



DR mit BlueXP DRaaS

NetApp Solutions

NetApp
December 19, 2024

Inhalt

- DR mit BlueXP DRaaS 1
 - Überblick 1
 - DR unter Verwendung von BlueXP DRaaS für NFS-Datstores 1
 - DR, die BlueXP DRaaS für VMFS-Datstores verwendet 22

DR mit BlueXP DRaaS

Überblick

Disaster Recovery steht allen VMware Administratoren an erster Stelle. Da VMware ganze Server in eine Reihe von Dateien einkapselt, aus denen die Virtual Machine besteht, nutzen Administratoren blockspeicherbasierte Techniken wie Klone, Snapshots und Replikate, um diese VMs zu sichern. ONTAP Arrays bieten integrierte Replizierung für die Übertragung von Volume-Daten und damit der Virtual Machines auf den designierten Datastore-LUNs von einem Standort zum anderen. BlueXP DRaaS lässt sich in vSphere integrieren und automatisiert den gesamten Workflow für nahtloses Failover und Failback bei einem Notfall. Durch die Kombination von Storage-Replizierung mit intelligenter Automatisierung verfügen Administratoren jetzt über einfaches Management. So können sie Disaster Recovery-Pläne nicht nur konfigurieren, automatisieren und testen, sondern auch im Notfall problemlos ausführen.

In einer VMware vSphere Umgebung sind die zeitaufwändigsten Teile eines DR-Failover durch die Ausführung der erforderlichen Schritte zum Inventarisieren, Registrieren, Neukonfigurieren und Hochfahren der VMs am DR-Standort. Eine ideale Lösung bietet sowohl niedrige RPOs (wie in Minuten gemessen) als auch ein niedriges RTO (in Minuten bis Stunden gemessen). Ein Faktor, der in einer DR-Lösung oft übersehen wird, ist die Möglichkeit, die DR-Lösung effizient und in regelmäßigen Abständen zu testen.

Für die Erstellung einer DR-Lösung sollten folgende Faktoren berücksichtigt werden:

- Die Recovery-Zeitvorgabe (RTO). Die RTO beschreibt, wie schnell ein Unternehmen nach einem Ausfall eine Wiederherstellung durchführen kann, genauer gesagt, wie lange es dauert, bis Business Services wieder verfügbar sind.
- Der Recovery-Zeitpunkt (RPO). Der RPO gibt an, wie alt die wiederhergestellten Daten sind, nachdem sie verfügbar gemacht wurden, relativ zum Zeitpunkt des Notfalls.
- Skalierbarkeit und Anpassungsfähigkeit: Zu diesem Faktor gehört auch die Möglichkeit, Storage-Ressourcen bei steigender Nachfrage inkrementell zu erweitern.

Weitere technische Informationen zu den verfügbaren Lösungen finden Sie unter:

- ["DR unter Verwendung von BlueXP DRaaS für NFS-Datastores"](#)
- ["DR, die BlueXP DRaaS für VMFS-Datastores verwendet"](#)

DR unter Verwendung von BlueXP DRaaS für NFS-Datastores

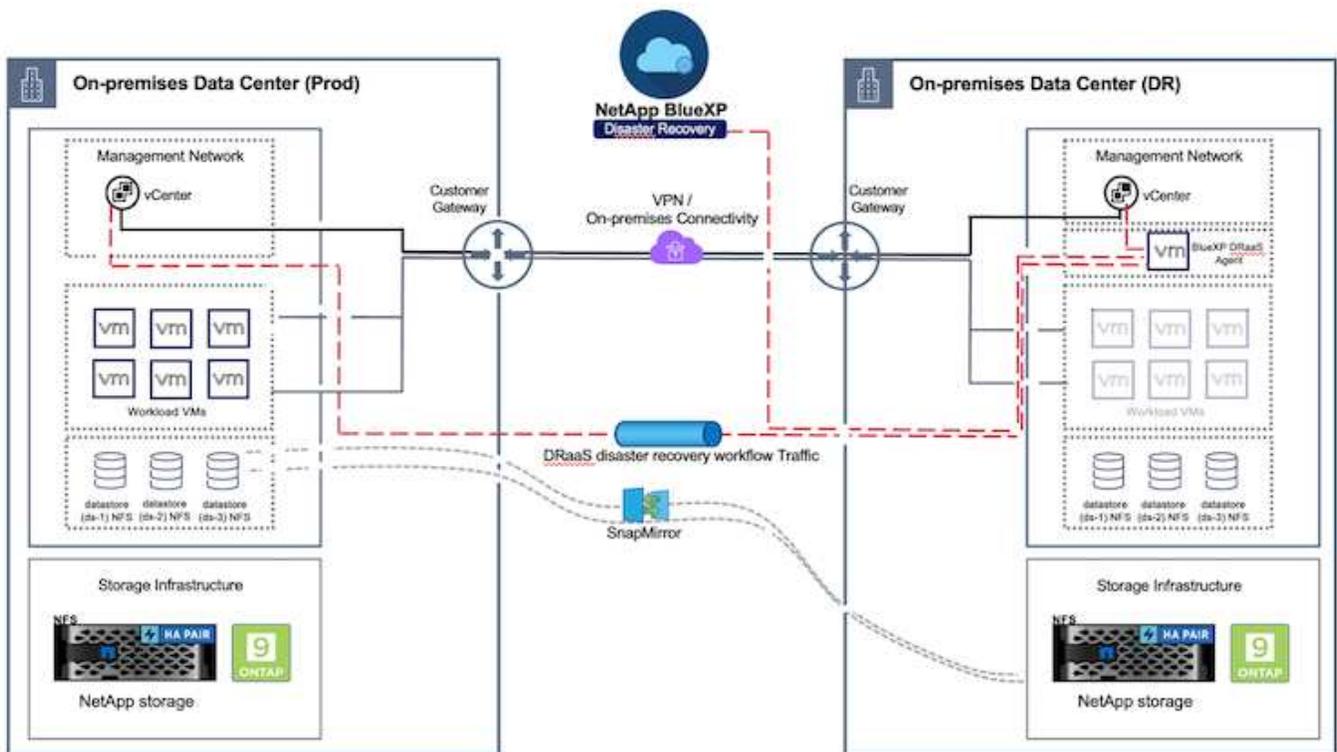
Disaster Recovery durch Replizierung auf Blockebene vom Produktionsstandort zum Disaster-Recovery-Standort ist eine ausfallsichere und kostengünstige Methode, um Workloads vor Standortausfällen und Datenbeschädigungen, z. B. durch Ransomware-Angriffe, zu schützen. Mithilfe der NetApp SnapMirror Replizierung können VMware Workloads, die auf lokalen ONTAP Systemen mit NFS-Datastore ausgeführt werden, auf ein anderes ONTAP Storage-System repliziert werden, das sich in einem festgelegten

Recovery-Datacenter befindet, in dem auch VMware implementiert wird.

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zur Einrichtung von Disaster Recovery für lokale VMware VMs an einem anderen designierten Standort beschrieben. Als Teil dieser Einrichtung, das BlueXP Konto, BlueXP Connector, die ONTAP-Arrays in BlueXP Workspace hinzugefügt, die erforderlich sind, um die Kommunikation von VMware vCenter zum ONTAP Storage zu ermöglichen. Darüber hinaus wird in diesem Dokument beschrieben, wie die Replikation zwischen Standorten konfiguriert und ein Recovery-Plan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Standort-Failover und zum Failback, wenn der primäre Standort wiederhergestellt und online gekauft wird.

Durch den BlueXP Disaster Recovery Service, der in die NetApp BlueXP Konsole integriert ist, können Unternehmen ihre lokalen VMware vCenter und ONTAP Storage mühelos erkennen. Auf diese Weise können Unternehmen Ressourcengruppen erstellen, einen Disaster-Recovery-Plan erstellen, diesen Ressourcengruppen zuordnen und Failover und Failback testen oder ausführen. SnapMirror bietet Block-Replizierung auf Storage-Ebene, sodass die beiden Standorte mit inkrementellen Änderungen aktualisiert werden können, was zu einem Recovery Point Objective (RPO) von bis zu 5 Minuten führt. Außerdem lassen sich Disaster Recovery-Verfahren simulieren, ohne dabei die Produktion zu beeinträchtigen oder zusätzliche Storage-Kosten zu verursachen.

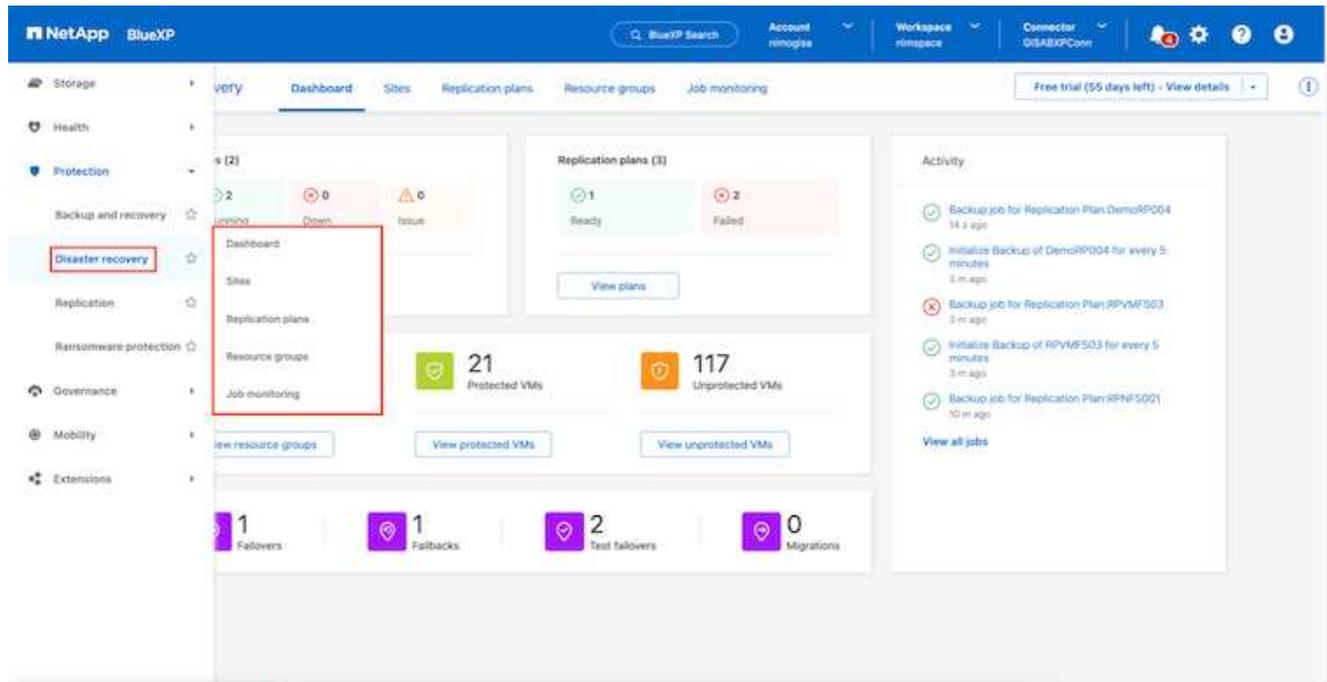
Bei der BlueXP Disaster Recovery wird mithilfe der FlexClone Technologie von ONTAP eine platzsparende Kopie des NFS-Datenspeichers aus dem letzten replizierten Snapshot am Disaster Recovery-Standort erstellt. Nach Abschluss des Disaster-Recovery-Tests können Kunden die Testumgebung einfach löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Wenn ein Failover tatsächlich erfolgt, orchestriert der BlueXP Disaster Recovery Service alle erforderlichen Schritte, um die geschützten Virtual Machines mit nur wenigen Klicks automatisch am designierten Disaster Recovery-Standort zu aktivieren. Der Service umkehrt auch die SnapMirror-Beziehung zum primären Standort und repliziert bei Bedarf alle Änderungen vom sekundären zum primären für einen Failback-Vorgang. All diese Funktionen verursachen jedoch nur einen Bruchteil der Kosten, die andere bekannte Alternativen bieten.



Erste Schritte

Um die BlueXP Disaster Recovery zu starten, verwenden Sie die BlueXP Konsole und greifen Sie dann auf den Service zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste des BlueXP die Option Schutz > Notfallwiederherstellung.
3. Das BlueXP Disaster Recovery Dashboard wird angezeigt.



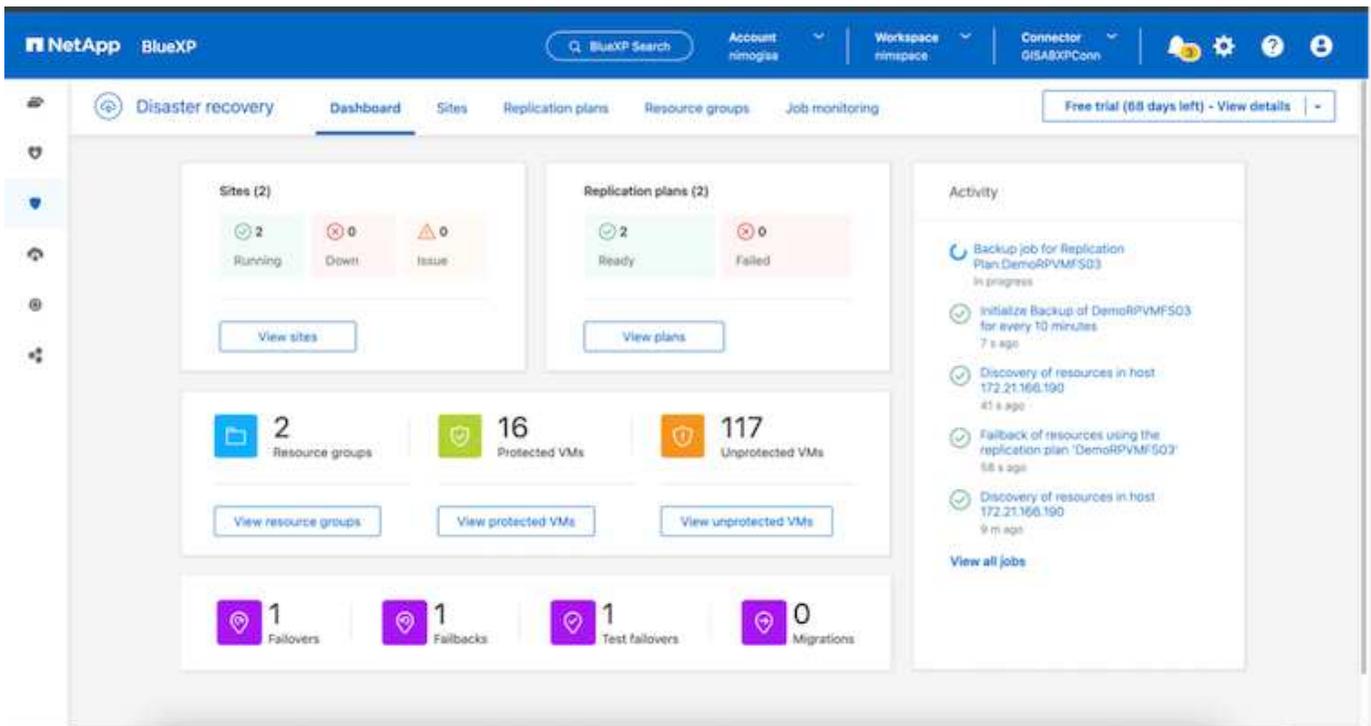
Stellen Sie vor der Konfiguration des Disaster Recovery-Plans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der BlueXP -Anschluss ist in NetApp BlueXP eingerichtet.
- Die BlueXP Connector-Instanz ist mit dem Quell- und Ziel-vCenter sowie mit den Storage-Systemen verbunden.
- NetApp Data ONTAP-Cluster für die Bereitstellung von Storage-NFS-Datstores.
- Lokale NetApp Storage-Systeme, die NFS-Datstores für VMware hosten, werden in BlueXP hinzugefügt.
- Bei der Verwendung von DNS-Namen sollte die DNS-Auflösung vorhanden sein. Verwenden Sie andernfalls IP-Adressen für vCenter.
- Die SnapMirror-Replizierung ist für die designierten NFS-basierten Datenspeicher-Volumes konfiguriert.
- Stellen Sie sicher, dass die Umgebung Versionen von vCenter Server und ESXi-Servern unterstützt.

Sobald die Verbindung zwischen dem Quell- und dem Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Dies sollte ein paar Klicks und ca. 3 bis 5 Minuten dauern.



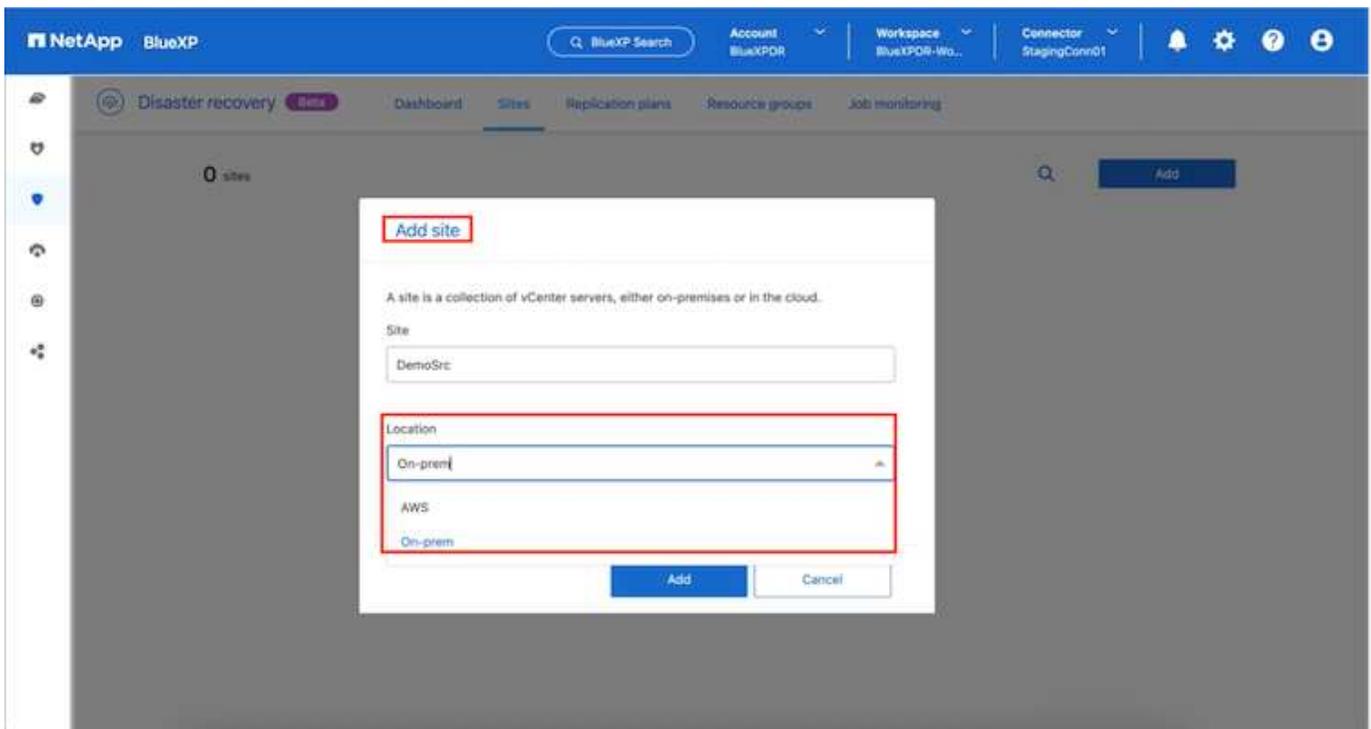
NetApp empfiehlt die Implementierung des BlueXP Connectors am Zielstandort oder an einem dritten Standort, damit der BlueXP Connector über das Netzwerk mit den Quell- und Zielressourcen kommunizieren kann.



BlueXP Disaster Recovery-Konfiguration

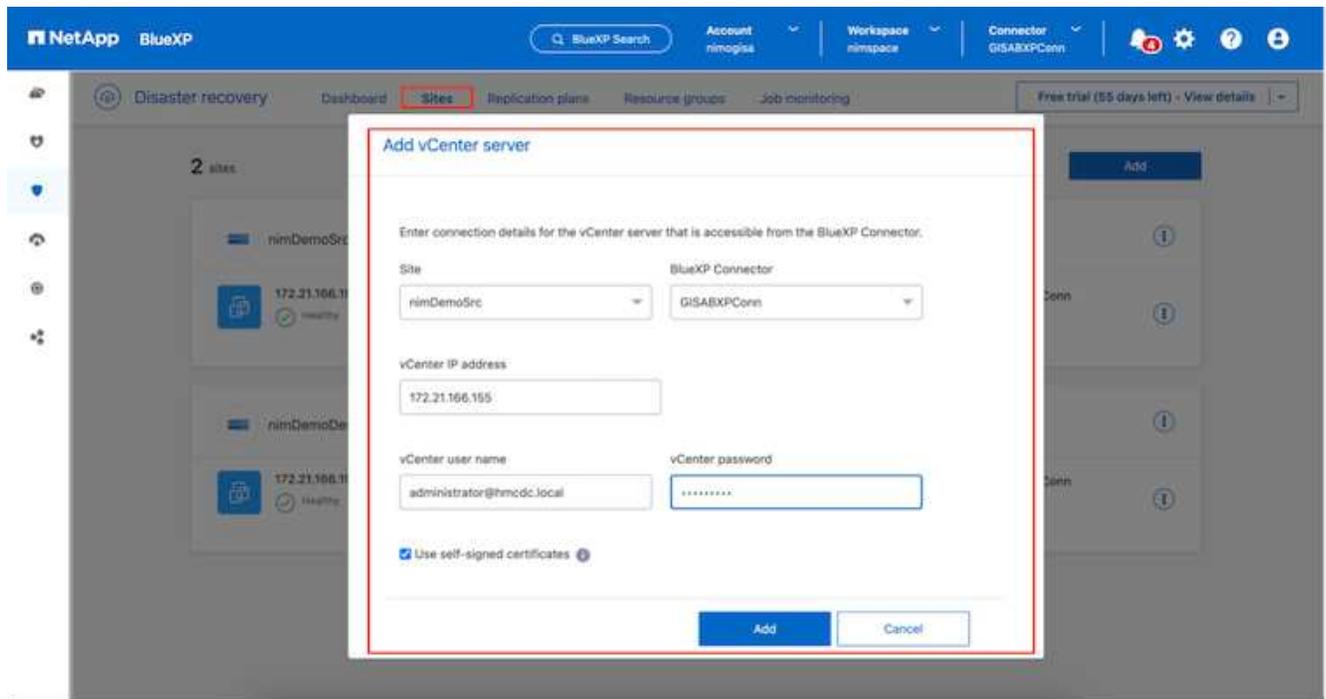
Der erste Schritt zur Vorbereitung auf Disaster Recovery besteht darin, die lokalen vCenter und Storage-Ressourcen zu erkennen und zu BlueXP Disaster Recovery hinzuzufügen.

Öffnen Sie die BlueXP -Konsole, und wählen Sie aus der linken Navigation **Schutz > Notfallwiederherstellung** aus. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü, Wählen Sie **Standorte > Hinzufügen > vCenter hinzufügen**.

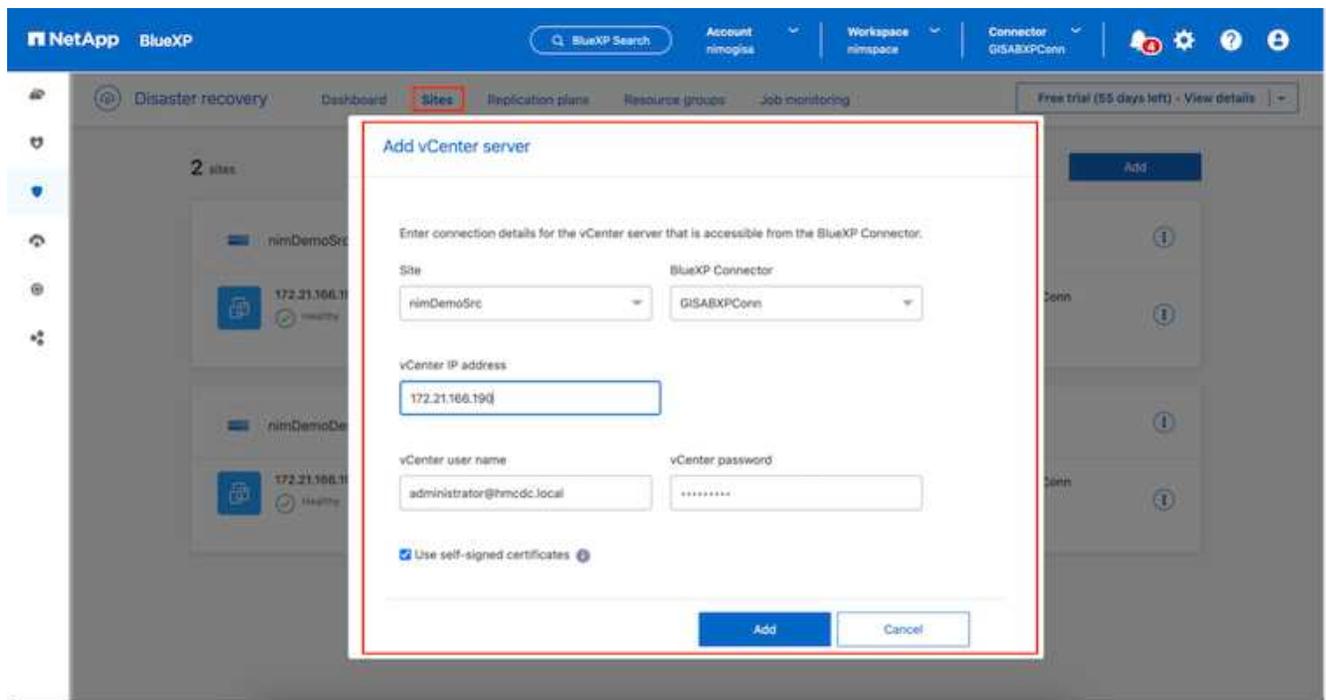


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle.** vCenter vor Ort.



