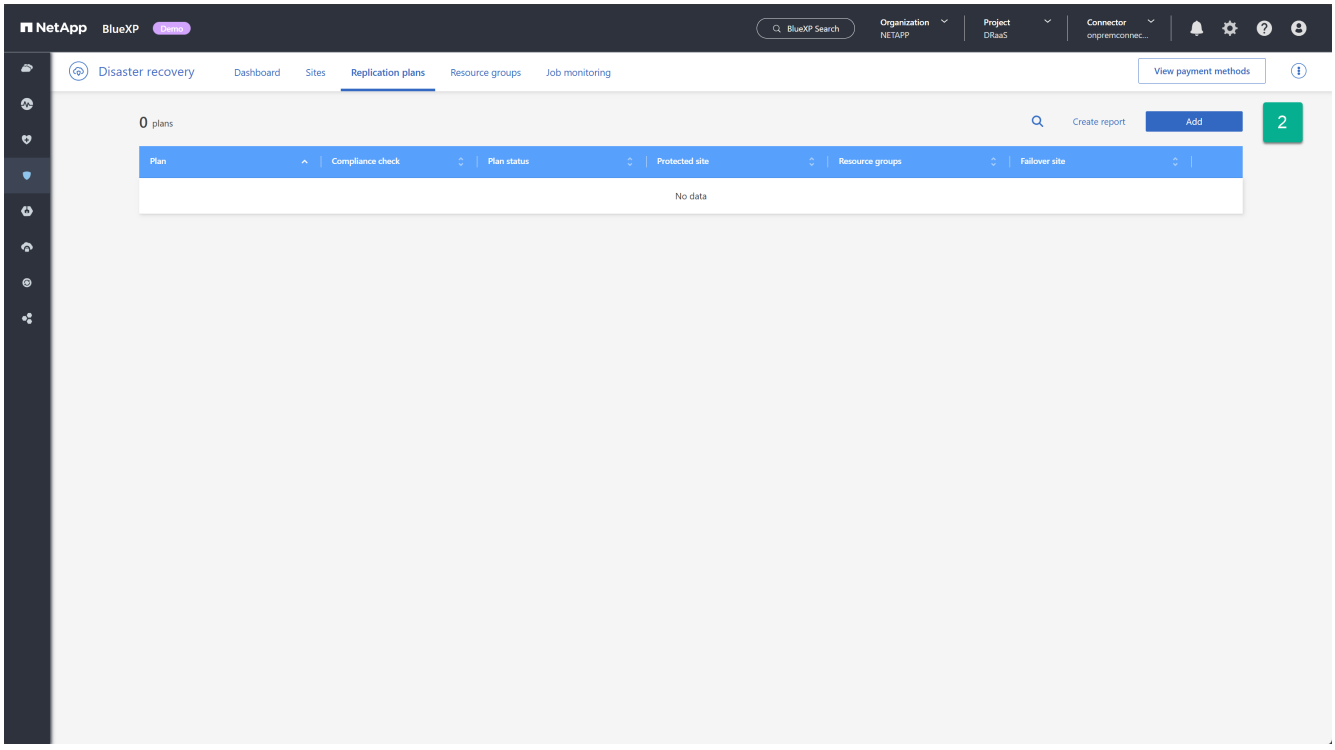
Nachdem Sie vCenter zum Schutz auf der lokalen Site haben und eine Amazon EVS-Site für die Verwendung von Amazon FSx für NetApp ONTAP konfiguriert haben, die Sie als DR-Ziel verwenden können, können Sie einen Replikationsplan (RP) erstellen, um alle auf dem vCenter-Cluster innerhalb Ihrer lokalen Site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

So starten Sie den Prozess zur Erstellung des Replikationsplans:

1. Wählen Sie auf einem beliebigen BlueXP-Notfallwiederherstellungsbildschirm die Registerkarte **Replikationspläne** aus.



2. Wählen Sie im Bildschirm „Replikationspläne“ die Option „Hinzufügen“ aus.



Dadurch wird der Assistent „Replikationsplan erstellen“ geöffnet.

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

Erstellen Sie einen Replikationsplan: Schritt 1 - Auswählen von vCentern in BlueXP Disaster Recovery

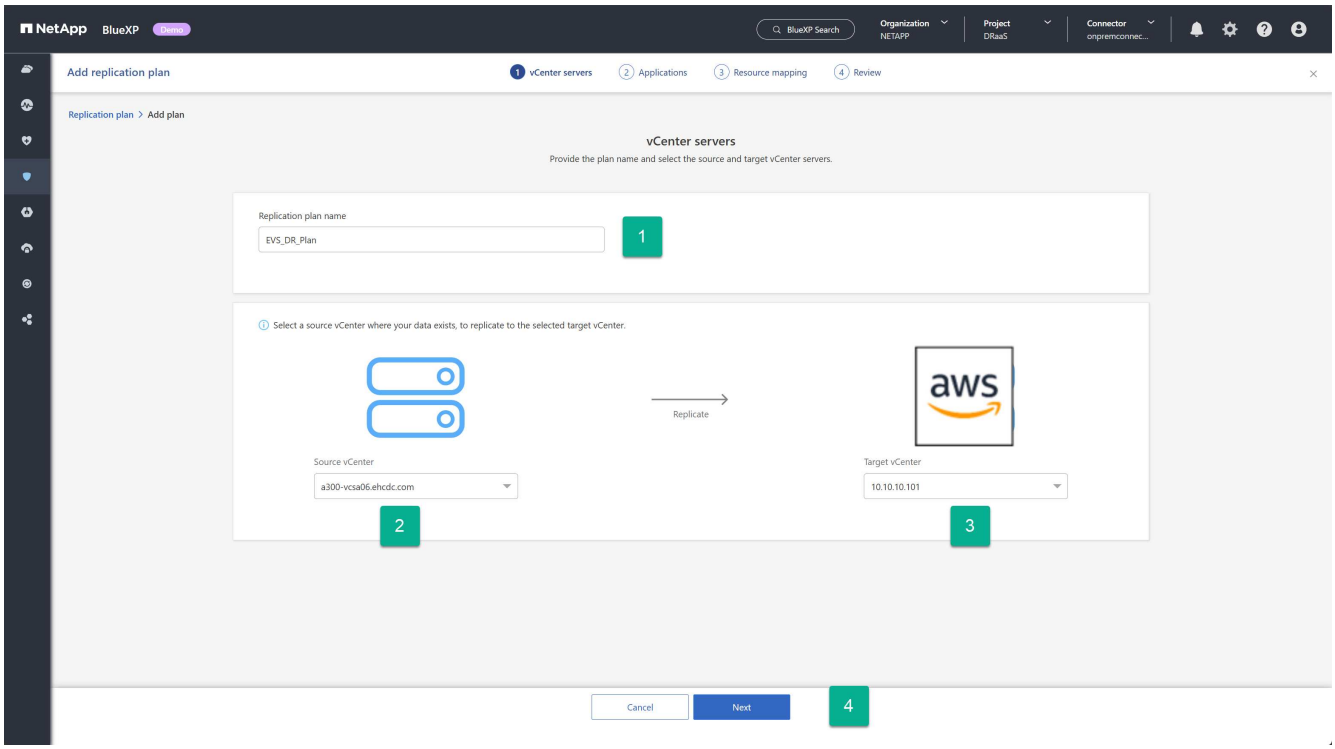
Geben Sie zunächst mithilfe der Notfallwiederherstellung von BlueXP einen

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 BlueXP Disaster Recovery

Wählen Sie die virtuellen Maschinen aus, die mit der Notfallwiederherstellung von BlueXP geschützt werden sollen.

Es gibt mehrere Möglichkeiten, VMs zum Schutz auszuwählen:

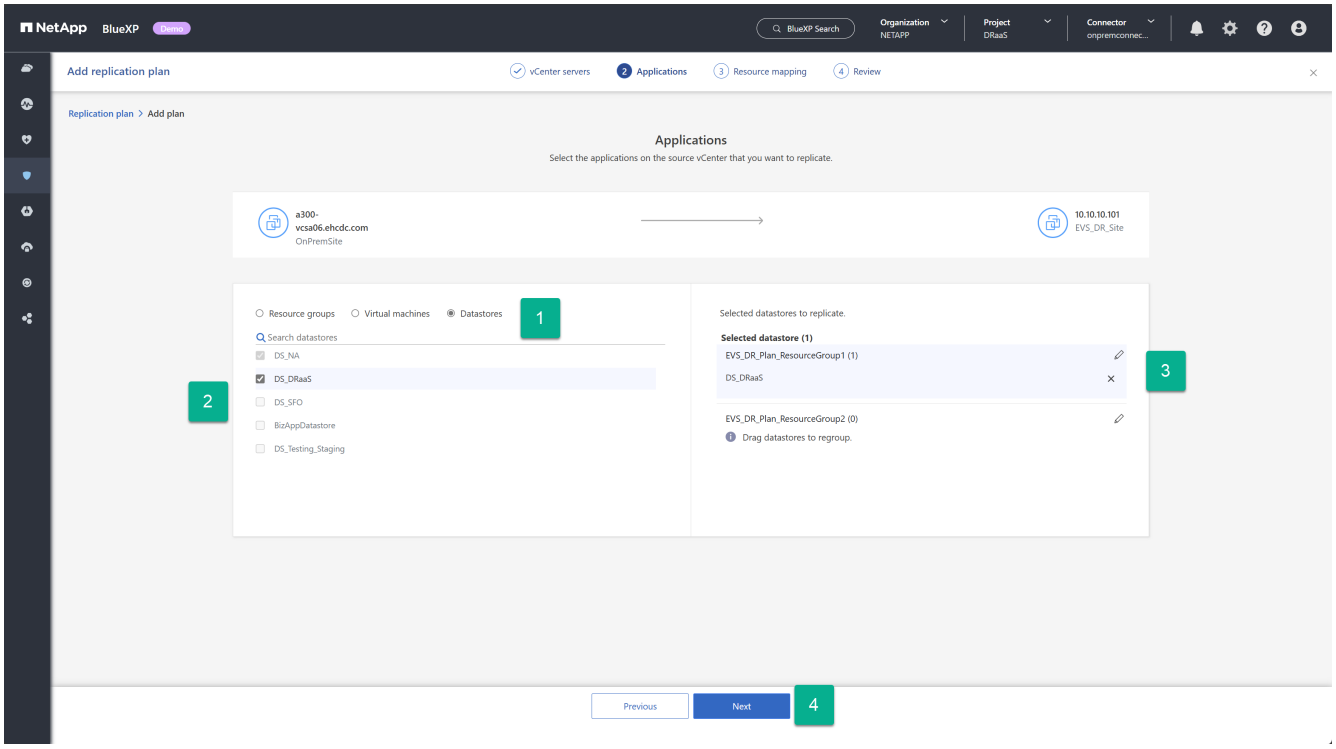
- **Einzelne VMs auswählen**: Durch Klicken auf die Schaltfläche **Virtuelle Maschinen** können Sie einzelne VMs zum Schutz auswählen. Sobald Sie eine VM ausgewählt haben, fügt der Dienst sie einer Standardressourcengruppe auf der rechten Bildschirmseite hinzu.
- **Zuvor erstellte Ressourcengruppen auswählen**: Sie können benutzerdefinierte Ressourcengruppen vorab über die Registerkarte „Ressourcengruppe“ oben in der BlueXP-Disaster-Recovery-Benutzeroberfläche erstellen. Dies ist jedoch nicht erforderlich, da Sie die beiden anderen Methoden zum Erstellen einer Ressourcengruppe im Rahmen des Replikationsplanprozesses verwenden können. Weitere Informationen finden Sie unter "Erstellen Sie einen Replizierungsplan".

- **Gesamte vCenter-Datenspeicher auswählen**: Wenn Sie mit diesem Replikationsplan viele VMs schützen möchten, ist die Auswahl einzelner VMs möglicherweise nicht so effizient. Da BlueXP Disaster Recovery die volumebasierte SnapMirror-Replikation zum Schutz der VMs nutzt, werden alle VMs eines Datenspeichers als Teil des Volumes repliziert. In den meisten Fällen sollte BlueXP Disaster Recovery alle VMs im Datenspeicher schützen und neu starten. Mit dieser Option weisen Sie den Dienst an, alle VMs eines ausgewählten Datenspeichers 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 oder der Datenspeicher:

1. Wählen Sie **Datastores**.
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 BlueXP Disaster Recovery

Nachdem Sie eine Liste der VMs erstellt haben, die Sie mithilfe der Notfallwiederherstellung von BlueXP schützen möchten, geben Sie die Failover-Zuordnung und die VM-Konfigurationsinformationen an, die während eines Failovers verwendet werden sollen.

Sie müssen vier primäre Informationstypen zuordnen:

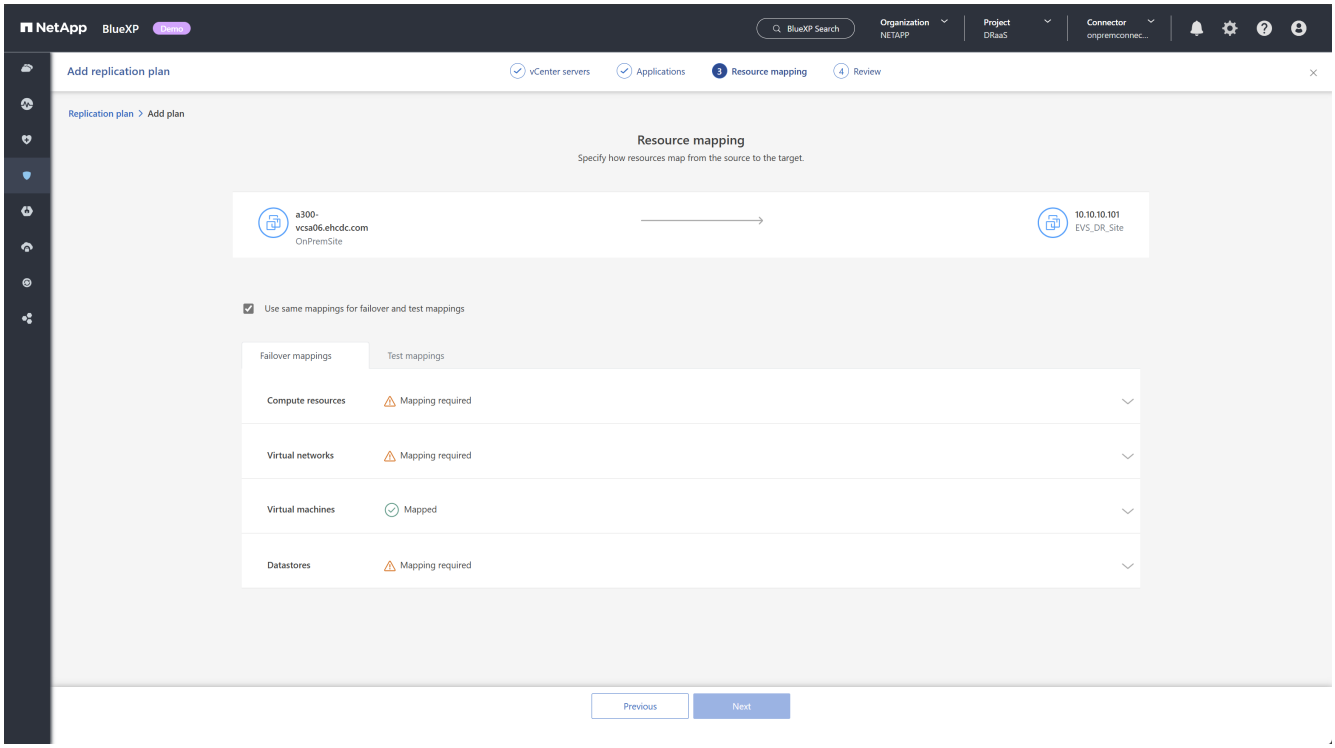
- Rechenressourcen
- Virtuelle Netzwerke
- VM-Neukonfiguration
- Datenspeicherzuordnung

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

- Die Abschnitte mit dem Vorsichtssymbol ( ) erfordern, dass Sie Zuordnungsinformationen angeben.
- Der mit dem Häkchensymbol ( ) wurden zugeordnet oder verfügen über Standardzuordnungen. Überprüfen Sie diese, 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 eine Site 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.

