



# Nutzen Sie BlueXP Disaster Recovery

## BlueXP disaster recovery

NetApp  
April 02, 2024

# Inhalt

- Nutzen Sie BlueXP Disaster Recovery ..... 1
  - Nutzen Sie die Disaster Recovery-Übersicht von BlueXP ..... 1
  - Zeigen Sie den Zustand Ihrer Disaster-Recovery-Pläne auf dem Dashboard an ..... 1
  - Fügen Sie vCenter Sites hinzu ..... 2
  - Erstellen Sie einen Replizierungsplan ..... 4
  - Replizierung von Applikationen an einen anderen Standort ..... 12
  - Migrieren von Anwendungen zu einem anderen Standort ..... 13
  - Failover von Anwendungen an einen Remote-Standort ..... 13
  - Führen Sie ein Failback von Anwendungen zur ursprünglichen Quelle durch ..... 15
  - Verwalten von Standorten, Plänen, Datastores und Informationen zu virtuellen Maschinen ..... 16
  - Überwachen Sie Disaster-Recovery-Jobs ..... 18

# Nutzen Sie BlueXP Disaster Recovery

## Nutzen Sie die Disaster Recovery-Übersicht von BlueXP

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

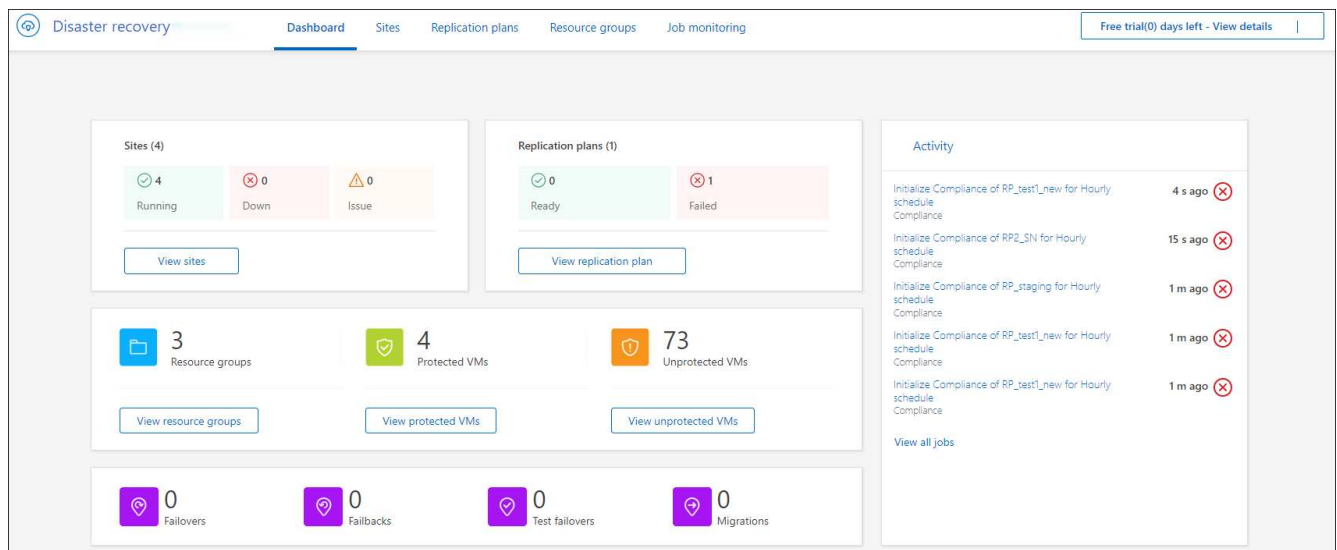
- "Zeigen Sie den Zustand Ihrer Disaster-Recovery-Pläne an"
- "Fügen Sie vCenter Sites hinzu".
- "Disaster-Recovery-Plan erstellen".
- "Replizierung von VMware Applikationen" Sie erfolgt an Ihrem primären Standort an einem Disaster-Recovery-Remote-Standort in der Cloud mithilfe von SnapMirror Replizierung.
- "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.