- **Ziel.** VMC SDDC vCenter:



Sobald die vCenters hinzugefügt wurden, wird eine automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen dem Quell-Standort-Array und dem Ziel-Standort-Array

SnapMirror bietet Datenreplizierung in einer NetApp-Umgebung. Die SnapMirror-Replikation basiert auf NetApp Snapshot®-Technologie und ist äußerst effizient, da sie nur die Blöcke repliziert, die seit dem letzten Update geändert oder hinzugefügt wurden. SnapMirror lässt sich einfach über den NetApp OnCommand® System Manager oder die ONTAP CLI konfigurieren. BlueXP DRaaS erstellt außerdem das über die SnapMirror-Beziehung bereitgestellte Cluster und SVM-Peering wird vorab konfiguriert.

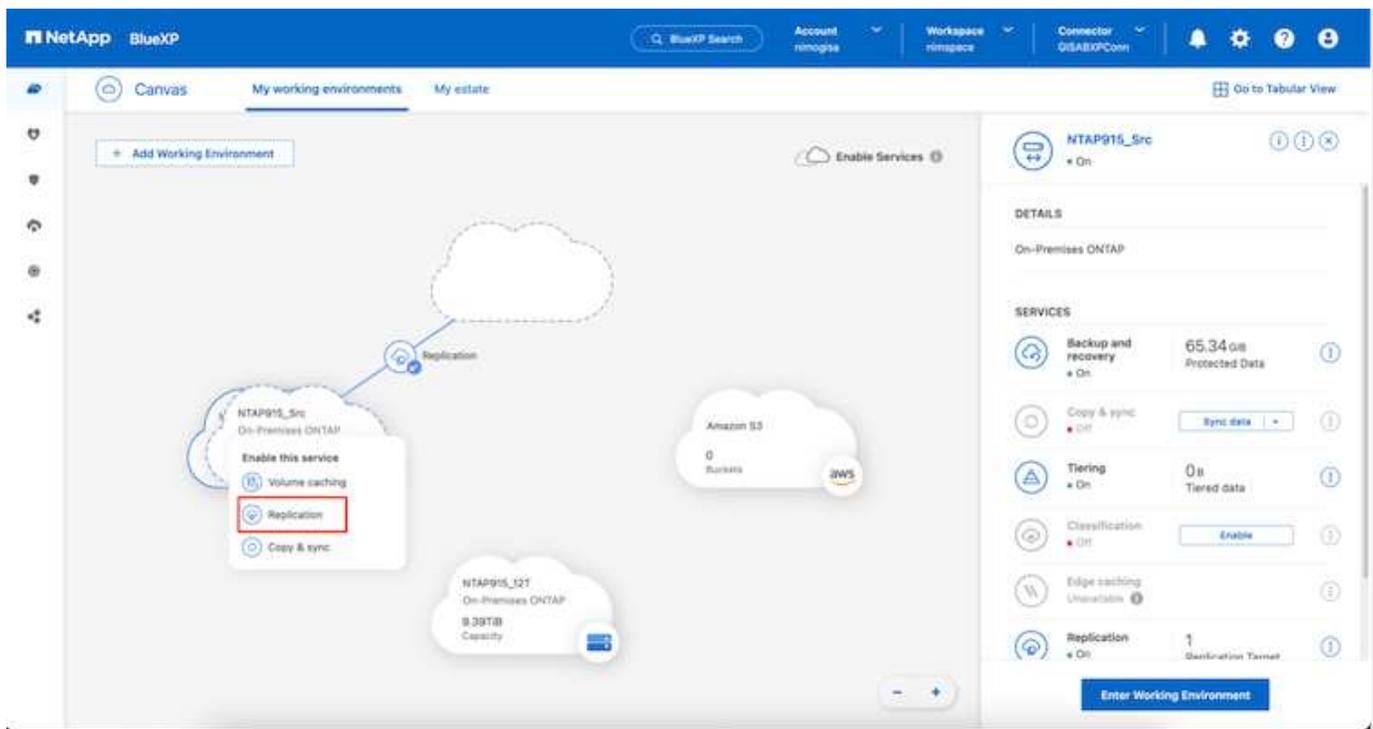
In Fällen, in denen der primäre Storage nicht komplett verloren geht, bietet SnapMirror eine effiziente Möglichkeit zur Neusynchronisierung des primären und DR-Standorts. SnapMirror kann die beiden Standorte neu synchronisieren. Dabei werden nur die geänderten oder neuen Daten vom DR-Standort zum primären Standort übertragen, indem die SnapMirror Beziehungen einfach umgekehrt werden. Das bedeutet, dass Replikationspläne in BlueXP DRaaS nach einem Failover in beide Richtungen resynchronisiert werden können, ohne das gesamte Volume neu zu erstellen. Wenn eine Beziehung in umgekehrter Richtung neu synchronisiert wird, werden nur neue Daten zurück zum Ziel gesendet, die seit der letzten erfolgreichen Synchronisierung der Snapshot Kopie geschrieben wurden.



Wenn die SnapMirror-Beziehung bereits über CLI oder System Manager für das Volume konfiguriert ist, nimmt BlueXP DRaaS die Beziehung auf und fährt mit den restlichen Workflow-Operationen fort.

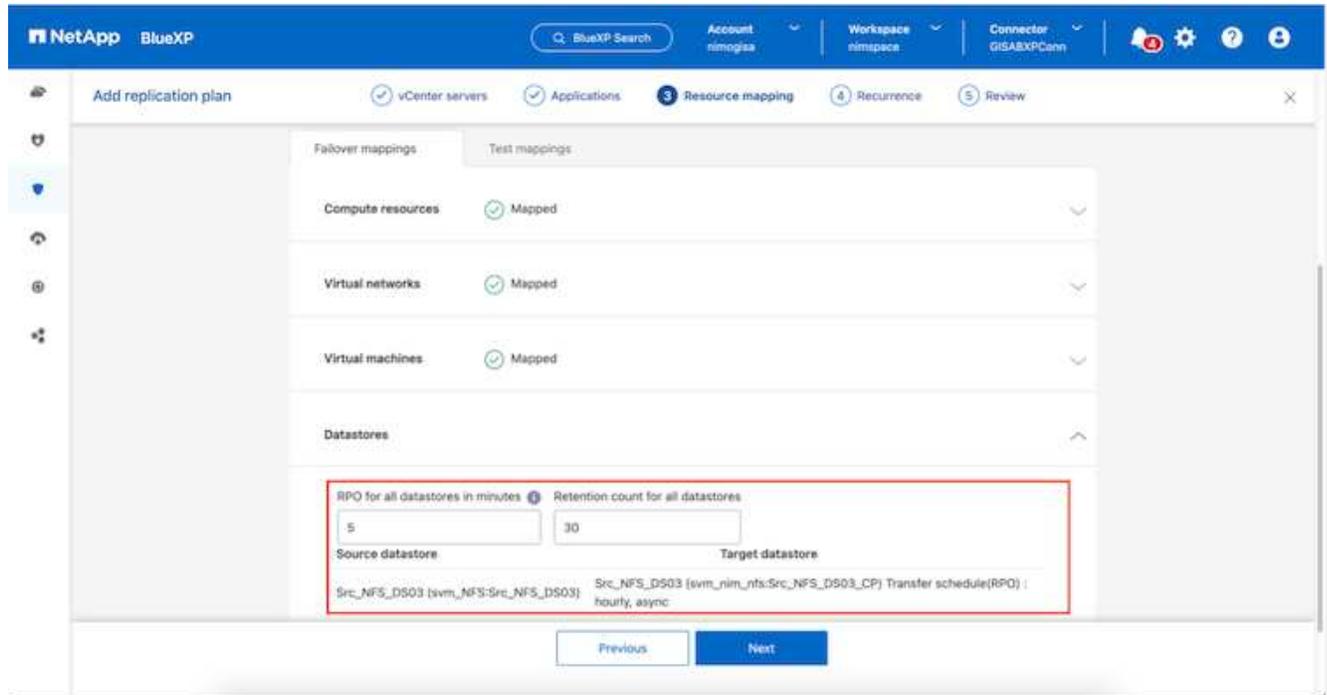
Wie Sie es für VMware Disaster Recovery einrichten

Der Prozess zur Erstellung der SnapMirror-Replizierung bleibt für jede Applikation unverändert. Der Prozess kann manuell oder automatisiert werden. Am einfachsten lässt sich BlueXP zur Konfiguration der SnapMirror Replizierung nutzen, indem das ONTAP Quell-System der Umgebung einfach per Drag & Drop auf das Ziel gezogen wird, um den Assistenten zu starten, der den Rest des Prozesses durchläuft.



Auch BlueXP DRaaS kann dasselbe automatisieren, wenn die folgenden beiden Kriterien erfüllt sind:

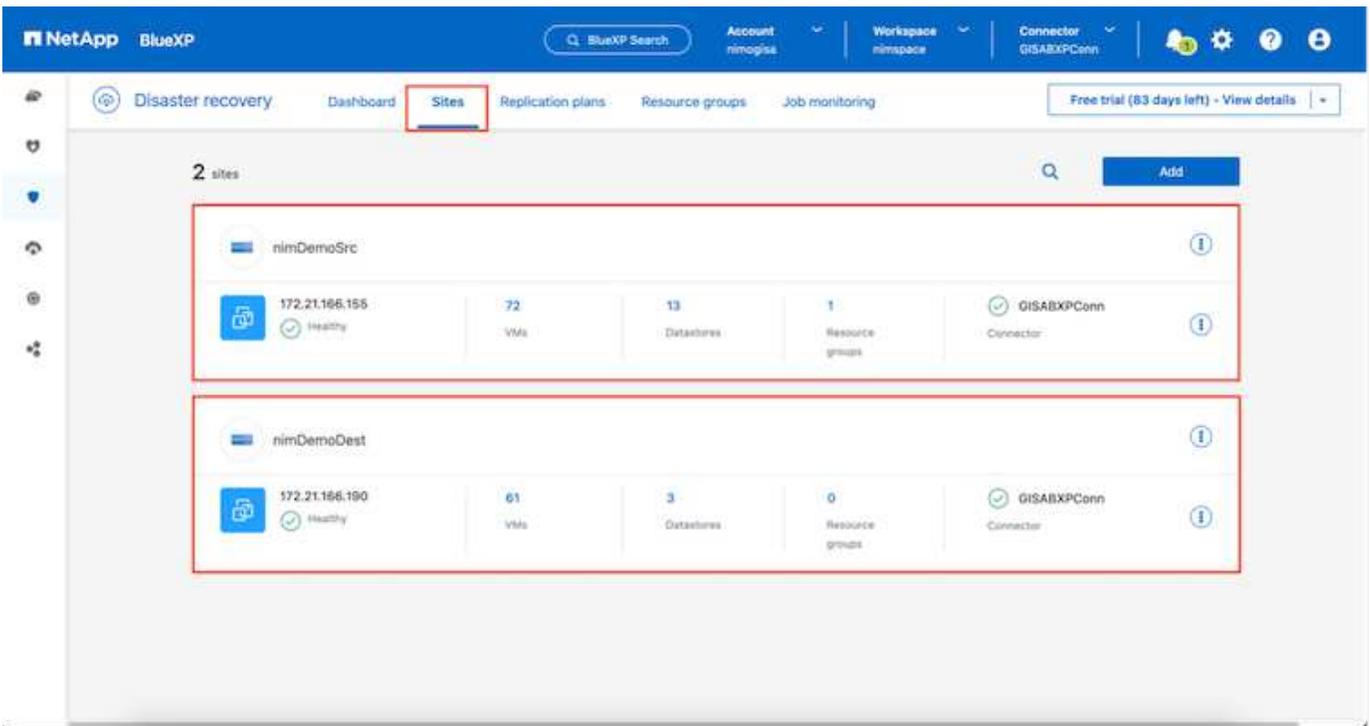
- Quell- und Ziel-Cluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



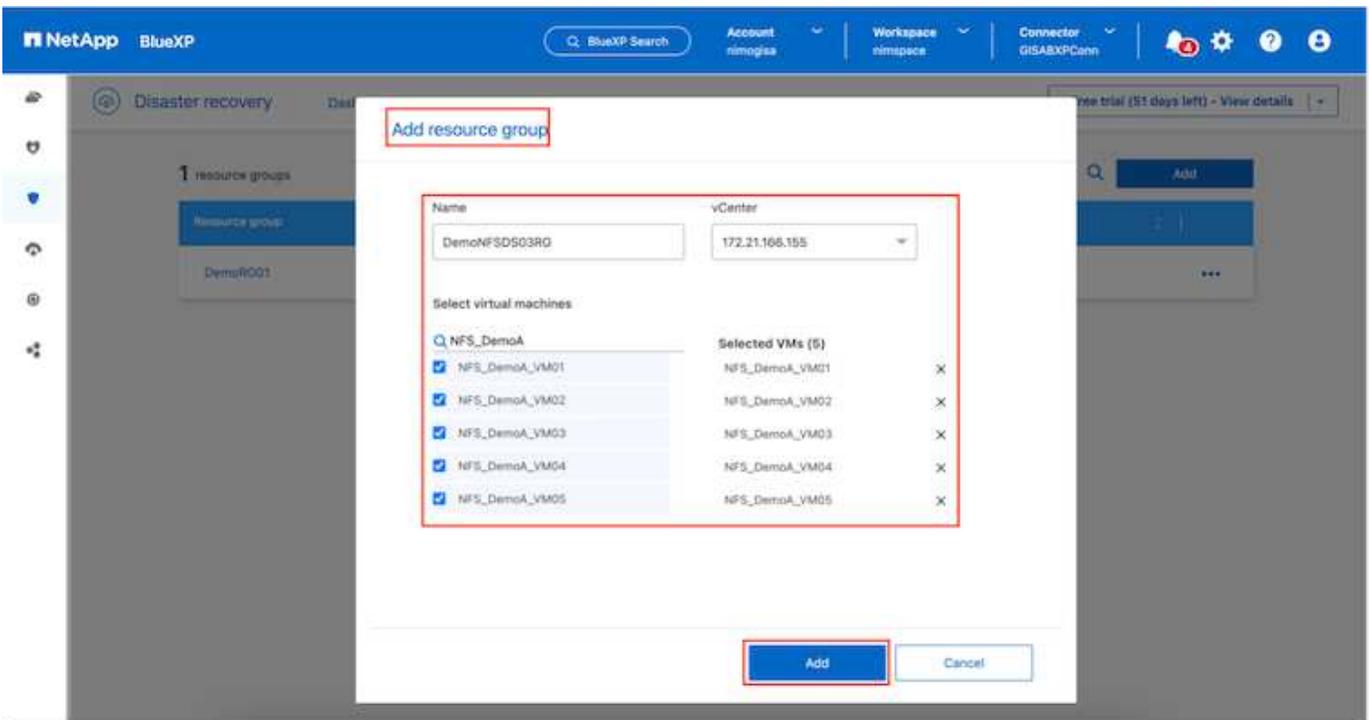
Wenn die SnapMirror-Beziehung bereits über CLI für das Volume konfiguriert ist, nimmt BlueXP DRaaS die Beziehung auf und fährt mit den restlichen Workflow-Operationen fort.

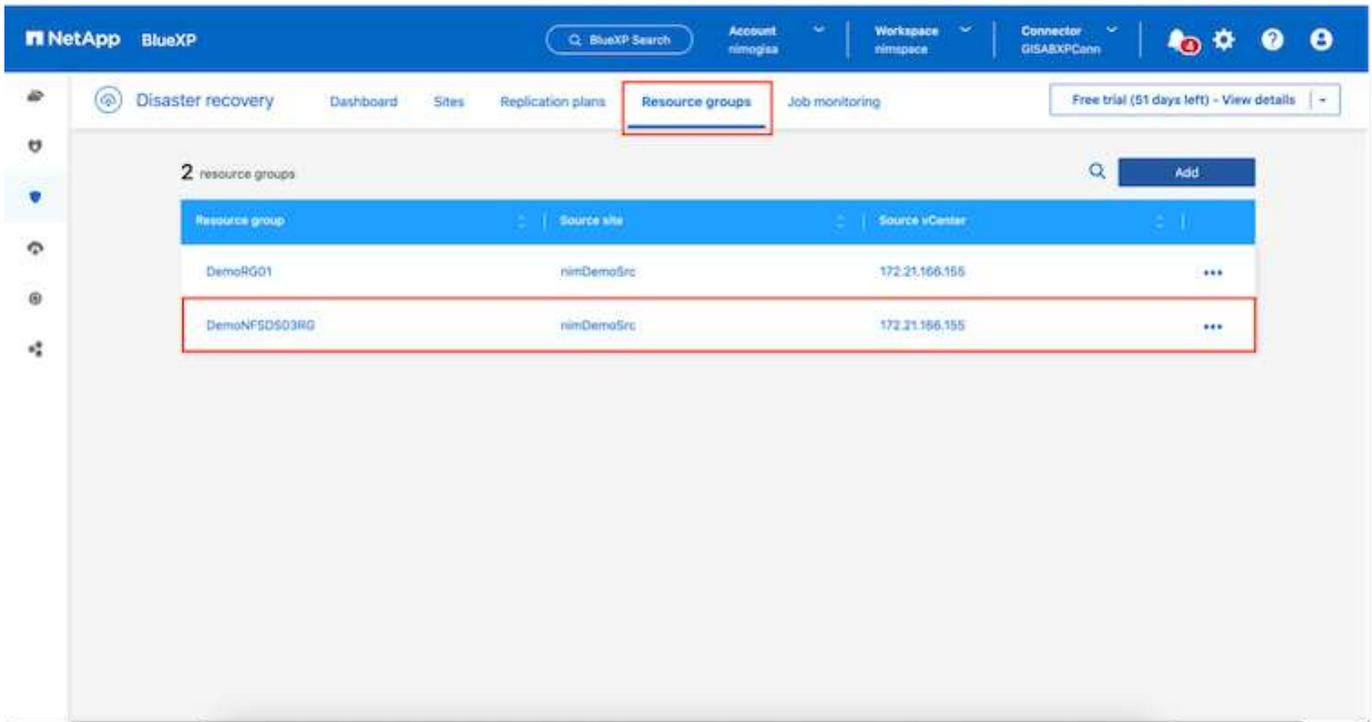
Welche Vorteile bietet BlueXP Disaster Recovery für Sie?

Nachdem die Quell- und Zielstandorte hinzugefügt wurden, führt die BlueXP Disaster Recovery automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. BlueXP Disaster Recovery erkennt auch automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt diese aus.



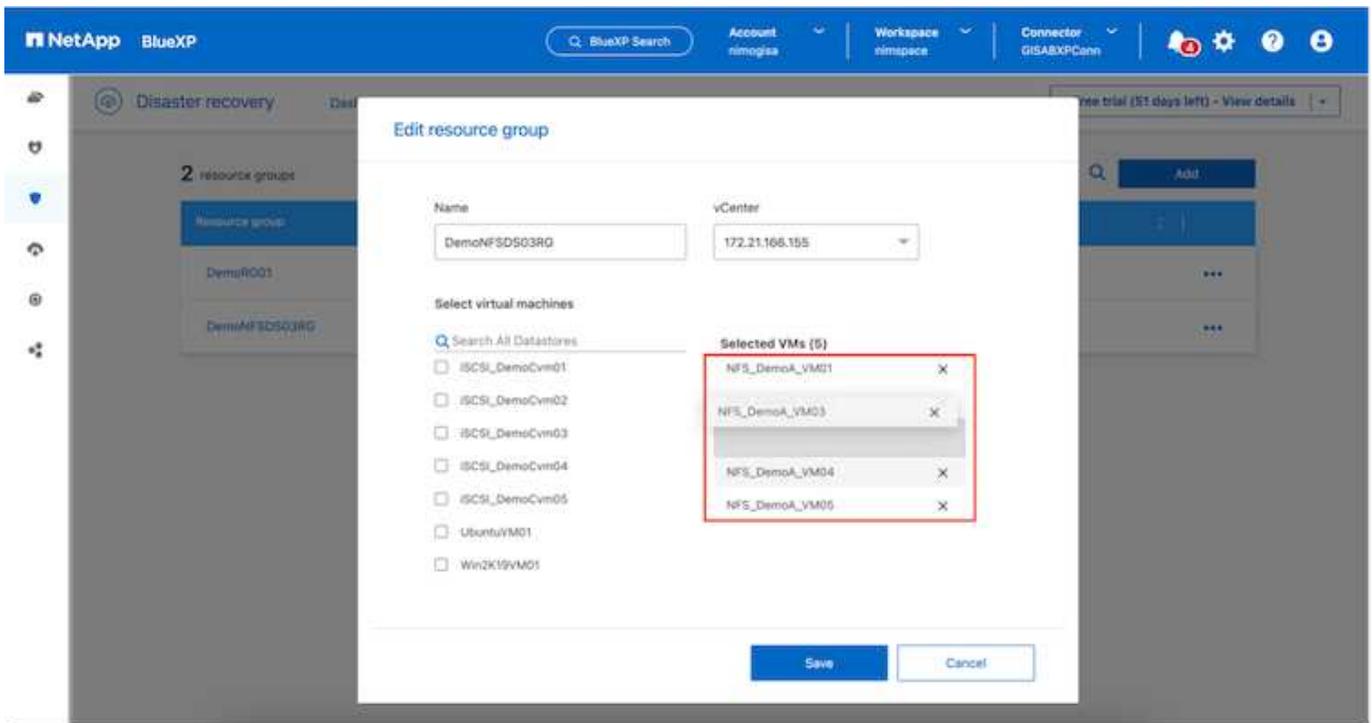
Nach dem Hinzufügen der Standorte können VMs zu Ressourcengruppen zusammengefasst werden. Mit den BlueXP Disaster Recovery-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logischen Gruppen gruppieren, die ihre Boot-Aufträge und Boot-Verzögerungen enthalten, die bei der Recovery ausgeführt werden können. Um Ressourcengruppen zu erstellen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.





Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

Die Boot-Reihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen Drag-and-Drop-Mechanismus definiert oder geändert werden.



Nach der Erstellung der Ressourcengruppen erstellen Sie im nächsten Schritt einen Ausführungsentwurf oder einen Plan für die Wiederherstellung von virtuellen Maschinen und Anwendungen bei einem Notfall. Wie in den Voraussetzungen erwähnt, kann die SnapMirror-Replikation vorab konfiguriert werden, oder DRaaS kann sie mithilfe der RPO und der Aufbewahrungszahl konfigurieren, die während der Erstellung des Replikationsplans

angegeben wurde.

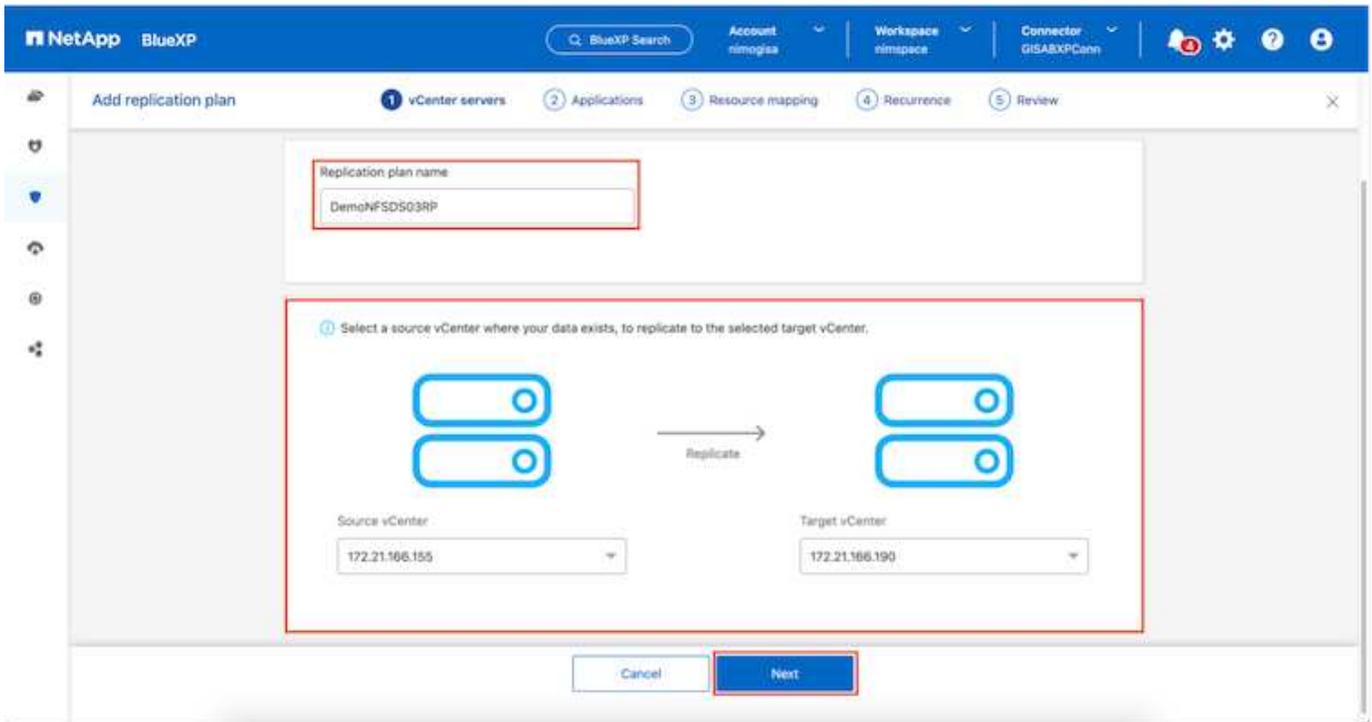
NetApp BlueXP interface showing 'My working environments'. The main area displays a replication diagram between two On-Premises ONTAP volumes: NTAP915_Src (2.01 TiB Capacity) and NTAP915_Destn (1.26 TiB Capacity). A replication link connects them. Other environments shown include Amazon S3 (4 Buckets) and NTAP915_12T (7.89 TiB Capacity). A sidebar on the right lists 'Working Environments' with 3 On-Premises ONTAP (11.16 TiB Provisioned Capacity) and Amazon S3 (4 Buckets).

NetApp BlueXP interface showing 'Replication' details. The main area displays a table of 'Volume Relationships (8)'. The table lists source and target volumes, transfer times, status, mirror state, and last successful transfer. One row is highlighted with a red box.

