



# **Notfallwiederherstellung mit BlueXP DRaaS**

NetApp public and hybrid cloud solutions

NetApp

February 04, 2026

# Inhalt

Notfallwiederherstellung mit BlueXP DRaaS .....	1
Überblick .....	1
DR mit BlueXP DRaaS für NFS-Datenspeicher .....	1
Erste Schritte .....	3
BlueXP disaster recovery .....	4
Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array .....	6
So richten Sie es für VMware Disaster Recovery ein .....	6
Was kann BlueXP disaster recovery für Sie tun? .....	8
Testen des Failovers .....	16
Bereinigungs-Failover-Testvorgang .....	18
Geplante Migration und Failover .....	19
Failback .....	21
Überwachung und Dashboard .....	22
DR mit BlueXP DRaaS für VMFS-Datenspeicher .....	23
Erste Schritte .....	24
BlueXP disaster recovery .....	26
Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort .....	28
So richten Sie es für VMware Disaster Recovery ein .....	28
Was kann BlueXP disaster recovery für Sie tun? .....	30
Was passiert während eines Failovers oder Test-Failover-Vorgangs? .....	38

# Notfallwiederherstellung mit BlueXP DRaaS

## Überblick

Die Notfallwiederherstellung hat für jeden VMware-Administrator oberste Priorität. Da VMware ganze Server in einer Reihe von Dateien kapselt, aus denen die virtuelle Maschine besteht, nutzen Administratoren blockspeicherbasierte Techniken wie Klone, Snapshots und Replikate, um diese VMs zu schützen. ONTAP -Arrays bieten integrierte Replikation zum Übertragen von Volume-Daten und damit der virtuellen Maschinen, die sich auf den angegebenen Datastore-LUNs befinden, von einem Standort zum anderen. BlueXP DRaaS lässt sich in vSphere integrieren und automatisiert den gesamten Workflow für nahtloses Failover und Failback im Katastrophenfall. Durch die Kombination von Speicherreplikation mit intelligenter Automatisierung verfügen Administratoren jetzt über eine handhabbare Möglichkeit, Notfallwiederherstellungspläne nicht nur zu konfigurieren, zu automatisieren und zu testen, sondern sie im Katastrophenfall auch problemlos auszuführen.

Der zeitaufwändigste Teil eines DR-Failovers in einer VMware vSphere-Umgebung ist die Ausführung der Schritte, die zum Inventarisieren, Registrieren, Neukonfigurieren und Einschalten der VMs am DR-Standort erforderlich sind. Eine ideale Lösung hat sowohl einen niedrigen RPO (gemessen in Minuten) als auch einen niedrigen RTO (gemessen in Minuten bis Stunden). Ein Faktor, der bei einer DR-Lösung oft übersehen wird, ist die Möglichkeit, die DR-Lösung in regelmäßigen Abständen effizient zu testen.

Berücksichtigen Sie beim Entwerfen einer DR-Lösung die folgenden Faktoren:

- Das Wiederherstellungszeitziel (RTO). Die RTO gibt an, wie schnell sich ein Unternehmen von einem Desaster erholen kann, oder genauer gesagt, wie lange es dauert, den Wiederherstellungsprozess auszuführen, um die Geschäftsdienste wieder verfügbar zu machen.
- Das Wiederherstellungspunktziel (RPO). Das RPO gibt an, wie alt die wiederhergestellten Daten nach ihrer Bereitstellung im Verhältnis zum Zeitpunkt des Katastrophenfalls sind.
- Skalierbarkeit und Anpassungsfähigkeit. Zu diesem Faktor gehört die Möglichkeit, die Speicherressourcen bei steigender Nachfrage schrittweise zu erweitern.

Weitere technische Informationen zu den verfügbaren Lösungen finden Sie unter:

- ["DR mit BlueXP DRaaS für NFS-Datenspeicher"](#)
- ["DR mit BlueXP DRaaS für VMFS-Datenspeicher"](#)

## DR mit BlueXP DRaaS für NFS-Datenspeicher

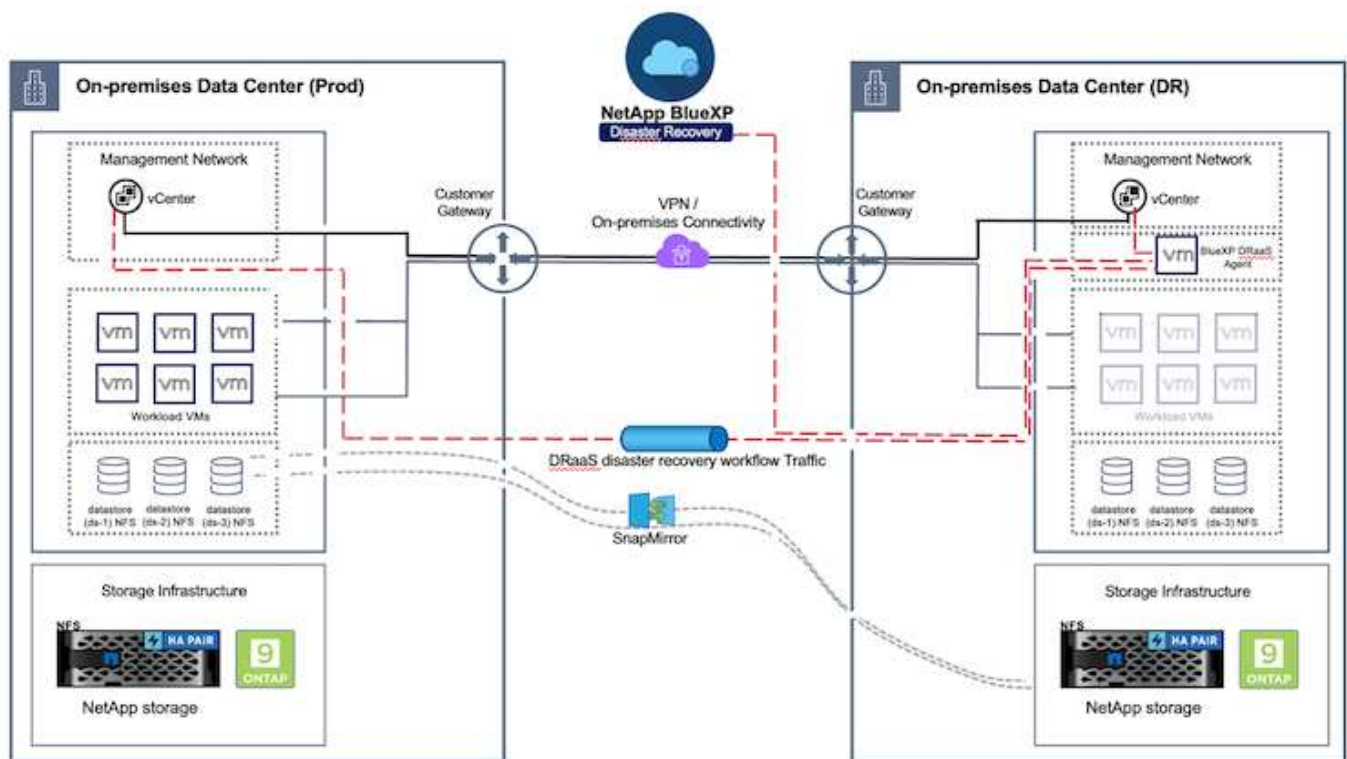
Die Implementierung einer Notfallwiederherstellung durch Blockreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Methode zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen, wie beispielsweise Ransomware-Angriffen. Mithilfe der NetApp SnapMirror Replikation können VMware-Workloads, die auf lokalen ONTAP -Systemen mit NFS-Datenspeicher ausgeführt werden, auf ein anderes ONTAP Speichersystem repliziert werden, das sich in einem dafür vorgesehenen Wiederherstellungs-

Rechenzentrum befindet, in dem auch VMware bereitgestellt wird.

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zum Einrichten der Notfallwiederherstellung für lokale VMware-VMs an einem anderen bestimmten Standort beschrieben. Als Teil dieser Einrichtung werden das BlueXP -Konto, der BlueXP Connector und die ONTAP Arrays im BlueXP Arbeitsbereich hinzugefügt, die für die Kommunikation von VMware vCenter mit dem ONTAP Speicher erforderlich sind. Darüber hinaus wird in diesem Dokument detailliert beschrieben, wie die Replikation zwischen Standorten konfiguriert wird und wie ein Wiederherstellungsplan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Site-Failovers und zum Failback, wenn die primäre Site wiederhergestellt und online gestellt wurde.