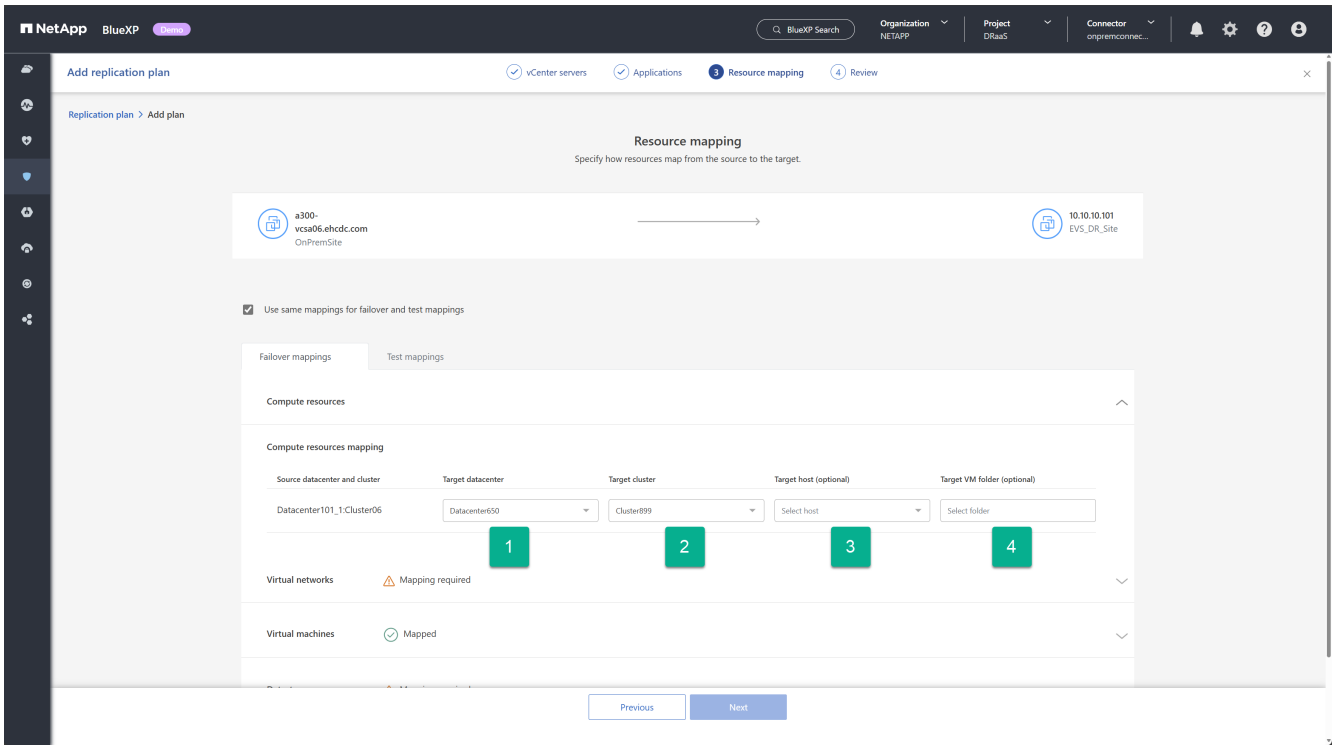
Schritte zum Zuordnen von Computeressourcen

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 BlueXP Disaster Recovery den ersten Host auswählt, der dem Cluster in vCenter hinzugefügt wird. Anschließend laufen die VMs entweder weiterhin auf diesem ESXi-Host, 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.

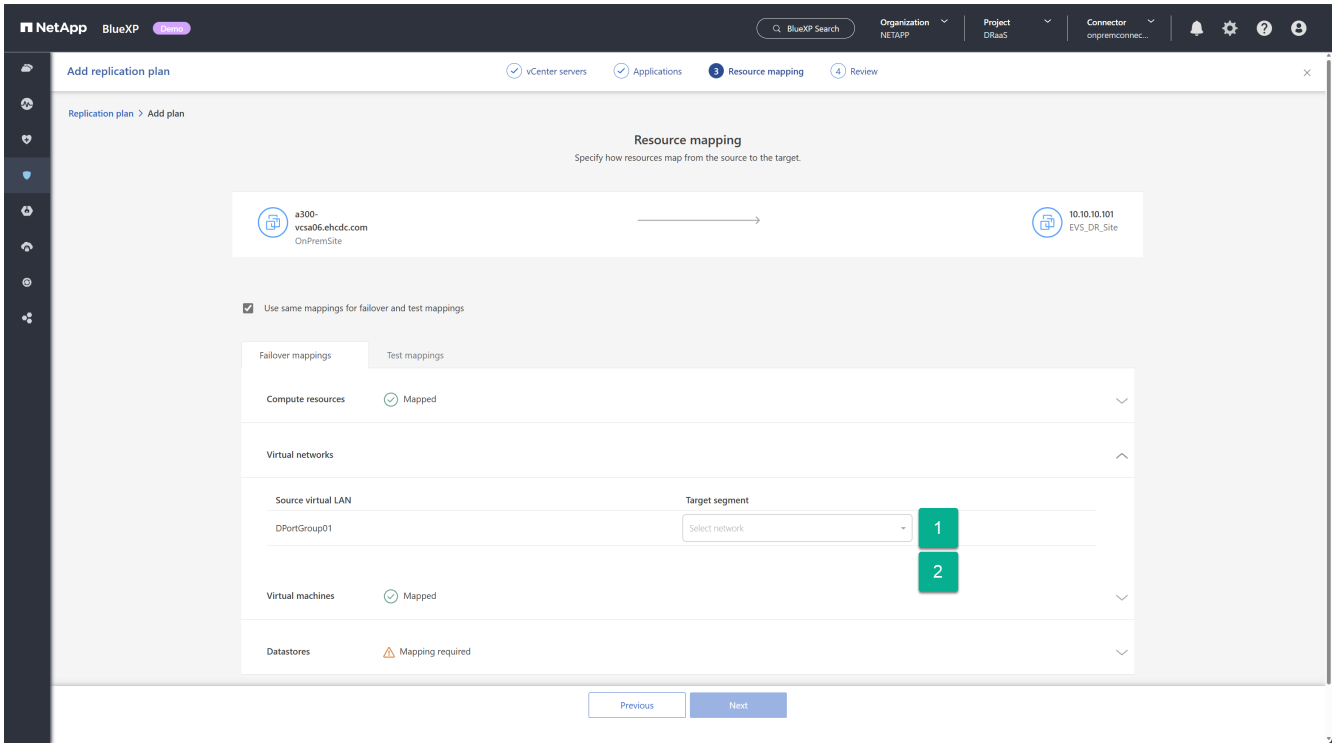


Zuordnen virtueller Netzwerkressourcen

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 die ordnungsgemäße Funktion jeder VM im DR vCenter-Standort sind möglicherweise Anpassungen erforderlich. Im Abschnitt „Virtuelle Maschinen“ können Sie die erforderlichen Änderungen vornehmen.

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

Netzwerkneukonfiguration

Unterstützte IP-Adresstypen sind statisch und DHCP. Für statische IP-Adressen gelten die folgenden Ziel-IP-Einstellungen:

- **Gleich wie Quelle**: Wie der Name schon sagt, verwendet der Dienst auf der Ziel-VM dieselbe IP-Adresse wie die VM am Quellstandort. Dies erfordert, dass Sie die im vorherigen Schritt zugeordneten virtuellen Netzwerke für dieselben Subnetzeinstellungen konfigurieren.
- **Abweichend von der Quelle**: Der Dienst stellt für jede VM eine Reihe von IP-Adressfeldern bereit, die für das entsprechende Subnetz des virtuellen Zielnetzwerks konfiguriert werden müssen, das Sie im vorherigen Abschnitt zugeordnet haben. Für jede VM müssen Sie eine IP-Adresse, eine Subnetzmaske, DNS-Werte und Standardgateway-Werte angeben. Optional können Sie für alle VMs dieselben Einstellungen für Subnetzmaske, DNS und Gateway verwenden, 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 nutzen, 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 Registerkarte „Sites“ geändert.

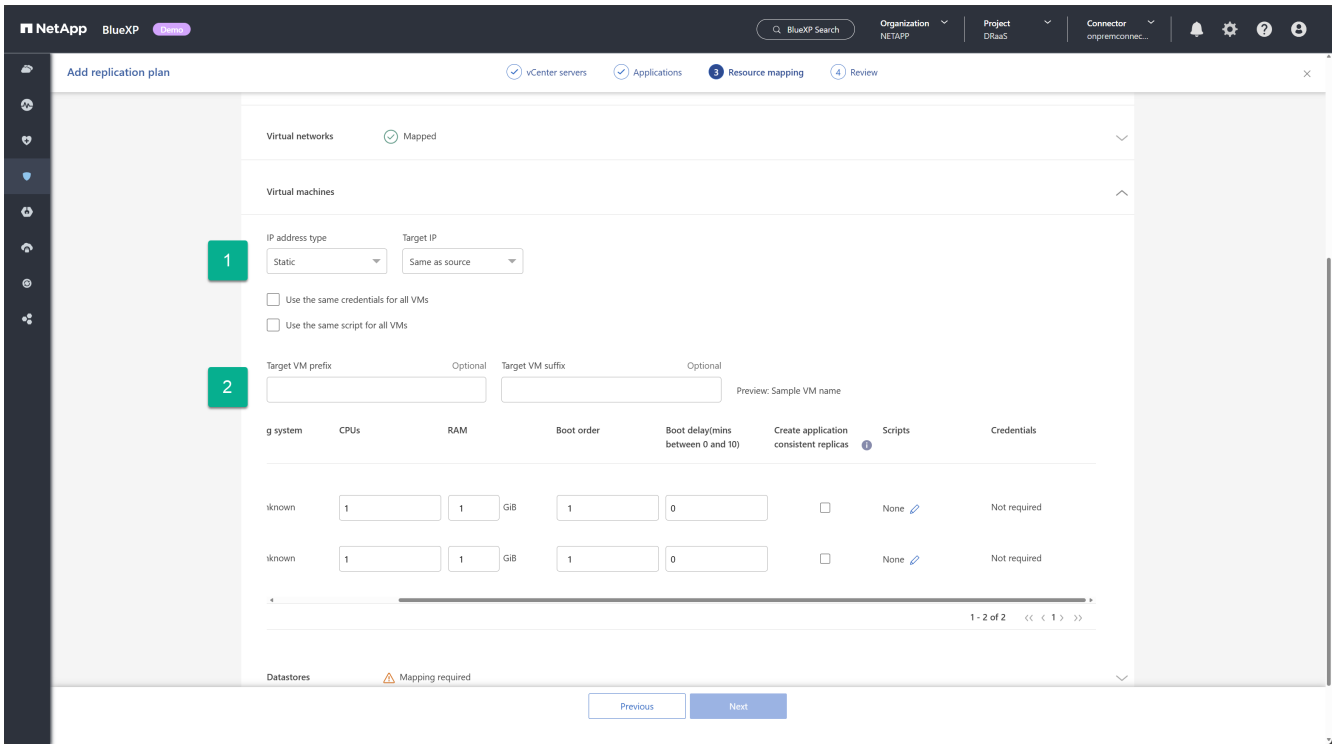
Nachdem Sie Subnetze konfiguriert haben, verwendet die Subnetzzuordnung dieselbe Einheitenkomponente der IP-Adresse für die Quell- und Ziel-VM-Konfiguration, ersetzt jedoch die Subnetzkomponente der IP-Adresse basierend auf den bereitgestellten CIDR-Informationen. Diese Funktion erfordert außerdem, dass

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.

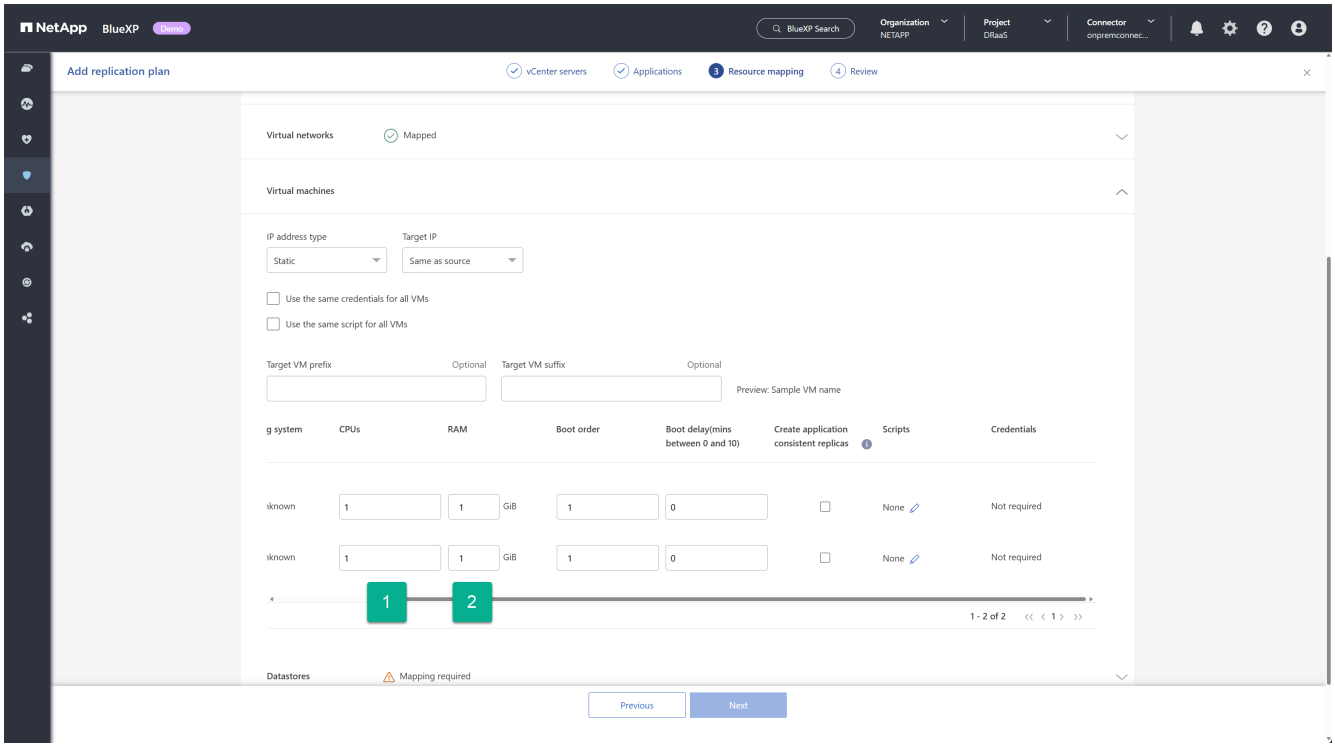


Neukonfiguration der VM-Rechenressourcen

Es gibt verschiedene Möglichkeiten, die VM-Rechenressourcen neu zu konfigurieren. BlueXP Disaster Recovery unterstützt die Änderung 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 Hosts des Quell-vCenter-Clusters.

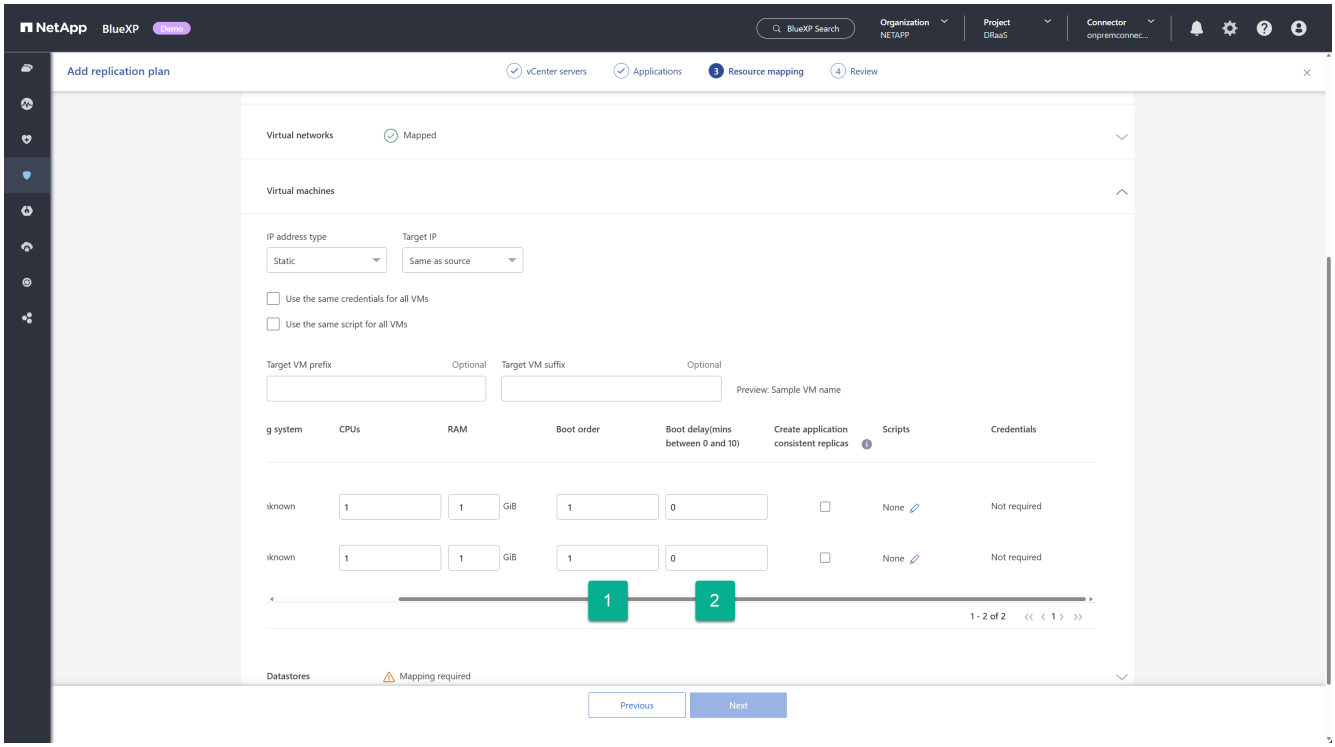


Startreihenfolge

BlueXP Disaster Recovery unterstützt einen geordneten Neustart von VMs basierend auf einem Bootreihenfolgefeld. Das Feld „Bootreihenfolge“ gibt an, wie die VMs in jeder Ressourcengruppe gestartet werden. VMs mit demselben 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 akzeptiert einen beliebigen numerischen Wert. BlueXP Disaster Recovery versucht, VMs mit demselben numerischen Wert parallel neu zu starten.
2. (Optional) Geben Sie eine Verzögerung zwischen den einzelnen VM-Neustarts an. Die Verzögerung wird nach dem Neustart dieser VM und vor den VMs mit der nächsthöheren Startreihenfolge eingefügt. Die Angabe erfolgt in Minuten.