## Zeigen Sie den Zustand Ihrer Disaster-Recovery-Pläne 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.

### 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 Ressourcengruppen zu überprüfen, wählen Sie **Alle anzeigen** für einen Status oder **Ressourcengruppen anzeigen**, um alle anzuzeigen.
  - 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**.

## Fügen Sie vCenter Sites hinzu

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

Nachdem sie hinzugefügt wurden, führt die Disaster Recovery von BlueXP eine umfassende Bestandsaufnahme der vCenter Umgebungen durch, einschließlich vCenter Cluster, ESXi Hosts, Datastores, Storage-Platzbedarf, Details zu Virtual Machines, SnapMirror Replikaten und Virtual Machine-Netzwerken.

### Schritte

1. Melden Sie sich bei BlueXP an und wählen Sie im linken Navigationsbereich **Protection > Disaster Recovery** aus.

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.

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.

- a. Fügen Sie eine Site hinzu, wählen Sie den BlueXP Connector aus und geben Sie vCenter Zugangsdaten an.
- b. 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.

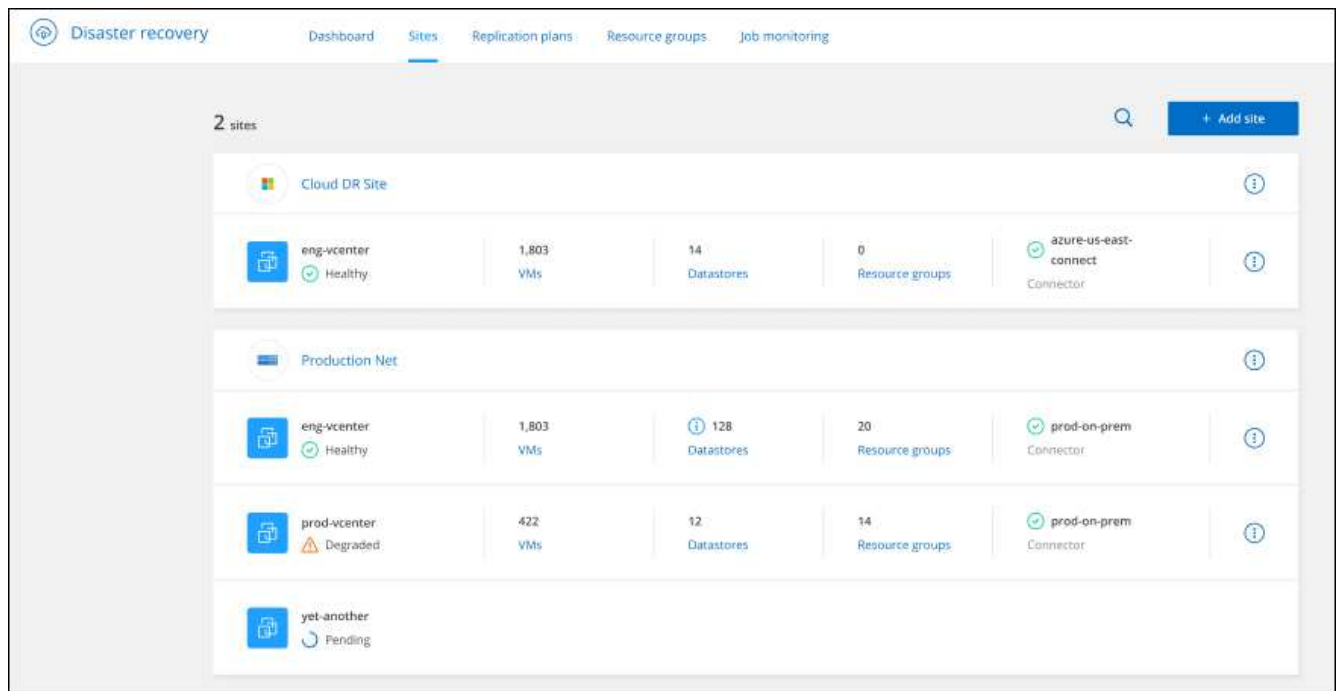
- c. Wählen Sie **Hinzufügen**.