Mithilfe des in die NetApp BlueXP Konsole integrierten BlueXP disaster recovery -Dienstes können Unternehmen ihre lokalen VMware vCenter- und ONTAP -Speicher problemlos ermitteln. Organisationen können dann Ressourcengruppierungen erstellen, einen Notfallwiederherstellungsplan erstellen, ihn mit Ressourcengruppen verknüpfen und Failover und Failback testen oder ausführen. SnapMirror bietet Blockreplikation auf Speicherebene, um die beiden Sites mit inkrementellen Änderungen auf dem neuesten Stand zu halten, was zu einem Recovery Point Objective (RPO) von bis zu 5 Minuten führt. Darüber hinaus ist es möglich, Disaster-Recovery-Verfahren zu simulieren, ohne die Produktion zu beeinträchtigen oder zusätzliche Speicherkosten zu verursachen.

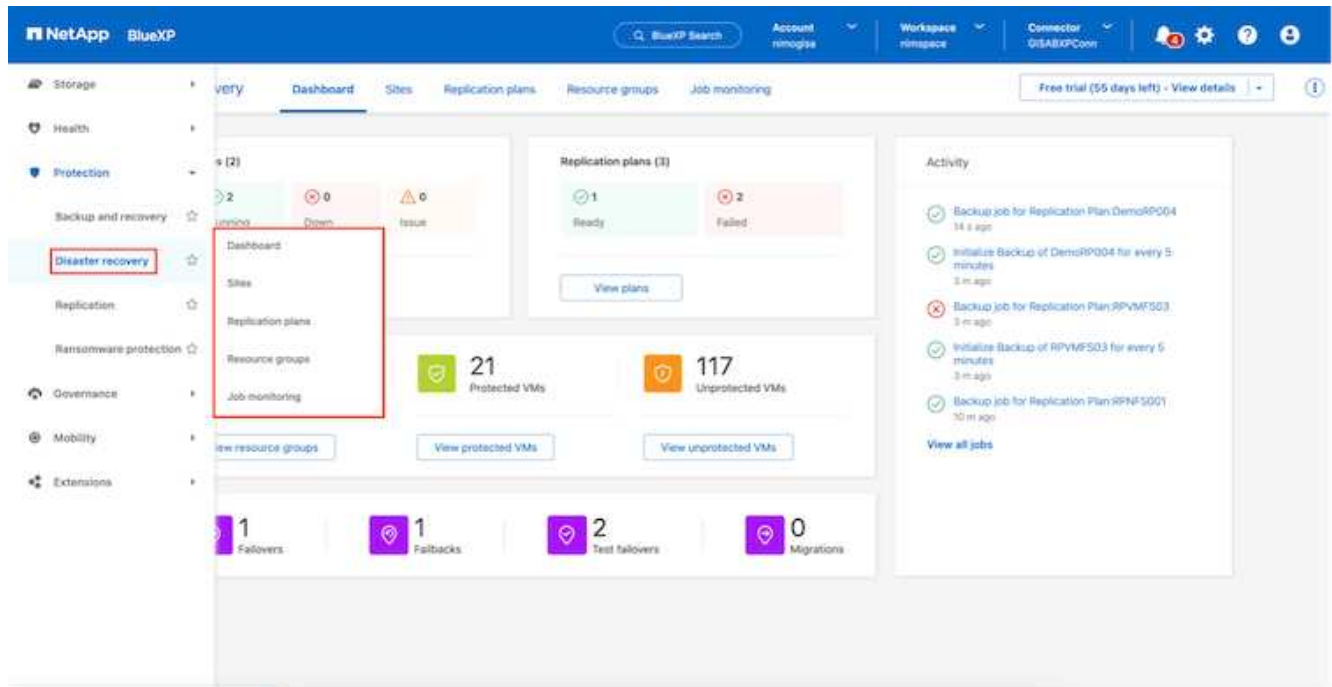
BlueXP disaster recovery nutzt die FlexClone -Technologie von ONTAP, um eine platzsparende Kopie des NFS-Datenspeichers vom letzten replizierten Snapshot auf der Disaster Recovery-Site zu erstellen. Nach Abschluss des Disaster-Recovery-Tests können Kunden die Testumgebung problemlos löschen, ohne die tatsächlich replizierten Produktionsressourcen zu beeinträchtigen. Im Falle eines tatsächlichen Failovers orchestriert der BlueXP disaster recovery -Dienst alle notwendigen Schritte, um die geschützten virtuellen Maschinen mit nur wenigen Klicks automatisch am vorgesehenen Disaster-Recovery-Standort hochzufahren. Der Dienst kehrt außerdem die SnapMirror -Beziehung zum primären Standort um und repliziert bei Bedarf alle Änderungen vom sekundären zum primären Standort für einen Failback-Vorgang. Alle diese Funktionen sind im Vergleich zu anderen bekannten Alternativen zu einem Bruchteil der Kosten erhältlich.



## Erste Schritte

Um mit der BlueXP disaster recovery zu beginnen, verwenden Sie die BlueXP -Konsole und greifen Sie dann auf den Dienst zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste von BlueXP „Schutz“ > „Notfallwiederherstellung“ aus.
3. Das BlueXP disaster recovery wird angezeigt.



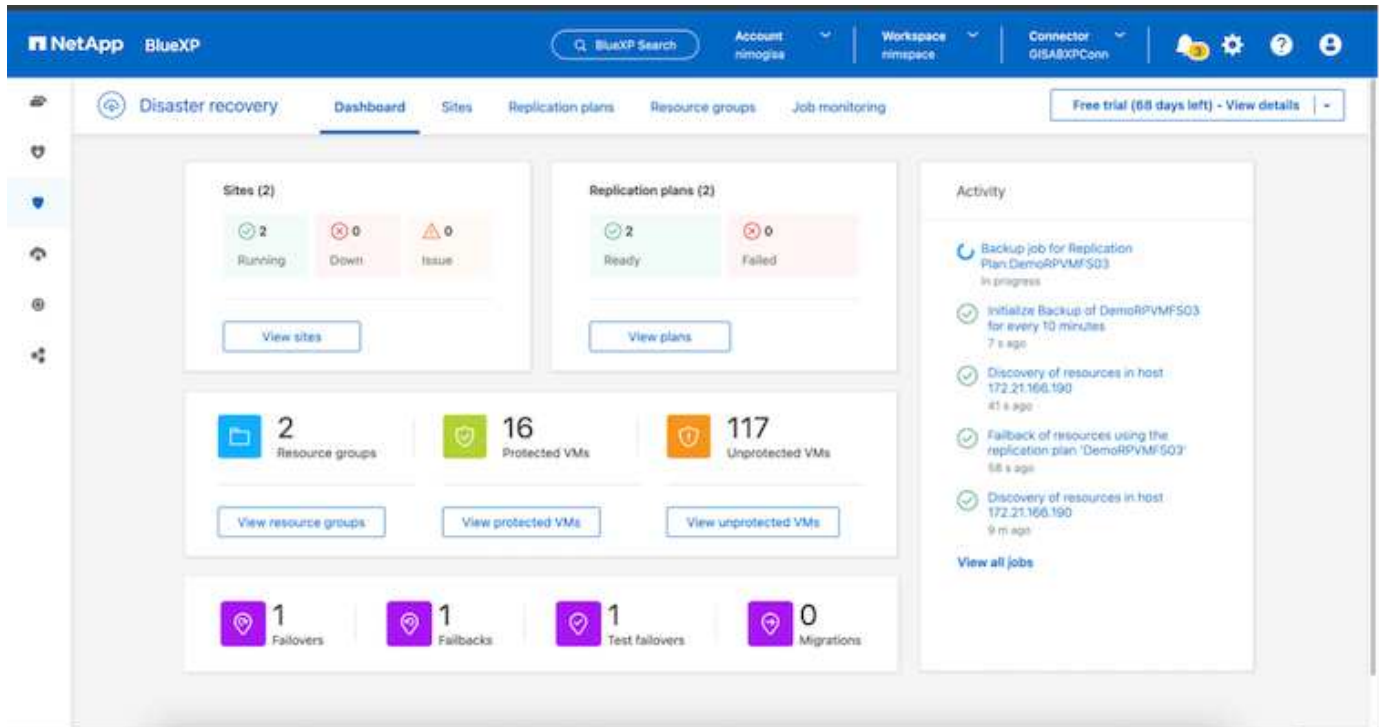
Stellen Sie vor der Konfiguration des Notfallwiederherstellungsplans sicher, dass die folgenden Voraussetzungen erfüllt sind:

- BlueXP Connector wird in NetApp BlueXP eingerichtet.
- Die BlueXP Connector-Instanz verfügt über eine Verbindung zum Quell- und Ziel-vCenter und den Speichersystemen.
- NetApp Data ONTAP Cluster zur Bereitstellung von NFS-Datenspeichern.
- In BlueXP werden lokale NetApp -Speichersysteme hinzugefügt, die NFS-Datenspeicher für VMware hosten.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen NFS-basierten Datenspeichervolumen konfiguriert.
- Stellen Sie sicher, dass die Umgebung über unterstützte Versionen von vCenter Server und ESXi-Servern verfügt.