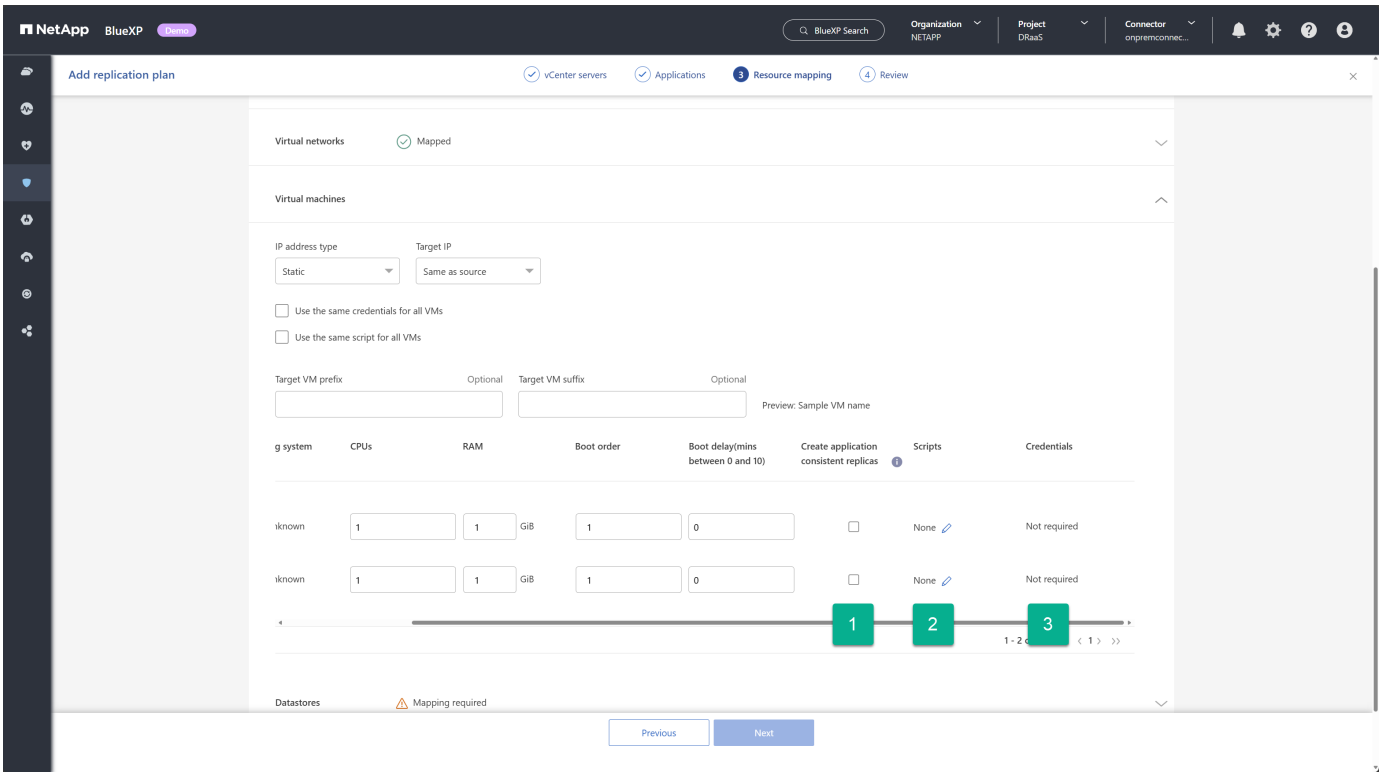
Benutzerdefinierte Gastbetriebssystemvorgänge

Die Notfallwiederherstellung von BlueXP unterstützt die Durchführung einiger Gastbetriebssystemvorgänge für jede VM:

- BlueXP Disaster Recovery kann anwendungskonsistente Backups von VMs für VMs erstellen, auf denen Oracle-Datenbanken und Microsoft SQL Server-Datenbanken ausgeführt werden.
- BlueXP Disaster Recovery kann für jede VM benutzerdefinierte, für das Gastbetriebssystem geeignete Skripte ausführen. Die Ausführung solcher Skripte erfordert vom Gastbetriebssystem akzeptierte Benutzeranmeldeinformationen mit ausreichenden Berechtigungen zur Ausführung der im Skript aufgeführten Operationen.

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 im Gastbetriebssystem 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 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 bei der Erstellung eines Replikationsplans besteht darin, festzulegen, wie ONTAP die Datenspeicher schützen soll. Diese Einstellungen definieren das Recovery Point Objective (RPO) des Replikationsplans, die Anzahl der zu verwaltenden Backups und den Replikationsstandort der ONTAP-Volumes jedes vCenter-Datenspeichers.

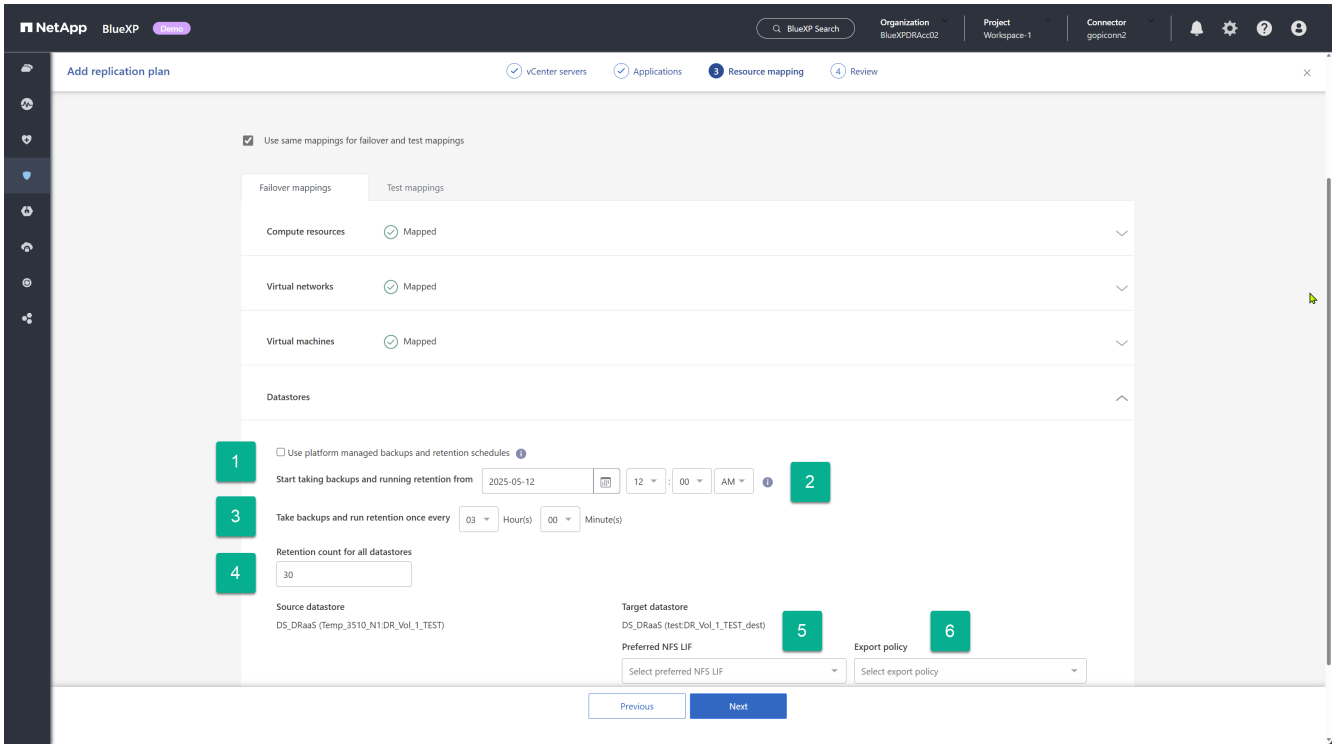
Standardmäßig verwaltet die Notfallwiederherstellung von BlueXP ihren eigenen Snapshot-Replikationszeitplan. Optional können Sie jedoch angeben, dass Sie den vorhandenen SnapMirror-Replikationsrichtlinienzeitplan zum Schutz des Datenspeichers verwenden möchten.

Darüber hinaus können Sie optional die zu verwendenden Daten-LIFs (logische Schnittstellen) und Exportrichtlinien anpassen. Wenn Sie diese Einstellungen nicht angeben, verwendet BlueXP Disaster Recovery alle Daten-LIFs des entsprechenden Protokolls (NFS, iSCSI oder FC) und die Standard-Exportrichtlinie 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 durch die Notfallwiederherstellung von BlueXP 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 Amazon FSx für NetApp ONTAP-Cluster replizieren soll.
4. Geben Sie an, wie viele historische Sicherungen aufbewahrt werden sollen. Der Dienst verwaltet im Quell- und Zielspeichercluster die gleiche Anzahl an Sicherungen.
5. (Optional) Wählen Sie für jedes Volume eine logische Standardschnittstelle (Daten-LIFs) aus. Wenn keine ausgewählt ist, werden alle Daten-LIFs in der Ziel-SVM konfiguriert, die das Volume-Zugriffsprotokoll unterstützen.
6. (Optional) Wählen Sie eine Exportrichtlinie für alle NFS-Volumes aus. Wenn diese Option nicht ausgewählt

ist, wird die Standard-Exportrichtlinie verwendet.



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

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

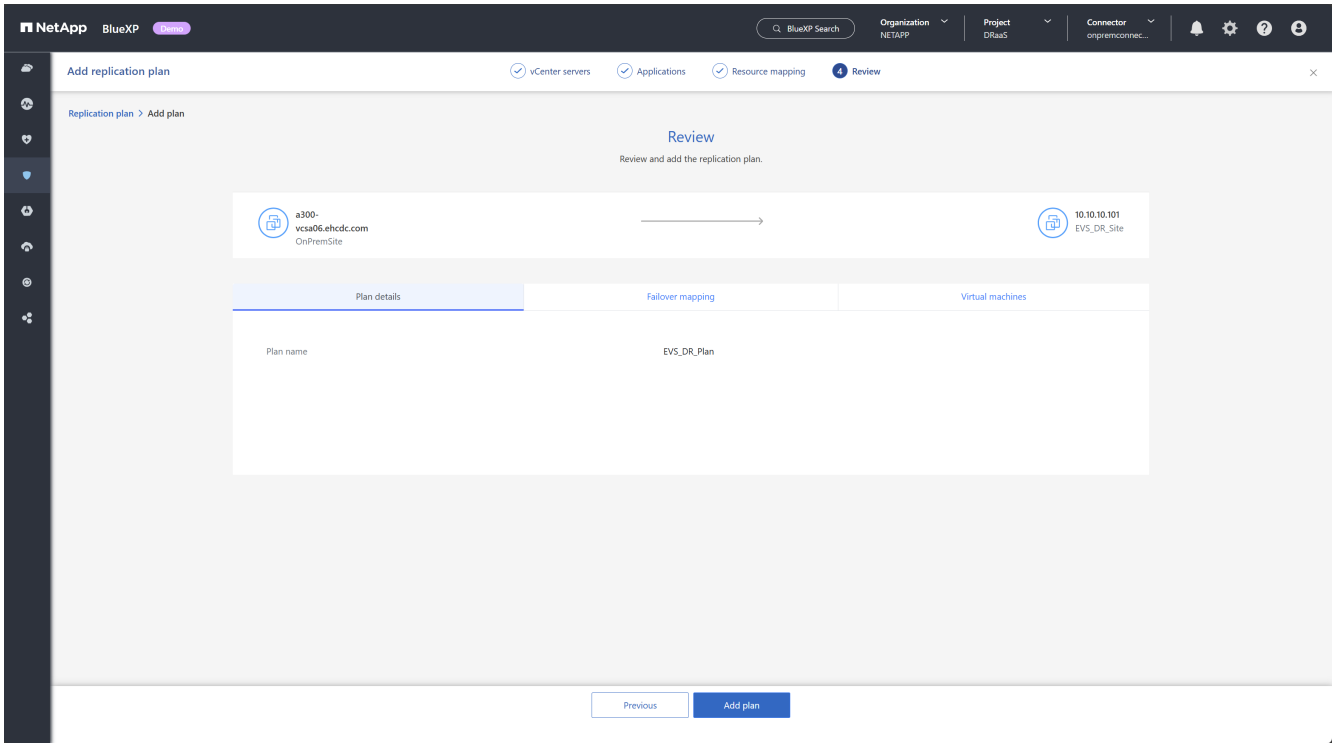
Nachdem Sie die Replikationsplaninformationen in der BlueXP-Notfallwiederherstellung hinzugefügt haben, überprüfen Sie, ob die eingegebenen Informationen richtig sind.

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



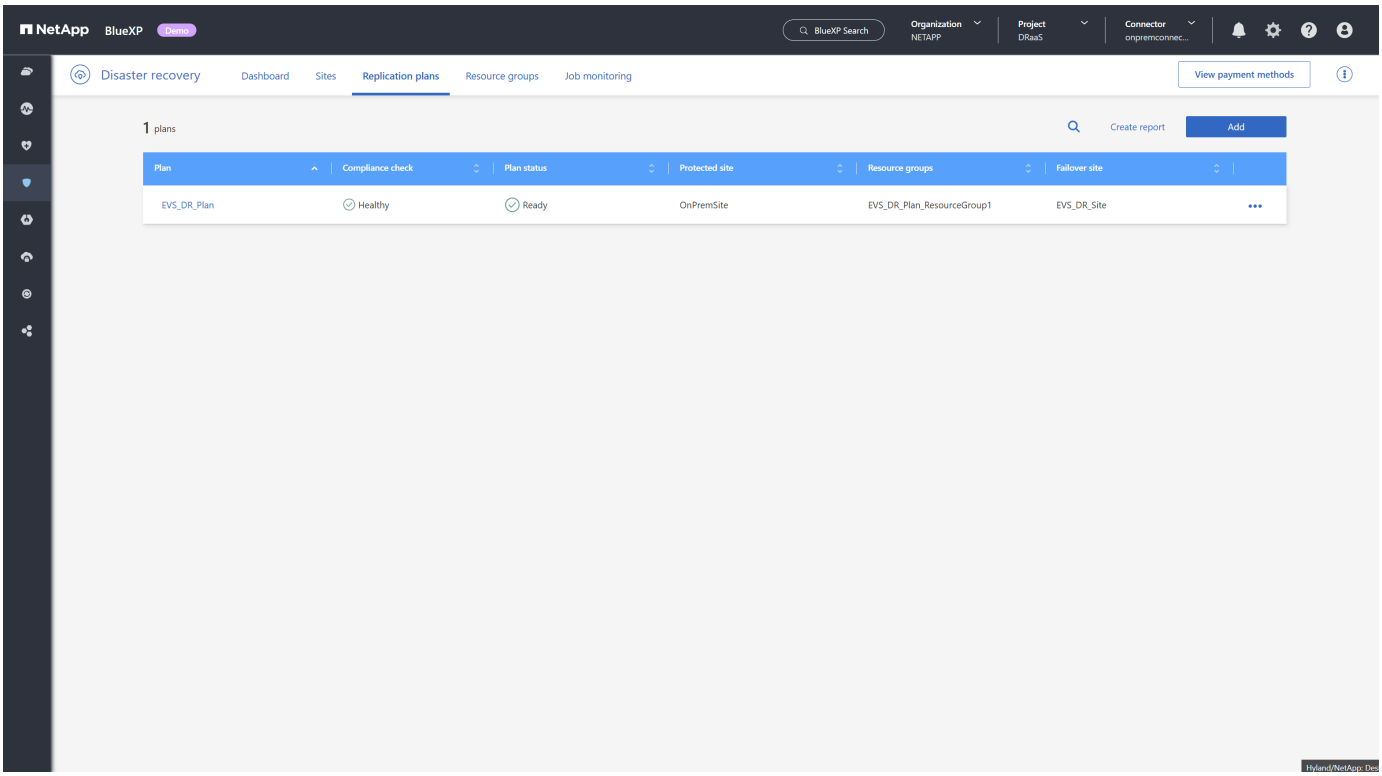
2. Wenn Sie sicher sind, dass alle Einstellungen korrekt sind, wählen Sie unten auf dem Bildschirm **Plan hinzufügen** aus.

Weiter mit "Überprüfen des Replikationsplans" .