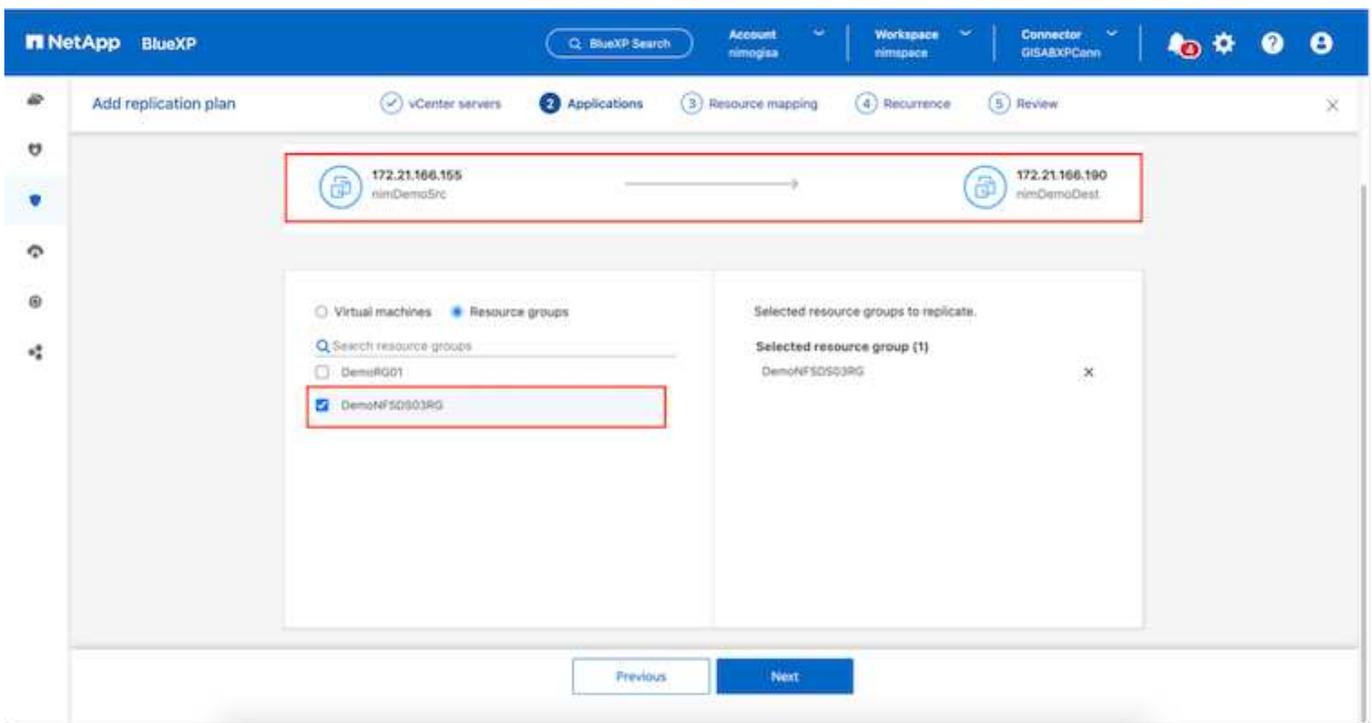
Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
✓	NTAP915_Src	NTAP915_Destn				20.3 MB
✓	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:15:38.63 MB
✓	Src_25G_Vol01 NTAP915_Src	Src_25G_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:17:23 MB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12:24.84 MB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12:47.38 MB
✓	Src_ISCSI_DS04 NTAP915_Src	Src_ISCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:108.87 MB
✓	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12:3.48 KiB

Konfigurieren Sie den Replizierungsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus dem Dropdown auswählen und die Ressourcengruppen auswählen, die in den Plan einbezogen werden sollen, sowie die Gruppierung der Art und Weise, wie Applikationen wiederhergestellt und eingeschaltet werden sollen, sowie die Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

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



Im nächsten Schritt wählen Sie vorhandene Ressourcengruppen aus. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent, die erforderlichen virtuellen Maschinen zu gruppieren (im Grunde erstellen Sie funktionale Ressourcengruppen) auf der Grundlage der Wiederherstellungsziele. Dies hilft auch dabei, die Reihenfolge der Wiederherstellung von virtuellen Maschinen der Anwendung festzulegen.

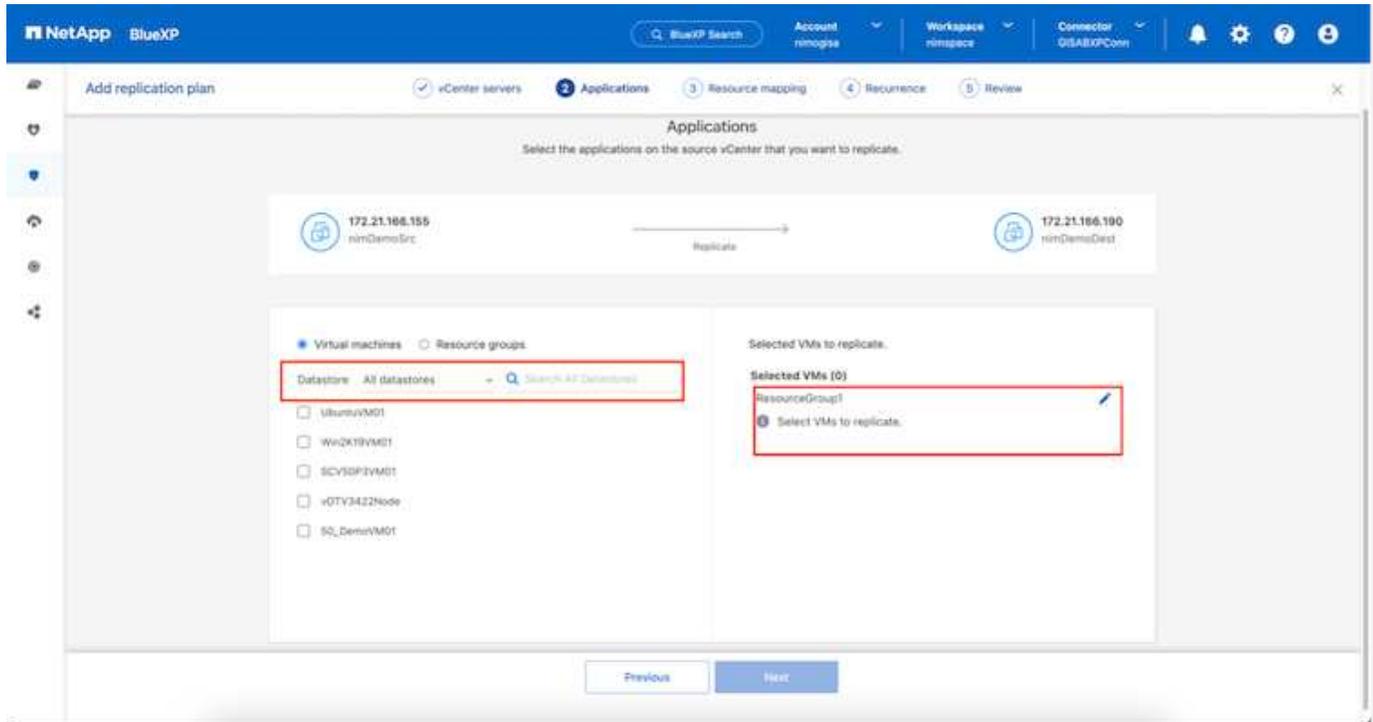


Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge mithilfe der Drag-and-Drop-Funktion. Damit kann die Reihenfolge, in der die VMs während des Recovery-Prozesses eingeschaltet werden, leicht geändert werden.

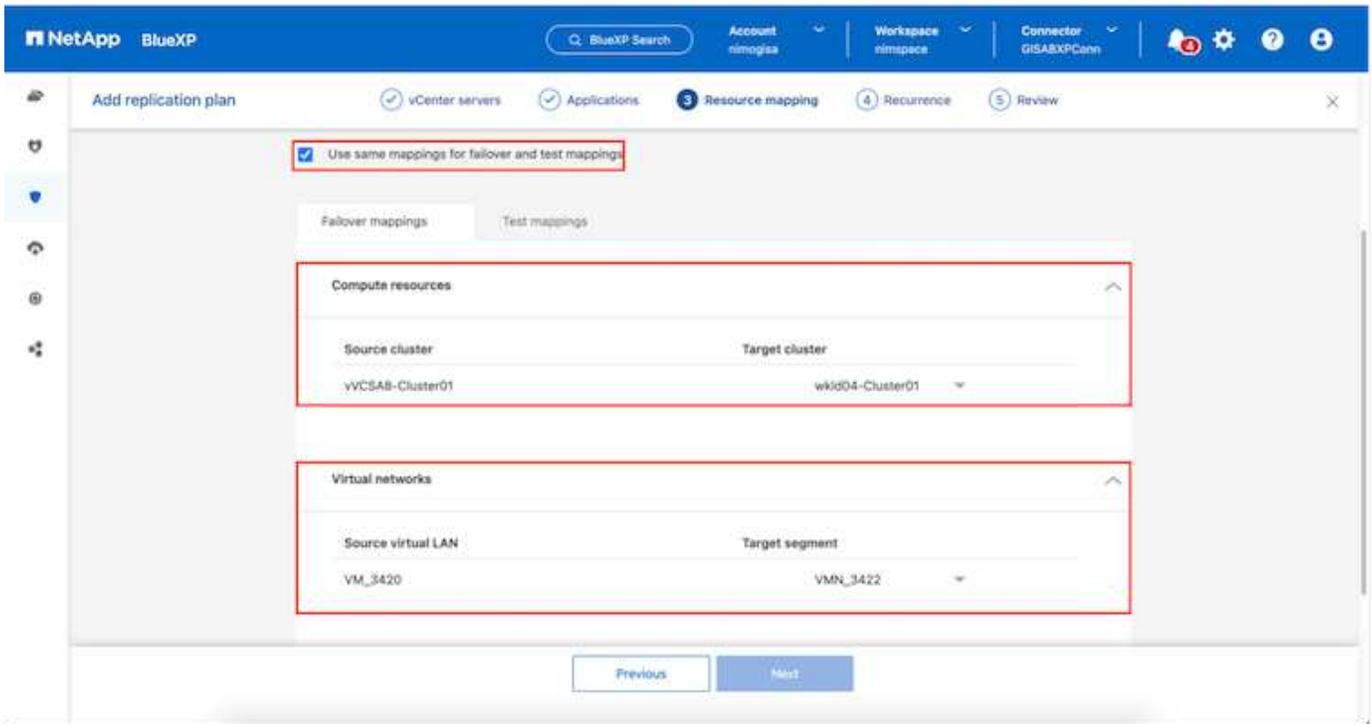


Jede virtuelle Maschine in einer Ressourcengruppe wird in der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

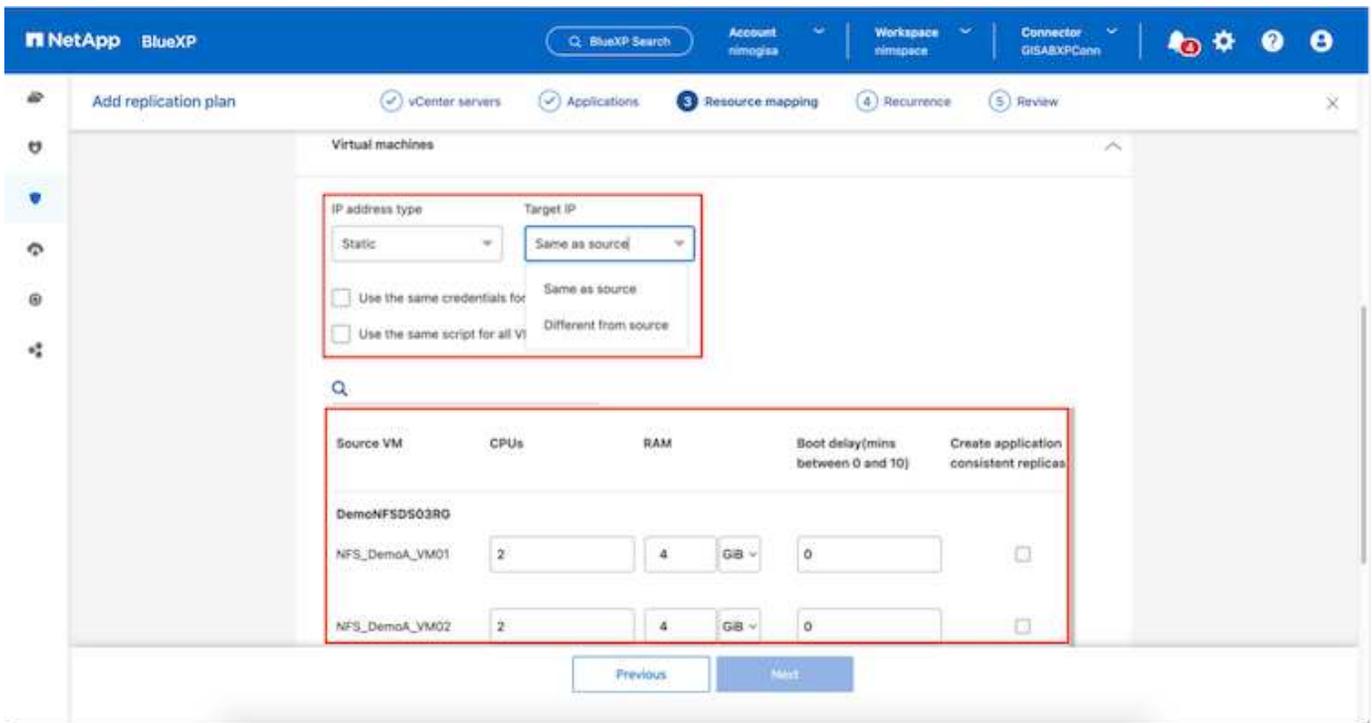
Der Screenshot unten zeigt die Option zum Filtern virtueller Maschinen oder spezieller Datastores nach Unternehmensanforderungen, wenn Ressourcengruppen nicht vorab erstellt werden.



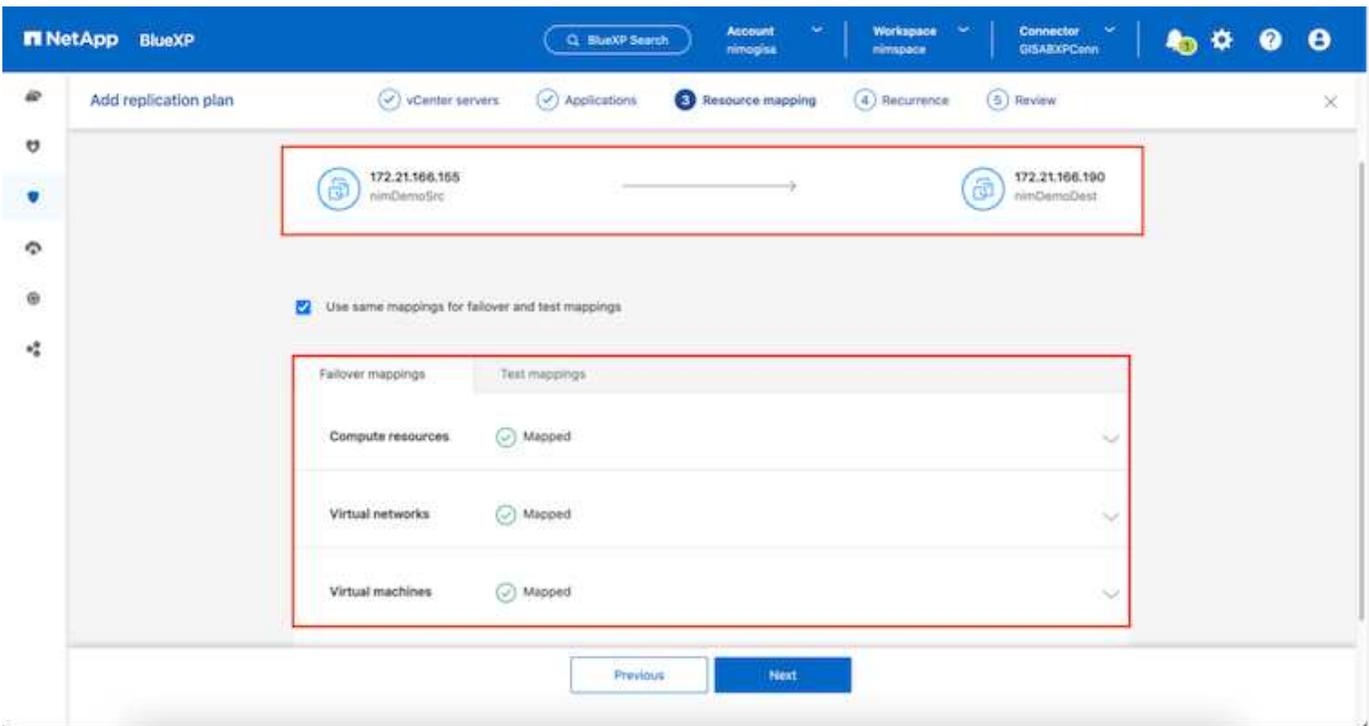
Sobald die Ressourcengruppen ausgewählt sind, erstellen Sie die Failover-Zuordnungen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen, virtuelle Netzwerke, IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Applikationskonsistenz usw. Weitere Informationen finden Sie unter ["Erstellen Sie einen Replizierungsplan"](#).



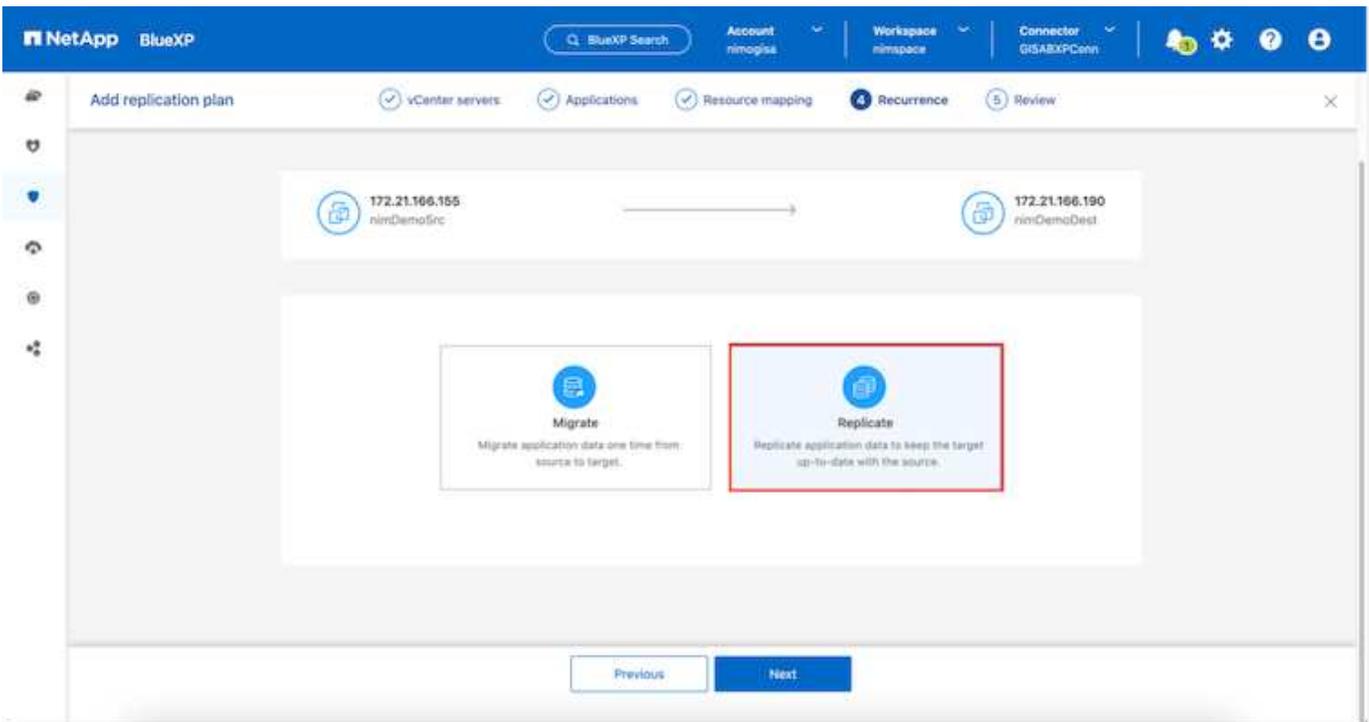
Standardmäßig werden für Test- und Failover-Vorgänge dieselben Zuordnungsparameter verwendet. Um unterschiedliche Zuordnungen für die Testumgebung festzulegen, aktivieren Sie die Option Testzuordnung, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:



Klicken Sie nach Abschluss der Ressourcenzuordnung auf Weiter.



Wählen Sie den Wiederholungstyp aus. In einfachen Worten: Wählen Sie Migrate (einmalige Migration mit Failover) oder die Option wiederkehrende kontinuierliche Replikation aus. In dieser Übersicht ist die Option „Replikat“ ausgewählt.



Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf **Plan hinzufügen**.



VMs von verschiedenen Volumes und SVMs können in einem Replizierungsplan enthalten sein. Abhängig von der VM-Platzierung (ob auf demselben Volume oder separaten Volumes innerhalb derselben SVM, separaten Volumes auf unterschiedlichen SVMs) erstellt das Disaster Recovery von BlueXP einen Snapshot einer Konsistenzgruppe.

NetApp BlueXP

Account nimogisa | Workspace nimspace | Connector GIGABXCann

Add replication plan

172.21.166.155 nimDemoSrc → Replicate → 172.21.166.190 nimDemoDest

Plan details | Fallover mapping | Virtual machines

Plan name: DemoNFSDS03RP

Recurrence: Replicate

Previous Add plan

NetApp BlueXP

Account nimogisa | Workspace nimspace | Connector GIGABXCann

Disaster recovery | Dashboard | Sites | **Replication plans** | Resource groups | Job monitoring

Free trial (51 days left) - View details

1 plans

Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Fallover site	
DemoNFSDS03RP	Healthy	Ready	nimDemoSrc	DemoNFSDS03RG	Replicate	nimDemoDest	...

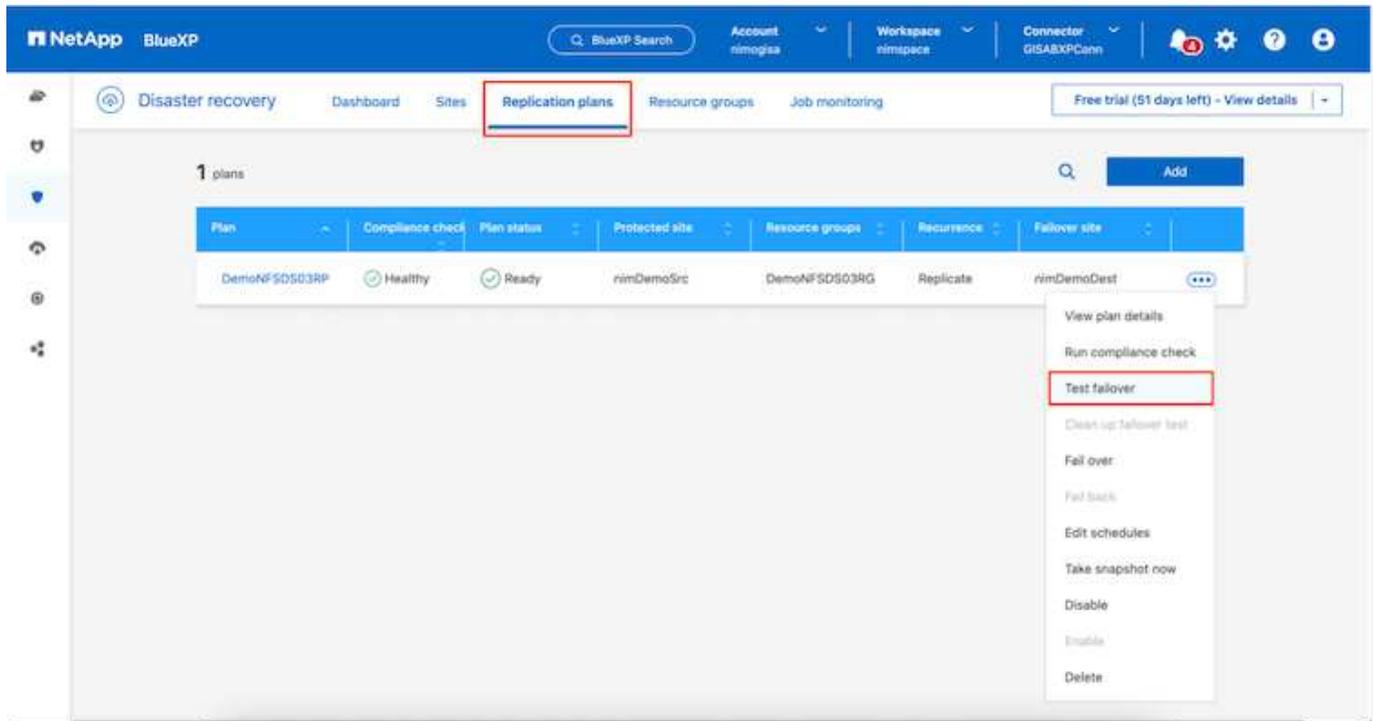
BlueXP DRaaS besteht aus den folgenden Workflows:

- Testen von Failover (einschließlich regelmäßiger, automatisierter Simulationen)
- Failover-Test bereinigen

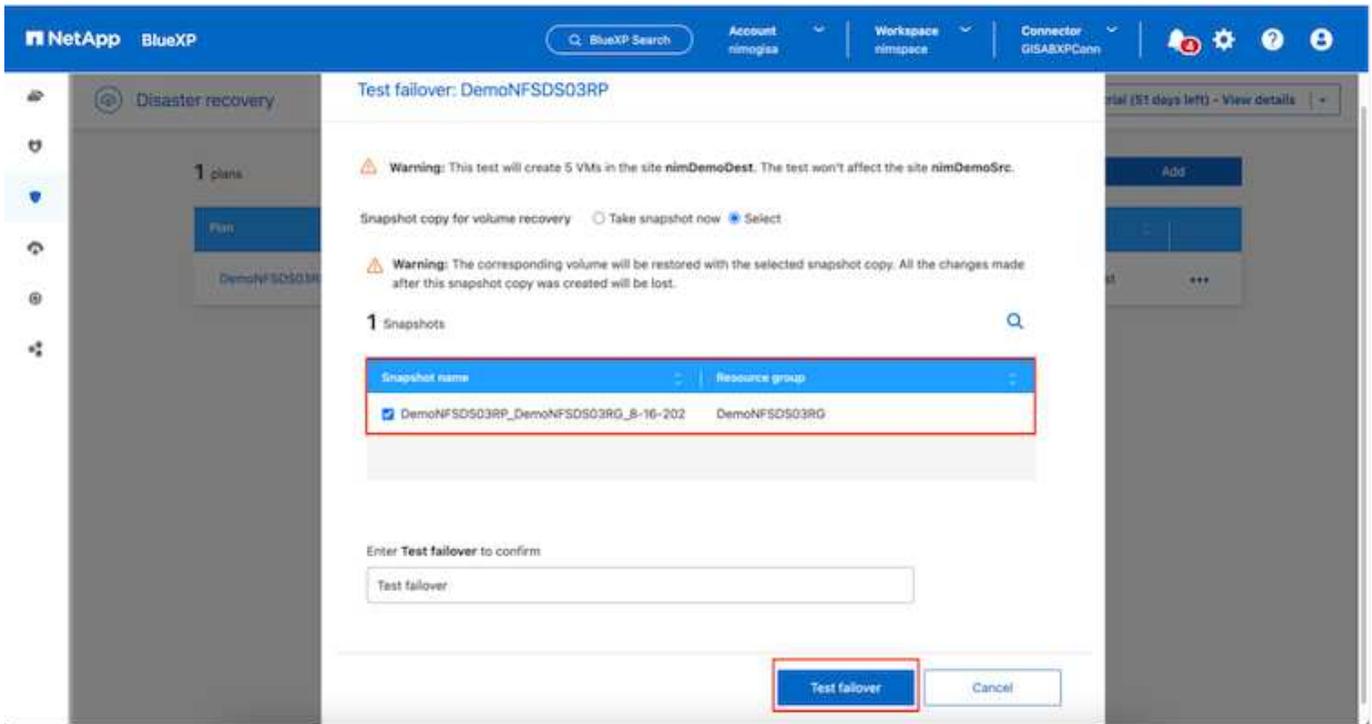
- Failover
- Failback

Testen Sie den Failover

Test-Failover in BlueXP DRaaS ist ein operatives Verfahren, mit dem VMware Administratoren ihre Recovery-Pläne vollständig validieren können, ohne ihre Produktionsumgebungen zu unterbrechen.