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



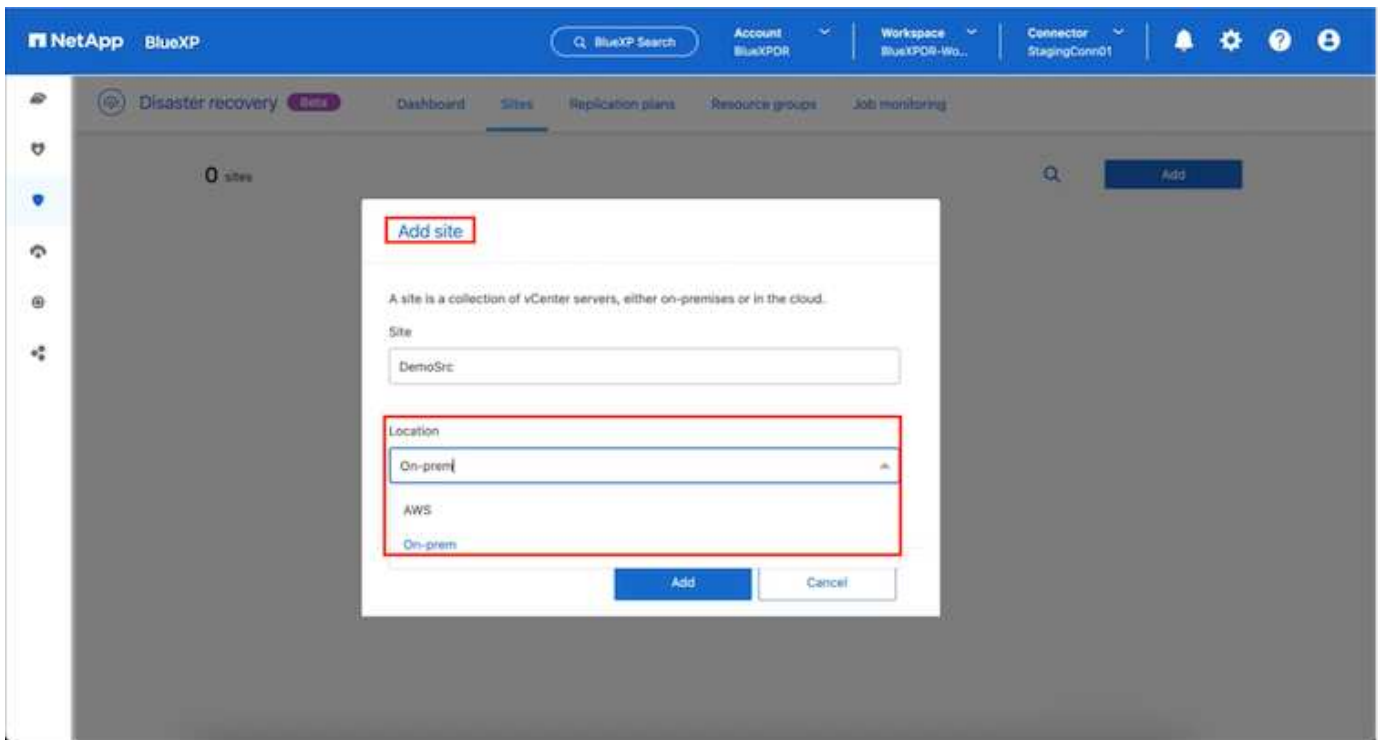
NetApp empfiehlt, den BlueXP Connector am Zielstandort oder an einem dritten Standort bereitzustellen, damit der BlueXP Connector über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.



## BlueXP disaster recovery

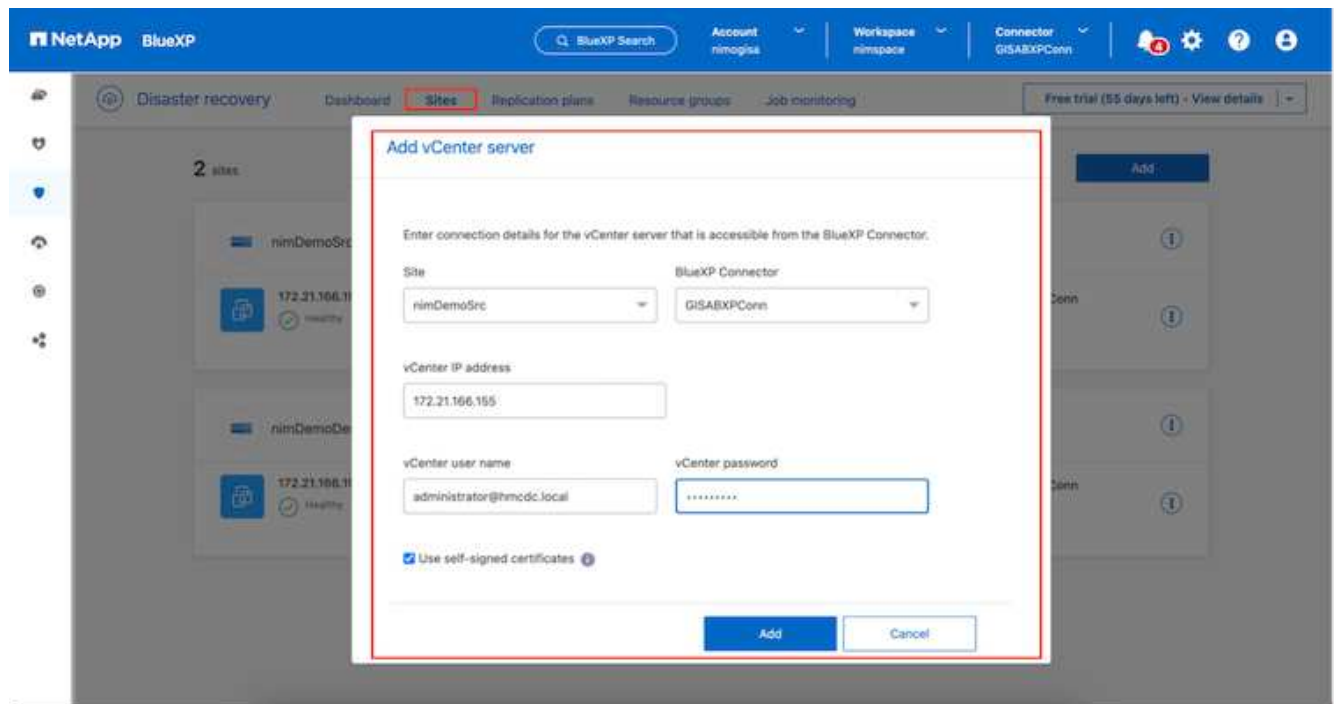
Der erste Schritt bei der Vorbereitung der Notfallwiederherstellung besteht darin, die lokalen vCenter- und Speicherressourcen zu ermitteln und zur BlueXP disaster recovery hinzuzufügen.

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



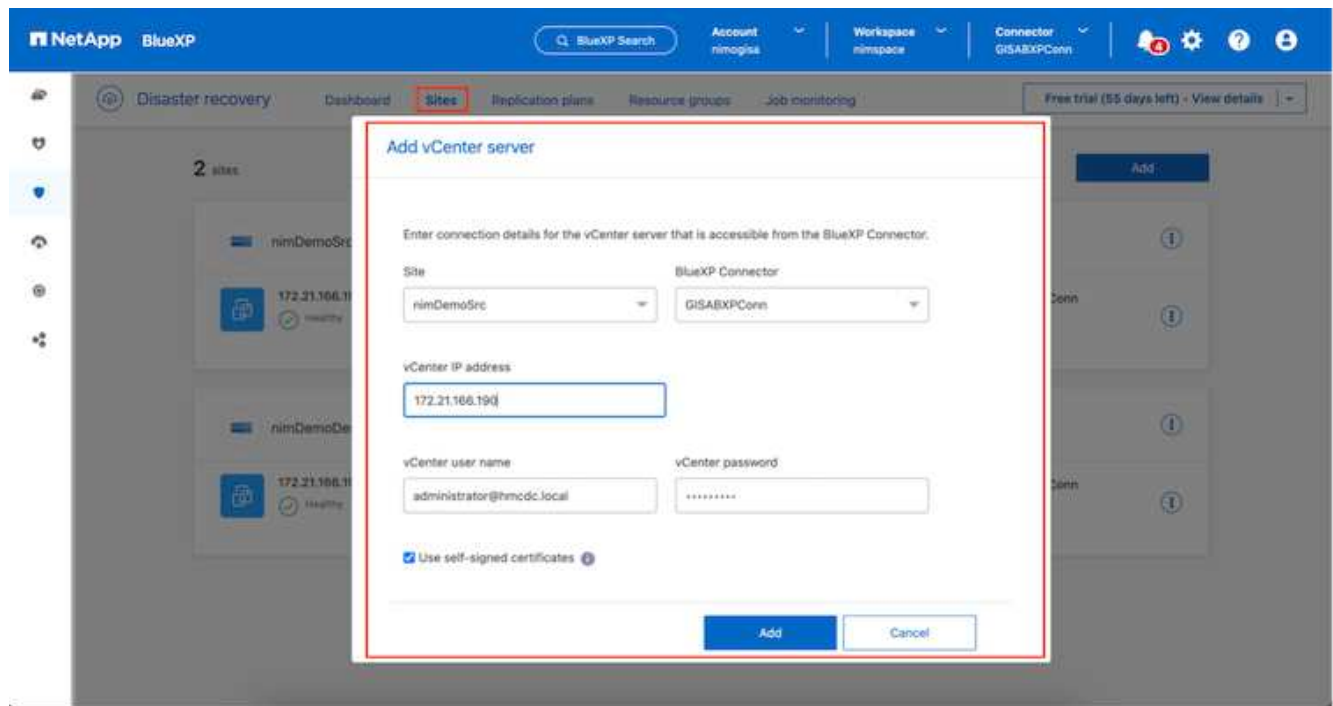
Fügen Sie die folgenden Plattformen hinzu:

- **Quelle.** Lokales vCenter.



- **Ziel.** VMC SDDC vCenter.





Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

## Konfigurieren der Speicherreplikation zwischen Quellstandort-Array und Zielstandort-Array

SnapMirror bietet Datenreplikation in einer NetApp Umgebung. Die SnapMirror -Replikation basiert auf der 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 mithilfe des NetApp OnCommand System Manager oder der ONTAP CLI konfigurieren. BlueXP DRaaS erstellt auch die SnapMirror -Beziehung, sofern Cluster- und SVM-Peering zuvor konfiguriert wurden.

In Fällen, in denen der primäre Speicher nicht vollständig verloren geht, bietet SnapMirror eine effiziente Möglichkeit zur Neusynchronisierung der primären und DR-Sites. SnapMirror kann die beiden Sites neu synchronisieren und nur geänderte oder neue Daten von der DR-Site zurück zur primären Site übertragen, indem einfach die SnapMirror Beziehungen umgekehrt werden. Dies bedeutet, dass Replikationspläne in BlueXP DRaaS nach einem Failover in beide Richtungen neu synchronisiert werden können, ohne das gesamte Volume erneut zu kopieren. Wenn eine Beziehung in umgekehrter Richtung erneut synchronisiert wird, werden nur neue Daten an das Ziel zurückgesendet, die seit der letzten erfolgreichen Synchronisierung der Snapshot-Kopie geschrieben wurden.

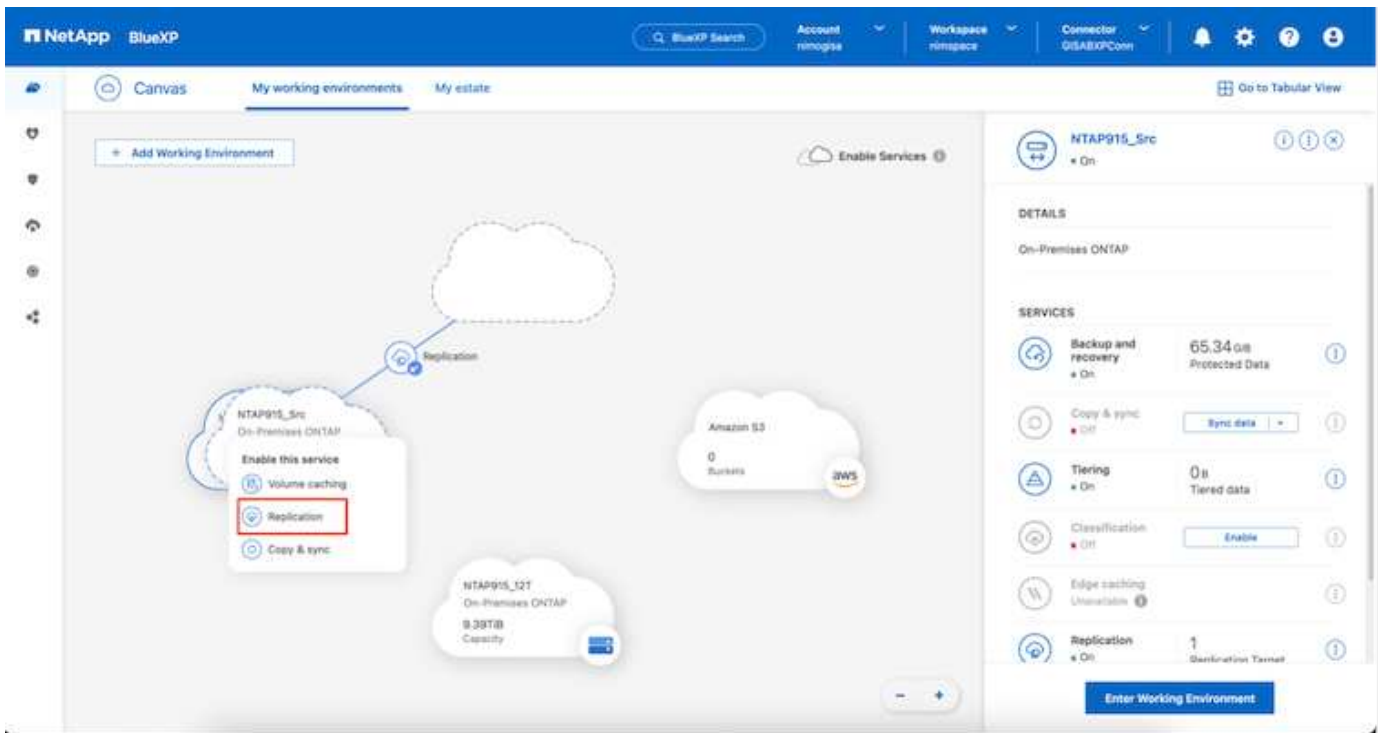


Wenn die SnapMirror -Beziehung für das Volume bereits über CLI oder System Manager konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.

## So richten Sie es für VMware Disaster Recovery ein

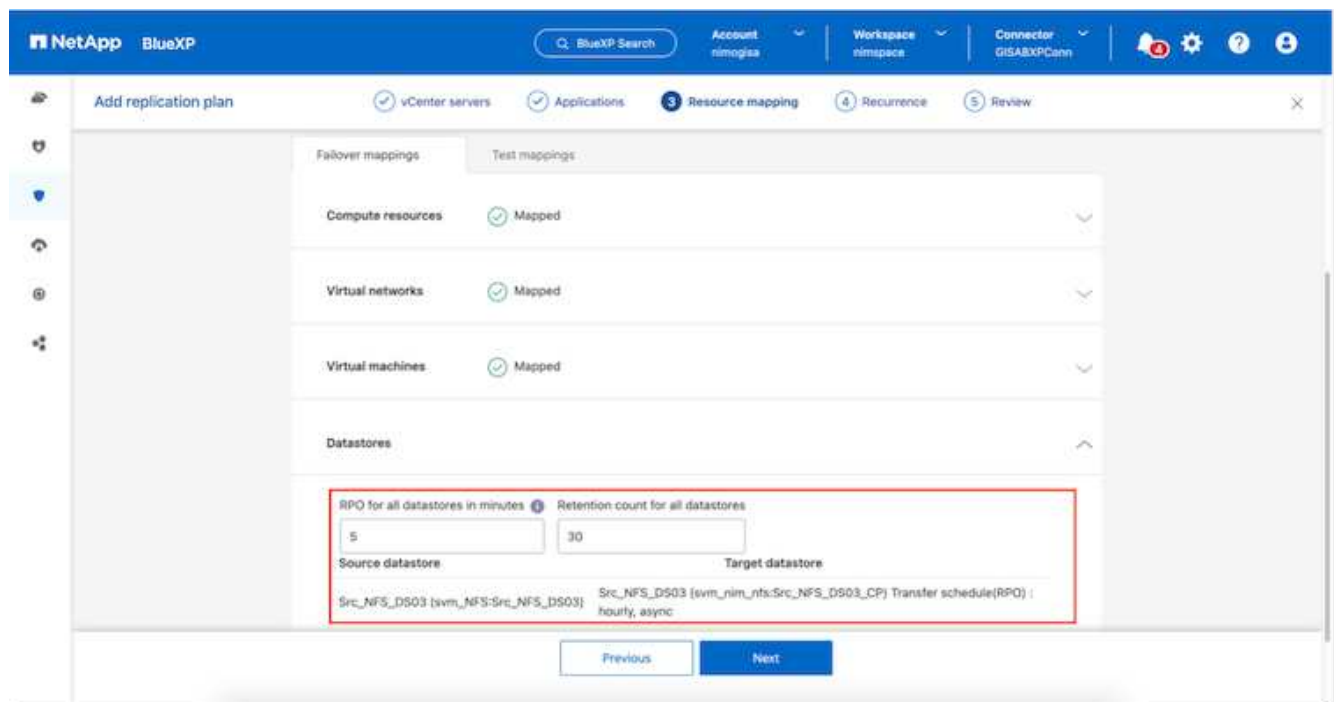
Der Vorgang zum Erstellen der SnapMirror Replikation bleibt für jede Anwendung derselbe. Der Vorgang kann manuell oder automatisiert erfolgen. Am einfachsten ist es, BlueXP zu nutzen, um die SnapMirror -Replikation zu konfigurieren. Dazu ziehen Sie das Quell ONTAP -System in der Umgebung einfach per Drag & Drop auf das Ziel, um den Assistenten zu starten, der Sie durch den Rest des Prozesses führt.