Überprüfen Sie, ob bei der Notfallwiederherstellung von BlueXP alles funktioniert

Nachdem Sie den Replikationsplan in BlueXP Disaster Recovery hinzugefügt haben, gelangen Sie zurück zur Seite „Replikationspläne“, wo Sie Ihre Replikationspläne und deren Status einsehen können. Stellen Sie sicher, dass der Replikationsplan den Status „Intakt“ aufweist. Ist dies nicht der Fall, überprüfen Sie den Status des Replikationsplans und beheben Sie alle Probleme, bevor Sie fortfahren.

Abbildung: Seite „Replikationspläne“



BlueXP Disaster Recovery führt eine Reihe von Tests durch, um sicherzustellen, dass alle Komponenten (ONTAP-Cluster, vCenter-Cluster und VMs) zugänglich sind und sich im korrekten Zustand befinden, damit der Dienst die VMs schützen kann. Dieser sogenannte Compliance-Check wird 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 (Ziel-Site)

Führen Sie Replikationsplanvorgänge mit BlueXP Disaster Recovery durch

Verwenden Sie die Notfallwiederherstellung von BlueXP mit Amazon EVS und Amazon FSx für 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 stattfindet: ein Failover zum DR-(Ziel-)Rechenzentrum im Falle eines katastrophalen Fehlers am Produktionsstandort vor Ort.

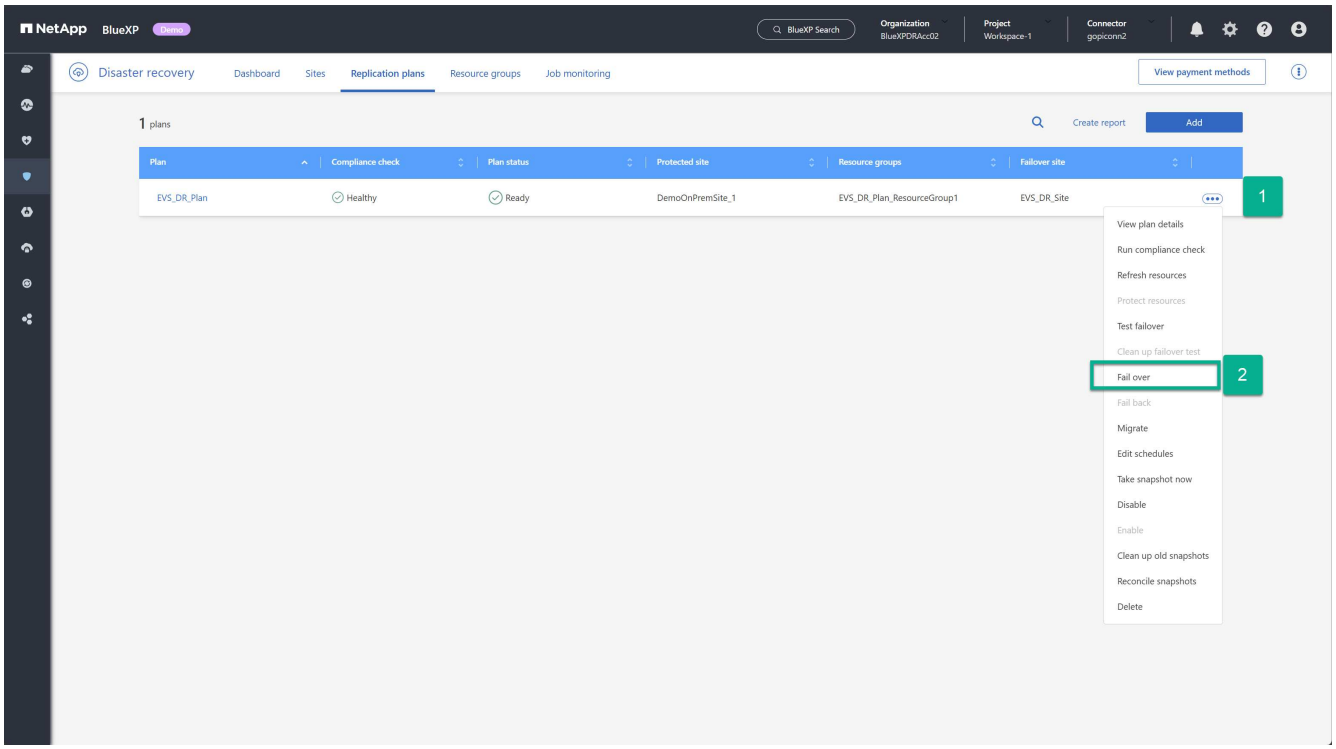
Failover ist ein manuell initiierter Prozess.

Schritte zum Zugriff auf den Failover-Vorgang

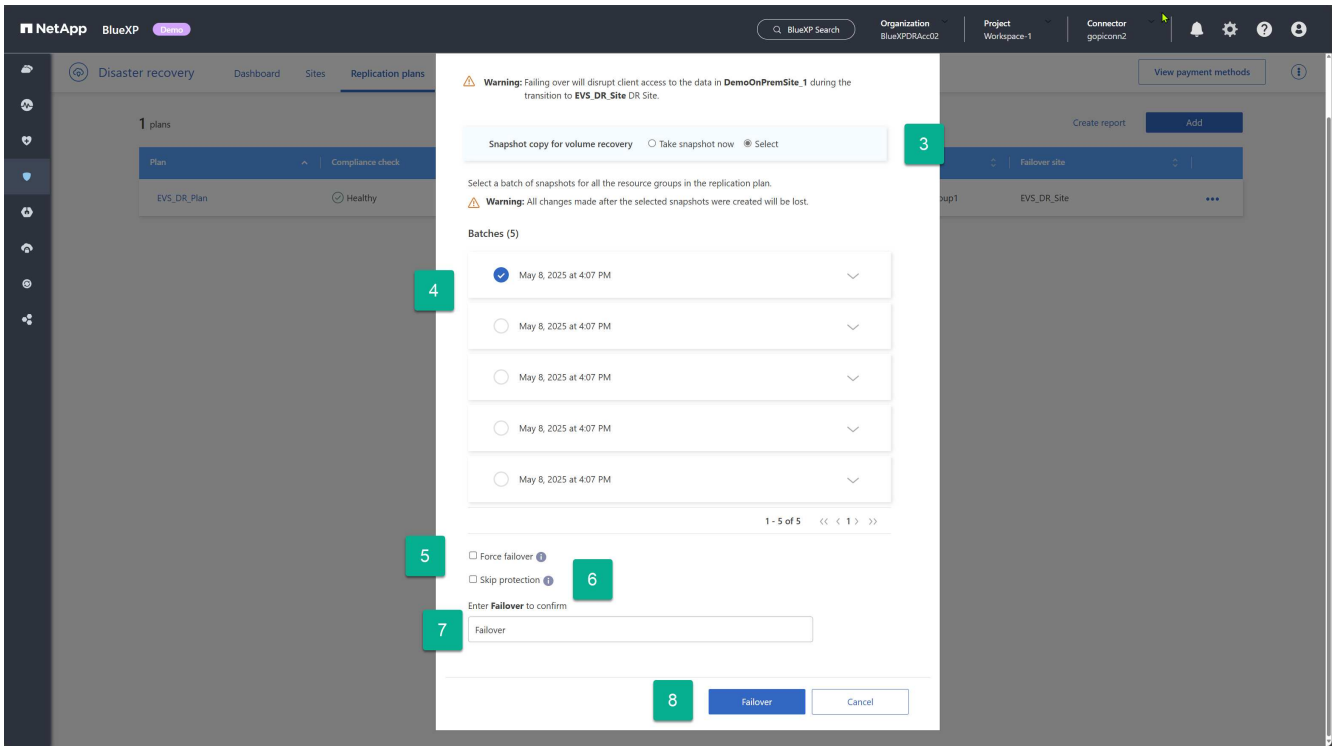
1. Wählen Sie in der linken Navigation von BlueXP **Schutz** > **Notfallwiederherstellung**.
2. Wählen Sie im BlueXP-Notfallwiederherstellungsmenü **Replikationspläne** aus.

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 (geschützte) Produktionssite 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 BlueXP 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 BlueXP Disaster Recovery nach der Wiederherstellung der Produktionssite 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 Sie den Failover

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

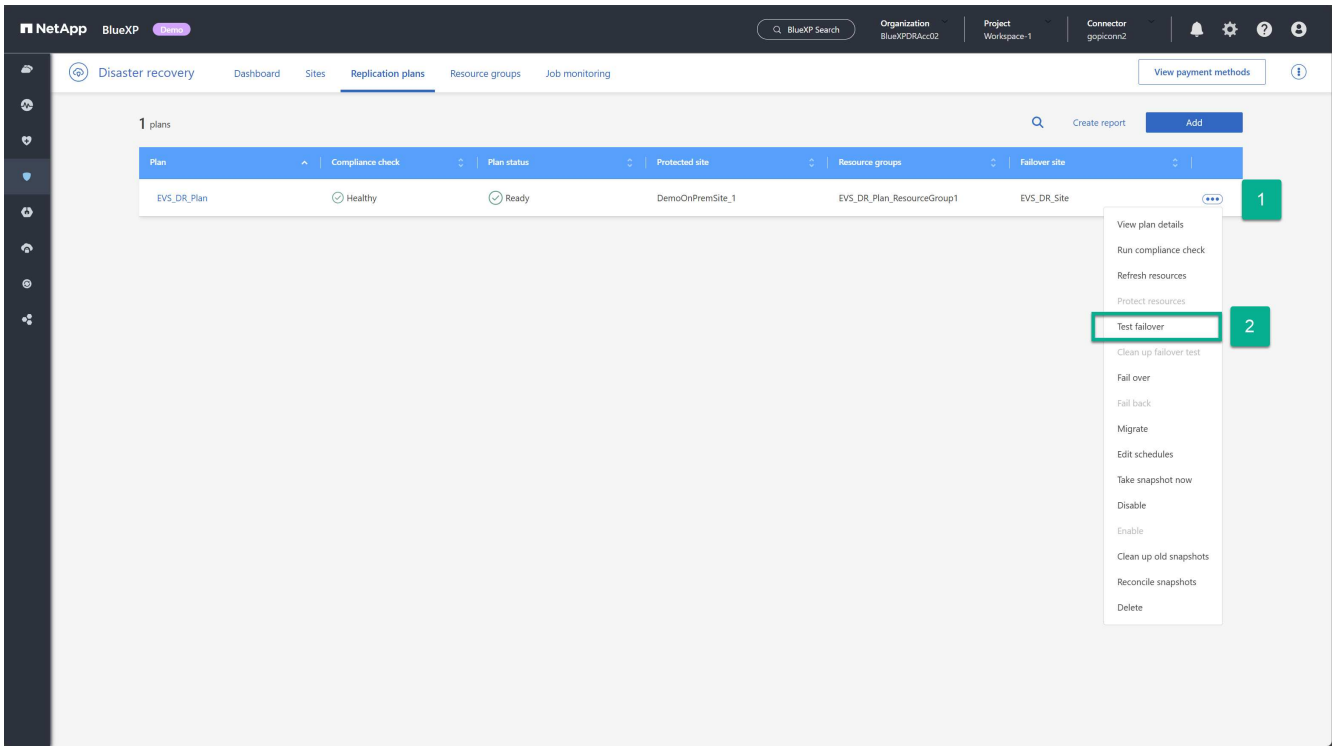
- Die Produktionssite ist noch aktiv und alle VMs funktionieren weiterhin wie erwartet.
- Der BlueXP-Notfallwiederherstellungsschutz der Produktions-VMs wird fortgesetzt.

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

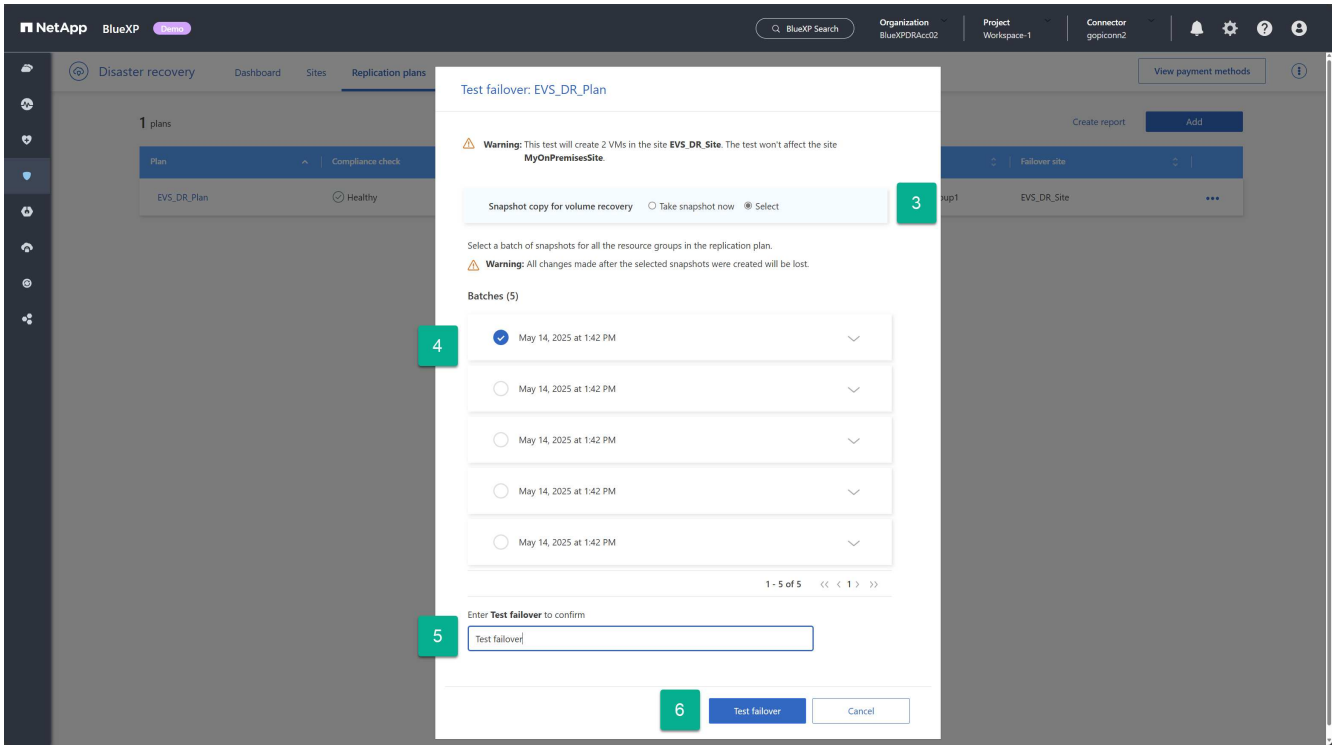
Die Schritte zum Ausführen eines Test-Failovers sind identisch mit denen zum Ausführen eines echten Failovers, mit der Ausnahme, dass Sie den Vorgang „Test-Failover“ im Kontextmenü des Replikationsplans verwenden.

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 eine zuvor erstellte Sicherung ausgewählt haben, wählen Sie die Sicherung aus, die 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**.

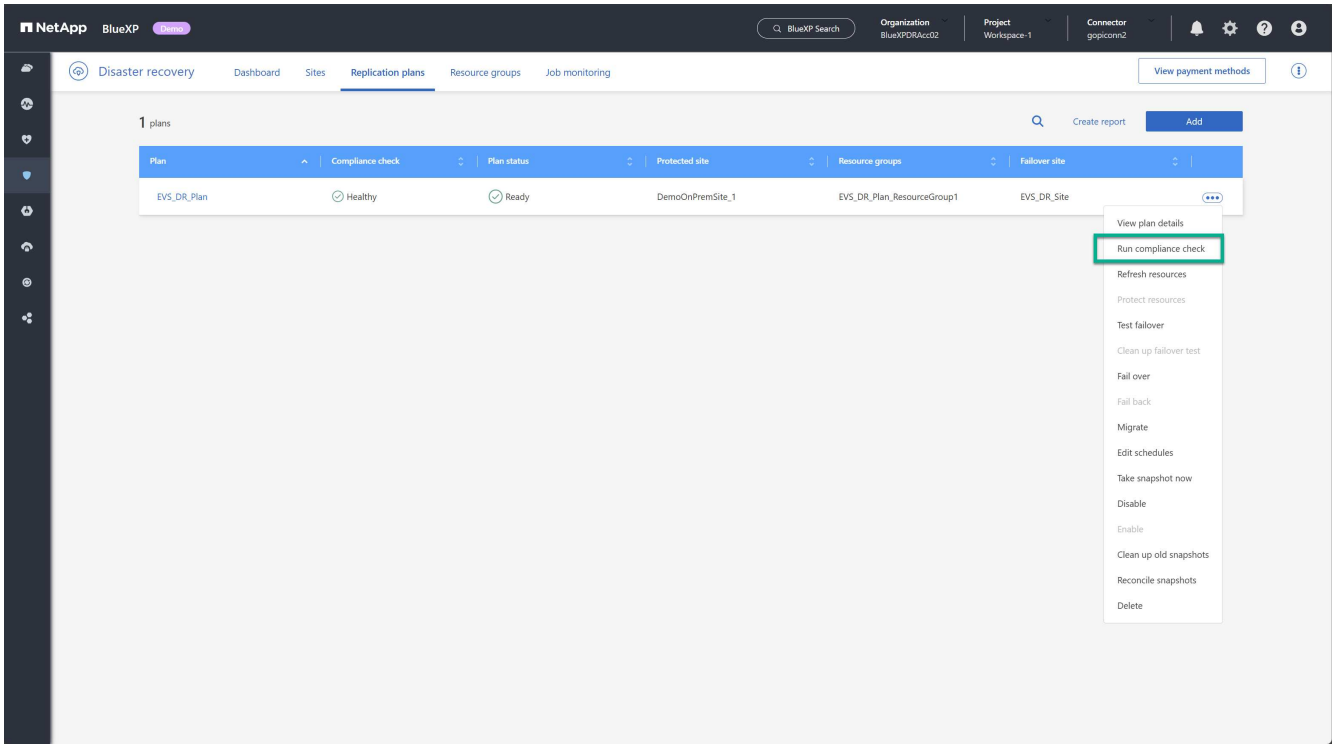


Führen Sie eine Konformitätsprüfung durch

Compliance-Prüfungen werden standardmäßig alle drei Stunden durchgeführt. Sie können jederzeit eine manuelle Compliance-Prüfung durchführen.