Als Nächstes fügen Sie ein Ziel-vCenter hinzu.

### 3. Ziel:

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

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



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

## Erstellen Sie einen Replizierungsplan

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 können Sie virtuelle Maschinen gruppieren, die einer Applikation zugeordnet sind, oder Anwendungen mit ähnlichen Tiers gruppieren.

Solche Pläne werden manchmal *Blueprints* genannt.

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

### Erstellen Sie den Plan

Ein Assistent führt Sie durch die folgenden Schritte:

- Wählen Sie vCenter-Server aus
- Wählen Sie die VMs aus, die Sie replizieren und Gruppen zuweisen möchten
- Zuordnen der Ressourcen aus der Quellumgebung zum Ziel
- Wiederholung identifizieren
- Überprüfen Sie den Plan

Während Sie den Replizierungsplan 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 in einer Konsistenzgruppe
- Von vielen auf viele

### 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 die Option **Replication Plans** 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 virtuellen Maschinen in funktionale Ressourcengruppen gruppiert. Mit Ressourcengruppen können Sie einen Satz abhängiger virtueller Maschinen in logische Gruppen gruppieren, die Ihren Anforderungen entsprechen. Gruppen könnten beispielsweise verzögerte Startaufträge enthalten, die bei der Wiederherstellung ausgeführt werden können.