BlueXP DRaaS kann dies auch automatisieren, sofern die folgenden beiden Kriterien erfüllt sind:

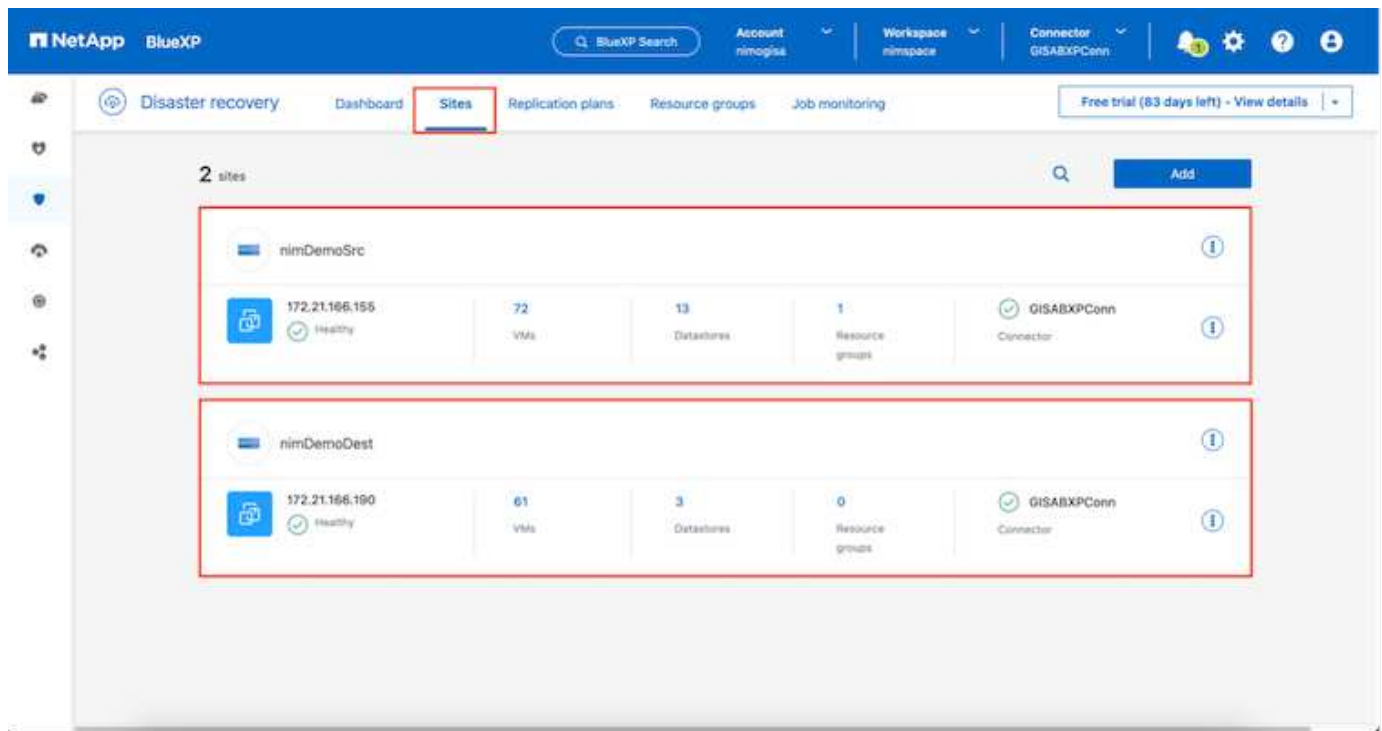
- Quell- und Zielcluster haben eine Peer-Beziehung.
- Quell-SVM und Ziel-SVM haben eine Peer-Beziehung.



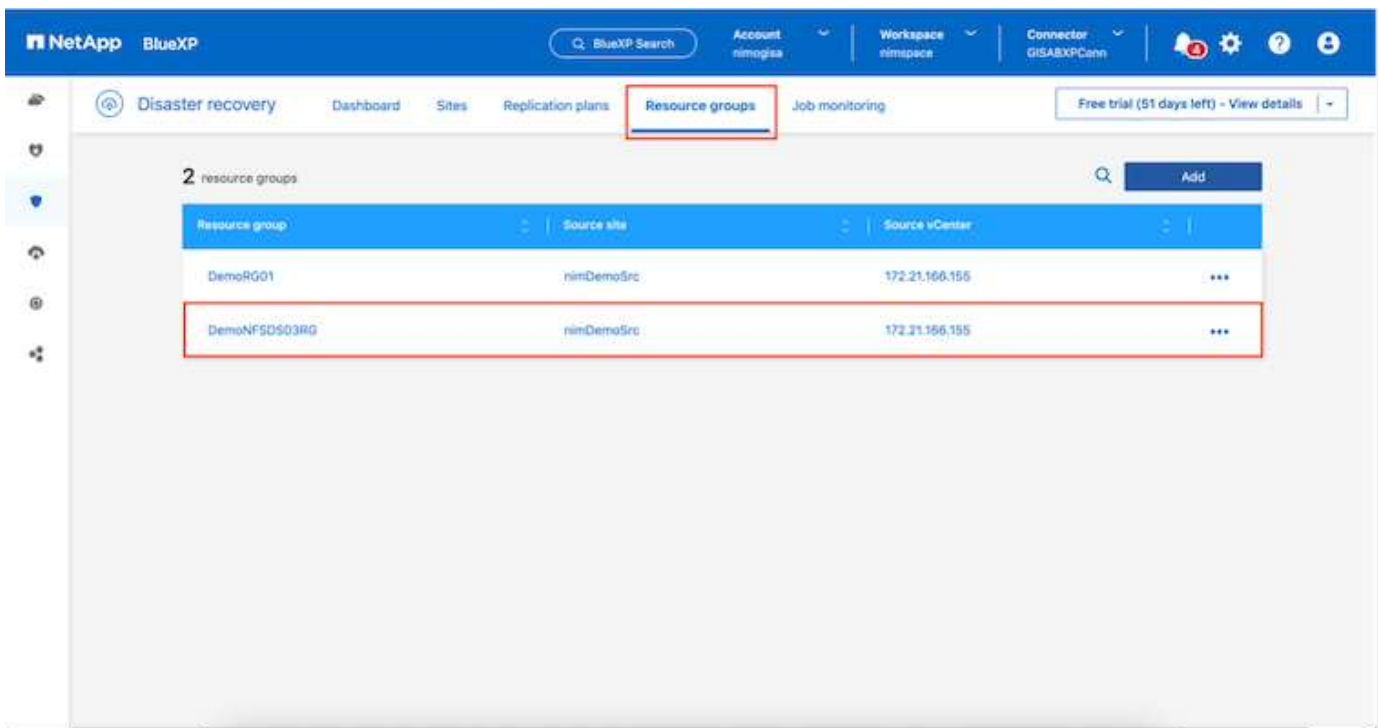
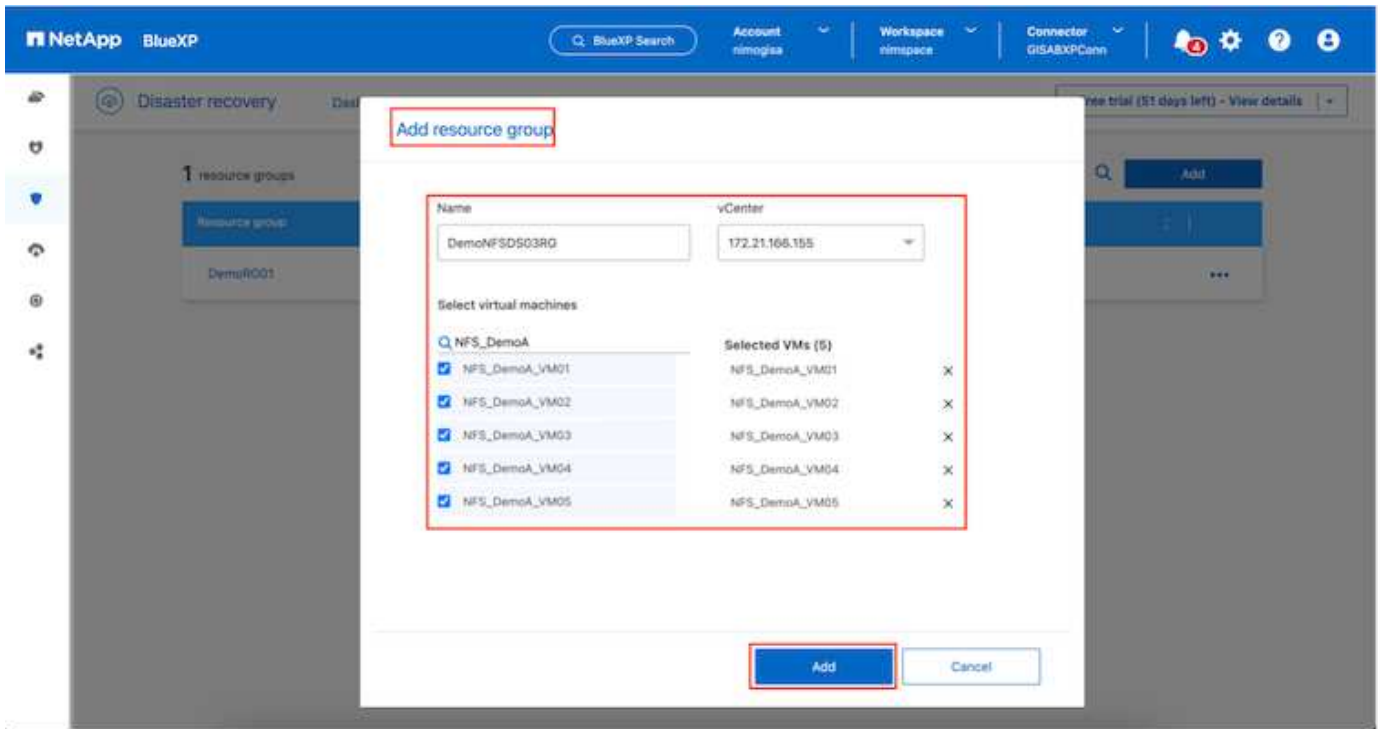
Wenn die SnapMirror -Beziehung für das Volume bereits über die CLI konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.