Schritte

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



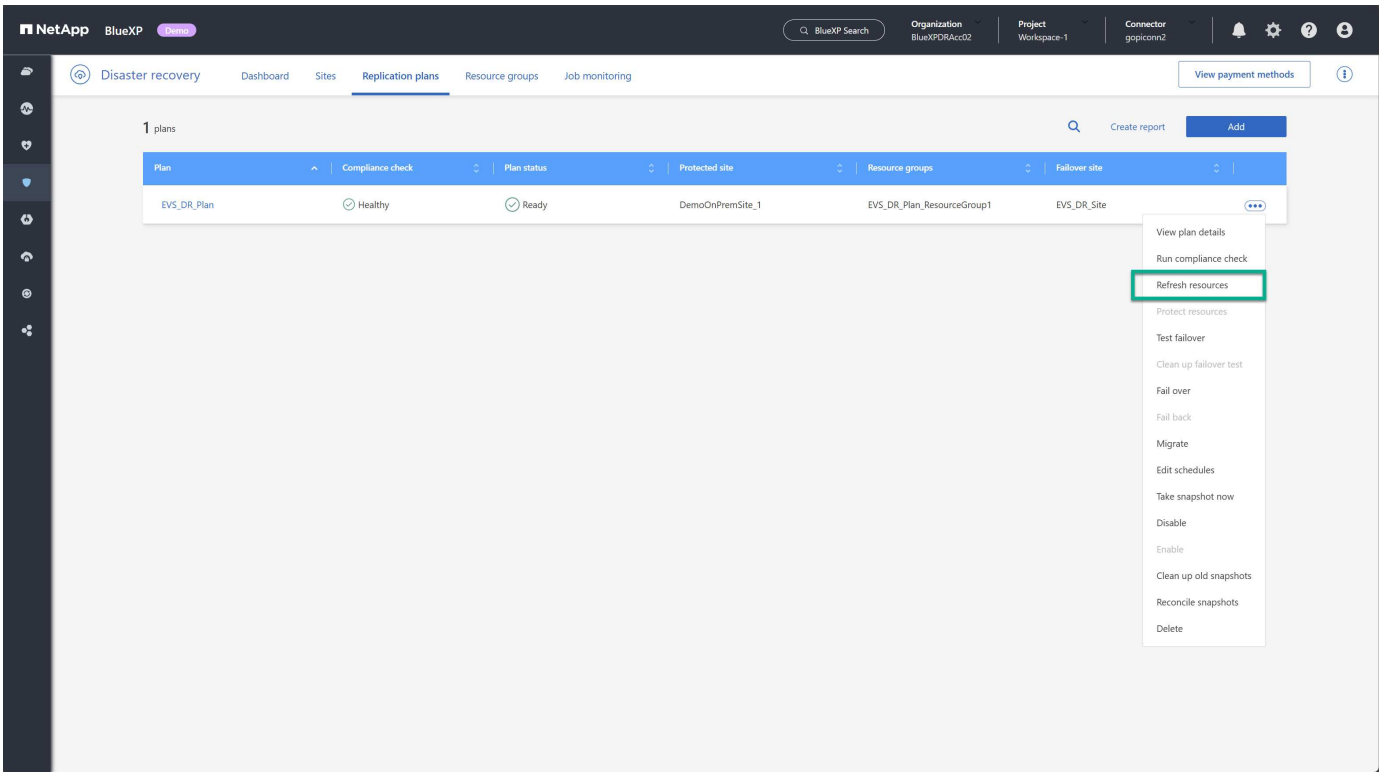
3. Um zu ändern, wie oft BlueXP Disaster Recovery automatisch Konformitätsprüfungen durchführt, wählen Sie die Option **Zeitpläne bearbeiten** aus dem Menü „Aktionen“ des Replikationsplans.

Ressourcen aktualisieren

Bei jeder Änderung Ihrer virtuellen Infrastruktur – beispielsweise beim Hinzufügen oder Löschen von VMs, beim Hinzufügen oder Löschen von Datenspeichern oder beim Verschieben von VMs zwischen Datenspeichern – müssen Sie die betroffenen vCenter-Cluster im BlueXP Disaster Recovery Service aktualisieren. Der Service 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:

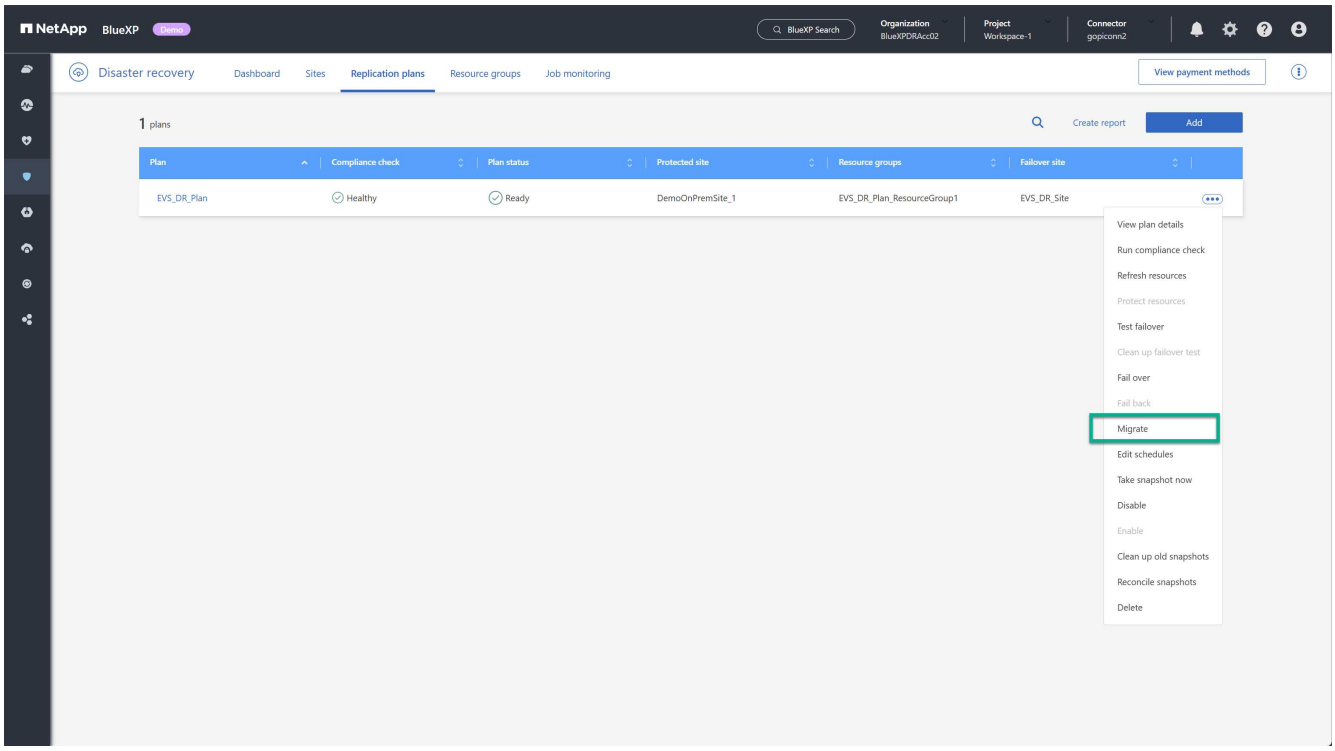
- vCenter-Aktualisierung: Führen Sie immer dann eine vCenter-Aktualisierung durch, wenn VMs zu einem vCenter-Cluster hinzugefügt, daraus gelöscht oder aus diesem verschoben werden:
- Aktualisierung des Replikationsplans: Führen Sie jedes Mal eine Aktualisierung des Replikationsplans durch, wenn eine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



Migrieren

BlueXP Disaster Recovery wird zwar primär für Notfallwiederherstellungsfälle eingesetzt, ermöglicht aber auch die einmalige Verschiebung einer Gruppe von VMs vom Quell- zum Zielstandort. Dies kann für eine konzertierte Migration in die Cloud oder zur Katastrophenvorbeugung – beispielsweise bei schlechtem Wetter, politischen Unruhen oder anderen potenziell vorübergehenden Katastrophen – genutzt werden.

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:

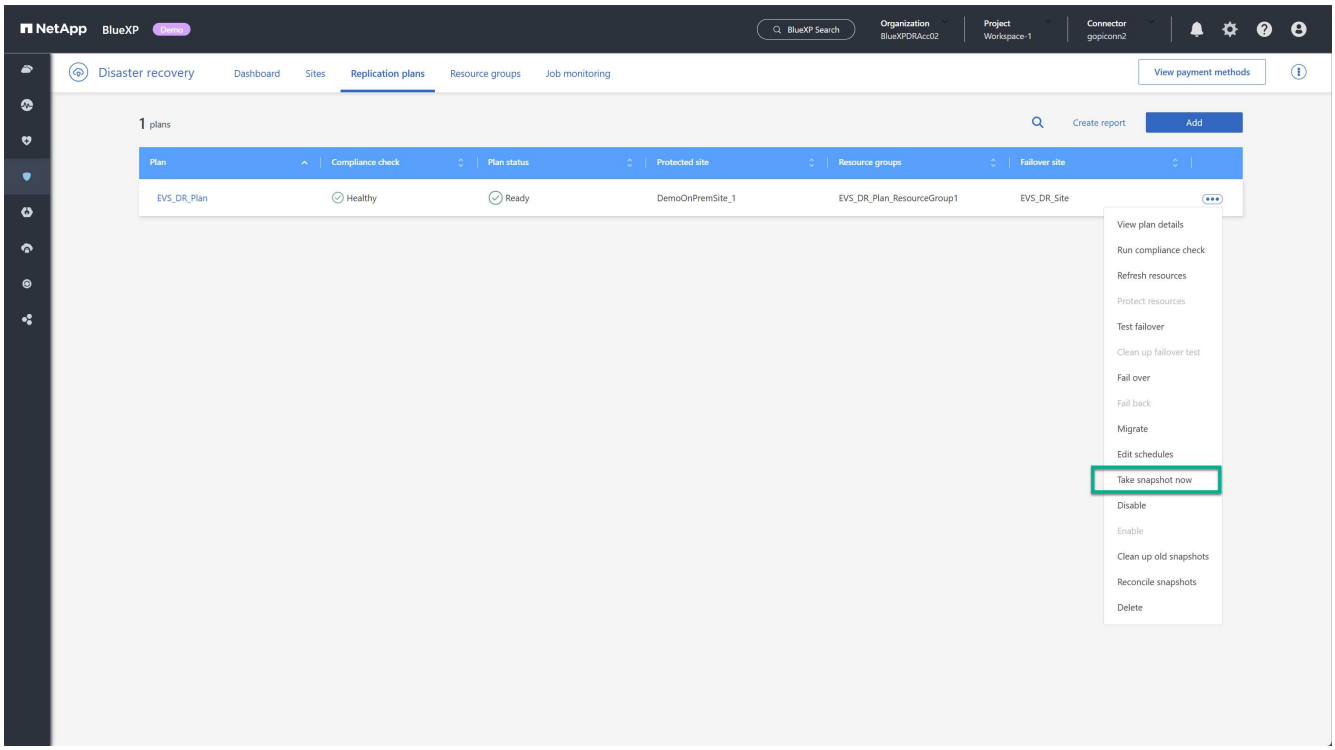


3. Geben Sie Informationen in das Dialogfeld „Migrieren“ ein.

Jetzt Schnappschuss machen

Sie können jederzeit einen sofortigen Snapshot des Replikationsplans erstellen. Dieser Snapshot wird in die Notfallwiederherstellungsüberlegungen von BlueXP einbezogen, 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:

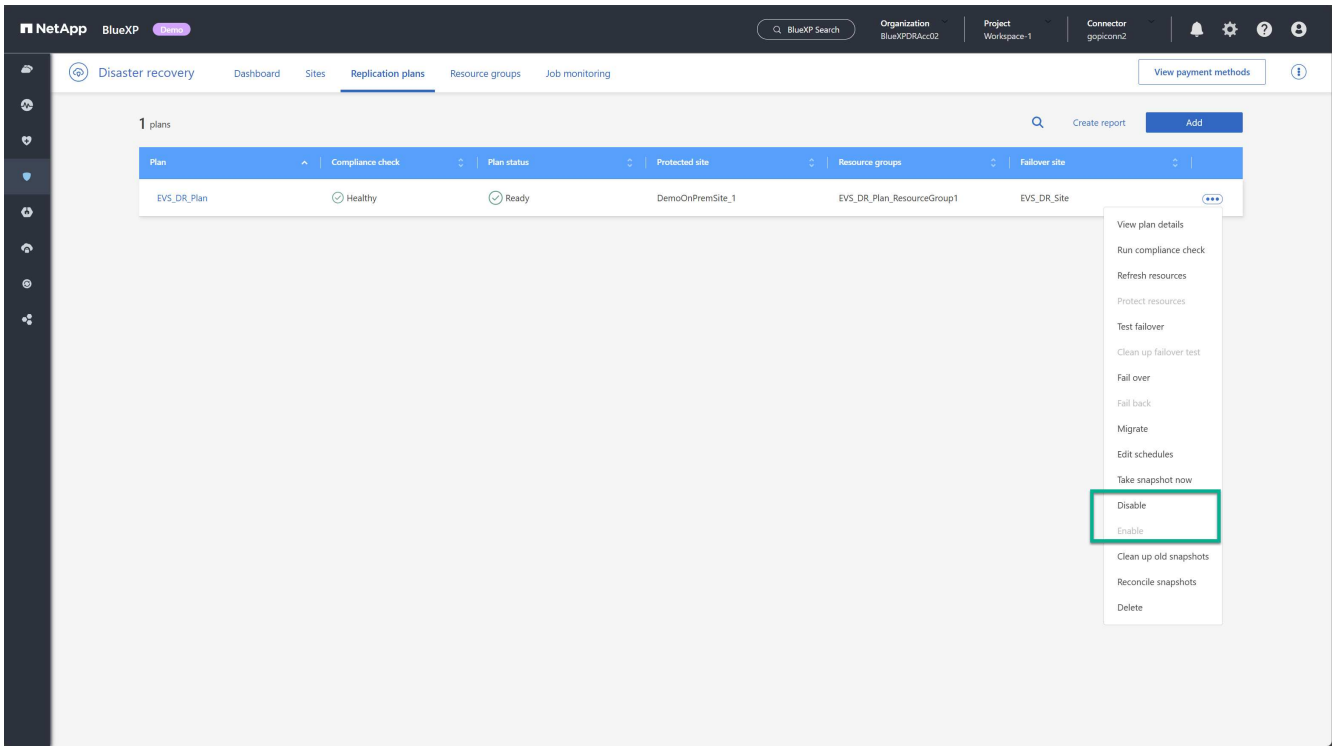


Replikationsplan deaktivieren oder aktivieren

Möglicherweise müssen Sie den Replikationsplan vorübergehend anhalten, um Vorgänge oder Wartungsarbeiten durchzuführen, die den Replikationsprozess beeinträchtigen könnten. Der Dienst bietet eine Methode zum Anhalten 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**.