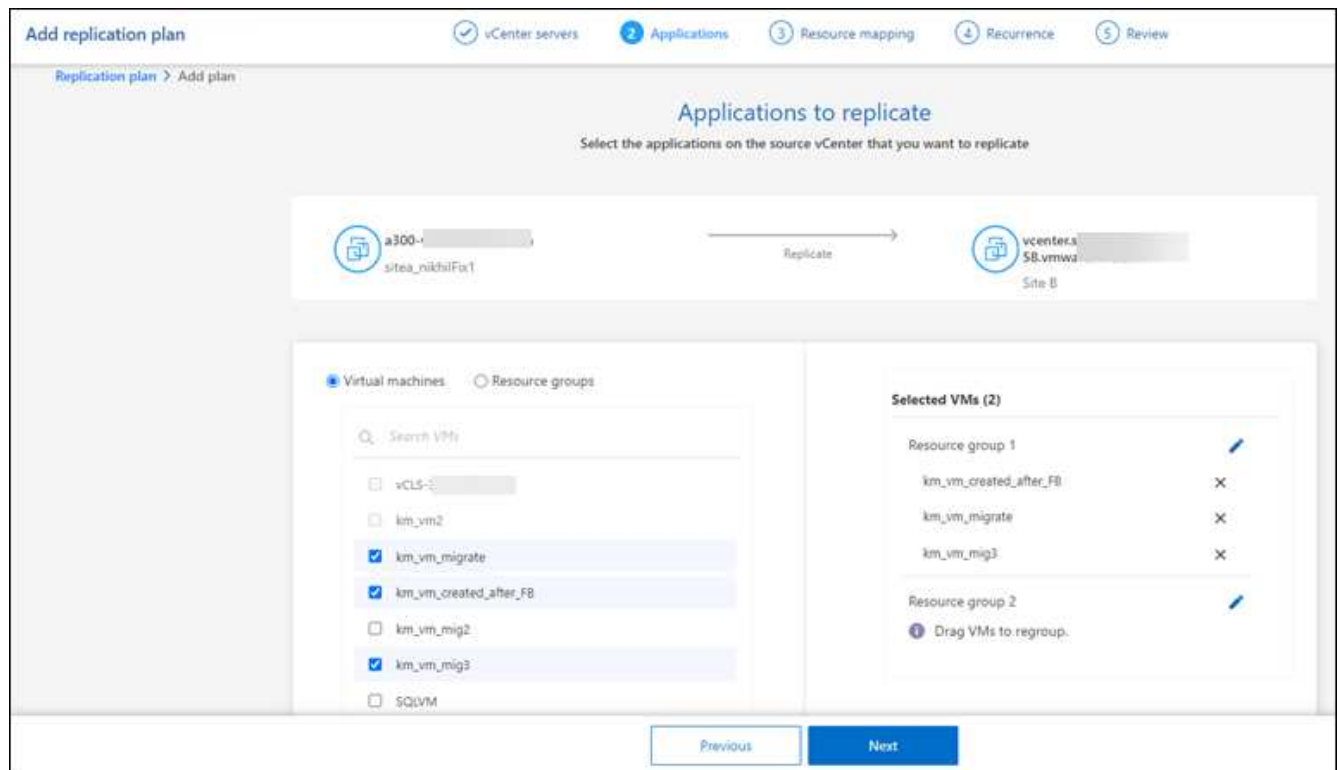


Jede Ressourcengruppe kann eine oder mehrere virtuelle Maschinen enthalten. Die virtuellen Maschinen werden basierend auf der Reihenfolge, in der Sie sie hier einfügen, eingeschaltet.

## Schritte

1. Wählen Sie auf der linken Seite der Seite Anwendungen die virtuellen Maschinen aus, die Sie replizieren möchten, und weisen Sie sie der ausgewählten Gruppe zu.

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



2. Führen Sie optional einen der folgenden Schritte aus:
  - Um Gruppen zu ändern, klicken Sie auf das Gruppensymbol **Bearbeiten**.
  - Um eine virtuelle Maschine aus einer Gruppe zu entfernen, wählen Sie **X** aus.
  - Um eine virtuelle Maschine in eine andere Gruppe zu verschieben, ziehen Sie sie in die neue Gruppe.
3. Wenn Sie mehrere Ressourcengruppen haben, stellen Sie sicher, dass die Reihenfolge der Gruppen mit der operativen Sequenz übereinstimmt, die auftreten soll.

Jede virtuelle Maschine in einer Gruppe wird in der Reihenfolge gestartet, die der hier angegebenen Reihenfolge entspricht. Zwei Gruppen werden parallel gestartet.

4. Alternativ können Sie die Gruppe umbenennen, indem Sie auf das Symbol **Bearbeiten** klicken.
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.



## 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 von jeder Ressource aus, und ordnen Sie die Ressourcen in den folgenden Ressourcen zu:
  - **Compute Resources**
  - **Virtuelle Netzwerke**
3. Wählen Sie auf der Registerkarte Failover Mappings den Abwärtspfeil rechts neben jeder Ressource aus:
  - **Virtuelle Maschinen:** Wählen Sie das Netzwerk-Mapping auf das entsprechende Segment aus. Die Segmente sollten bereits bereitgestellt werden. Wählen Sie daher das entsprechende Segment für die Zuordnung der virtuellen Maschine aus.

SnapMirror befindet sich auf Volume-Ebene. Somit werden alle Virtual Machines zum Replikationsziel repliziert. Stellen Sie sicher, dass Sie alle virtuellen Maschinen auswählen, die Teil des Datenspeichers sind. Wenn sie nicht ausgewählt sind, werden nur die virtuellen Maschinen verarbeitet, die Teil des Replikationsplans sind.

- **VM CPU und RAM:** Unter den Virtual Machines Details können Sie optional die VM CPU und RAM Parameter anpassen.
- **Boot Order Delay:** Sie können auch die Boot-Reihenfolge für alle ausgewählten virtuellen Maschinen in den Ressourcengruppen ändern. Standardmäßig wird die während der Auswahl der Ressourcengruppe ausgewählte Startreihenfolge verwendet. Sie können jedoch in dieser Phase Änderungen vornehmen.
- **DHCP oder statische IP:** Wenn Sie Netzwerke zwischen Quell- und Zielorten im Abschnitt „virtuelle Maschinen“ des Replikationsplans zuordnen, bietet BlueXP Disaster Recovery zwei Optionen: DHCP oder statische IP. Konfigurieren Sie für statische IPs das Subnetz, das Gateway und die DNS-Server. Geben Sie außerdem die Anmeldeinformationen für virtuelle Maschinen ein.
  - **DHCP:** Wenn Sie diese Option wählen, geben Sie nur die 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 die Anmeldeinformationen, die IP-Adresse der VM, die Subnetzmaske, das DNS und die Gateway-Informationen angeben. Die Anmeldeinformationen für das VM-Gastbetriebssystem sollten entweder auf globaler Ebene oder auf jeder VM-Ebene bereitgestellt werden.