## Was kann BlueXP disaster recovery für Sie tun?

Nachdem die Quell- und Zielsites hinzugefügt wurden, führt die BlueXP disaster recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Die BlueXP disaster recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.

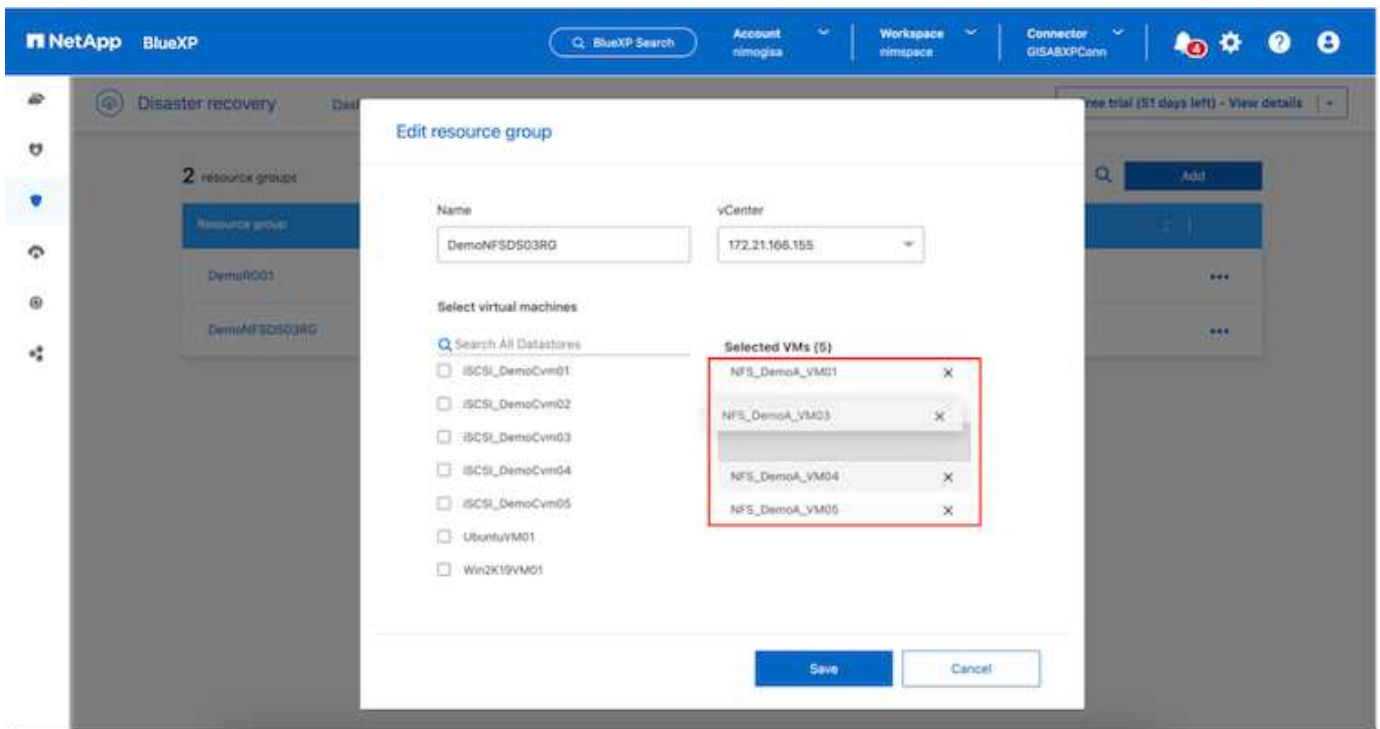


Nachdem die Sites hinzugefügt wurden, können VMs in Ressourcengruppen gruppiert werden. Mit den BlueXP disaster recovery können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen und Startverzögerungen enthalten, die bei der Wiederherstellung ausgeführt werden können. Um mit der Erstellung von Ressourcengruppen zu beginnen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.