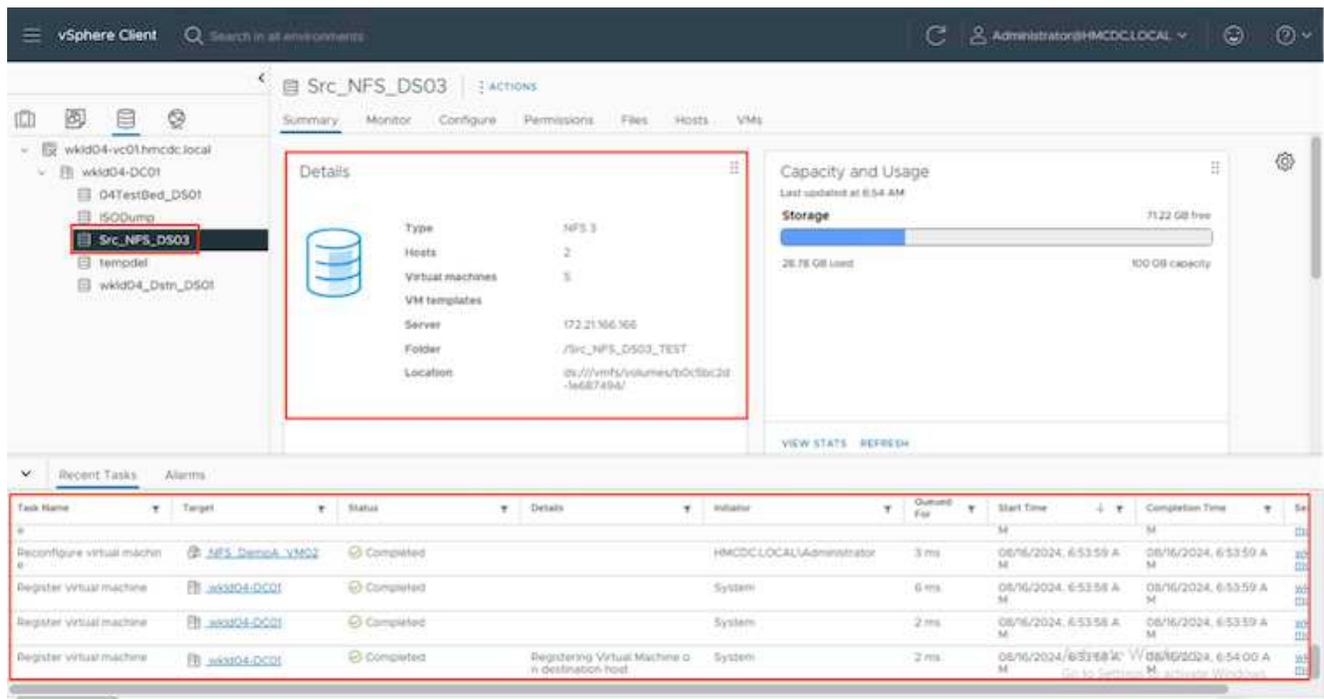


BlueXP DRaaS umfasst die Möglichkeit, den Snapshot als optionale Funktion im Test-Failover-Vorgang auszuwählen. Mit dieser Funktion kann der VMware Administrator überprüfen, ob alle kürzlich in der Umgebung vorgenommenen Änderungen am Zielstandort repliziert und somit während des Tests vorhanden sind. Zu diesen Änderungen gehören auch Patches für das VM-Gastbetriebssystem



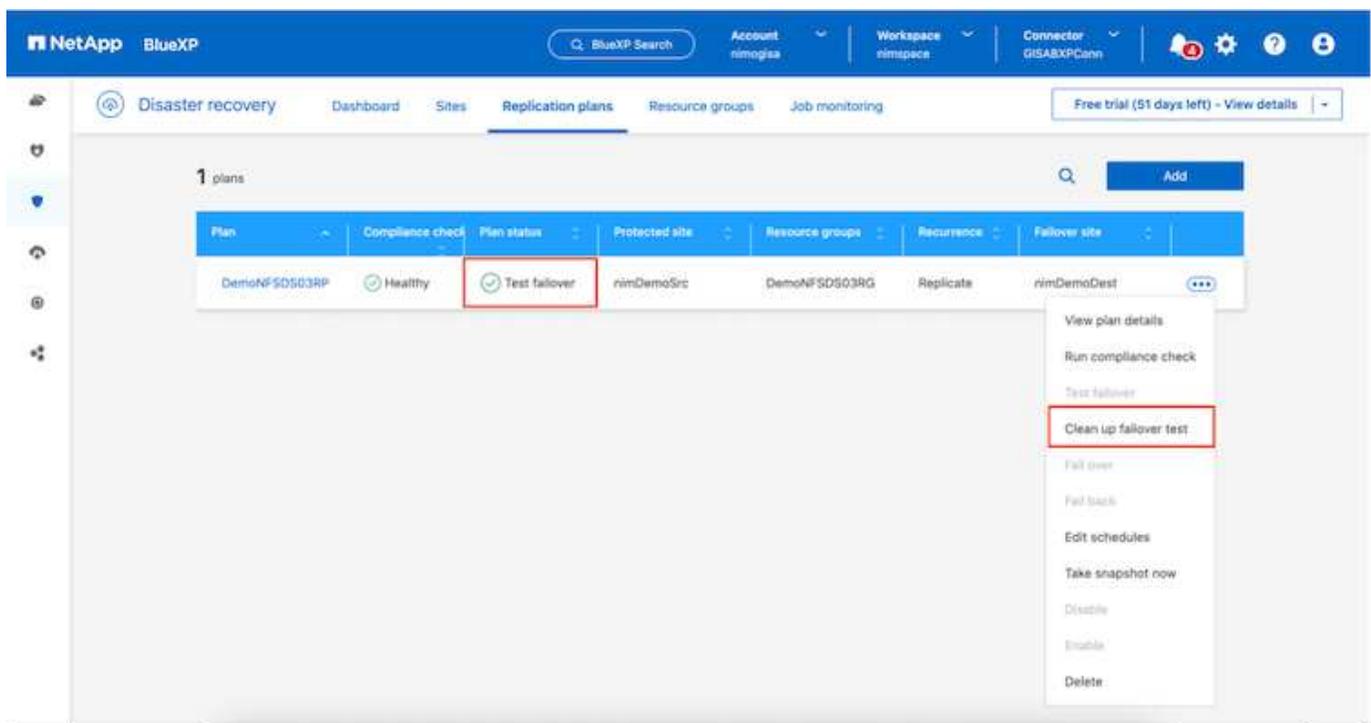
Wenn der VMware-Administrator einen Test-Failover ausführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

- Auslösung von SnapMirror-Beziehungen zur Aktualisierung des Speichers am Zielstandort auf kürzlich am Produktionsstandort vorgenommene Änderungen
- Erstellen von NetApp FlexClone Volumes der FlexVol Volumes auf dem DR-Storage-Array.
- Verbinden der NFS-Datstores in den FlexClone-Volumes mit den ESXi-Hosts am DR-Standort.
- Verbinden der VM-Netzwerkadapter mit dem während der Zuordnung angegebenen Testnetzwerk.
- Neukonfigurieren der Netzwerkeinstellungen des VM-Gastbetriebssystems, wie für das Netzwerk am DR-Standort definiert.
- Ausführen von benutzerdefinierten Befehlen, die im Replizierungsplan gespeichert wurden.
- Einschalten der VMs in der im Replizierungsplan definierten Reihenfolge



Bereinigen Sie den Failover-Testvorgang

Der Bereinigungetest für das Failover findet statt, nachdem der Test des Replikationsplans abgeschlossen wurde, und der VMware-Administrator reagiert auf die Bereinigungsaufforderung.



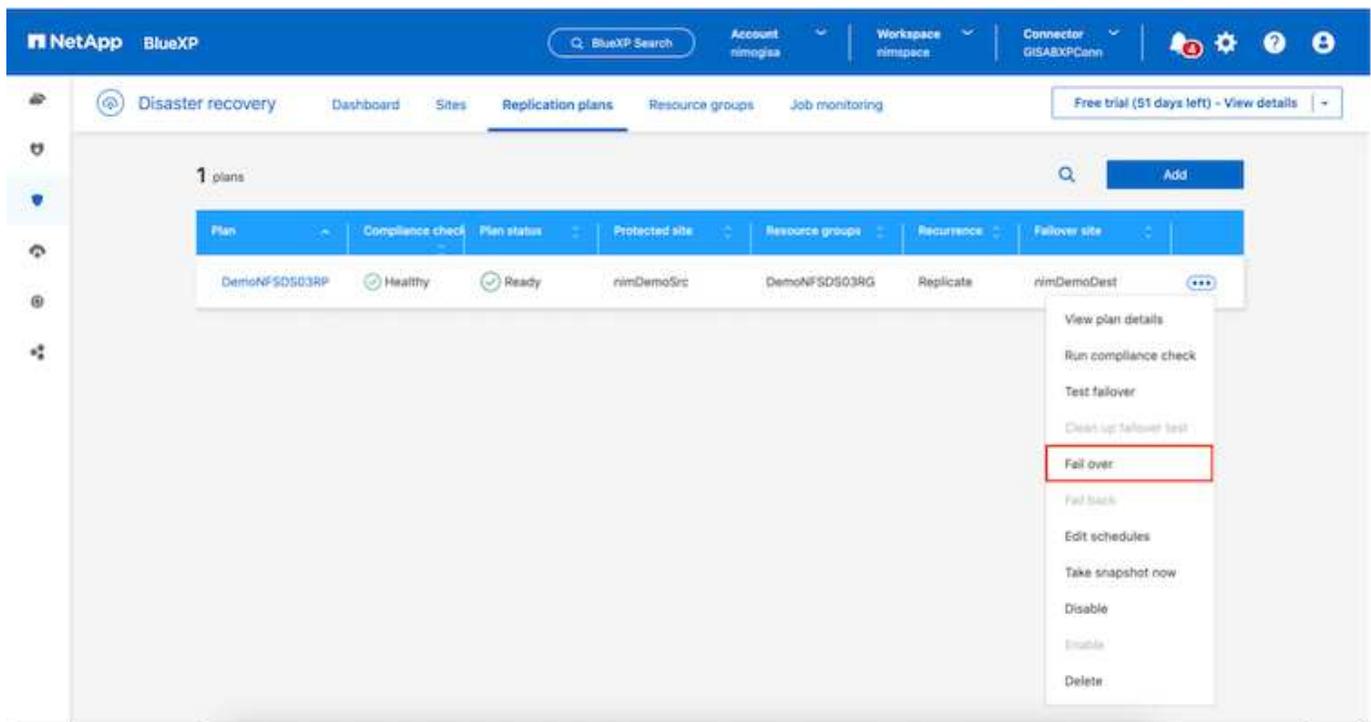
Durch diese Aktion werden die virtuellen Maschinen (VMs) und der Status des Replikationsplans auf den Bereitschaftszustand zurückgesetzt.

Wenn der VMware-Administrator einen Recovery-Vorgang durchführt, führt BlueXP DRaaS den folgenden Prozess aus:

1. Er schaltet jede wiederhergestellte VM in der FlexClone-Kopie, die für Tests verwendet wurde, ab.
2. Es löscht das FlexClone Volume, das verwendet wurde, um die wiederhergestellten VMs während des Tests darzustellen.

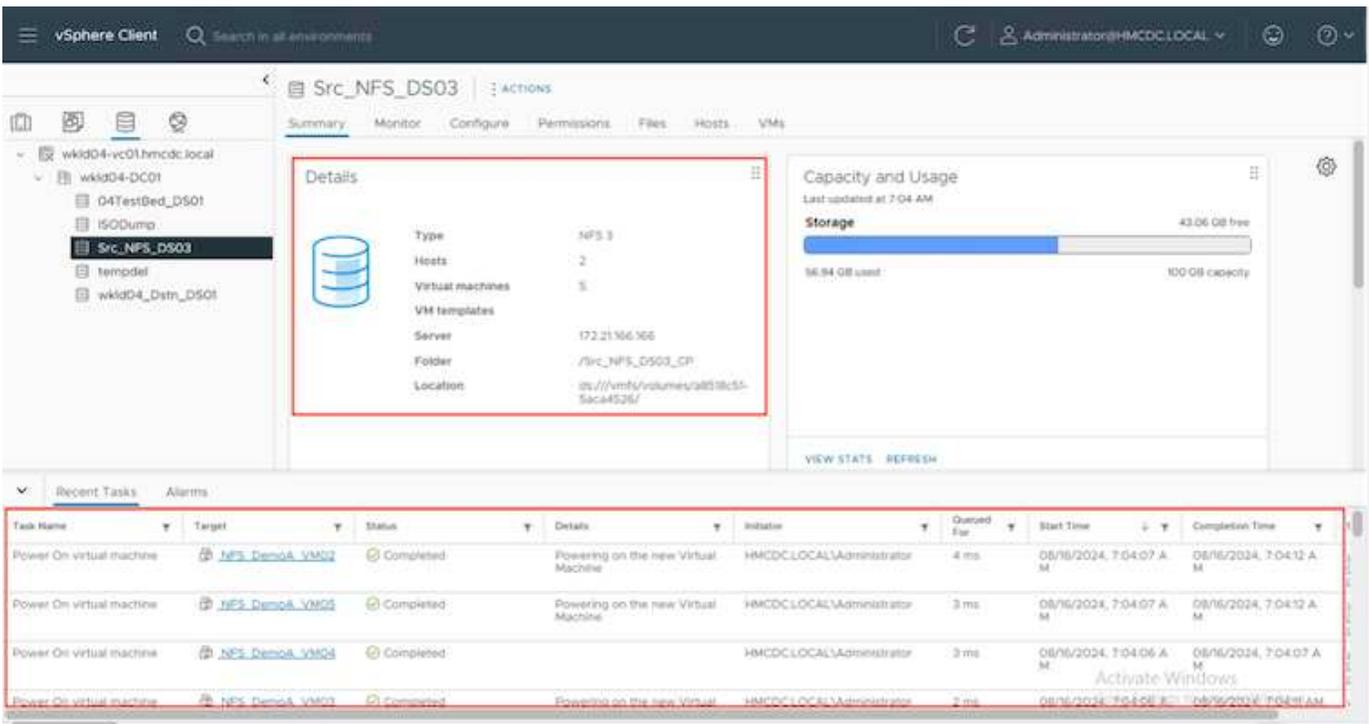
Geplante Migration und Failover

BlueXP DRaaS bietet zwei Methoden zur Durchführung eines echten Failover: Geplante Migration und Failover. Die erste Methode, die geplante Migration, umfasst die Synchronisierung von VM Shutdown und Storage-Replizierung in den Prozess, um die VMs wiederherzustellen oder effektiv zum Zielstandort zu verschieben. Für die geplante Migration ist der Zugriff auf den Quellstandort erforderlich. Die zweite Methode, Failover, ist ein geplantes/ungeplantes Failover, bei dem die VMs vom letzten Storage-Replizierungsintervall, das abgeschlossen werden konnte, am Zielstandort wiederhergestellt werden. Abhängig von dem RPO, der in die Lösung integriert wurde, kann im DR-Szenario ein gewisser Datenverlust erwartet werden.



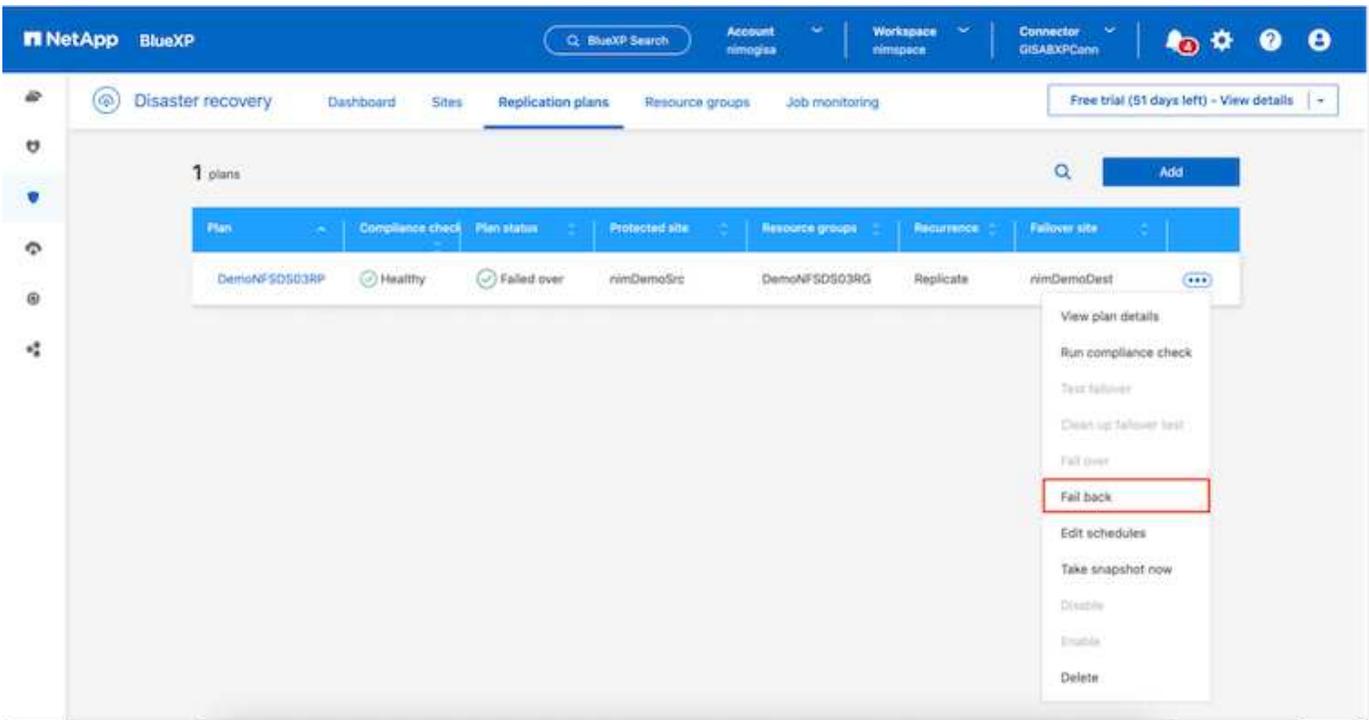
Wenn der VMware-Administrator einen Failover durchführt, automatisiert BlueXP DRaaS die folgenden Aufgaben:

- Trennung und Failover der NetApp SnapMirror Beziehungen
- Verbinden Sie die replizierten NFS-Datstores mit den ESXi-Hosts am DR-Standort.
- Verbinden Sie die VM-Netzwerkadapter mit dem entsprechenden Netzwerk des Zielstandorts.
- Konfigurieren Sie die Netzwerkeinstellungen des VM-Gastbetriebssystems wie für das Netzwerk am Zielstandort definiert neu.
- Führen Sie alle benutzerdefinierten Befehle (falls vorhanden) aus, die im Replizierungsplan gespeichert wurden.
- Schalten Sie die VMs in der im Replizierungsplan definierten Reihenfolge ein.



Failback

Ein Failback ist ein optionales Verfahren, das die ursprüngliche Konfiguration der Quell- und Zielstandorte nach einer Wiederherstellung wiederherstellt.



VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie Services am ursprünglichen Quellstandort wiederherstellen möchten.

HINWEIS: BlueXP DRaaS repliziert (resynchronisiert) alle Änderungen zurück auf die ursprüngliche virtuelle Quellmaschine, bevor die Replikationsrichtung umkehrt. Dieser Prozess beginnt mit einer Beziehung, die das

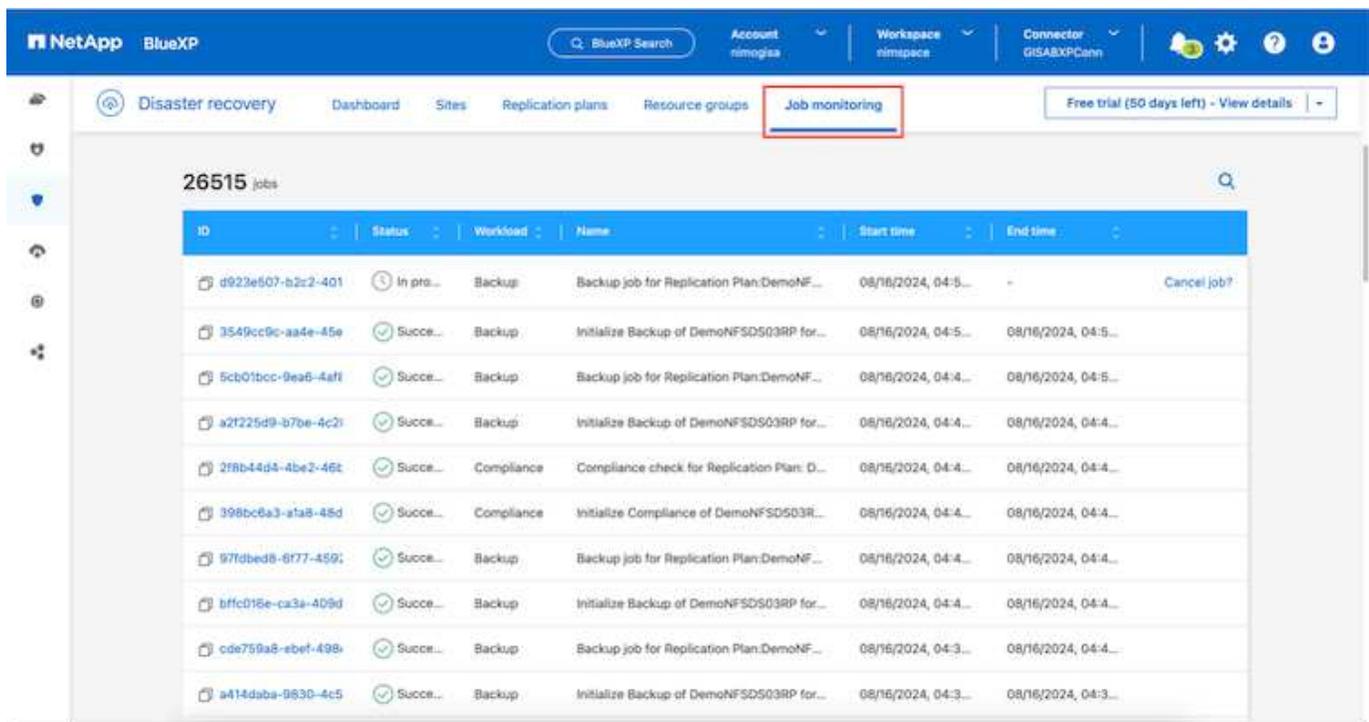
Failover zu einem Ziel abgeschlossen hat, und umfasst die folgenden Schritte:

- Das aus- und Abschalten der virtuellen Maschinen und Volumes am Zielstandort wird aufgehoben.
- Break die SnapMirror Beziehung auf der ursprünglichen Quelle ist gebrochen, um sie zu lesen/schreiben.
- Synchronisieren Sie die SnapMirror-Beziehung erneut, um die Replikation umzukehren.
- Mounten Sie das Volume auf der Quelle, schalten Sie die virtuellen Quellmaschinen ein und registrieren Sie sie.

Weitere Informationen über den Zugriff auf und die Konfiguration von BlueXP -DRaaS finden Sie im "[Erfahren Sie mehr über BlueXP Disaster Recovery für VMware](#)".

Monitoring und Dashboard

Über BlueXP oder die ONTAP-CLI können Sie den Replikationsstatus für die entsprechenden Datenspeicher-Volumes überwachen und den Status eines Failover oder Test-Failovers über die Jobüberwachung nachverfolgen.