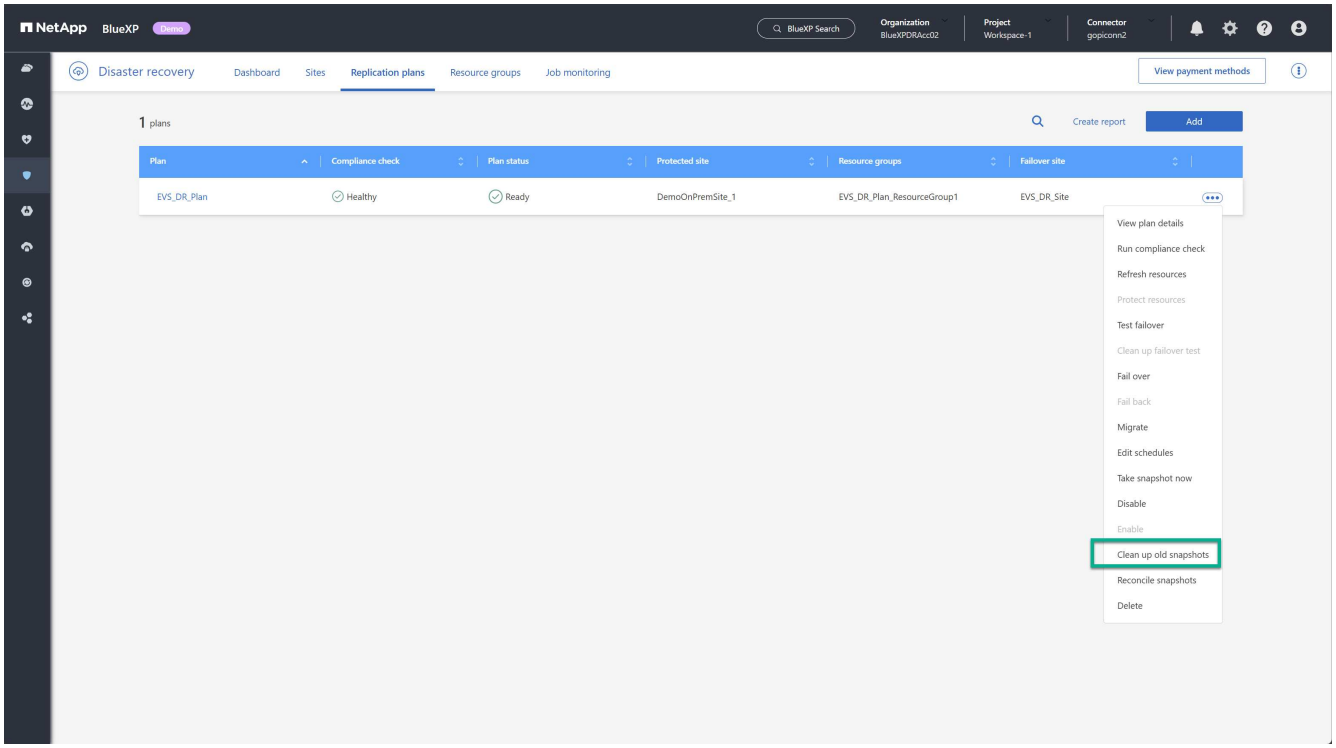
   Wenn der Replikationsplan aktiv ist, ist der Befehl **Aktivieren** ausgegraut. Wenn der Replikationsplan deaktiviert ist, ist der Befehl **Deaktivieren** ausgegraut.



Alte Snapshots bereinigen

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.

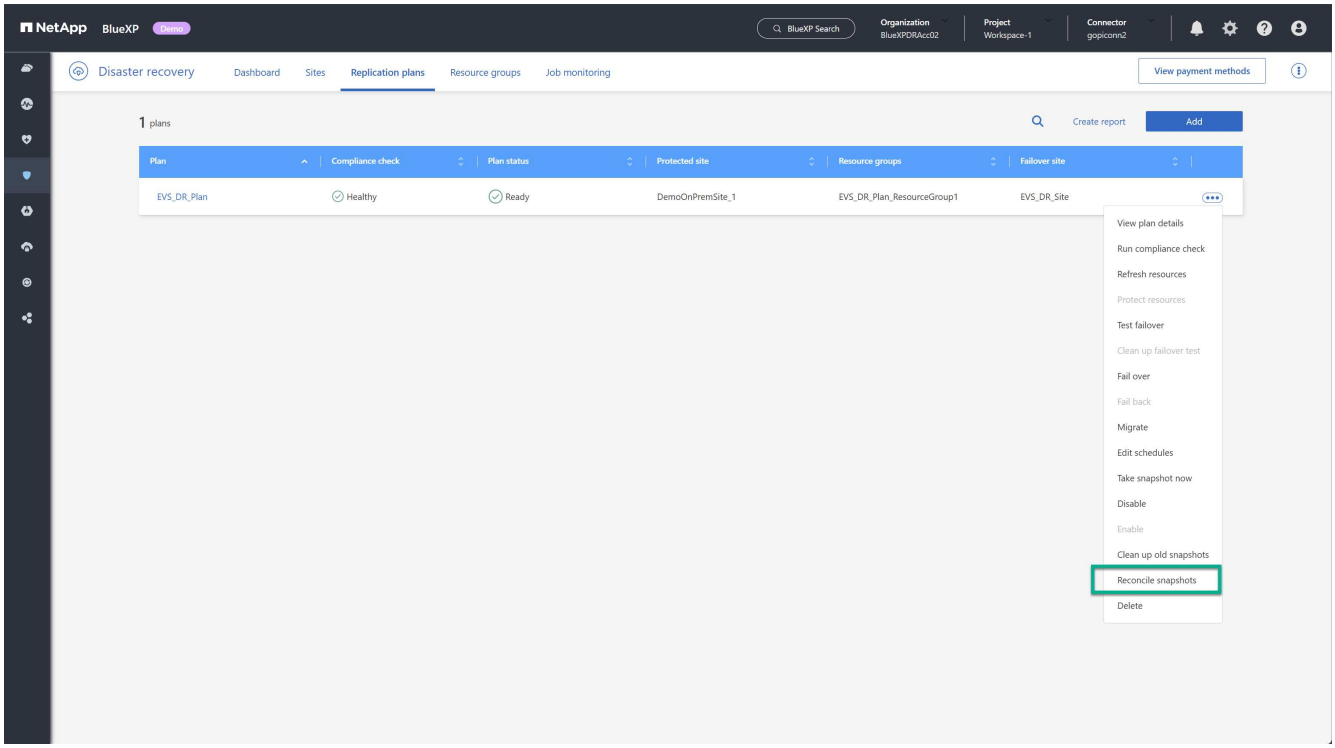
1. Wählen Sie die Option **Aktionen** ••• neben dem Replikationsplan.
2. Um diese älteren Snapshots manuell zu entfernen, wählen Sie im Aktionsmenü des Replikationsplans die Option **Alte Snapshots bereinigen**.



Snapshots abgleichen

Da der Service ONTAP Volume Snapshots orchestriert, kann ein ONTAP Storage-Administrator Snapshots direkt über den ONTAP System Manager, die ONTAP CLI oder die ONTAP REST APIs löschen, ohne dass der Service davon Kenntnis hat. Snapshots auf der Quelle, die sich nicht im Zielcluster befinden, werden automatisch alle 24 Stunden gelöscht. Sie können dies jedoch nach Bedarf durchführen. Mit dieser Funktion können Sie sicherstellen, dass die Snapshots über alle Standorte hinweg konsistent sind.

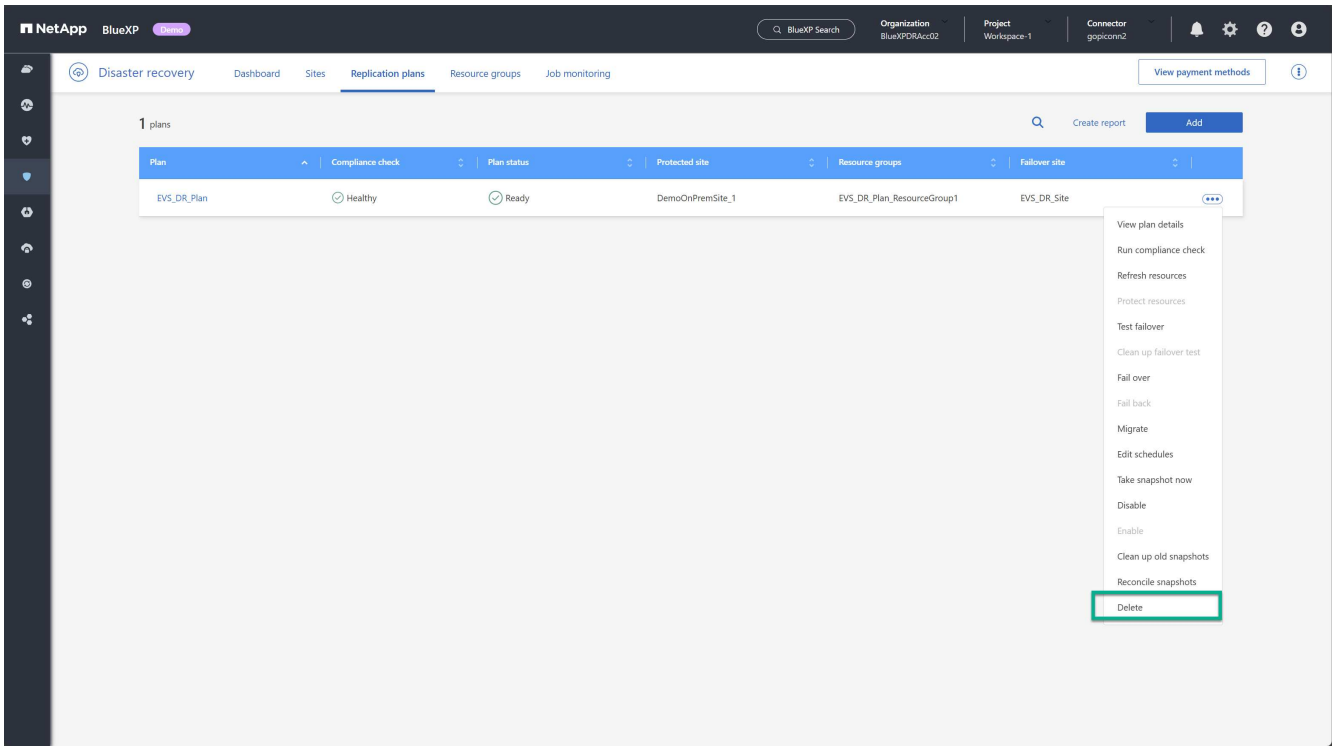
1. Wählen Sie die Option **Aktionen** ••• neben dem Replikationsplan.
2. Um Snapshots aus dem Quellcluster zu löschen, die im Zielcluster nicht vorhanden sind, wählen Sie im Menü „Aktionen“ des Replikationsplans die Option „Snapshots abgleichen“ aus.



Replikationsplan löschen

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

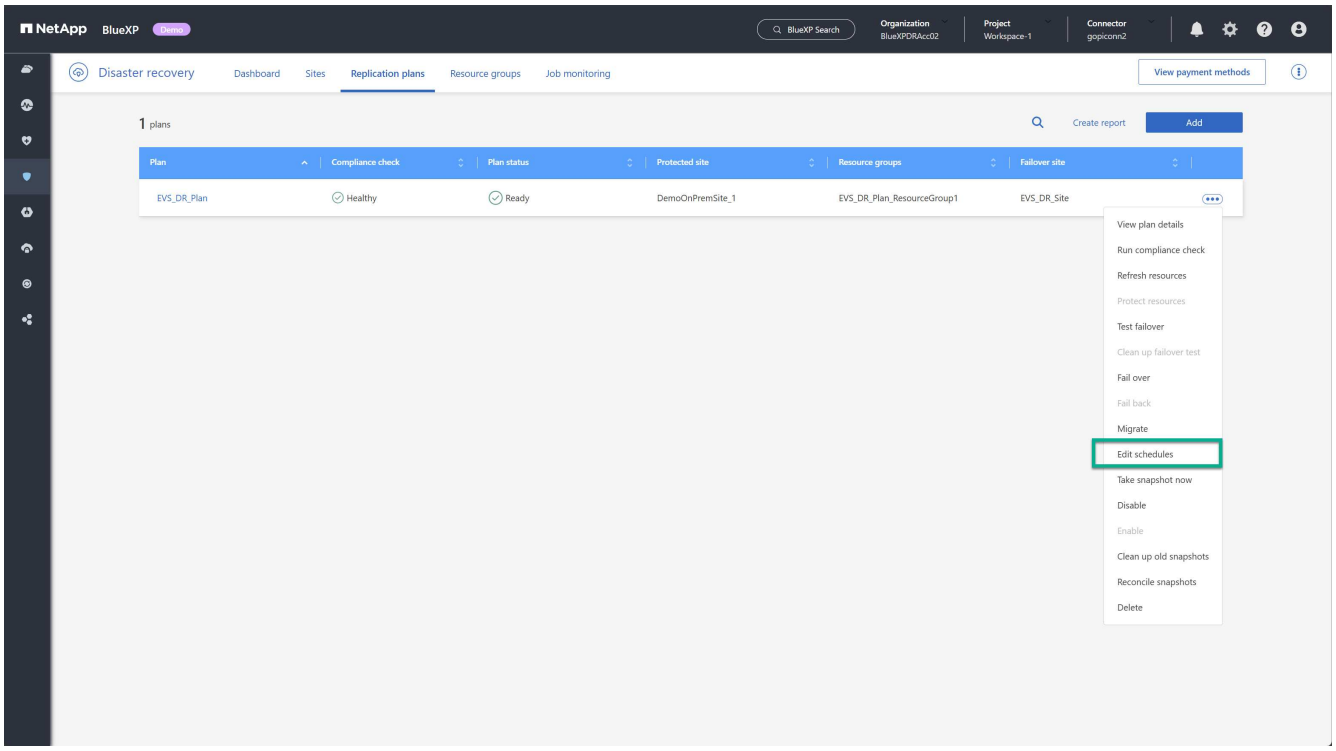
1. Wählen Sie die Option **Aktionen** ••• neben dem Replikationsplan.
2. Um den Replikationsplan zu löschen, wählen Sie **Löschen** aus dem Kontextmenü des Replikationsplans.



Schichtpläne bearbeiten

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

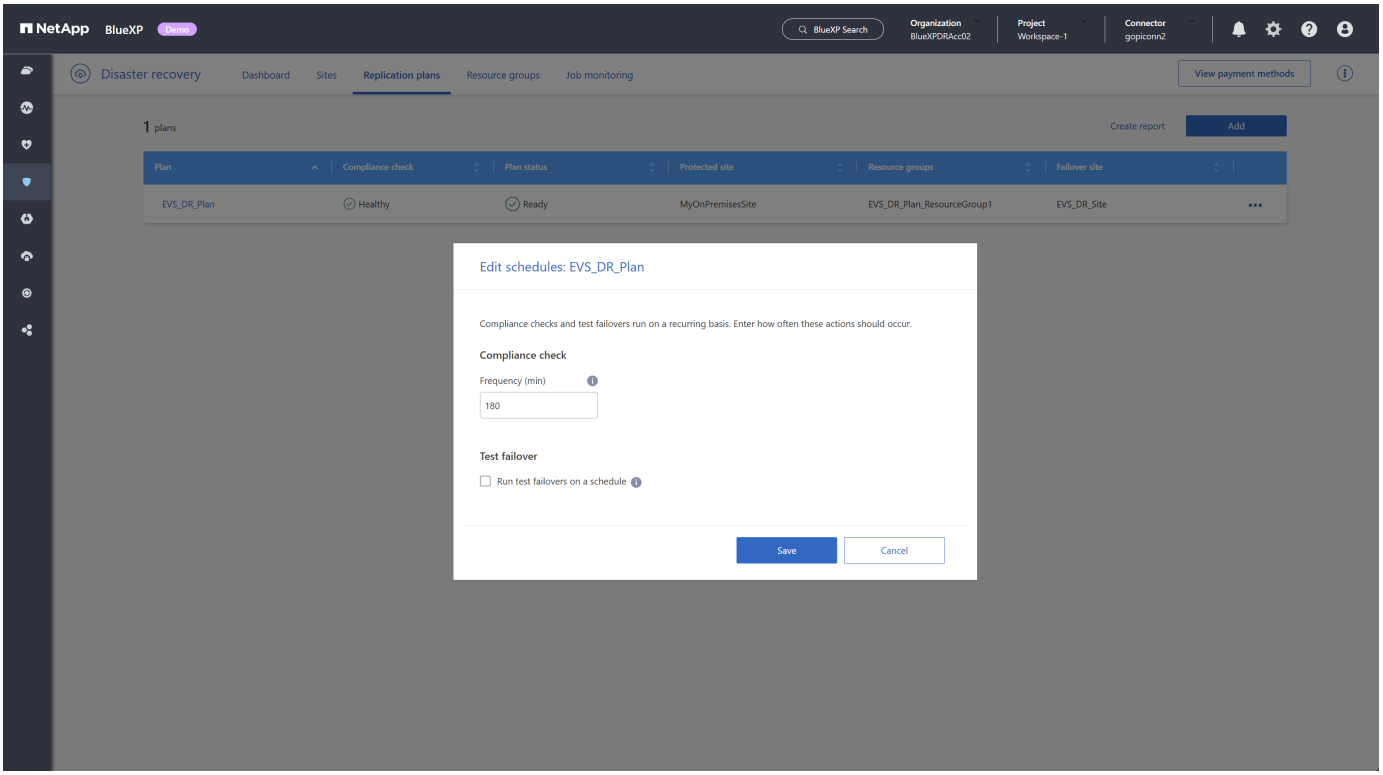
1. Wählen Sie die Option **Aktionen** ••• neben dem Replikationsplan.
2. Um diese Zeitpläne für einen dieser beiden Vorgänge zu ändern, wählen Sie **Zeitpläne bearbeiten** für den Replikationsplan aus.