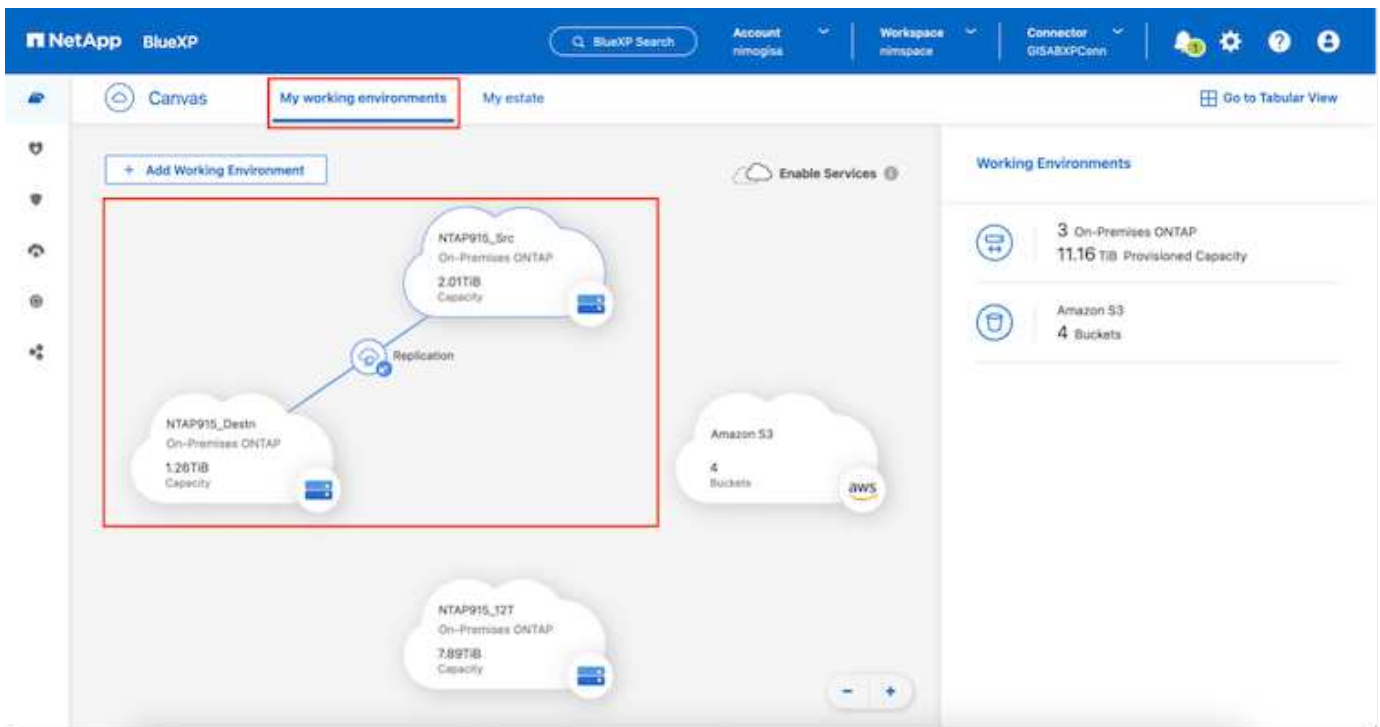


Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

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



Sobald die Ressourcengruppen erstellt sind, besteht der nächste Schritt darin, den Ausführungsentwurf oder einen Plan zur Wiederherstellung virtueller Maschinen und Anwendungen im Katastrophenfall zu erstellen. Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des Replikationsplans angegeben wurden.



NetApp BlueXP							
Replication							
Volume Relationships (8)							
Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer	
	NTAP915_Src	NTAP915_Destn				2023 Sep	
✓	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:15 386.63 MiB	
✓	Src_250_Vol01 NTAP915_Src	Src_250_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 79.23 MiB	
✓	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_CP NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 24.64 MiB	
✓	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_CP NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 47.38 MiB	
✓	Src_JSCSI_DS04 NTAP915_Src	Src_JSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 108.87 MiB	
✓	nimpra NTAP915_Src	nimpra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12:1 3.48 KiB	

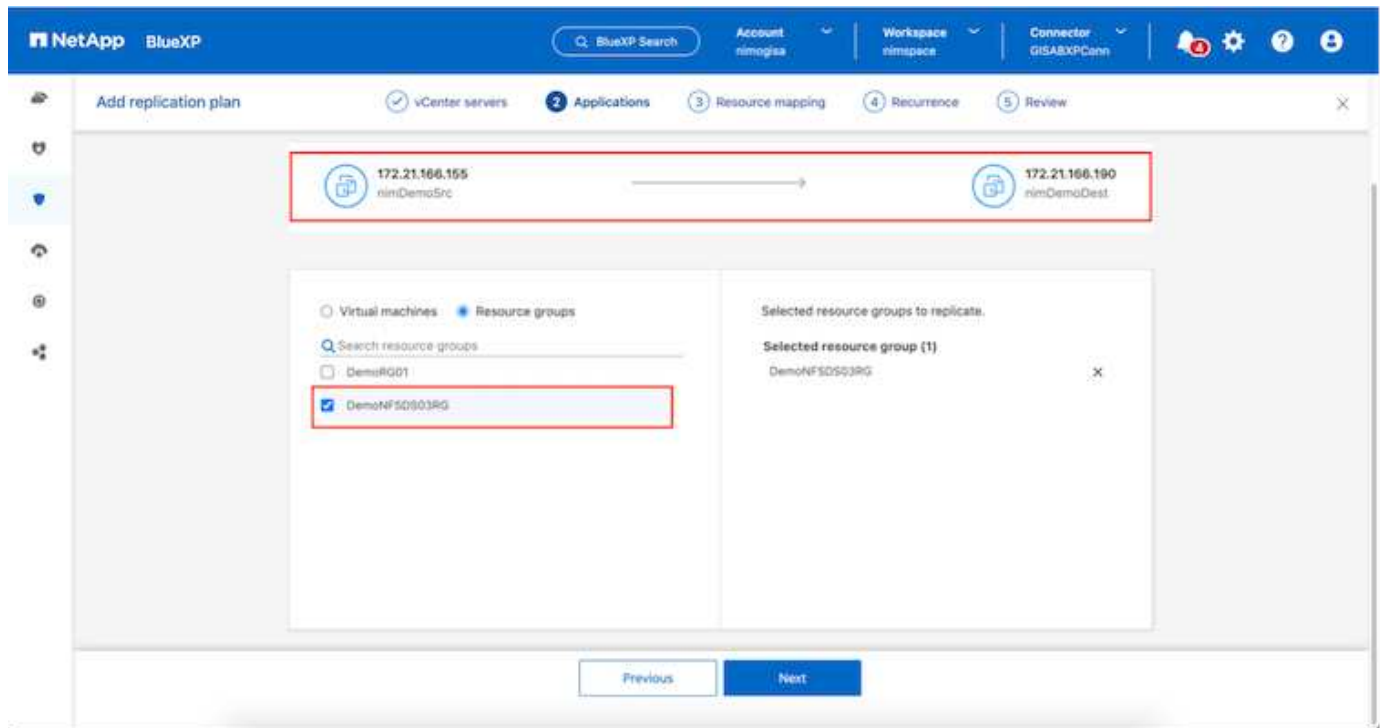
Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

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

NetApp BlueXP										
Add replication plan										
1 vCenter servers		2 Applications	3 Resource mapping	4 Recurrence	5 Review					
<div>Replication plan name</div> <div>DemoNFS03RP</div>										
<div> <div>Select a source vCenter where your data exists, to replicate to the selected target vCenter.</div> <div> <div> <div>Source vCenter</div> <div>172.21.166.155</div> </div> <div> <div>Target vCenter</div> <div>172.21.166.190</div> </div> </div> </div>										
Cancel		Next								

Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend

auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.