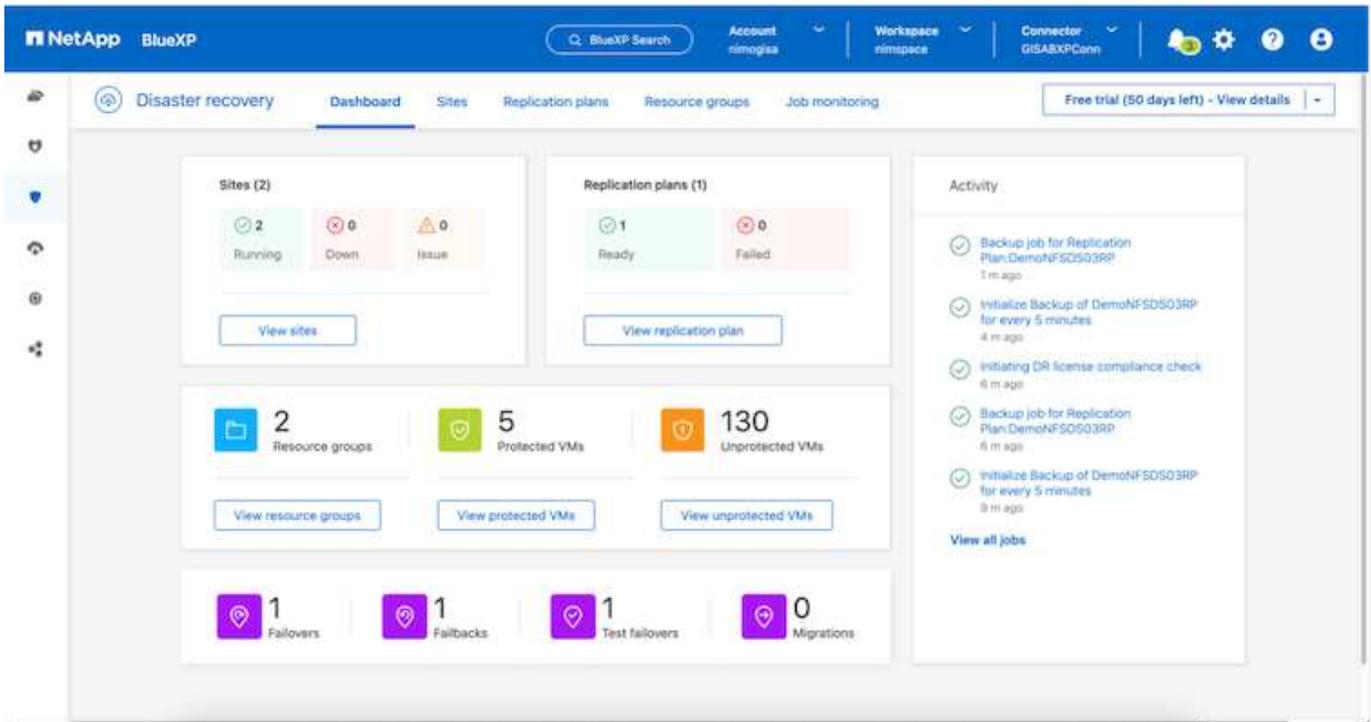


ID	Status	Workload	Name	Start time	End time	
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc9c-aa4e-45e	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4af1	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a21225d9-b7be-4c2f	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2f8b44d4-4be2-46f	Succe...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-ata8-48d	Succe...	Compliance	Initialize Compliance of DemoNFSD503R...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-6f77-459	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bffc016e-ca3a-409d	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-sbef-498b	Succe...	Backup	Backup job for Replication Plan:DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-883d-4c5	Succe...	Backup	Initialize Backup of DemoNFSD503RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



Wenn ein Job derzeit in Bearbeitung ist oder in der Warteschlange steht und Sie ihn anhalten möchten, gibt es eine Option, um ihn abubrechen.

Bewerten Sie mit dem BlueXP Dashboard für Disaster Recovery mühelos den Status von Disaster-Recovery-Standorten und Replizierungsplänen. So können Administratoren schnell gesunde, nicht verbundene oder beeinträchtigte Standorte und Pläne identifizieren.



Auf diese Weise erhalten Sie eine leistungsstarke Lösung, die einen individuellen Disaster-Recovery-Plan umsetzt. Failover lässt sich als geplanter Failover oder Failover mit einem Mausklick durchführen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung des DR-Standorts getroffen wird.

Um mehr über diesen Prozess zu erfahren, folgen Sie dem ausführlichen Walkthrough-Video oder verwenden Sie die ["Lösungssimulator"](#).

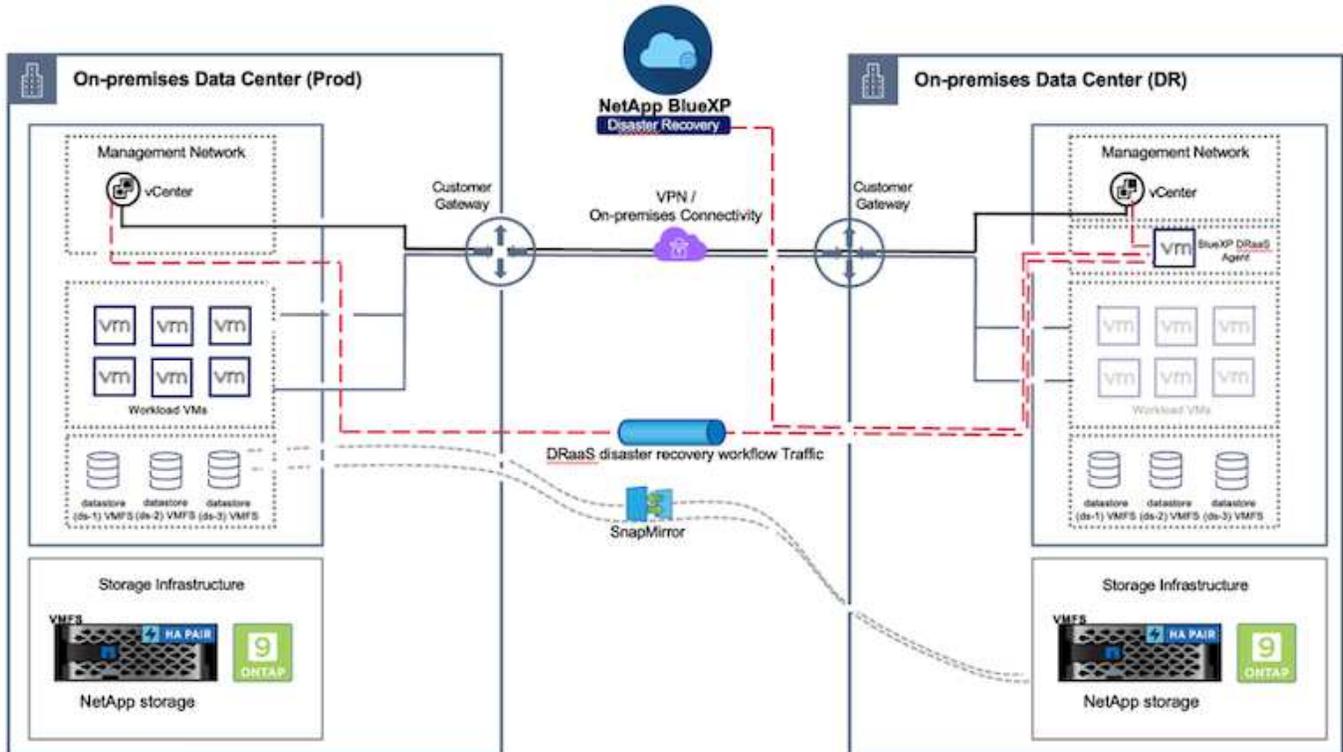
DR, die BlueXP DRaaS für VMFS-Datstores verwendet

Disaster Recovery mit Replizierung auf Blockebene vom Produktionsstandort zum Disaster-Recovery-Standort ist eine ausfallsichere und kostengünstige Möglichkeit, um Workloads vor Standortausfällen und Datenbeschädigung, z. B. Ransomware-Angriffen, zu schützen. Durch die NetApp SnapMirror-Replizierung können VMware Workloads, die lokale ONTAP Systeme mit VMFS Datastore ausführen, auf ein anderes ONTAP Storage-System in einem festgelegten Recovery-Datacenter repliziert werden, in dem sich VMware befindet

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zur Einrichtung von Disaster Recovery für lokale VMware VMs an einem anderen designierten Standort beschrieben. Als Teil dieser Einrichtung, das BlueXP Konto, BlueXP Connector, die ONTAP-Arrays in BlueXP Workspace hinzugefügt, die erforderlich sind, um die Kommunikation von VMware vCenter zum ONTAP Storage zu ermöglichen. Darüber hinaus wird in diesem Dokument beschrieben, wie die Replikation zwischen Standorten konfiguriert und ein Recovery-Plan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Standort-Failover und zum Failback, wenn der primäre Standort wiederhergestellt und online gekauft wird.

Mithilfe des BlueXP Disaster Recovery Service, der in die NetApp BlueXP Konsole integriert ist, können Kunden ihre lokalen VMware vCenter zusammen mit ONTAP Storage erkennen, Ressourcengruppen erstellen, einen Disaster Recovery-Plan erstellen, ihn Ressourcengruppen zuordnen und Failover und Failback testen oder ausführen. SnapMirror bietet Block-Replizierung auf Storage-Ebene, sodass die beiden Standorte mit

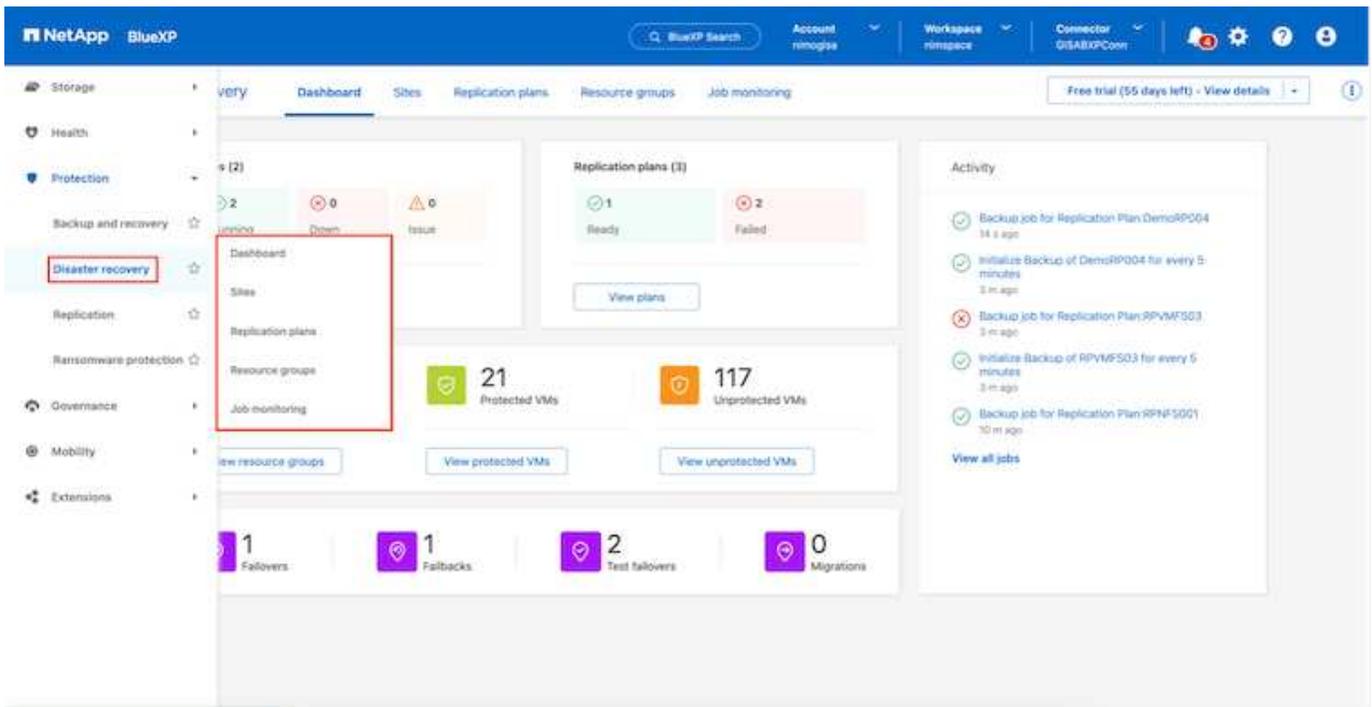
inkrementellen Änderungen aktualisiert werden können, was zu einem RPO von bis zu 5 Minuten führt. Außerdem ist es möglich, DR-Verfahren als regelmäßiges Drill-Verfahren zu simulieren, ohne Auswirkungen auf die Produktion und replizierte Datenspeicher zu haben oder zusätzliche Storage-Kosten entstehen. Bei BlueXP Disaster Recovery wird mithilfe der FlexClone Technologie von ONTAP eine platzsparende Kopie des VMFS Datastore vom letzten replizierten Snapshot am DR-Standort erstellt. Nach Abschluss des DR-Tests können Kunden die Testumgebung wieder löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Wenn (geplant oder ungeplant) das eigentliche Failover mit nur wenigen Klicks ausgeführt werden muss, orchestriert der BlueXP Disaster Recovery Service alle Schritte, die zum automatischen Einrichten der geschützten Virtual Machines am designierten Disaster Recovery-Standort erforderlich sind. Der Service umkehrt auch die SnapMirror-Beziehung zum primären Standort und repliziert bei Bedarf alle Änderungen für einen Failback-Vorgang von sekundär zu primär. All dies kann mit einem Bruchteil der Kosten im Vergleich zu anderen bekannten Alternativen erreicht werden.



Erste Schritte

Um die BlueXP Disaster Recovery zu starten, verwenden Sie die BlueXP Konsole und greifen Sie dann auf den Service zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste des BlueXP die Option Schutz > Notfallwiederherstellung.
3. Das BlueXP Disaster Recovery Dashboard wird angezeigt.



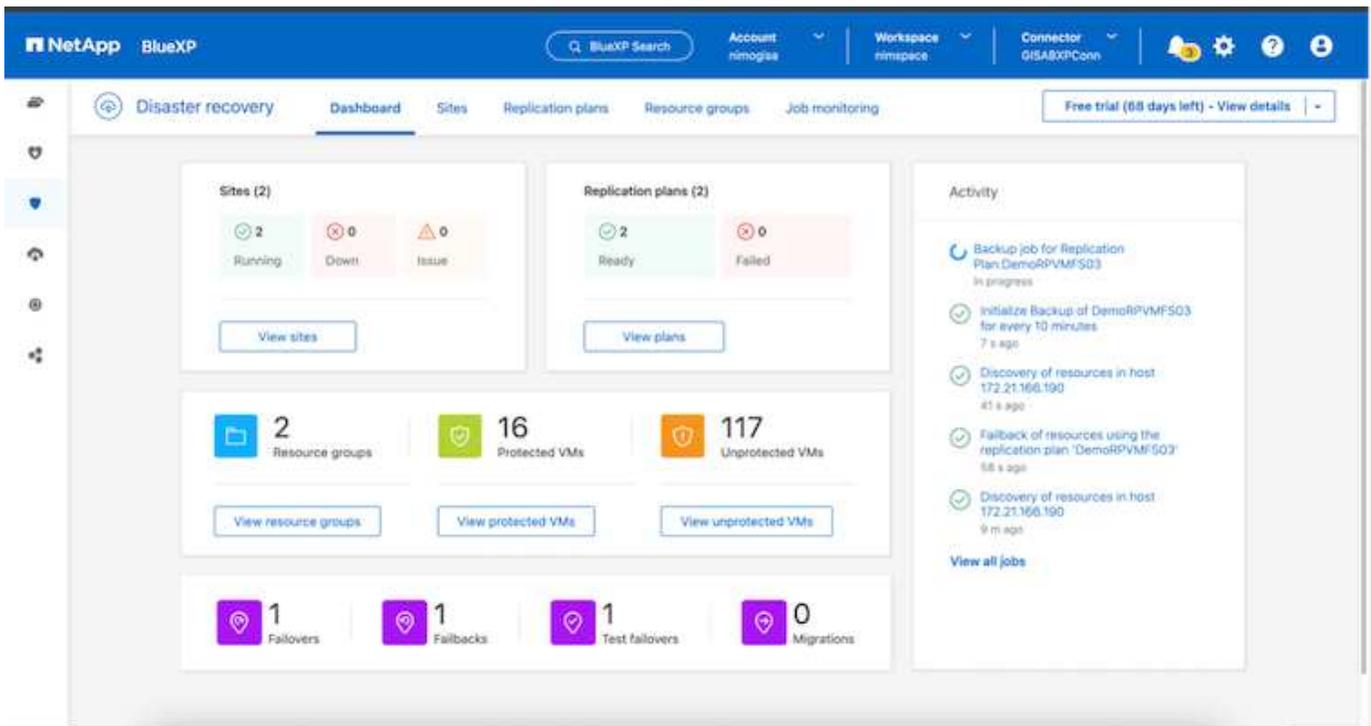
Stellen Sie vor der Konfiguration des Disaster Recovery-Plans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Der BlueXP -Anschluss ist in NetApp BlueXP eingerichtet. Der Connector sollte in AWS VPC implementiert werden.
- Die BlueXP Connector-Instanz ist mit dem Quell- und Ziel-vCenter sowie mit den Storage-Systemen verbunden.
- Lokale NetApp Storage-Systeme, die VMFS-Datstores für VMware hosten, werden in BlueXP hinzugefügt.
- Bei der Verwendung von DNS-Namen sollte die DNS-Auflösung vorhanden sein. Verwenden Sie andernfalls IP-Adressen für vCenter.
- Die SnapMirror-Replikation ist für die festgelegten VMFS-basierten Datastore Volumes konfiguriert.

Sobald die Verbindung zwischen dem Quell- und dem Zielstandort hergestellt ist, fahren Sie mit den Konfigurationsschritten fort. Diese dauert etwa 3 bis 5 Minuten.



NetApp empfiehlt die Implementierung des BlueXP Connectors am Disaster Recovery-Standort oder an einem dritten Standort, damit der BlueXP Connector über das Netzwerk mit den Quell- und Zielressourcen kommunizieren kann, wenn es zu echten Ausfällen oder Naturkatastrophen kommt.



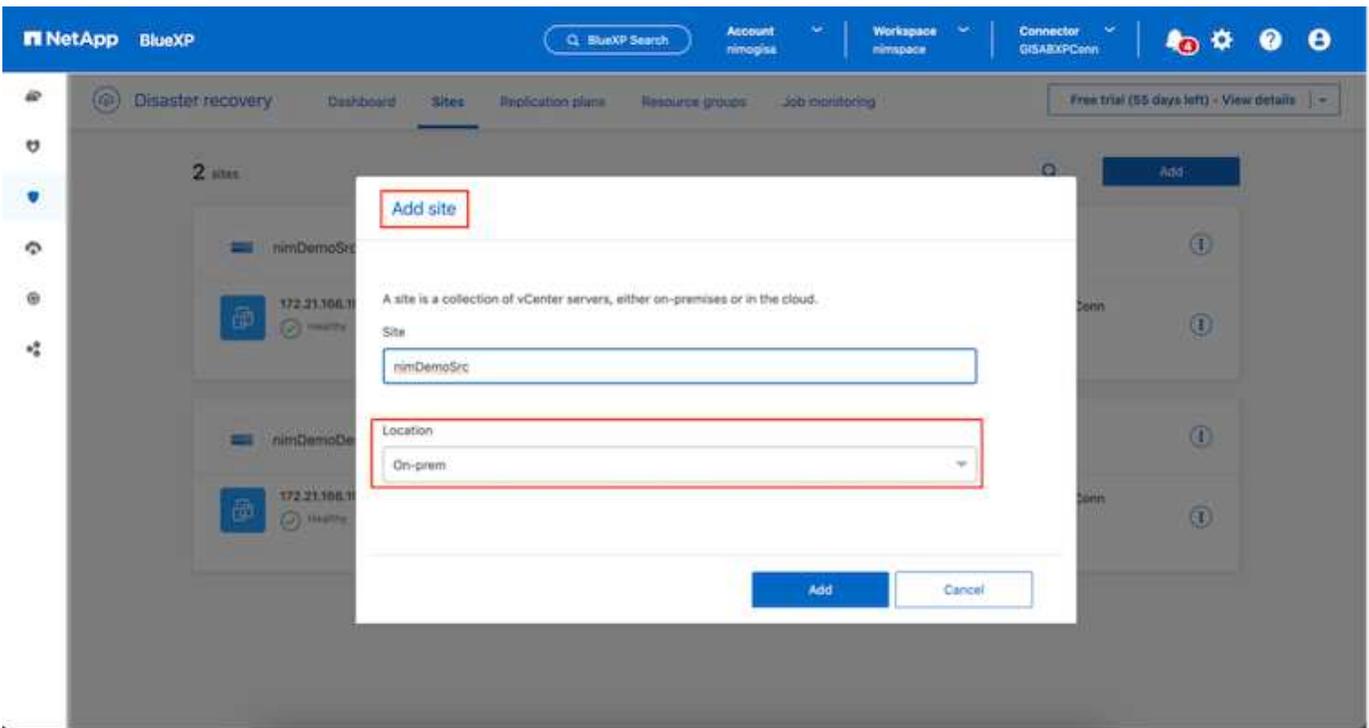
Die Unterstützung von lokalen zu lokalen VMFS-Datstores wird in einer Vorschau auf Technologie ausgeführt, während dieses Dokument verfasst wird. Die Funktion wird sowohl bei FC- als auch bei ISCSI-protokollbasierten VMFS-Datenspeichern unterstützt.

BlueXP Disaster Recovery-Konfiguration

Der erste Schritt zur Vorbereitung auf Disaster Recovery besteht darin, die lokalen vCenter und Storage-Ressourcen zu erkennen und zu BlueXP Disaster Recovery hinzuzufügen.

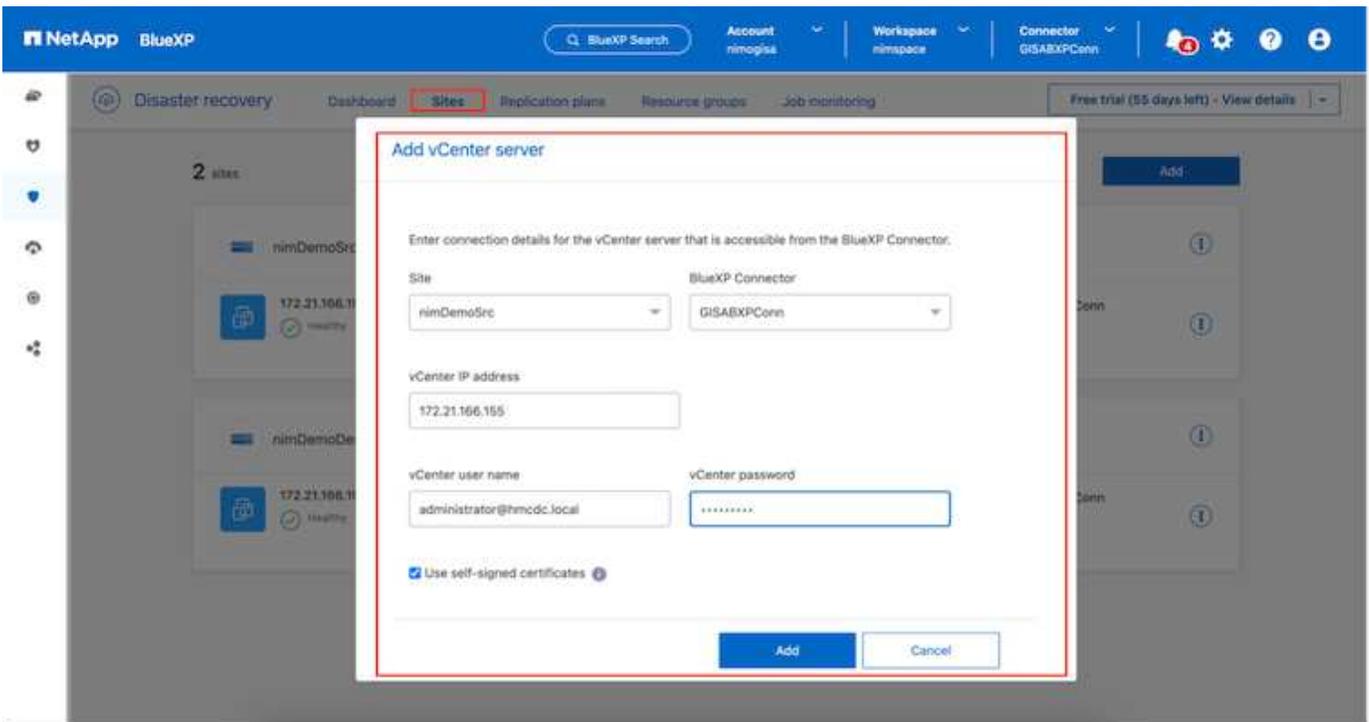


Stellen Sie sicher, dass die ONTAP-Speichersysteme der Arbeitsumgebung innerhalb des Arbeitsbereichs hinzugefügt werden. Öffnen Sie die BlueXP-Konsole, und wählen Sie aus der linken Navigation **Schutz > Notfallwiederherstellung** aus. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü, Wählen Sie **Standorte > Hinzufügen > vCenter hinzufügen**.