The screenshot shows a configuration window titled 'VMs'. At the top is a search bar labeled 'Search VMs'. Below it is a table with columns: Source VM, CPUs, RAM, Boot delay, IP address, Subnet mask, DNS, Create app-consistent replicas (with an info icon), and Credentials. The table is divided into two sections: 'Resource group 1' and 'Resource group 2'. In 'Resource group 1', there is one row for 'SQL\_PRD\_1' with 4 CPUs, 16 GB RAM, 0 boot delay, and 'Auto' for IP, Subnet, and DNS. In 'Resource group 2', there are two rows for 'SQL\_PRD\_2' with 4 and 8 CPUs, 32 GB and 64 GB RAM, and 2 min and 4 min boot delays. The 'Credentials' section has two radio buttons: 'Set for all VMs' (selected) and 'Set for each VM individually'. Below are input fields for 'User name' and 'Password'.

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.

- **App-konsistente Replikate:** Geben Sie an, ob applikationskonsistente Snapshot-Kopien erstellt werden sollen. Der Service setzt die Applikation still und erstellt dann einen Snapshot, um einen konsistenten Status der Applikation zu erhalten.
- **Datstores:** Anhand der Auswahl der virtuellen Maschinen werden automatisch Datastore-Mappings ausgewählt.
  - **RPO:** Geben Sie das Recovery Point Objective (RPO) ein, um die Datenmenge anzugeben, die wiederhergestellt werden soll (gemessen in der Zeit). Wenn Sie beispielsweise einen RPO von 60 Minuten eingeben, müssen für die Recovery jederzeit Daten vorhanden sein, die nicht älter als 60 Minuten sind. Bei einem schwerwiegenden Ausfall lassen sich bis zu 60 Minuten an Daten verlieren. Geben Sie außerdem die Anzahl der Snapshot Kopien ein, die für alle Datstores beibehalten werden sollen.
  - **SnapMirror Beziehungen:** Wenn ein Volume bereits eine SnapMirror Beziehung hat, können Sie die entsprechenden Quell- und Ziel-Datstores auswählen. Wenn Sie ein Volume auswählen, das nicht über eine SnapMirror-Beziehung verfügt, können Sie jetzt ein Volume erstellen, indem Sie die Arbeitsumgebung und die zugehörige Peer-SVM auswählen.



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.

- **Consistency Groups:** Wenn Sie einen Replikationsplan erstellen, können Sie VMs mit unterschiedlichen Volumes und SVMs einbeziehen. Bei der Disaster Recovery von BlueXP wird ein Snapshot einer Konsistenzgruppe erstellt.
  - Wenn Sie das Recovery Point Objective (RPO) angeben, plant der Service ein primäres Backup auf der Grundlage des RPO und aktualisiert die sekundären Ziele.
  - 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 Consistency Group Snapshot, 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 festzuführenden Snapshot 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.
4. Um verschiedene Zuordnungen für die Testumgebung festzulegen, deaktivieren Sie das Kontrollkästchen und wählen Sie die Registerkarte **Testzuordnungen** aus. Gehen Sie die einzelnen Registerkarten wie zuvor durch, jedoch diesmal für die Testumgebung.