Ändern des Intervalls für die Konformitätsprüfung

Standardmäßig werden Konformitätsprüfungen alle drei Stunden durchgeführt. Sie können dieses Intervall 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“:



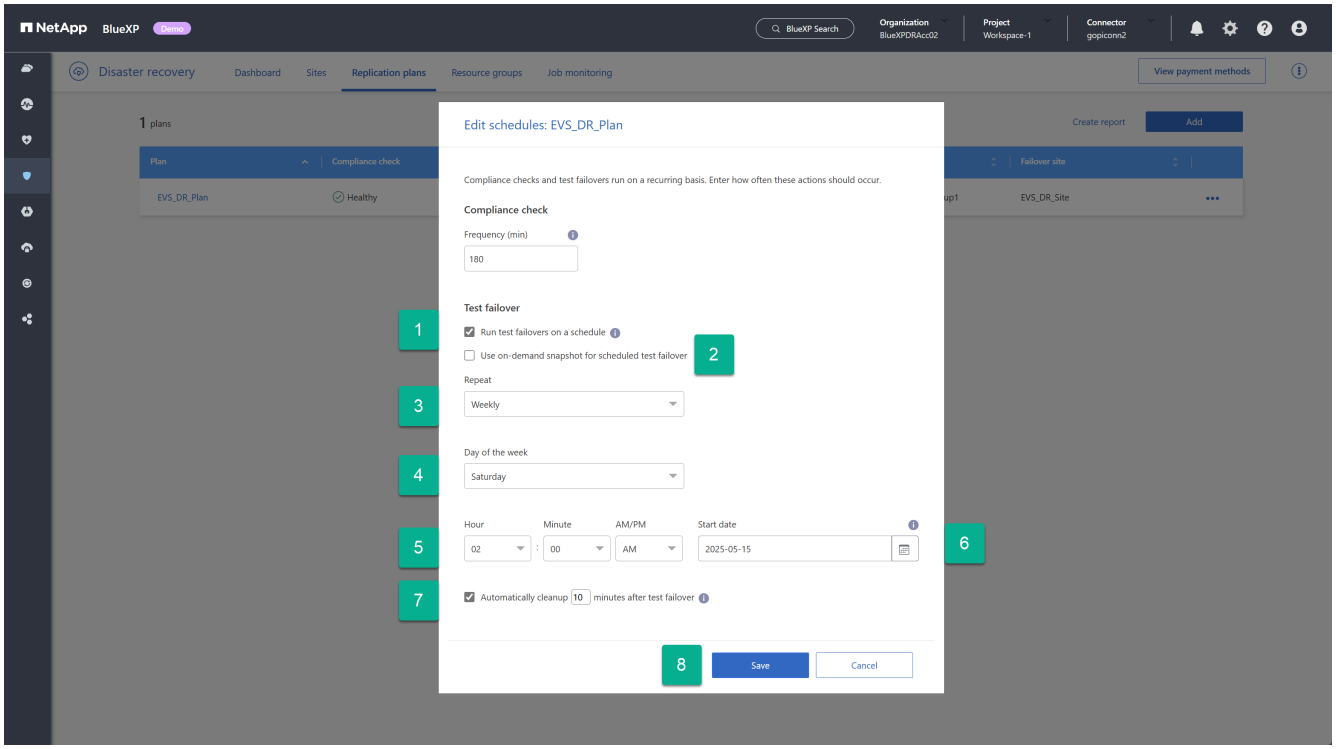
Planen Sie automatisierte Test-Failover

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 Sie den Failover-Prozess" .

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**.



Wissen und Support

Für den Support anmelden

Für den Support von BlueXP und seinen Storage-Lösungen und Services ist eine Support-Registrierung erforderlich. Um wichtige Workflows für Cloud Volumes ONTAP Systeme zu ermöglichen, ist außerdem eine Support-Registrierung erforderlich.

Durch die Registrierung für den Support wird die NetApp-Unterstützung für einen Fileservice eines Cloud-Providers nicht aktiviert. Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Google Cloud NetApp Volumes"

Übersicht über die Support-Registrierung

Es gibt zwei Registrierungsformulare, um die Support-Berechtigung zu aktivieren:

- Registrieren der Seriennummer Ihres BlueXP -Kontos (Ihre 20-stellige Seriennummer 960xxxxxxxxx finden Sie auf der Seite „Support-Ressourcen“ in BlueXP).

  Dies dient als Ihre einzige Support-Abonnement-ID für jeden Service in BlueXP. Jedes BlueXP-Abonnement für Support auf Kontoebene muss registriert werden.

- Registrieren der Cloud Volumes ONTAP Seriennummern für ein Abonnement auf dem Markt Ihres Cloud-Providers (dies sind 20-stellige Seriennummern von 909201xxxxxx).

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

Durch das Registrieren beider Arten von Seriennummern können Kunden Funktionen wie das Öffnen von Support-Tickets und die automatische Erstellung von Support-Cases nutzen. Die Registrierung ist abgeschlossen, indem wie unten beschrieben Konten der NetApp Support Website (NSS) zu BlueXP hinzugefügt werden.

Registrieren Sie BlueXP , um NetApp Support zu erhalten

Um sich für den Support zu registrieren und die Supportberechtigung zu aktivieren, muss ein Benutzer in Ihrer BlueXP Organisation (oder Ihrem Konto) einem NetApp Support Site Konto seine BlueXP Anmeldedaten zuweisen. Wie Sie sich für den NetApp Support registrieren, hängt davon ab, ob Sie bereits über einen NSS Account (NetApp Support Site) verfügen.

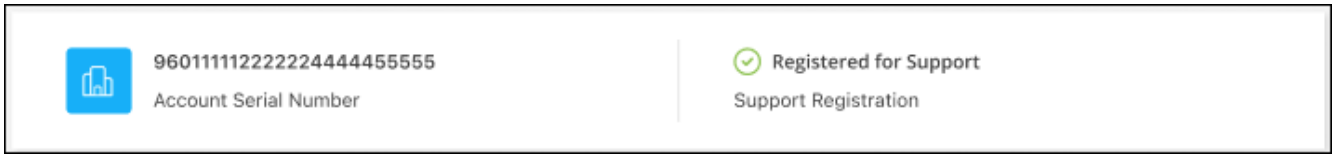
Bestandskunde mit NSS-Konto

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

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Symbol Einstellungen, und wählen Sie **Credentials** aus.
2. Wählen Sie **Benutzeranmeldeinformationen**.
3. Wählen Sie **NSS-Anmeldeinformationen hinzufügen** und folgen Sie der Eingabeaufforderung für die NetApp-Support-Website (NSS)-Authentifizierung.
4. Um zu bestätigen, dass die Registrierung erfolgreich war, wählen Sie das Hilfesymbol und dann **Support**.

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



   Beachten Sie, dass andere BlueXP Benutzer diesen Support-Registrierungsstatus nicht sehen, wenn sie ihrem BlueXP Login kein NetApp Support Site Konto zugeordnet haben. Das bedeutet jedoch nicht, dass Ihre BlueXP -Organisation nicht für Support registriert ist. Solange ein Benutzer in der Organisation diese Schritte befolgt hat, wurde Ihr Unternehmen registriert.

Vorhandener Kunde, aber kein NSS-Konto

Wenn Sie bereits NetApp Kunde sind und über vorhandene Lizenzen und Seriennummern sowie *No* NSS Konto verfügen, müssen Sie ein NSS Konto erstellen und es Ihren BlueXP Anmeldedaten zuordnen.

Schritte

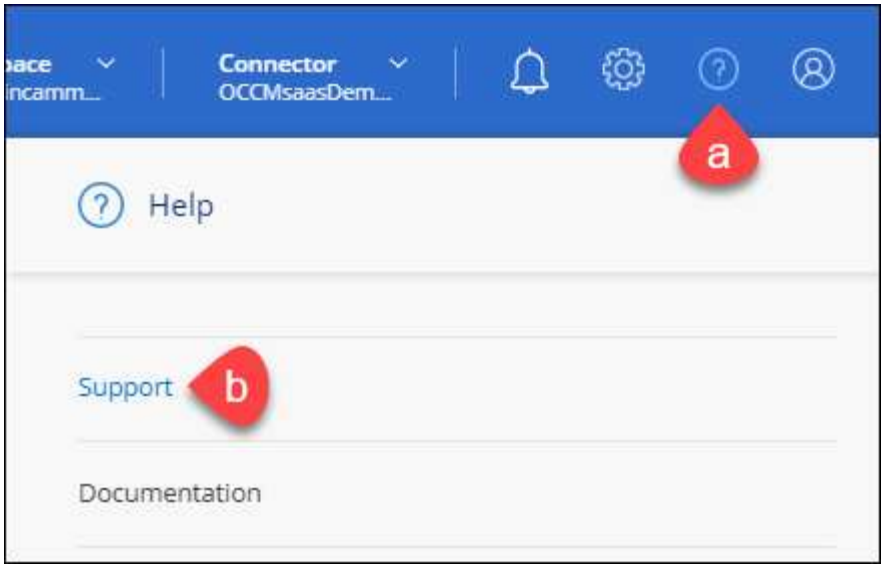
1. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie unbedingt die oben verwendete BlueXP-Kontonummer (960xxxx) für das Feld Seriennummer. Dadurch wird die Kontobearbeitung beschleunigt.
2. Ordnen Sie Ihr neues NSS-Konto Ihrer BlueXP Anmeldung zu, indem Sie die unter aufgeführten Schritte durchführen Bestandskunde mit NSS-Konto.

Neu bei NetApp

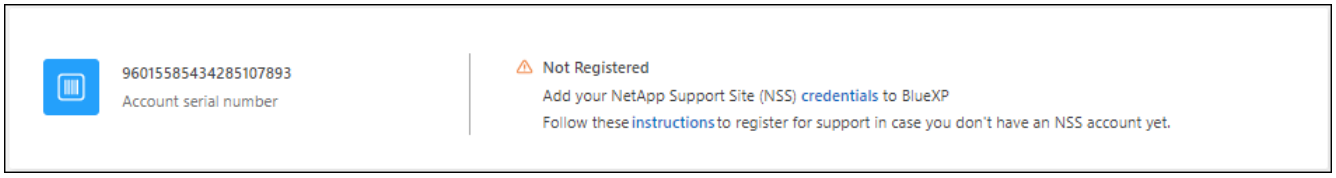
Wenn Sie neu bei NetApp sind und über keinen NSS-Account verfügen, befolgen Sie jeden Schritt unten.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



2. Suchen Sie auf der Seite für die Support-Registrierung die Seriennummer Ihres Kontos.



3. Navigieren Sie zu "Die Support-Registrierungs-Website von NetApp" Und wählen Sie **Ich bin kein registrierter NetApp Kunde**.
4. Füllen Sie die Pflichtfelder aus (mit roten Sternchen).
5. Wählen Sie im Feld **Product Line** die Option **Cloud Manager** aus, und wählen Sie dann den gewünschten Abrechnungsanbieter aus.
6. Kopieren Sie die Seriennummer des Kontos von Schritt 2 oben, füllen Sie die Sicherheitsprüfung aus und bestätigen Sie dann, dass Sie die globale Datenschutzrichtlinie von NetApp lesen.

   Zur Fertigstellung dieser sicheren Transaktion wird sofort eine E-Mail an die angegebene Mailbox gesendet. Überprüfen Sie Ihre Spam-Ordner, wenn die Validierungs-E-Mail nicht in wenigen Minuten ankommt.

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

   Indem Sie Ihre Anfrage an NetApp senden, wird Ihnen die Erstellung eines NetApp Support Site Kontos empfohlen.

8. Erstellen Sie einen NetApp Support Site Account, indem Sie den ausfüllen "NetApp Support Site-Formular zur Benutzerregistrierung"
   a. Stellen Sie sicher, dass Sie die entsprechende Benutzerebene wählen, die normalerweise **NetApp Kunde/Endbenutzer** ist.
   b. Kopieren Sie die oben angegebene Seriennummer (960xxxx) für das Feld „Seriennummer“. Dadurch wird die Verarbeitung beschleunigt.

Nachdem Sie fertig sind

NetApp sollte sich bei diesem Prozess mit Ihnen in Verbindung setzen. Dies ist eine einmalige Onboarding-Übung für neue Benutzer.

Wenn Sie über Ihren NetApp Support Site Account verfügen, ordnen Sie das Konto Ihrer BlueXP Anmeldung zu, indem Sie die Schritte unter ausführen Bestandskunde mit NSS-Konto.

Verknüpfen von NSS-Anmeldeinformationen für den Cloud Volumes ONTAP-Support

Um die folgenden wichtigen Workflows für Cloud Volumes ONTAP zu ermöglichen, müssen die Zugangsdaten auf der NetApp Support Website Ihrer BlueXP Abteilung zugeordnet werden:

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

  Die Bereitstellung Ihres NSS Kontos ist erforderlich, um Support für Ihr System zu aktivieren und Zugang zu den technischen Support-Ressourcen von NetApp zu erhalten.

- Implementierung von Cloud Volumes ONTAP unter Verwendung von BYOL (Bring-Your-Own-License)

  Die Bereitstellung Ihres NSS-Kontos ist erforderlich, damit BlueXP Ihren Lizenzschlüssel hochladen und das Abonnement für den von Ihnen erworbenen Zeitraum aktivieren kann. Dies schließt automatische Updates für Vertragsverlängerungen ein.

- Aktualisieren der Cloud Volumes ONTAP Software auf die neueste Version

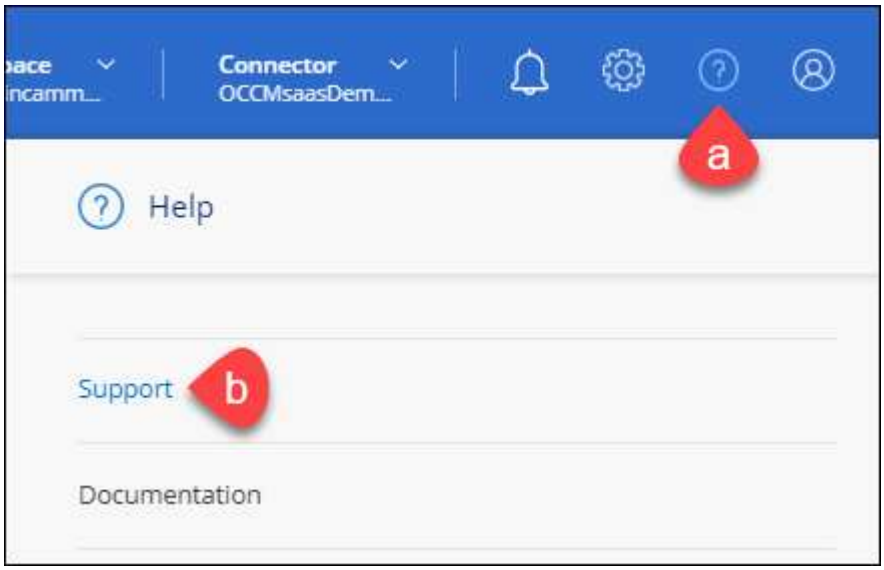
Das Zuordnen von NSS-Anmeldeinformationen zu Ihrer BlueXP -Organisation unterscheidet sich von dem NSS-Konto, das mit einer BlueXP -Benutzeranmeldung verknüpft ist.

Diese NSS-Anmeldedaten 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 einen Partner- oder Reseller-Account haben, können Sie ein oder mehrere NSS-Konten hinzufügen, können aber nicht neben Kunden-Level Accounts hinzugefügt werden.

Schritte

1. Klicken Sie oben rechts auf der BlueXP Konsole auf das Hilfesymbol und wählen Sie **Support** aus.



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

   NetApp verwendet Microsoft Entra ID als Identitätsanbieter für Authentifizierungsservices, die speziell auf Support und Lizenzierung zugeschnitten sind.

4. Geben Sie auf der Anmeldeseite die registrierte E-Mail-Adresse und das Kennwort Ihrer NetApp Support Site an, um den Authentifizierungsvorgang durchzuführen.

   Mit diesen Aktionen kann BlueXP Ihr NSS-Konto für Dinge wie Lizenzdownloads, Softwareaktualisierungs-Verifizierung und zukünftige Support-Registrierungen verwenden.

   Beachten Sie Folgendes:

   - Das NSS-Konto muss ein Konto auf Kundenebene sein (kein Gast- oder Temporärkonto). Sie können mehrere NSS-Konten auf Kundenebene haben.
   - Es kann nur ein NSS-Konto vorhanden sein, wenn es sich bei diesem Konto um ein Partner-Level-Konto 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 es bereits NSS-Benutzer unterschiedlichen Typs gibt.“

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

   - Bei der erfolgreichen Anmeldung wird NetApp den NSS-Benutzernamen speichern.

     Dies ist eine vom System generierte ID, die Ihrer E-Mail zugeordnet ist. Auf der Seite **NSS Management** können Sie Ihre E-Mail über anzeigen ••• Menü.

   - Wenn Sie jemals Ihre Anmeldeinformationen aktualisieren müssen, gibt es im auch eine **Anmeldeinformationen aktualisieren**-Option ••• Menü.

     Wenn Sie diese Option verwenden, werden Sie aufgefordert, sich erneut anzumelden. Beachten Sie, dass das Token für diese Konten nach 90 Tagen abläuft. Eine Benachrichtigung wird gesendet, um Sie darüber zu informieren.