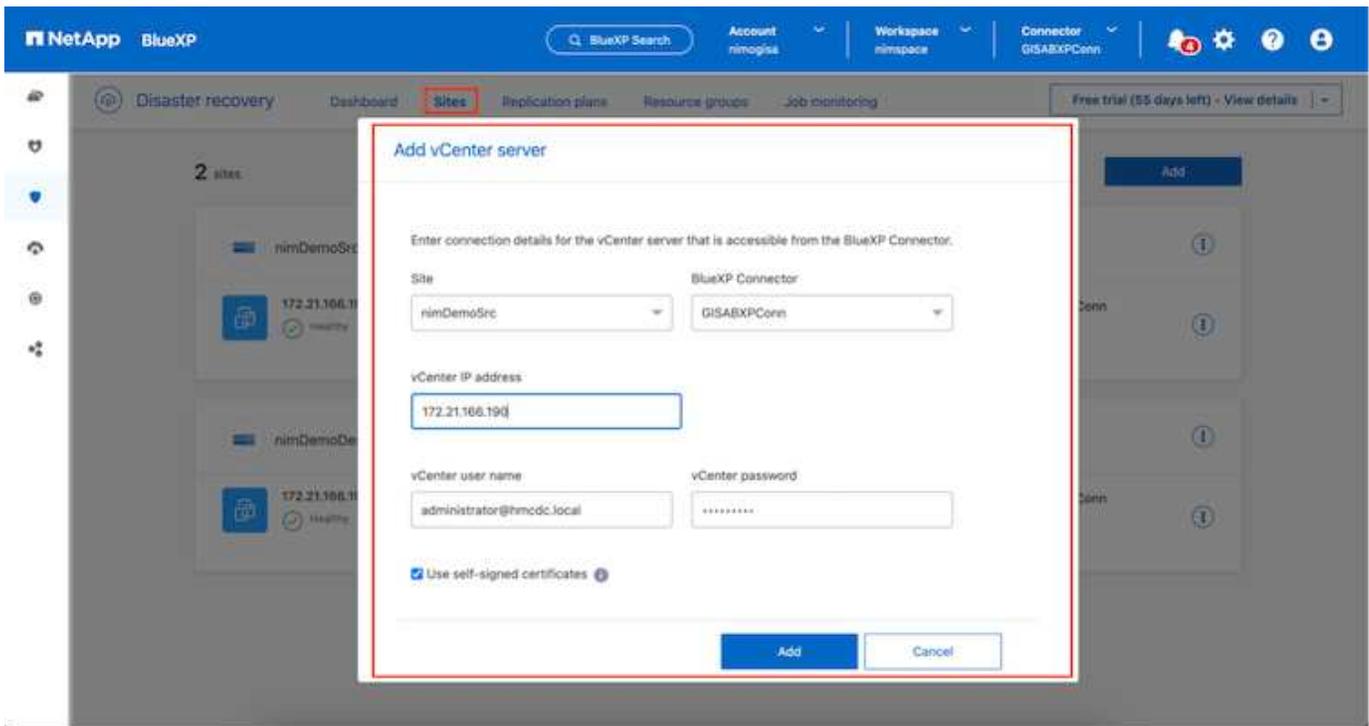


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle.** VCenter vor Ort.



- **Ziel.** VMC SDDC vCenter:



Sobald die vCenters hinzugefügt wurden, wird eine automatische Erkennung ausgelöst.

Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort

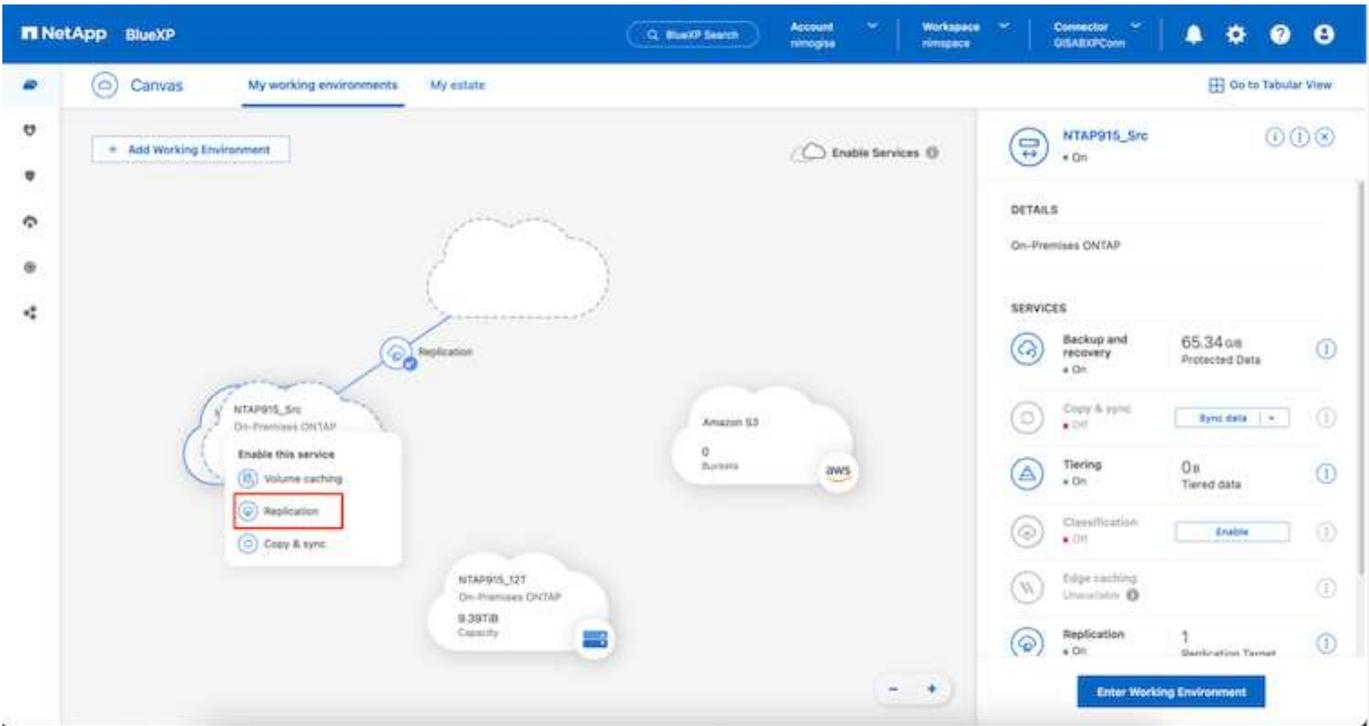
SnapMirror nutzt ONTAP Snapshots, um die Übertragung von Daten von einem Ort zum anderen zu verwalten. Zunächst wird eine vollständige Kopie, die auf einem Snapshot des Quell-Volumens basiert, zum Ziel kopiert, um eine Basissynchronisierung durchzuführen. Wenn an der Quelle Datenänderungen auftreten, wird ein neuer Snapshot erstellt und mit dem Basis-Snapshot verglichen. Die gefundenen Blöcke werden dann auf das Zielsystem repliziert. Der neuere Snapshot wird dabei zur aktuellen Basislinie oder zum neuesten gemeinsamen Snapshot. Dadurch kann der Prozess wiederholt und inkrementelle Updates an das Ziel gesendet werden.

Wenn eine SnapMirror Beziehung hergestellt wurde, befindet sich das Ziel-Volumen in einem schreibgeschützten Online-Zustand und ist somit noch zugänglich. SnapMirror arbeitet mit physischen Storage-Blöcken und nicht auf File- oder logischer Ebene. Das heißt, das Ziel-Volumen ist ein identisches Replikat der Quelle, einschließlich Snapshots, Volume-Einstellungen usw. Wenn das Quell-Volumen ONTAP-Funktionen zur Speicherplatzeffizienz wie Datenkomprimierung und Datendeduplizierung verwendet, so behält das replizierte Volumen diese Optimierungen bei.

Wenn die SnapMirror Beziehung unterbrochen wird, wird das Ziel-Volumen beschreibbar gemacht und normalerweise für einen Failover verwendet, wenn SnapMirror zur Synchronisierung von Daten mit einer DR-Umgebung verwendet wird. SnapMirror ist ausreichend ausgereift, damit die am Failover-Standort geänderten Daten effizient zurück zum primären System resynchronisiert werden können, falls sie später wieder online sind, und dann die ursprüngliche SnapMirror Beziehung wiederhergestellt werden kann.

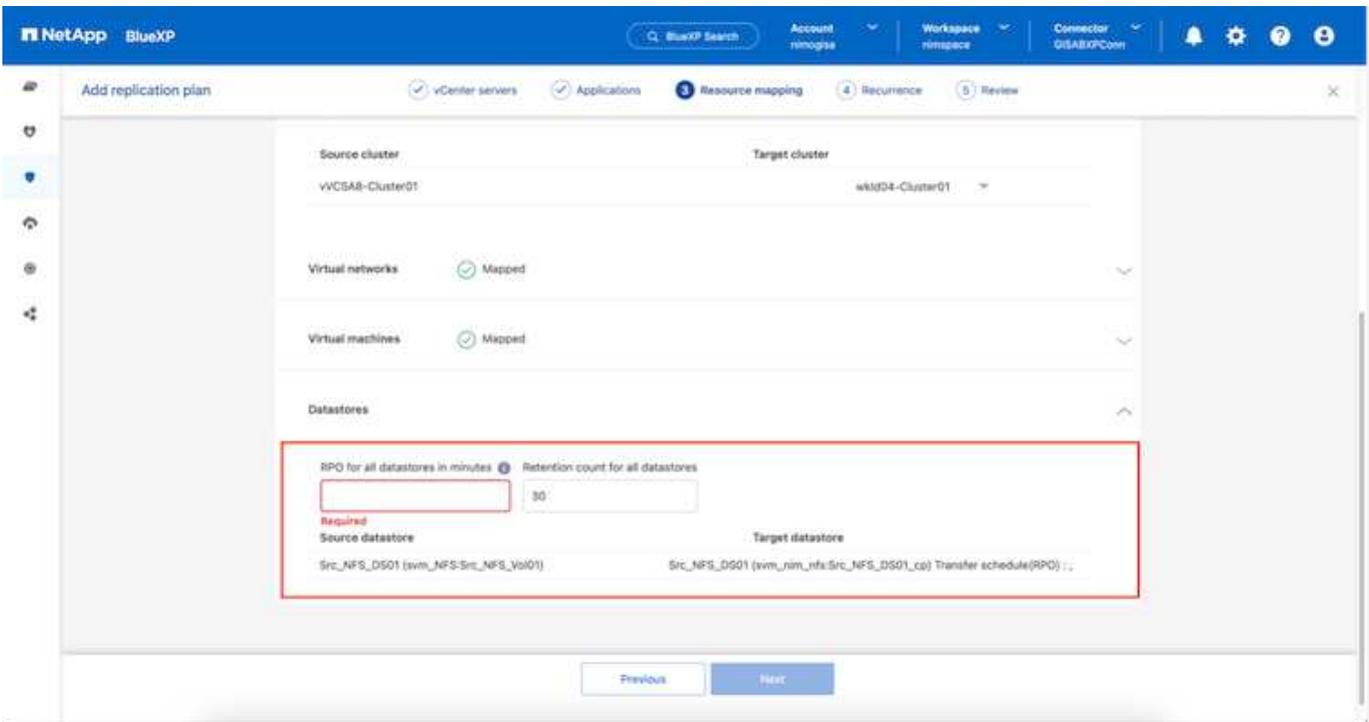
Wie Sie es für VMware Disaster Recovery einrichten

Der Prozess zur Erstellung der SnapMirror-Replizierung bleibt für jede Applikation unverändert. Der Prozess kann manuell oder automatisiert werden. Am einfachsten lässt sich BlueXP zur Konfiguration der SnapMirror Replizierung nutzen, indem das ONTAP Quell-System der Umgebung einfach per Drag & Drop auf das Ziel gezogen wird, um den Assistenten zu starten, der den Rest des Prozesses durchläuft.



Auch BlueXP DRaaS kann dasselbe automatisieren, wenn die folgenden beiden Kriterien erfüllt sind:

- Quell- und Ziel-Cluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



Wenn die SnapMirror-Beziehung bereits über CLI für das Volume konfiguriert ist, nimmt BlueXP DRaaS die Beziehung auf und fährt mit den restlichen Workflow-Operationen fort.



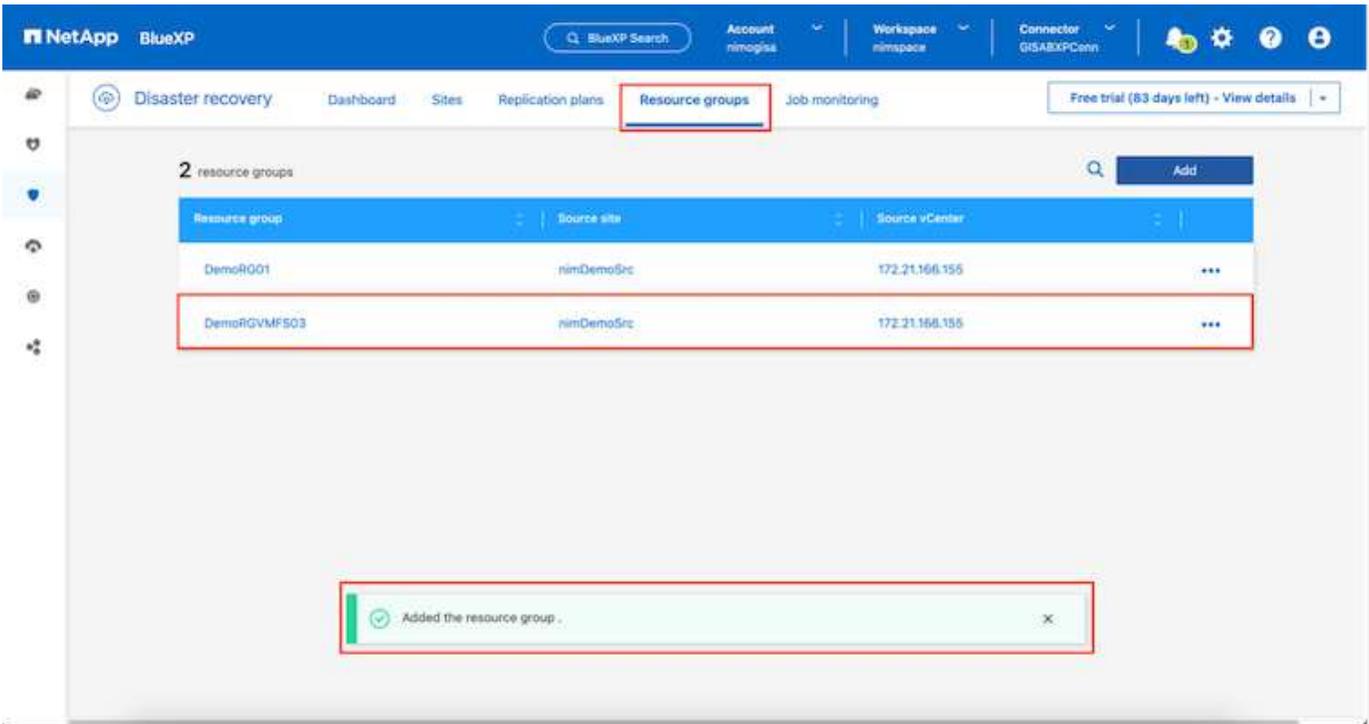
Abgesehen von den oben genannten Ansätzen kann die SnapMirror Replikation auch über ONTAP CLI oder System Manager erstellt werden. Unabhängig vom Ansatz zur Datensynchronisierung mit SnapMirror orchestriert BlueXP DRaaS den Workflow für nahtlose und effiziente Disaster-Recovery-Vorgänge.

Welche Vorteile bietet BlueXP Disaster Recovery für Sie?

Nachdem die Quell- und Zielstandorte hinzugefügt wurden, führt die BlueXP Disaster Recovery automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. BlueXP Disaster Recovery erkennt auch automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt diese aus.

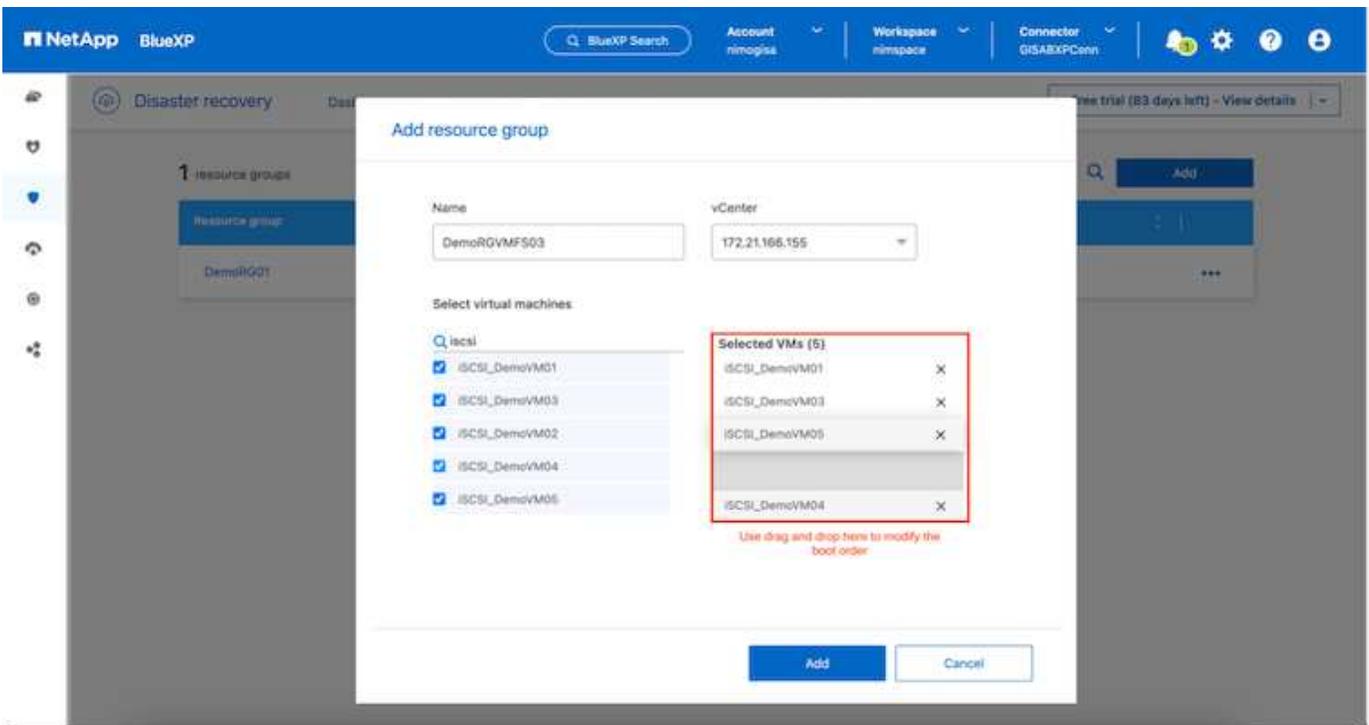
Site Name	IP Address	Health	VMs	Databases	Resource groups	Connector
nimDemoSrc	172.21.166.155	Healthy	72	13	1	GISABXPConn
nimDemoDest	172.21.166.190	Healthy	61	3	0	GISABXPConn

Nach dem Hinzufügen der Standorte können VMs zu Ressourcengruppen zusammengefasst werden. Mit den BlueXP Disaster Recovery-Ressourcengruppen können Sie eine Reihe abhängiger VMs in logischen Gruppen gruppieren, die ihre Boot-Aufträge und Boot-Verzögerungen enthalten, die bei der Recovery ausgeführt werden können. Um Ressourcengruppen zu erstellen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.



Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

Die Boot-Reihenfolge der VMs kann während der Erstellung von Ressourcengruppen mithilfe eines einfachen Drag-and-Drop-Mechanismus definiert oder geändert werden.



Nach der Erstellung der Ressourcengruppen erstellen Sie im nächsten Schritt einen Ausführungsentwurf oder einen Plan für die Wiederherstellung von virtuellen Maschinen und Anwendungen bei einem Notfall. Wie in den Voraussetzungen erwähnt, kann die SnapMirror-Replikation vorab konfiguriert werden, oder DRaaS kann sie mithilfe der RPO und der Aufbewahrungszahl konfigurieren, die während der Erstellung des Replikationsplans

angegeben wurde.

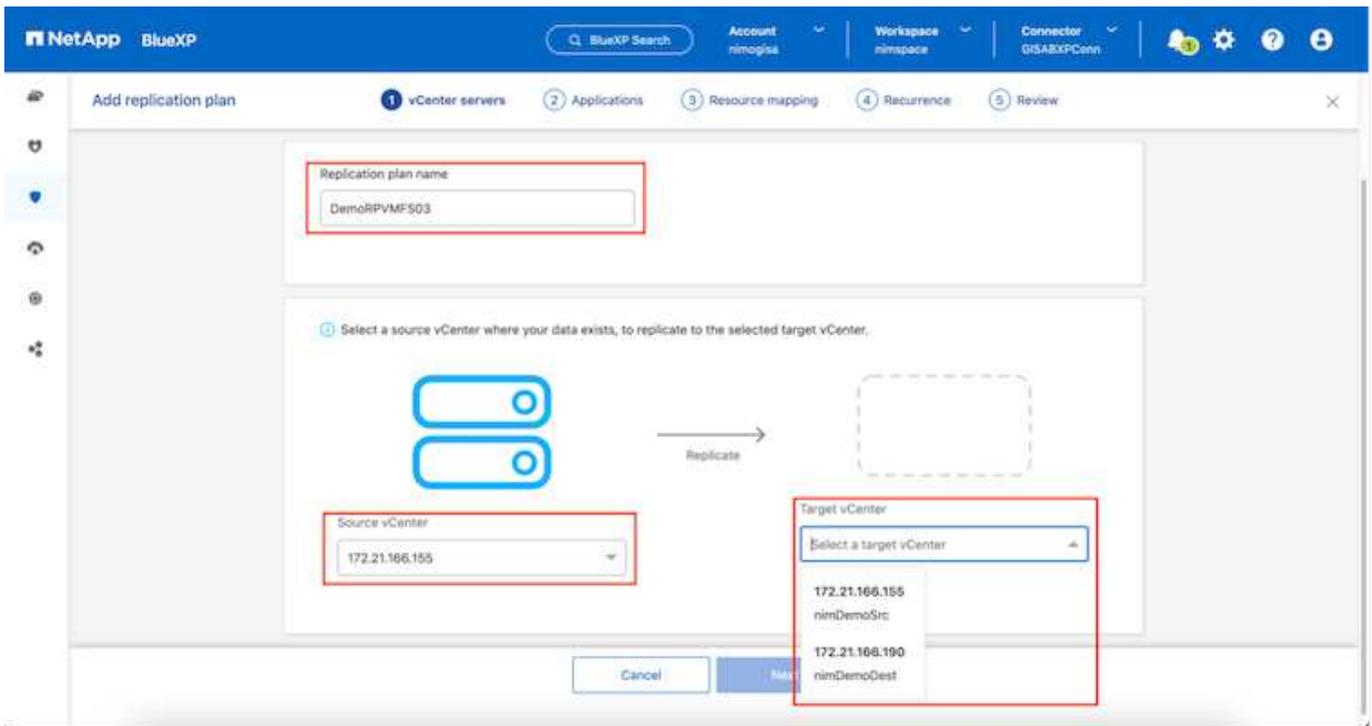
NetApp BlueXP interface showing 'My working environments'. A red box highlights a replication relationship between 'NTAP915_Src' (2.01 TiB Capacity) and 'NTAP915_Destn' (1.26 TiB Capacity). Other environments shown include 'NTAP915_127' (7.89 TiB Capacity) and 'Amazon S3' (4 Buckets). The right sidebar shows 'Working Environments' with 3 On-Premises ONTAP (11.16 TiB Provisioned Capacity) and Amazon S3 (4 Buckets).

NetApp BlueXP interface showing 'Replication' details. Summary statistics: 6 Volume Relationships, 495.27 GiB Replicated Capacity, 0 Currently Transferring, 6 Healthy, 0 Failed.

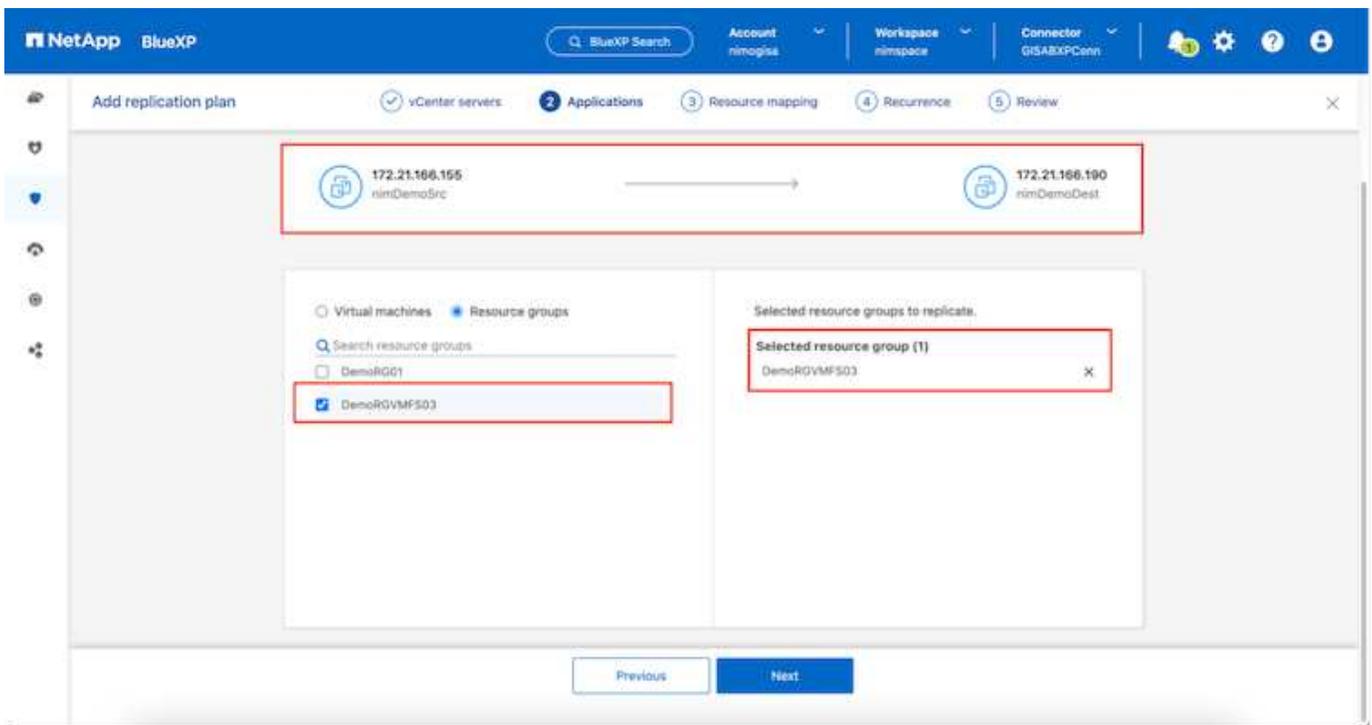
Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful
✓	DRaaS_src NTAP915_Src	DRaaS_src_copy NTAP915_Destn	5 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:05 28.41 MiB
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	13 seconds	idle	snapmirrored	Jul 15, 2024, 8:07:13 183.41 MiB
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 183.58 MiB
✓	Src_NFS_Vol01 NTAP915_Src	Src_NFS_DS01_cp NTAP915_Destn	14 seconds	idle	snapmirrored	Jul 15, 2024, 8:43:22 546.23 MiB
✓	Src_JSCSI_DS01 NTAP915_Src	Src_JSCSI_DS01_cp NTAP915_Destn	20 seconds	idle	snapmirrored	Jul 12, 2024, 4:24:34 22.35 MiB
✓	Src_JSCSI_DS03 NTAP915_Src	Src_JSCSI_DS03_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 254.89 MiB

Konfigurieren Sie den Replizierungsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus dem Dropdown auswählen und die Ressourcengruppen auswählen, die in den Plan einbezogen werden sollen, sowie die Gruppierung der Art und Weise, wie Applikationen wiederhergestellt und eingeschaltet werden sollen, sowie die Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

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



Im nächsten Schritt wählen Sie vorhandene Ressourcengruppen aus. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent, die erforderlichen virtuellen Maschinen zu gruppieren (im Grunde erstellen Sie funktionale Ressourcengruppen) auf der Grundlage der Wiederherstellungsziele. Dies hilft auch dabei, die Reihenfolge der Wiederherstellung von virtuellen Maschinen der Anwendung festzulegen.