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

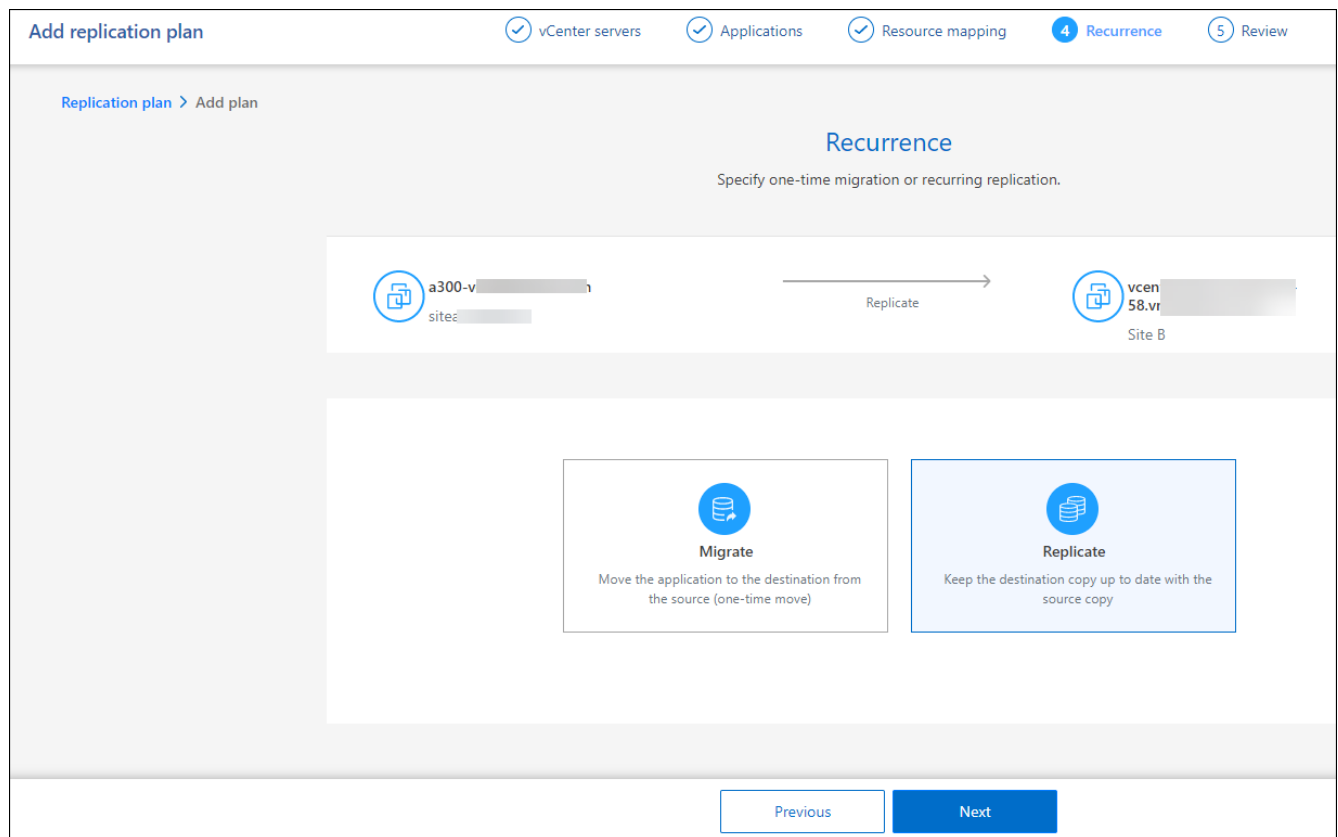
### Identifizieren Sie die Wiederholung

Wählen Sie aus, ob Sie Daten (eine einmalige Verschiebung) zu einem anderen Ziel migrieren oder sie mit der Frequenz von SnapMirror replizieren möchten.

Ermitteln Sie, wie oft die Daten gespiegelt werden sollen, wenn Sie sie replizieren möchten.

### Schritte

1. Wählen Sie auf der Seite Rezidive **Migrate** oder **Replicate** aus.
  - **Migrate**: Wählen Sie, um die Anwendung an den Zielspeicherort zu verschieben.
  - **Replicate**: Halten Sie die Zielkopie mit Änderungen von der Quellkopie in einer wiederkehrenden Replikation auf dem neuesten Stand.



2. Wählen Sie **Weiter**.

### Bestätigen Sie den Replikationsplan

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



Sie können den Replikationsplan später deaktivieren oder löschen.