Holen Sie sich Hilfe

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.

Unterstützung für Fileservices von Cloud-Providern

Technischen Support zu Fileservices von Cloud-Providern, zu seiner Infrastruktur oder zu beliebigen Lösungen, die den Service verwenden, finden Sie im Abschnitt „Hilfe erhalten“ in der BlueXP Dokumentation zu diesem Produkt.

- "Amazon FSX für ONTAP"
- "Azure NetApp Dateien"
- "Google Cloud NetApp Volumes"

Wenn Sie technischen Support für BlueXP und seine Storage-Lösungen und -Services erhalten möchten, nutzen Sie die unten beschriebenen Support-Optionen.

Nutzen Sie Self-Support-Optionen

Diese Optionen sind kostenlos verfügbar, 24 Stunden am Tag, 7 Tage die Woche:

- Dokumentation

  Die BlueXP-Dokumentation, die Sie gerade anzeigen.

- "Wissensdatenbank"

  Suchen Sie in der BlueXP Knowledge Base nach hilfreichen Artikeln zur Fehlerbehebung.

- "Communitys"

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

Erstellen Sie einen Fall mit dem NetApp Support

Zusätzlich zu den oben genannten Self-Support-Optionen können Sie gemeinsam mit einem NetApp Support-Experten eventuelle Probleme nach der Aktivierung des Supports beheben.

Bevor Sie beginnen

- Um die Funktion **Fall erstellen** nutzen zu können, müssen Sie zunächst Ihre Anmeldedaten für die NetApp Support-Website mit Ihren BlueXP Anmeldedaten verknüpfen. "Managen Sie Zugangsdaten für Ihre BlueXP Anmeldung".
- Wenn Sie einen Fall für ein ONTAP System mit einer Seriennummer eröffnen, muss Ihr NSS-Konto mit der Seriennummer des Systems verknüpft sein.

Schritte

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

   a. Wählen Sie **Rufen Sie uns an**, wenn Sie mit jemandem am Telefon sprechen 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 mit einem NetApp-Supportspezialisten zu öffnen:

      - **Service**: Wählen Sie den Dienst aus, mit dem das Problem verknüpft ist. Beispiel: BlueXP, wenn es sich um ein Problem des technischen Supports mit Workflows oder Funktionen im Service handelt.
      - **Arbeitsumgebung**: Wählen Sie **Cloud Volumes ONTAP** oder **On-Prem** und anschließend die zugehörige Arbeitsumgebung aus.

        Die Liste der Arbeitsumgebungen liegt im Bereich der BlueXP -Organisation (oder des Accounts), des Projekts (oder des Arbeitsbereichs) und des Connectors, den Sie im oberen Banner des

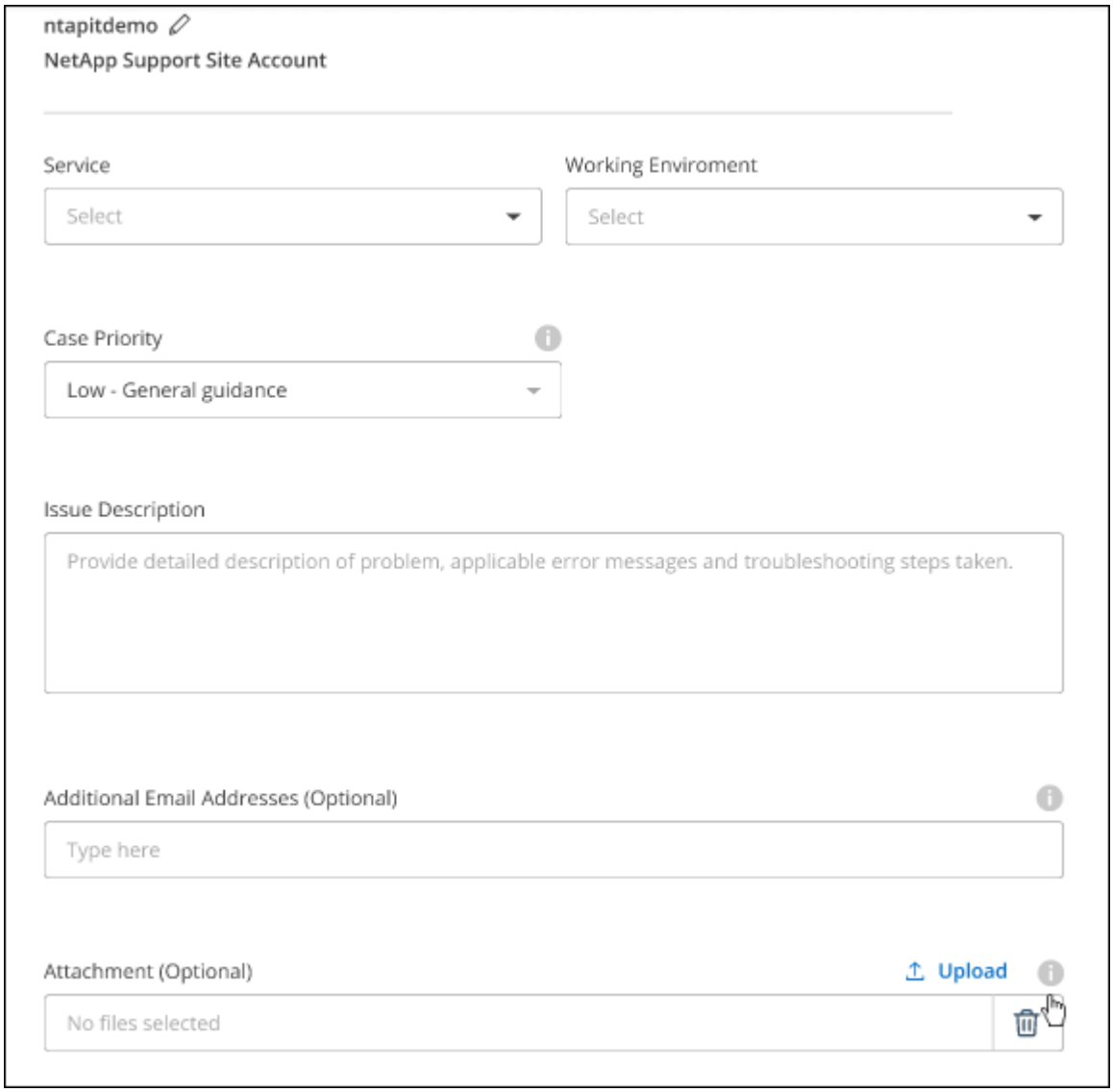
Service ausgewählt haben.

- **Case Priority**: Wählen Sie die Priorität für den Fall, der niedrig, Mittel, hoch oder kritisch sein kann.

  Wenn Sie weitere Informationen zu diesen Prioritäten wünschen, bewegen Sie den Mauszeiger über das Informationssymbol neben dem Feldnamen.

- **Problembeschreibung**: Geben Sie eine detaillierte Beschreibung Ihres Problems an, einschließlich aller anwendbaren Fehlermeldungen oder Fehlerbehebungsschritte, die Sie durchgeführt haben.
- **Zusätzliche E-Mail-Adressen**: Geben Sie zusätzliche E-Mail-Adressen ein, wenn Sie jemand anderes auf dieses Problem aufmerksam machen möchten.
- **Anhang (optional)**: Laden Sie bis zu fünf Anhänge nacheinander hoch.

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



Nachdem Sie fertig sind

Es wird ein Popup-Fenster mit der Support-Fallnummer angezeigt. Ein NetApp Support-Experte prüft Ihren Fall

und macht Sie umgehend mit.

Um eine Historie deiner Support-Fälle anzuzeigen, kannst du **Einstellungen > Chronik** auswählen und nach Aktionen mit dem Namen „Support-Case erstellen“ suchen. Mit einer Schaltfläche ganz rechts können Sie die Aktion erweitern, um Details anzuzeigen.

Es ist möglich, dass beim Versuch, einen Fall zu erstellen, möglicherweise die folgende Fehlermeldung angezeigt wird:

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

Dieser Fehler könnte bedeuten, dass das NSS-Konto und das Unternehmen des Datensatzes, mit dem es verbunden ist, nicht das gleiche Unternehmen des Eintrags für die BlueXP Account Seriennummer (dh 960xxxx) oder Seriennummer der Arbeitsumgebung. Sie können Hilfe mit einer der folgenden Optionen anfordern:

- Verwenden Sie den Chat im Produkt
- Übermitteln eines nicht-technischen Cases unter https://mysupport.netapp.com/site/help

Managen Ihrer Support-Cases (Vorschau)

Sie können aktive und gelöste Support-Cases direkt über BlueXP anzeigen und managen. Sie können die mit Ihrem NSS-Konto und Ihrem Unternehmen verbundenen Fälle verwalten.

Case Management ist als Vorschau verfügbar. Wir planen, diese Erfahrungen weiter zu verbessern und in zukünftigen Versionen Verbesserungen hinzuzufügen. Bitte senden Sie uns Ihr Feedback über den Product-Chat.

Beachten Sie Folgendes:

- Das Case-Management-Dashboard oben auf der Seite bietet zwei Ansichten:
  - Die Ansicht auf der linken Seite zeigt die Gesamtzahl der Fälle, die in den letzten 3 Monaten durch das von Ihnen angegebene NSS-Benutzerkonto eröffnet wurden.
  - Die Ansicht auf der rechten Seite zeigt die Gesamtzahl der in den letzten 3 Monaten auf Unternehmensebene eröffneten Fälle basierend auf Ihrem NSS-Benutzerkonto an.

  Die Ergebnisse in der Tabelle geben die Fälle in Bezug auf die ausgewählte Ansicht wieder.
- Sie können interessante Spalten hinzufügen oder entfernen und den Inhalt von Spalten wie Priorität und Status filtern. Andere Spalten bieten nur Sortierfunktionen.

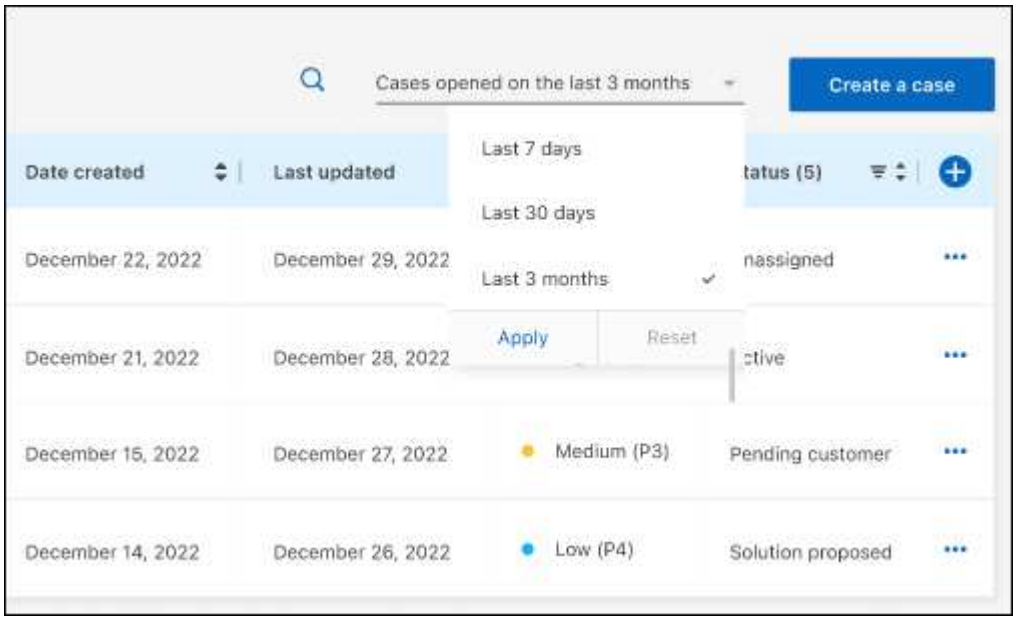
  Weitere Informationen erhalten Sie in den Schritten unten.
- Auf Fallebene bieten wir die Möglichkeit, Fallnotizen zu aktualisieren oder einen Fall zu schließen, der sich noch nicht im Status „Geschlossen“ oder „Geschlossen“ befindet.

Schritte

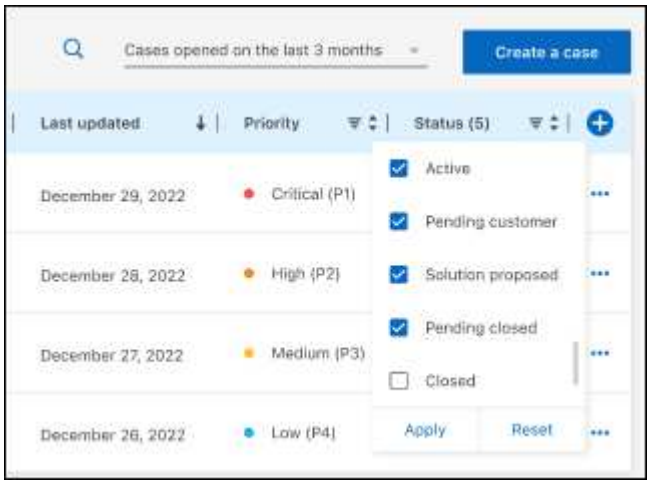
1. Wählen Sie in BlueXP **Hilfe > Support** aus.
2. Wählen Sie **Case Management** aus und fügen Sie bei Aufforderung Ihr NSS-Konto zu BlueXP hinzu.

   Auf der Seite **Case Management** werden offene Fälle im Zusammenhang mit dem NSS-Konto angezeigt, das mit Ihrem BlueXP Benutzerkonto verknüpft ist. Dies ist das gleiche NSS-Konto, das oben auf der Seite **NSS Management** angezeigt wird.

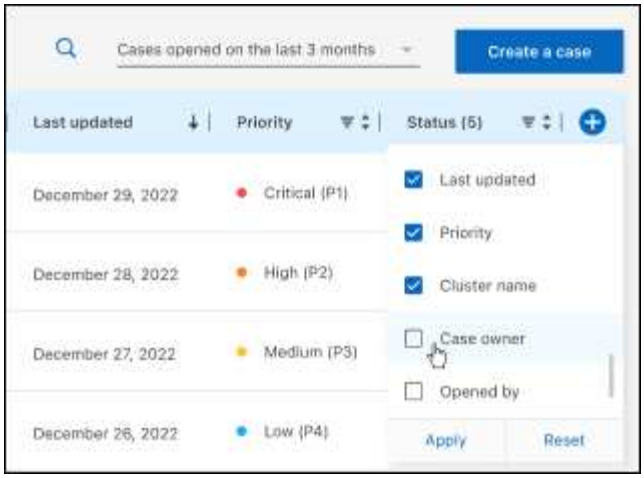
3. Ändern Sie optional die in der Tabelle angezeigten Informationen:
   - Wählen Sie unter **Vorgänge der Organisation Ansicht** aus, um alle mit Ihrem Unternehmen verbundenen Fälle anzuzeigen.
   - Ändern Sie den Datumsbereich, indem Sie einen genauen Datumsbereich oder einen anderen Zeitrahmen auswählen.



   - Filtern Sie den Inhalt der Spalten.



   - Ändern Sie die Spalten, die in der Tabelle angezeigt werden, indem Sie auswählen ⊕ Und wählen Sie dann die Spalten, die Sie anzeigen möchten.

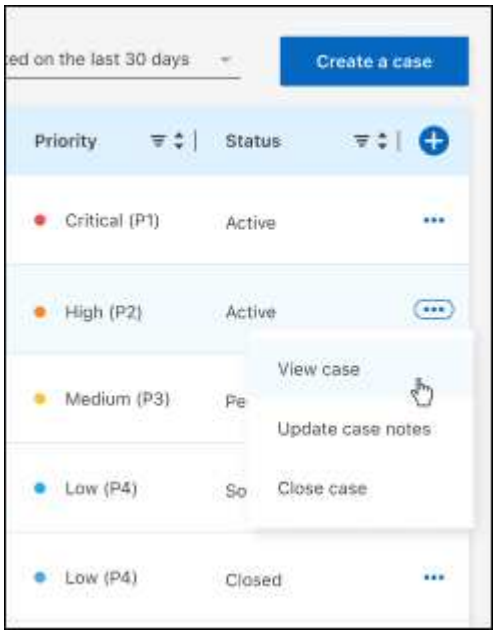


4. Managen Sie einen bestehenden Fall, indem Sie auswählen ••• Und eine der verfügbaren Optionen auswählen:

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

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

   - **Fall schließen**: Geben Sie Einzelheiten darüber an, warum Sie den Fall schließen und wählen Sie **Fall schließen**.



Rechtliche Hinweise

Rechtliche Hinweise ermöglichen den Zugriff auf Copyright-Erklärungen, Marken, Patente und mehr.

Urheberrecht

"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 der jeweiligen Eigentümer sein.

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

Patente

Eine aktuelle Liste der NetApp Patente 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

In den Benachrichtigungsdateien finden Sie Informationen zu Urheberrechten und Lizenzen von Drittanbietern, die in der NetApp Software verwendet werden.

"Hinweis zur Disaster Recovery von BlueXP"