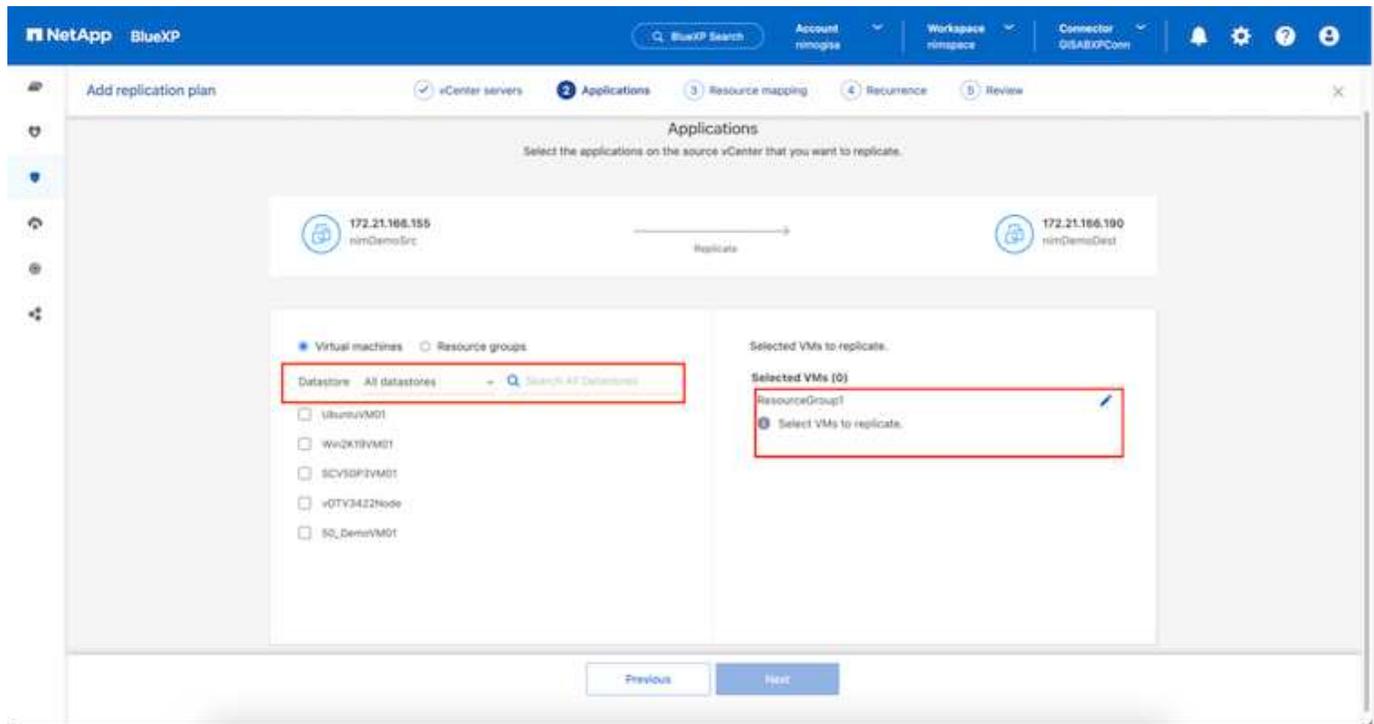


Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge mithilfe der Drag-and-Drop-Funktion. Damit kann die Reihenfolge, in der die VMs während des Recovery-Prozesses eingeschaltet werden, leicht geändert werden.

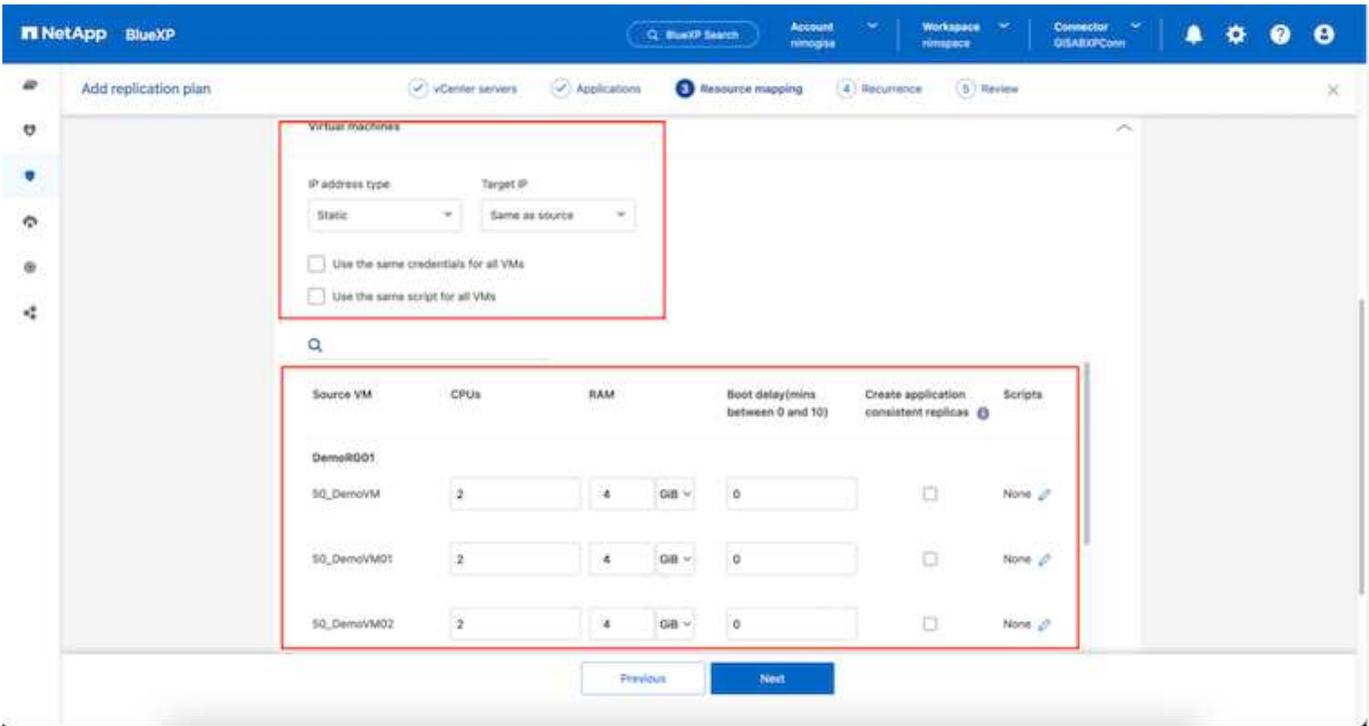


Jede virtuelle Maschine in einer Ressourcengruppe wird in der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

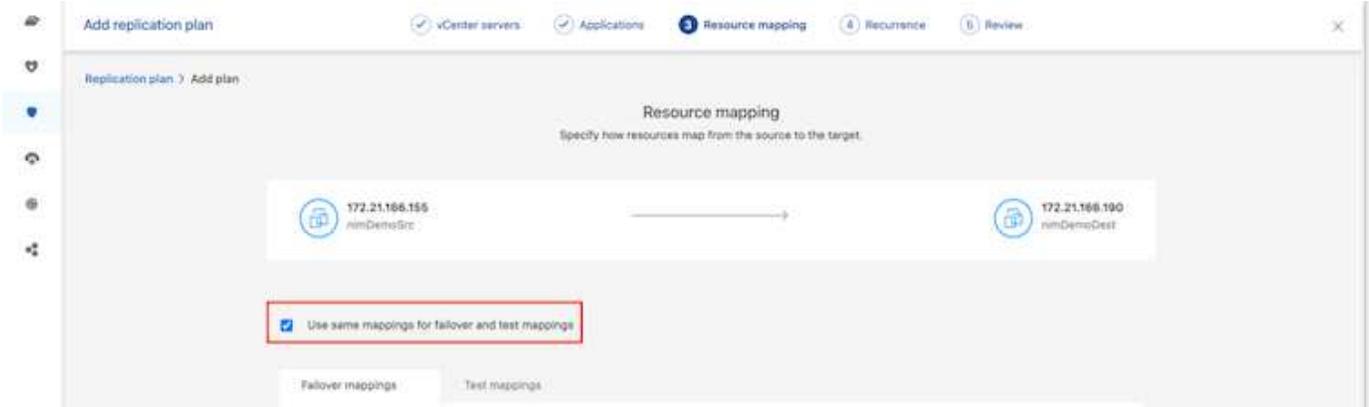
Der Screenshot unten zeigt die Option zum Filtern virtueller Maschinen oder spezieller Datastores nach Unternehmensanforderungen, wenn Ressourcengruppen nicht vorab erstellt werden.



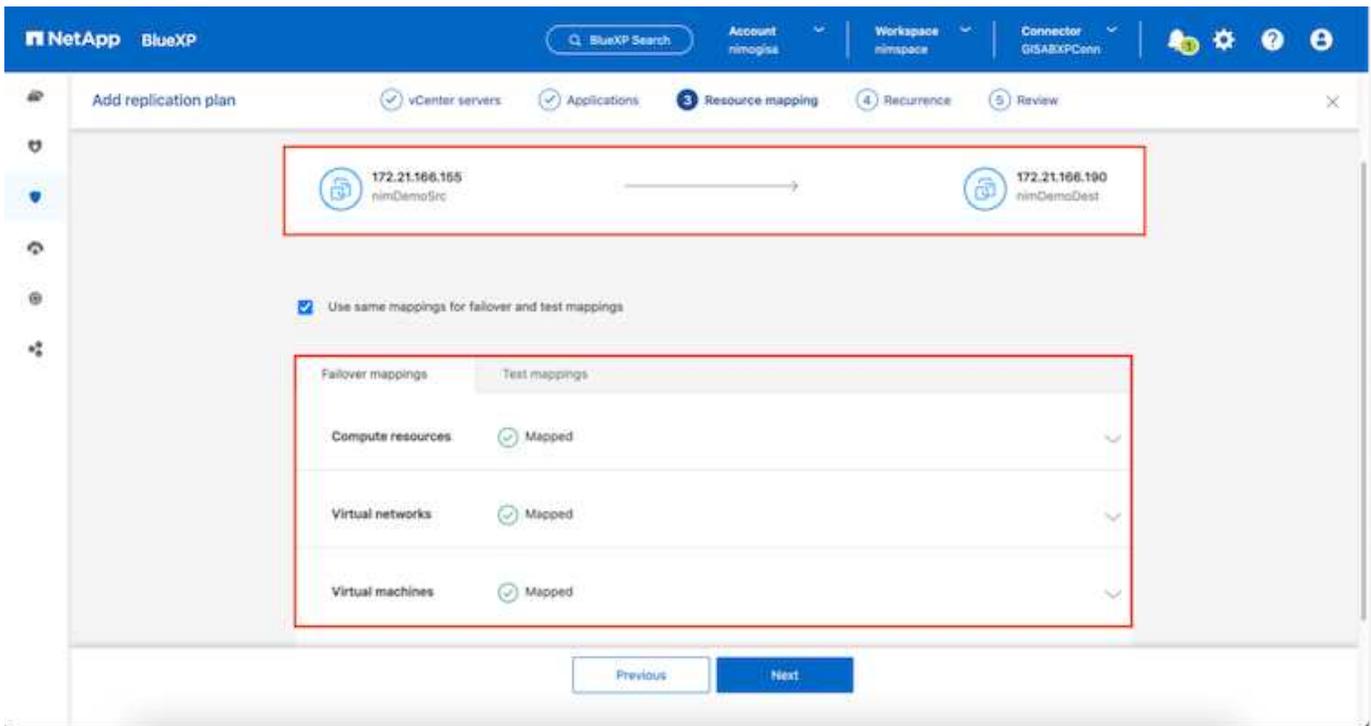
Sobald die Ressourcengruppen ausgewählt sind, erstellen Sie die Failover-Zuordnungen. Geben Sie in diesem Schritt an, wie die Ressourcen aus der Quellumgebung dem Ziel zugeordnet werden. Dazu gehören Rechenressourcen, virtuelle Netzwerke, IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Applikationskonsistenz usw. Weitere Informationen finden Sie unter ["Erstellen Sie einen Replizierungsplan"](#).



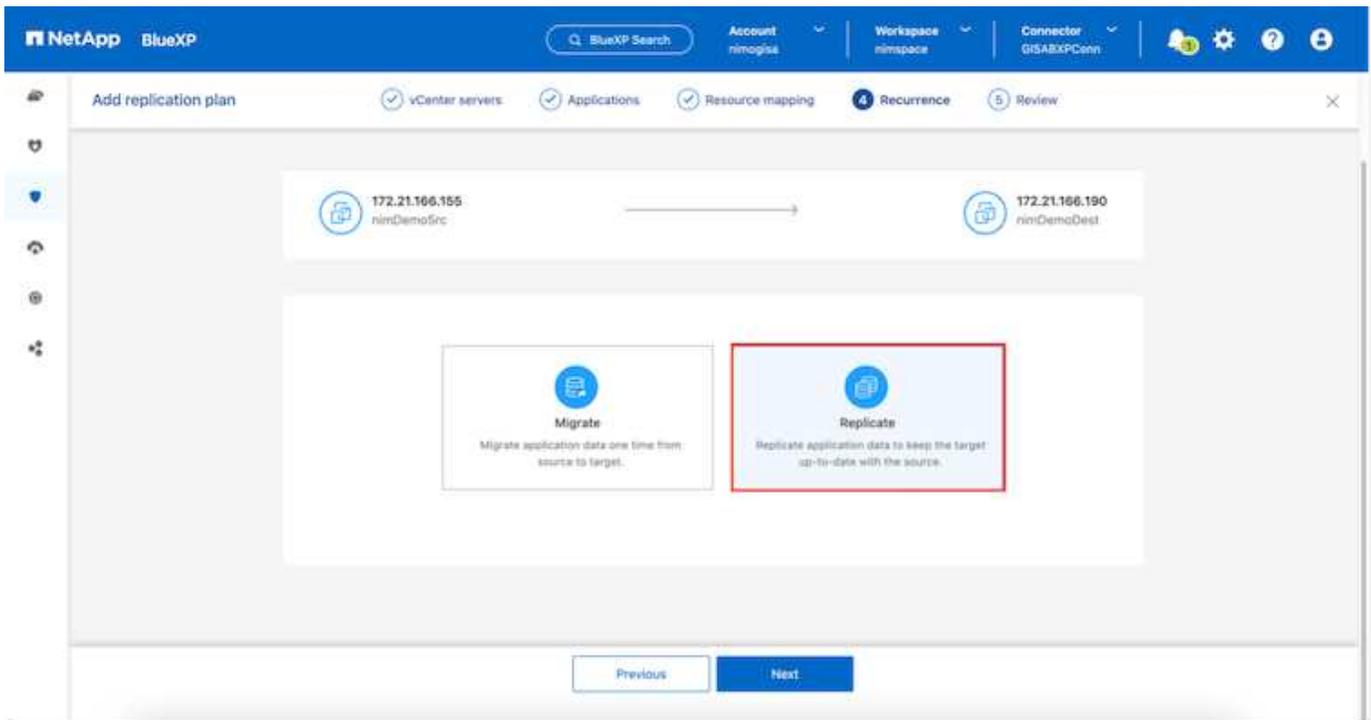
Standardmäßig werden für Test- und Failover-Vorgänge dieselben Zuordnungsparameter verwendet. Um unterschiedliche Zuordnungen für die Testumgebung anzuwenden, aktivieren Sie die Option Testzuordnung, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:



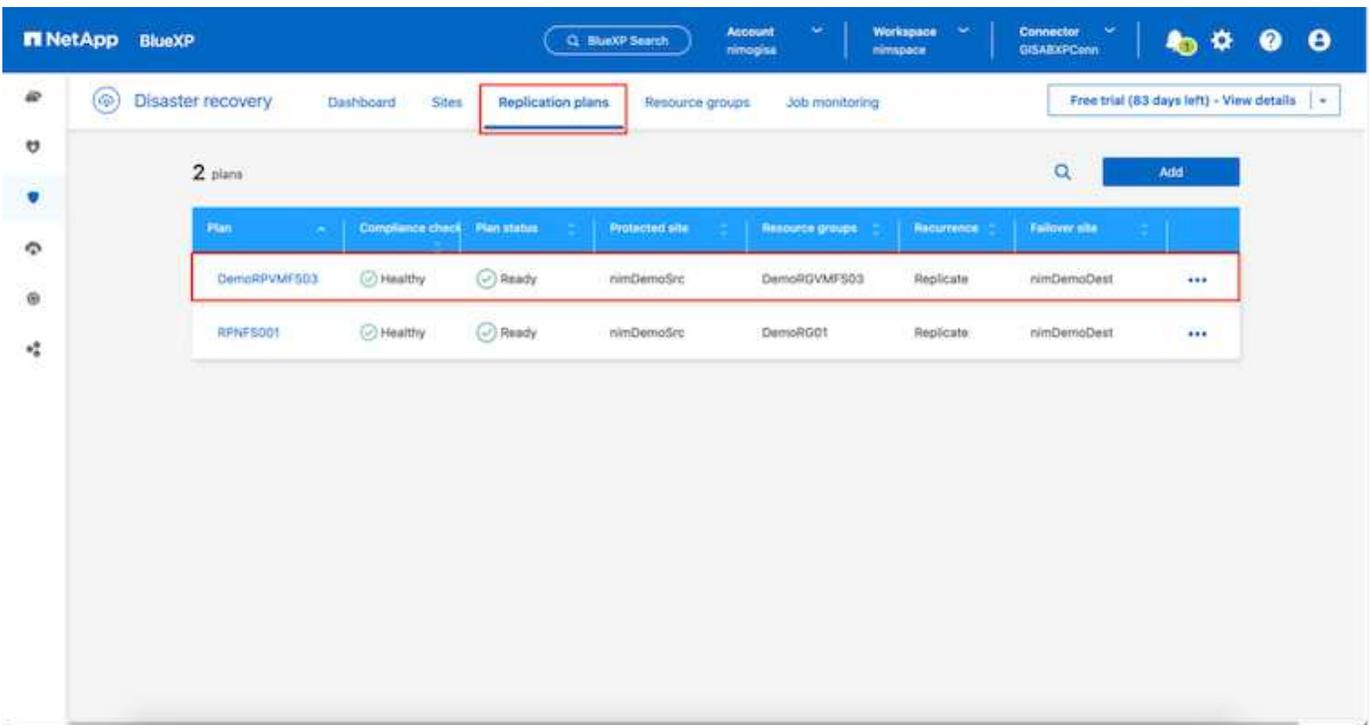
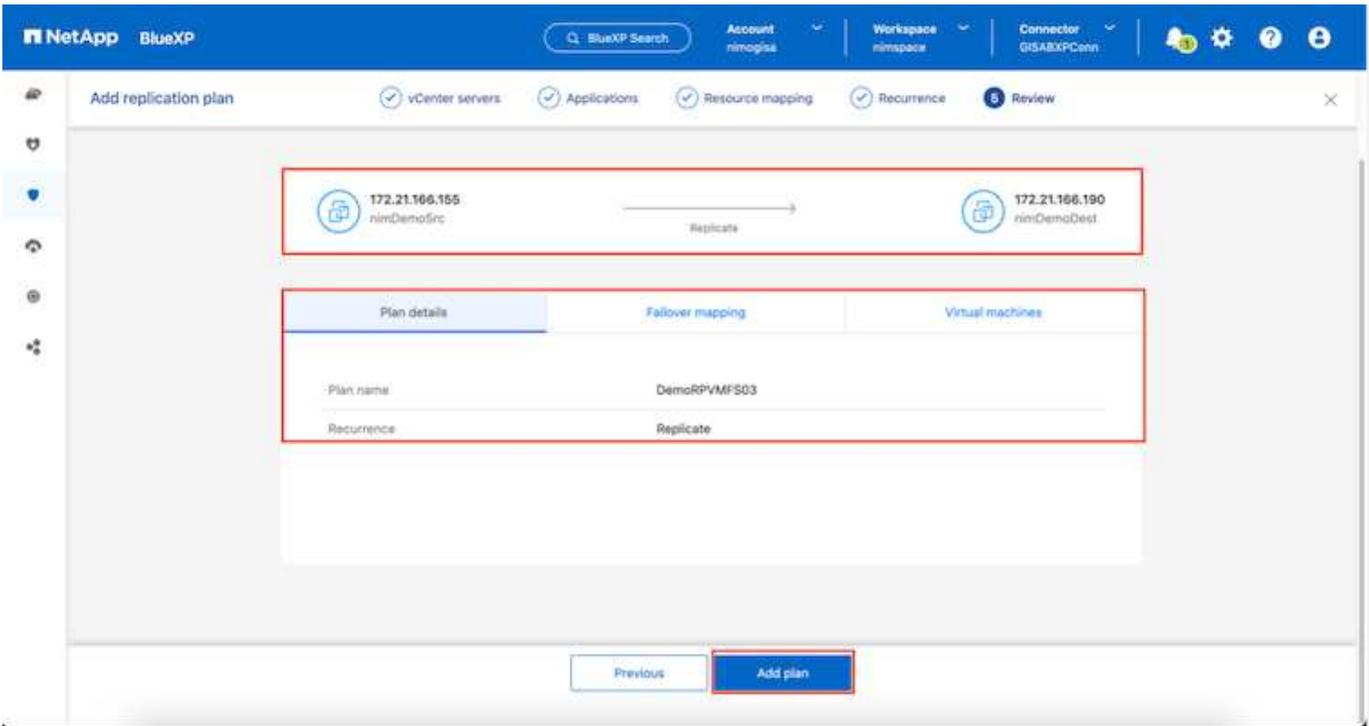
Klicken Sie nach Abschluss der Ressourcenzuordnung auf Weiter.



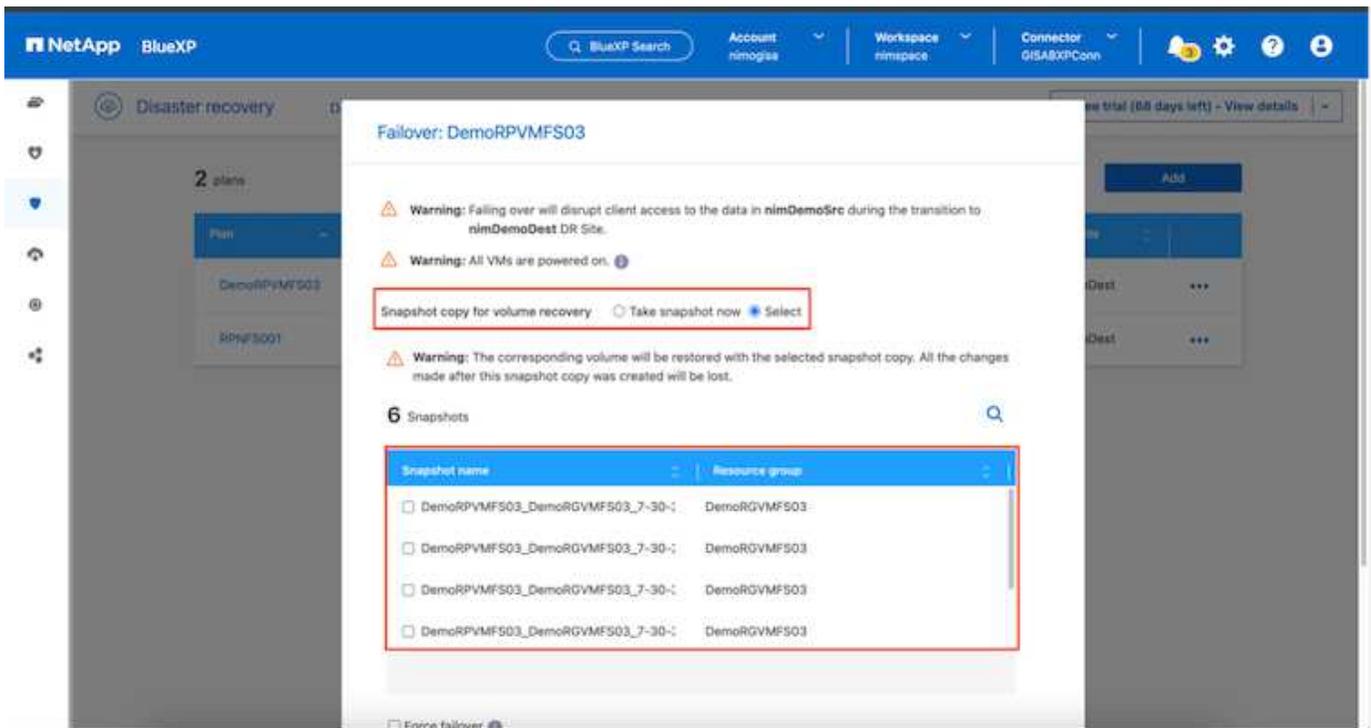
Wählen Sie den Wiederholungstyp aus. In einfachen Worten: Wählen Sie Migrate (einmalige Migration mit Failover) oder die Option wiederkehrende kontinuierliche Replikation aus. In dieser Übersicht ist die Option „Replikat“ ausgewählt.