### Schritte

1. Überprüfen Sie die Informationen auf den einzelnen Registerkarten: Plandetails, Failover Mapping, Virtuelle Maschinen.
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.

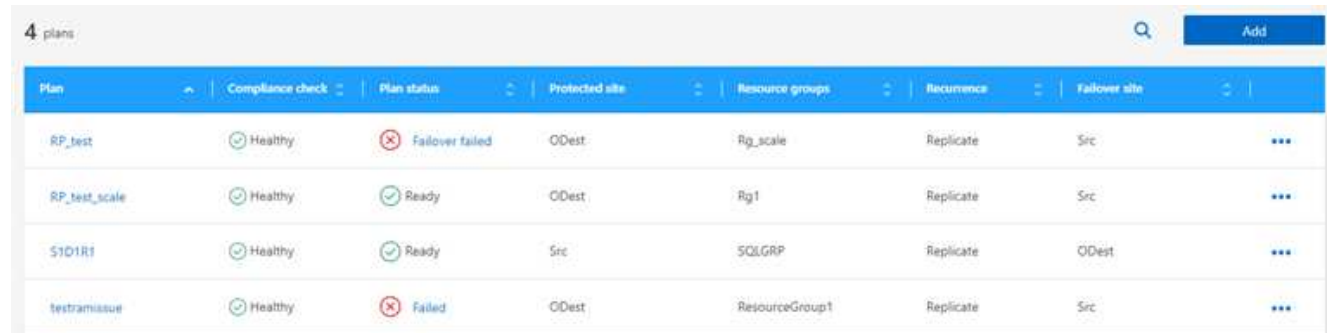
- **Auswirkungen auf die Compliance-Zeit:** Wenn ein Replikationsplan erstellt wird, erstellt der Dienst standardmäßig einen Compliance-Zeitplan. Die Standard-Compliance-Zeit beträgt 30 Minuten. Um diese Zeit zu ändern, können Sie den Zeitplan im Replikationsplan bearbeiten verwenden.
- **Auswirkungen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



Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
RP_test	Healthy	Failover failed	ODest	Rg_scale	Replicate	Src	...
RP_test_scale	Healthy	Ready	ODest	Rg1	Replicate	Src	...
STD1R1	Healthy	Ready	Src	SQLGRP	Replicate	ODest	...
tetramissue	Healthy	Failed	ODest	ResourceGroup1	Replicate	Src	...

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.

**Edit schedules: RP\_test\_scale**

Compliance checks and test failovers run on a recurring basis. Enter how often these actions should occur.

**Compliance check**

Frequency (min) i

**Test failover**

Run test failovers on a monthly schedule

Day of the month Time Start date i

i

**Required** **Required** **Required**

Automatically clean up after test failover i

5. Um die Testumgebung nach Abschluss des Failover-Tests zu bereinigen, aktivieren Sie **Automatically clean up after Test Failover**.



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

6. Wählen Sie **Speichern**.

## Replizierung von Applikationen an einen anderen Standort

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.



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 von Anwendungen zu einem 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

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.

Während des Failovers wird die neueste SnapMirror Snapshot Kopie verwendet. Sie können auch eine bestimmte Snapshot Kopie aus einer zeitpunktgenauen Snapshot Kopie 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.

Durch dieses Verfahren wird die Replikationsbeziehung unterbrochen, die vCenter Quell-VMs offline gestellt und Lese-/Schreibvorgänge auf dem Zielstandort ermöglicht.

Sie können benutzerdefinierte Skripts im .sh-, .bat- oder .ps1-Format als Post-Failover-Prozesse verwenden. 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.

Bevor Sie das Failover starten, können Sie den Prozess testen und so sicherstellen, dass er bei Bedarf erfolgreich ist. Durch den Test werden die Virtual Machines nicht offline geschaltet.

## Testen Sie den Failover-Prozess

Bevor Sie einen tatsächlichen Failover starten, sollten Sie den Failover-Prozess testen.

Während eines Failover-Tests werden vorübergehend virtuelle Maschinen erstellt. Bei der Disaster Recovery von BlueXP wird das Ziel-Volumen 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-Volumen wird nicht geändert, und Replikationsjobs 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 das SnapMirror Update ausgeführt, um die neuesten Änderungen zu replizieren.
- Die virtuellen Quellmaschinen sind heruntergefahren.
- Die SnapMirror Beziehung ist unterbrochen und das Zielvolumen wird Lese-/Schreibzugriff gemacht.
- Auf Basis der Auswahl des Snapshots wird das aktive Filesystem auf den angegebenen Snapshot wiederhergestellt (neueste oder ausgewählte)
- 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. Geben Sie auf der Seite Failover testen den Namen des Replikationsplans zur Bestätigung ein, und wählen Sie **Failover** aus.
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**.

## Führen Sie ein Failback von Anwendungen zur ursprünglichen Quelle durch


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 aus die Wiederherstellung durchgeführt werden soll.

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 von Standorten, Plänen, Datastores und Informationen zu virtuellen Maschinen


Sie erhalten einen schnellen Überblick über alle Disaster Recovery-Ressourcen oder sehen sich die einzelnen Ressourcen im Detail an:

- Standorte
- Replizierungspläne
- Datenspeicher
- Virtual Machines
- Ressourcengruppen

### VCenter-Sites verwalten

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

#### 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 Replikationsplänen

Sie können Replikationspläne deaktivieren, aktivieren und löschen.

- 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.

Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
Customer1	Healthy	Ready	ScaleOnPremSrc	Cust1RG	Replicate	ScaleFsXDest	...
Customer2	Healthy	Ready	ScaleOnPremSrc	Cust2RG	Replicate	ScaleFsXDest	...
Customer3	Healthy	Ready	ScaleOnPremSrc	Cust3RG	Replicate	ScaleFsXDest	...
Customer4	Healthy	Ready	ScaleOnPremSrc	Cust4RG	Replicate	ScaleFsXDest	...
Customer5	Healthy	Ready	ScaleOnPremSrc	Cust5RG	Replicate	ScaleFsXDest	...

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 Maschine** und wählen Sie das **Bearbeiten**-Symbol.
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** aus **...** Rechts neben dem Plan und wählen Sie eine der Optionen aus, wie z. B. **Zeitpläne bearbeiten**, **Failover testen**, **Failover**, **Failback**, **Deaktivieren**, **enable**, oder **Delete**.

## Anzeigen von Datenspeicherinformationen

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

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.

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.

## 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 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**.

## Überwachen Sie Disaster-Recovery-Jobs

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

### 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 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.

Um einen Job abzubrechen, verwenden Sie Swagger.

### Bevor Sie beginnen

Um einen Job abzubrechen, müssen Sie über die Konto-ID verfügen.

### 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.
4. BlueXP Disaster Recovery Swagger-URL aufrufen: "**Swagger**".

```
"<a href="https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/Jobs/put_jobmanager_v2_jobs__jobld_"" class="bare">https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#!/Jobs/put_jobmanager_v2_jobs__jobld_ "</a>
```

## Jobs

PUT /jobmanager/v2/jobs/{jobId}

Updates Job Status to Canceled or Failed

Parameters Try it out

Name	Description
<b>x-account-id</b> * required string (header)	Account ID
	<input type="text" value="x-account-id - Account ID"/>
<b>jobId</b> * required string (path)	jobId
	<input type="text" value="jobId"/>
body object (body)	Example Value   Model
	<pre>{   "jobStatus": "Cancelled" }</pre>
Parameter content type	<input type="text" value="application/json-patch+json"/>

Weitere Informationen zu Swagger finden Sie unter ["Swagger-Dokumente"](#).

5. Von Swagger erhalten Sie das Sicherheitstoken, auch *Bearer Token* genannt, von der Option Autorisieren.
6. Geben Sie die Konto-ID und die Job-ID ein.
7. Wählen Sie **Probieren Sie es aus**.

## Copyright-Informationen

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

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

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

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

## Markeninformationen

NETAPP, das NETAPP Logo und die unter <http://www.netapp.com/TM> aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.