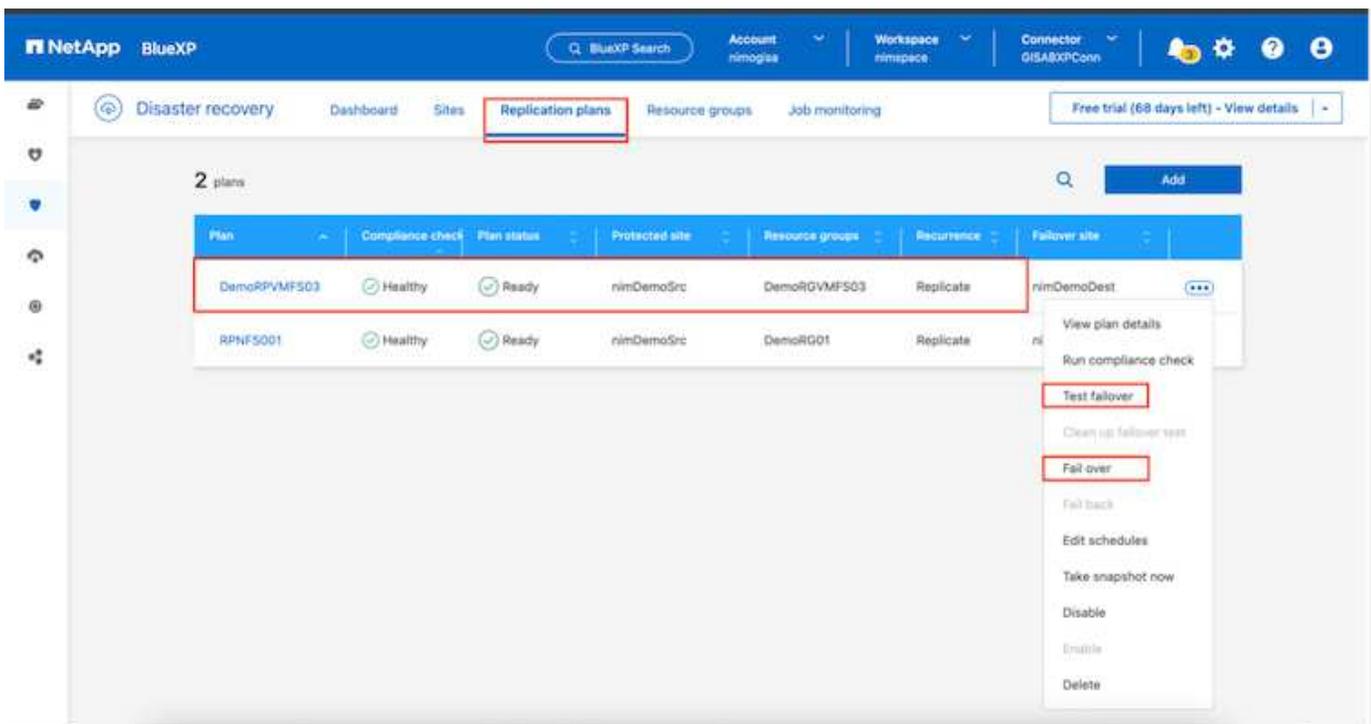
Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie auf Plan hinzufügen.



Sobald der Replizierungsplan erstellt wurde, kann ein Failover entsprechend den Anforderungen durchgeführt werden. Wählen Sie dazu die Failover-Option, die Test-Failover-Option oder die Option „Migrieren“. Die BlueXP Disaster Recovery gewährleistet, dass der Replizierungsprozess alle 30 Minuten planmäßig ausgeführt wird. Während der Optionen für Failover und Test-Failover können Sie die neueste SnapMirror SnapShot Kopie verwenden oder eine bestimmte SnapShot Kopie aus einer zeitpunktgenauen SnapShot Kopie auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann sehr hilfreich sein, wenn es ein Korruptionsereignis wie Ransomware gibt, wo die neuesten Replikate bereits kompromittiert oder verschlüsselt sind. BlueXP Disaster Recovery zeigt alle verfügbaren Recovery-Punkte an.



Um Failover oder Test Failover mit der im Replikationsplan angegebenen Konfiguration auszulösen, klicken Sie auf **Failover** oder **Test Failover**.



Was geschieht während eines Failover oder eines Test-Failovers?

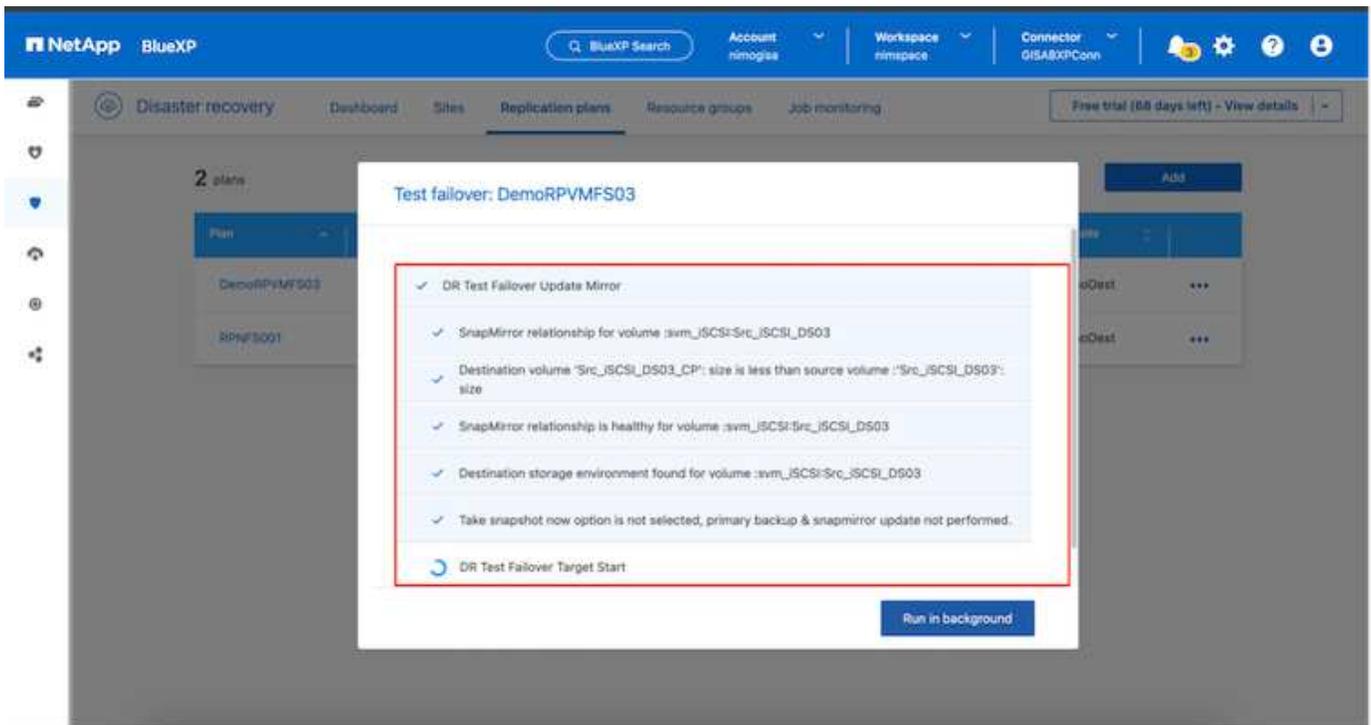
Während eines Test-Failover-Vorgangs erstellt die Disaster Recovery von BlueXP ein FlexClone Volume auf dem ONTAP Zielsystem. Dabei wird die neueste Snapshot Kopie oder ein ausgewählter Snapshot des Ziel-Volume verwendet.



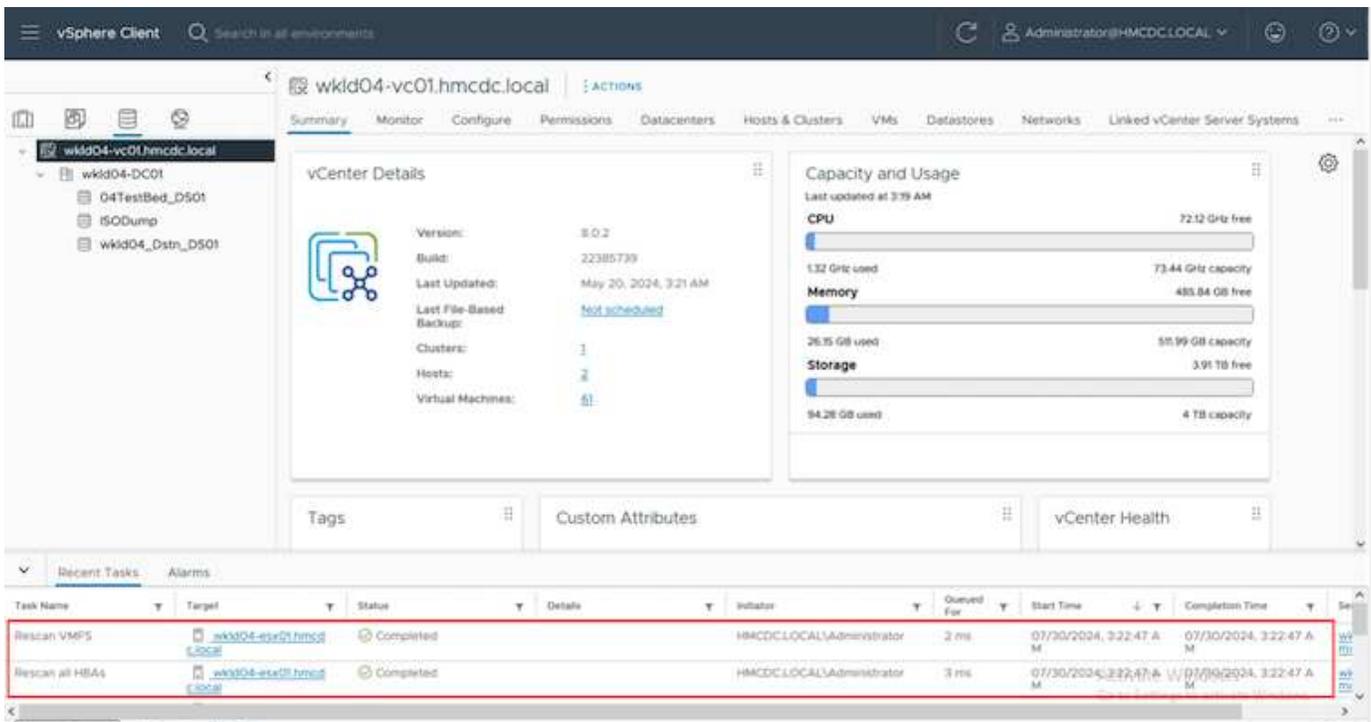
Ein Test-Failover-Vorgang erstellt ein geklontes Volume auf dem ONTAP Zielsystem.

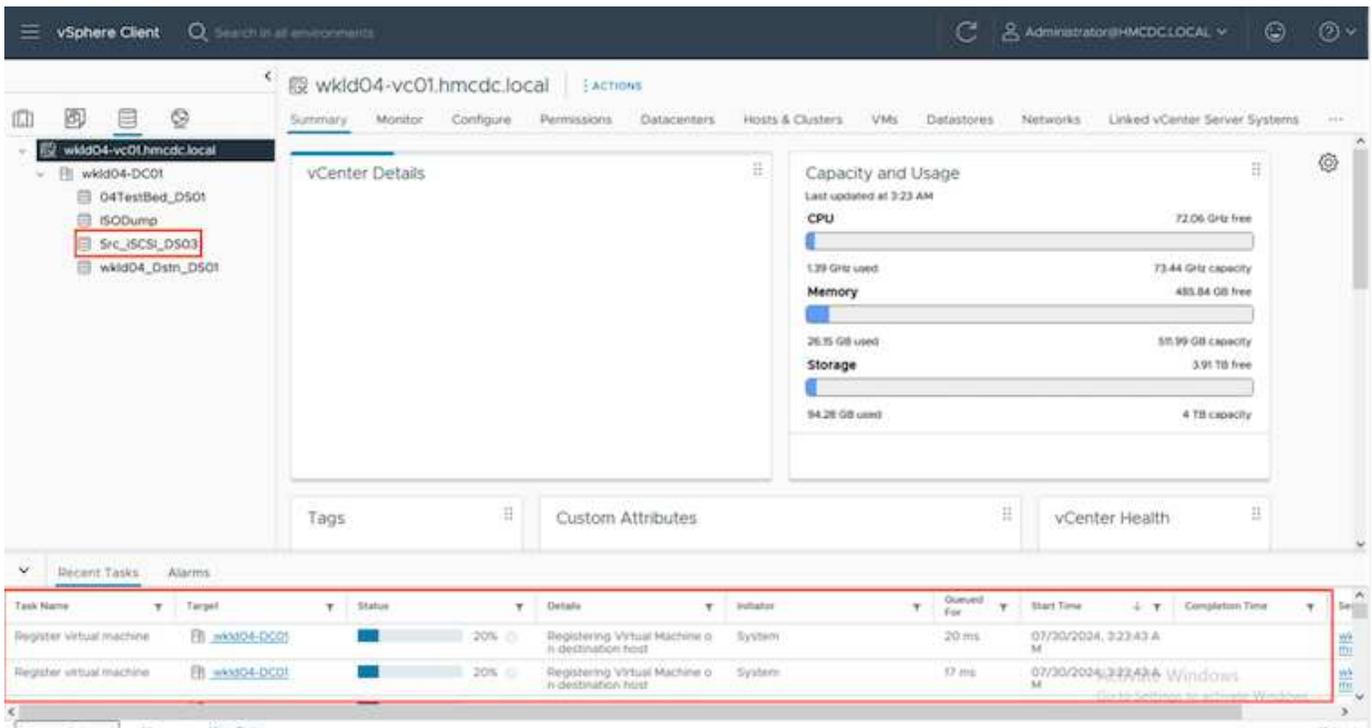


Das Ausführen einer Testwiederherstellung hat keine Auswirkungen auf die SnapMirror-Replikation.



Während des Prozesses ordnet die Disaster Recovery von BlueXP das ursprüngliche Ziel-Volume nicht zu. Stattdessen wird ein neues FlexClone-Volume aus dem ausgewählten Snapshot erstellt und ein temporärer Datastore, der das FlexClone-Volume sichert, den ESXi Hosts zugeordnet.

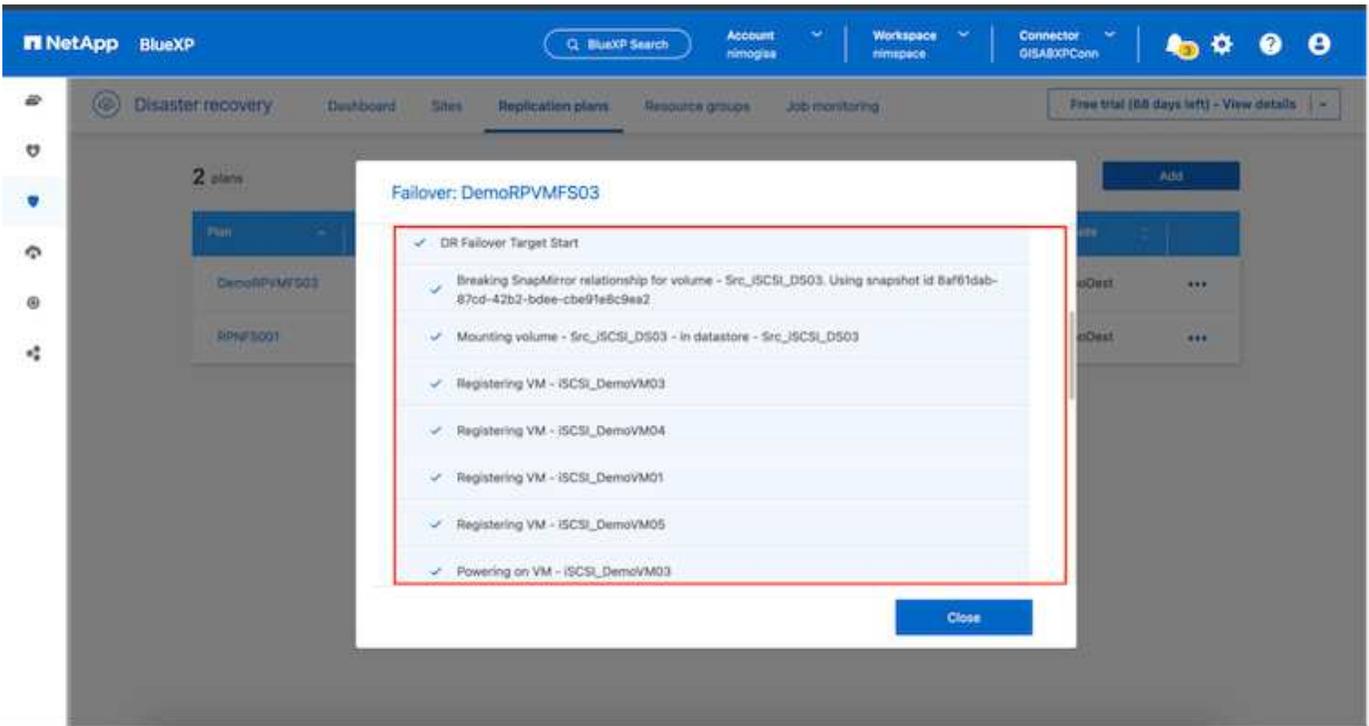




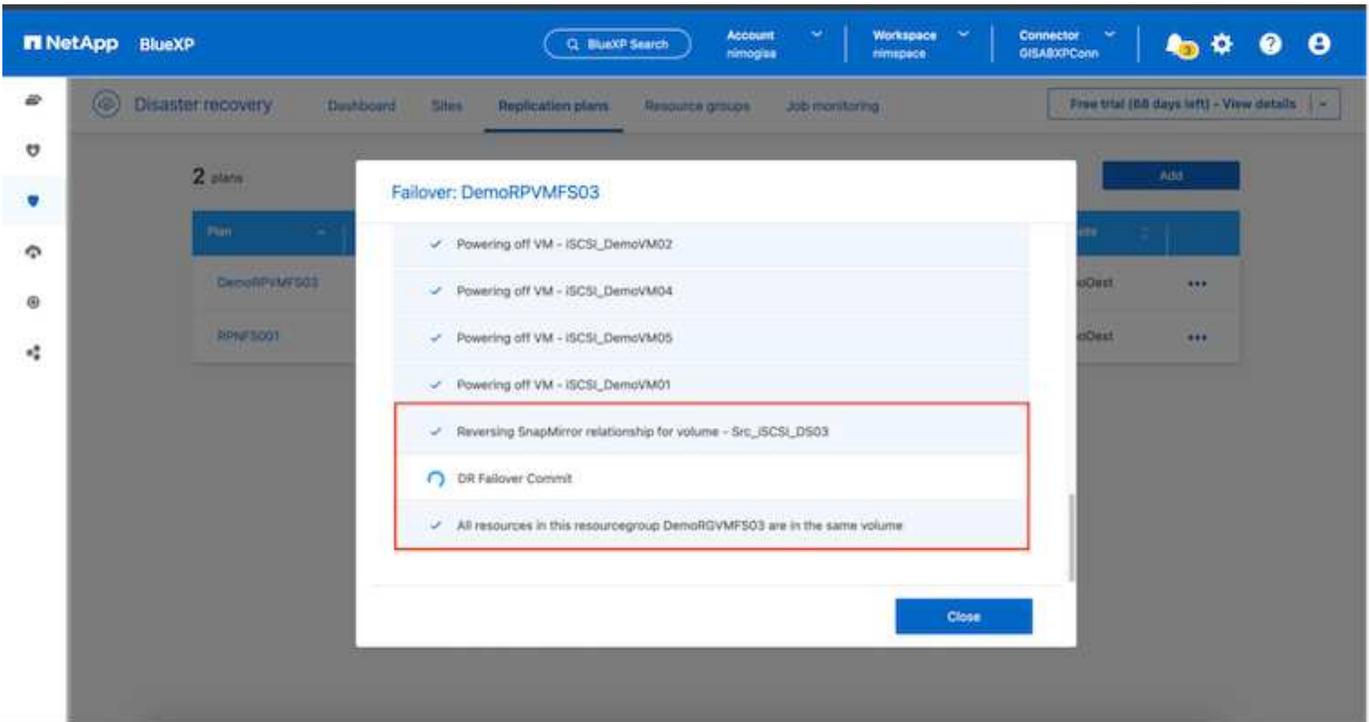
Nach Abschluss des Test-Failovers kann der Bereinigungsverfahren mit * „Clean up Failover Test“ ausgelöst werden. Während dieses Vorgangs zerstört die BlueXP Disaster Recovery das FlexClone Volume, das bei diesem Vorgang verwendet wurde.

Wenn ein echter Notfall eintritt, führt BlueXP Disaster Recovery folgende Schritte durch:

1. Bricht die SnapMirror-Beziehung zwischen den Standorten.
2. Bindet das VMFS-Datstore Volume nach der Neusignatur für die sofortige Verwendung ein.
3. Registrieren Sie die VMs
4. Schalten Sie die VMs ein



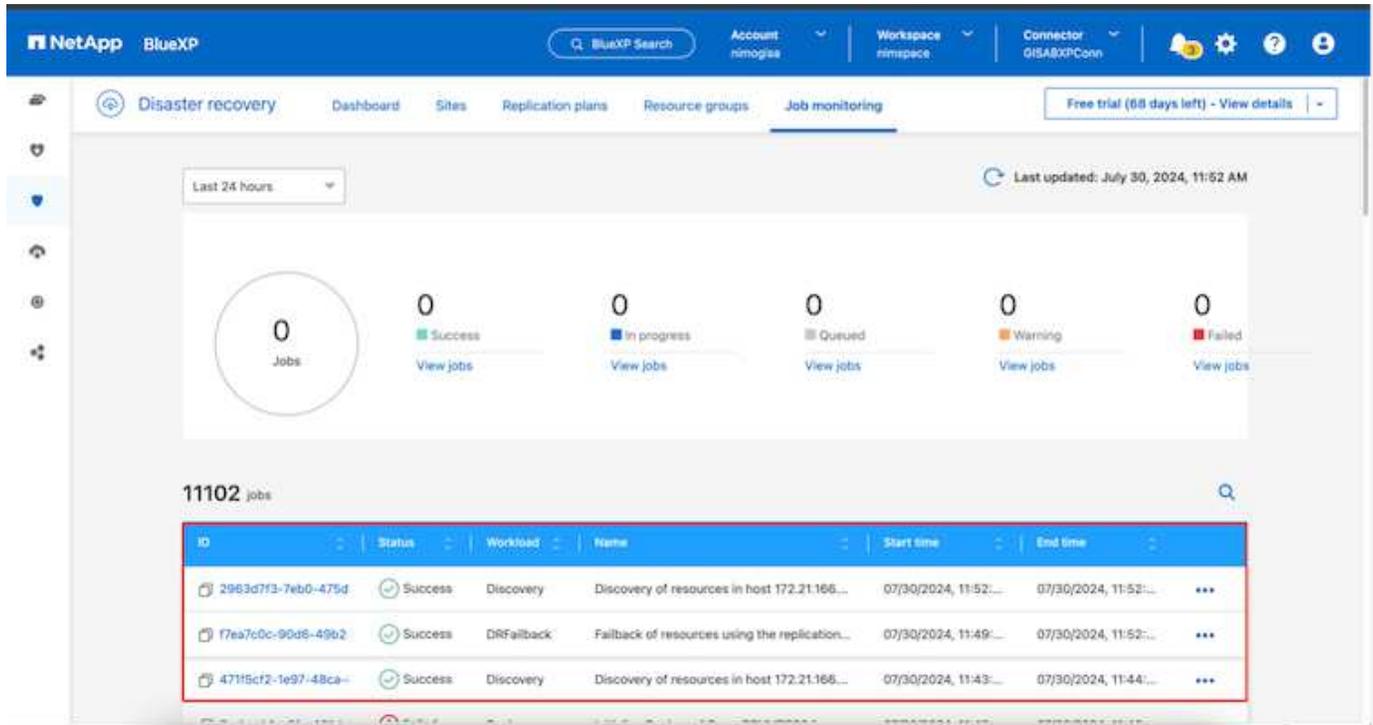
Sobald der primäre Standort in Betrieb ist, ermöglicht das BlueXP Disaster Recovery die umgekehrte Resynchronisierung für SnapMirror und ermöglicht Failback, das auch hier mit nur einem Mausklick durchgeführt werden kann.



Wenn die Option „Migration“ gewählt wird, wird dies als geplantes Failover-Ereignis angesehen. In diesem Fall wird ein zusätzlicher Schritt ausgelöst, der das Herunterfahren der virtuellen Maschinen am Quellstandort umfasst. Die restlichen Schritte bleiben dem Failover-Ereignis gleich.

Über BlueXP oder die ONTAP-CLI können Sie den Replikationsstatus für die entsprechenden Datenspeicher-Volumes überwachen und den Status eines Failover oder Test-Failovers über die Jobüberwachung

nachverfolgen.



Auf diese Weise erhalten Sie eine leistungsstarke Lösung, die einen individuellen Disaster-Recovery-Plan umsetzt. Failover lässt sich als geplanter Failover oder Failover mit einem Mausklick durchführen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung des DR-Standorts getroffen wird.

Um mehr über diesen Prozess zu erfahren, folgen Sie dem ausführlichen Walkthrough-Video oder verwenden Sie die "[Lösungssimulator](#)".

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtlich geschützten Urhebers 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.