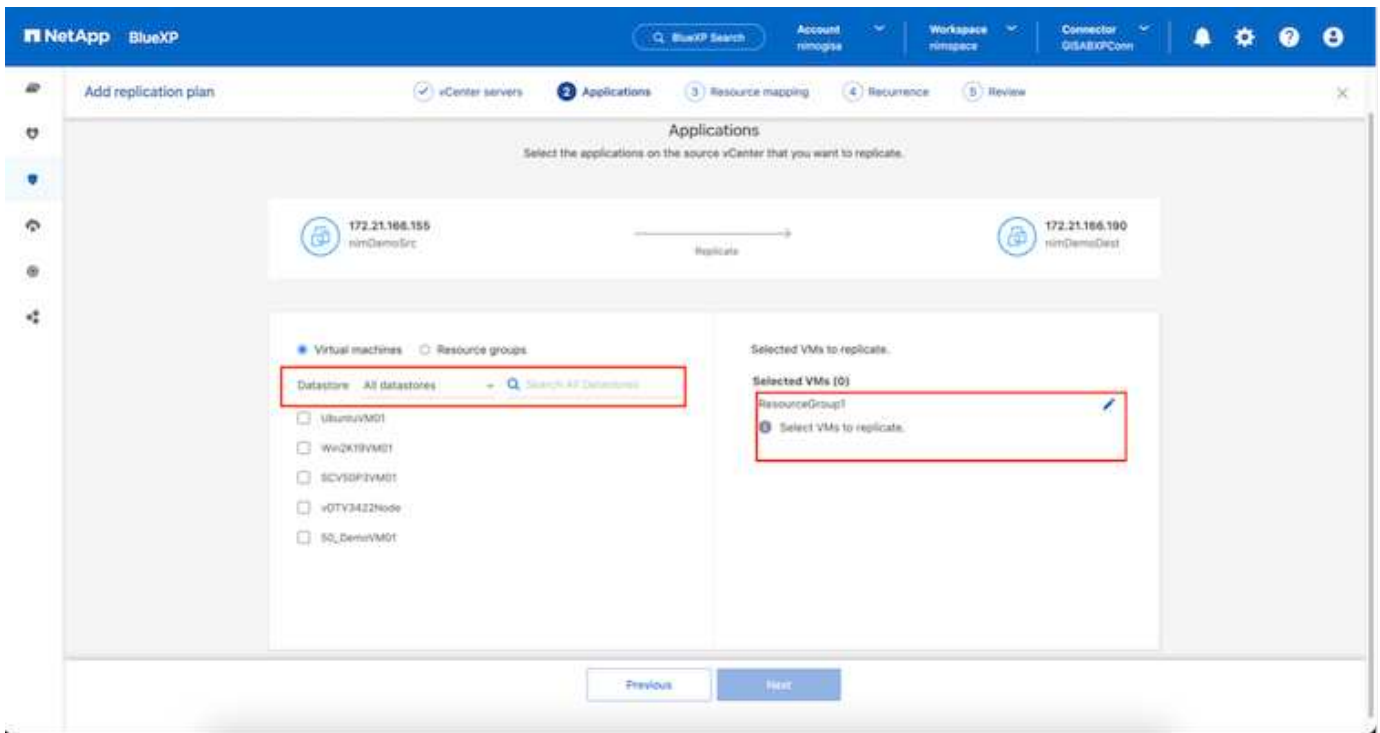


Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

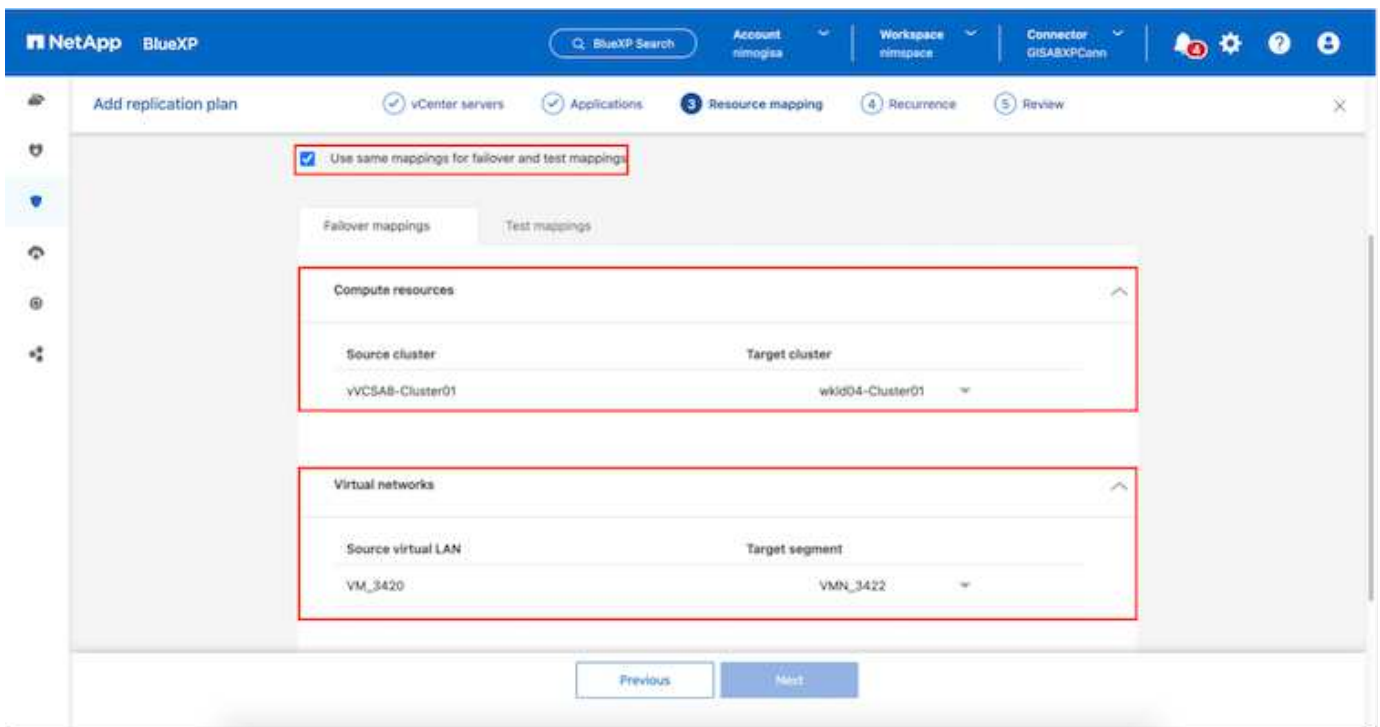


Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

Der folgende Screenshot zeigt die Option zum Filtern virtueller Maschinen oder bestimmter Datenspeicher basierend auf organisatorischen Anforderungen, wenn nicht zuvor Ressourcengruppen erstellt wurden.



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 und virtuelle Netzwerke. IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Anwendungskonsistenz und so weiter. Ausführliche Informationen finden Sie unter ["Erstellen eines Replikationsplans"](#).







Standardmäßig werden für Test- und Failovervorgänge dieselben Zuordnungsparameter verwendet. Um verschiedene Zuordnungen für die Testumgebung festzulegen, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:

NetApp BlueXP

Account nimogisa Workspace nimspace Connector GISABXPCenn

Add replication plan

Virtual machines

IP address type: Static Target IP: Same as source

☐ Use the same credentials for Same as source

☐ Use the same script for all V Different from source

Source VM	CPU(s)	RAM	Boot delay (mins between 0 and 10)	Create application consistent replicas
DemoNFS03RQ				
NFS_DemoA_VM01	2	4 GB	0	<input type="checkbox"/>
NFS_DemoA_VM02	2	4 GB	0	<input type="checkbox"/>

Previous Next

Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.

NetApp BlueXP

Account nimogisa Workspace nimspace Connector GISABXPCenn

Add replication plan

172.21.166.165 nimDemoSrc → 172.21.166.190 nimDemoDest

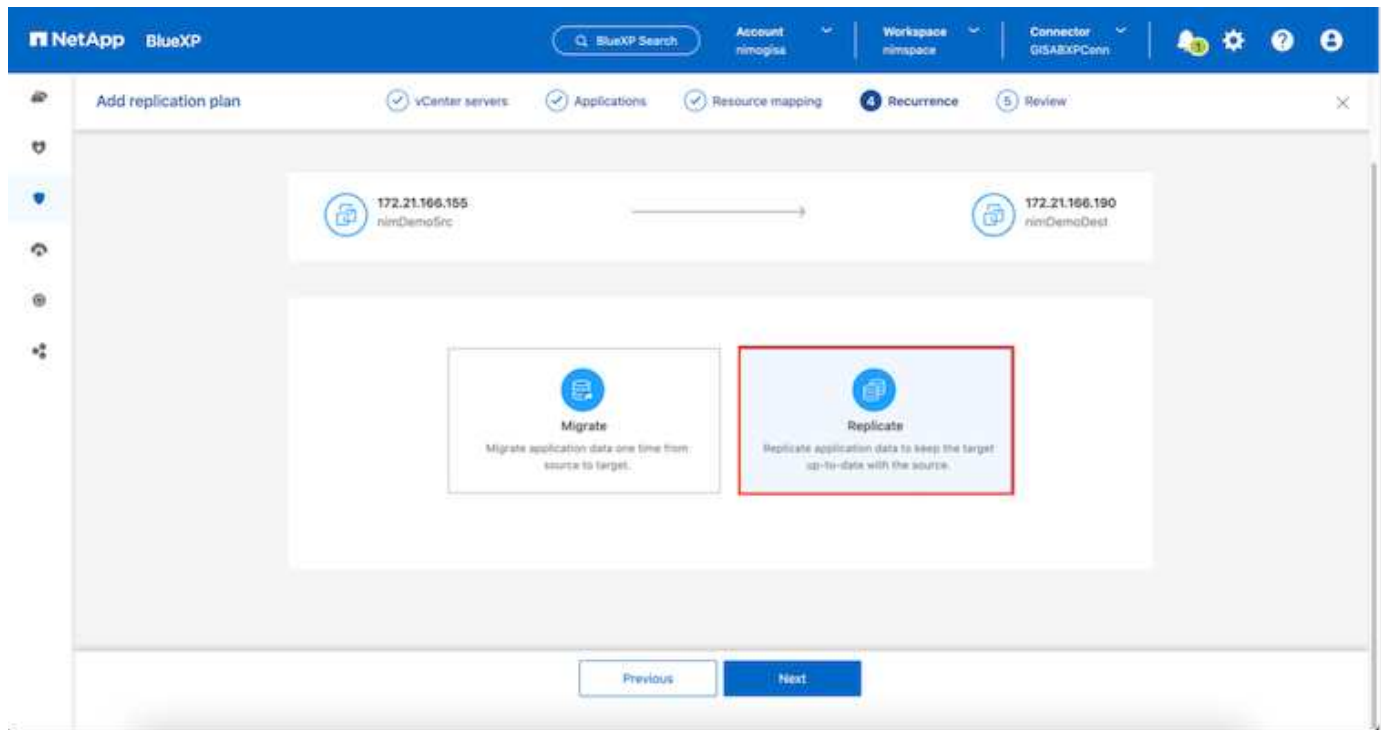
☒ Use same mappings for failover and test mappings

Failover mappings	Test mappings	
Compute resources	Mapped	▼
Virtual networks	Mapped	▼
Virtual machines	Mapped	▼

Previous Next

Wählen Sie den Wiederholungstyp aus. Einfach ausgedrückt: Wählen Sie „Migrieren“ (einmalige Migration mit Failover) oder die Option „Wiederkehrende kontinuierliche Replikation“. In dieser exemplarischen

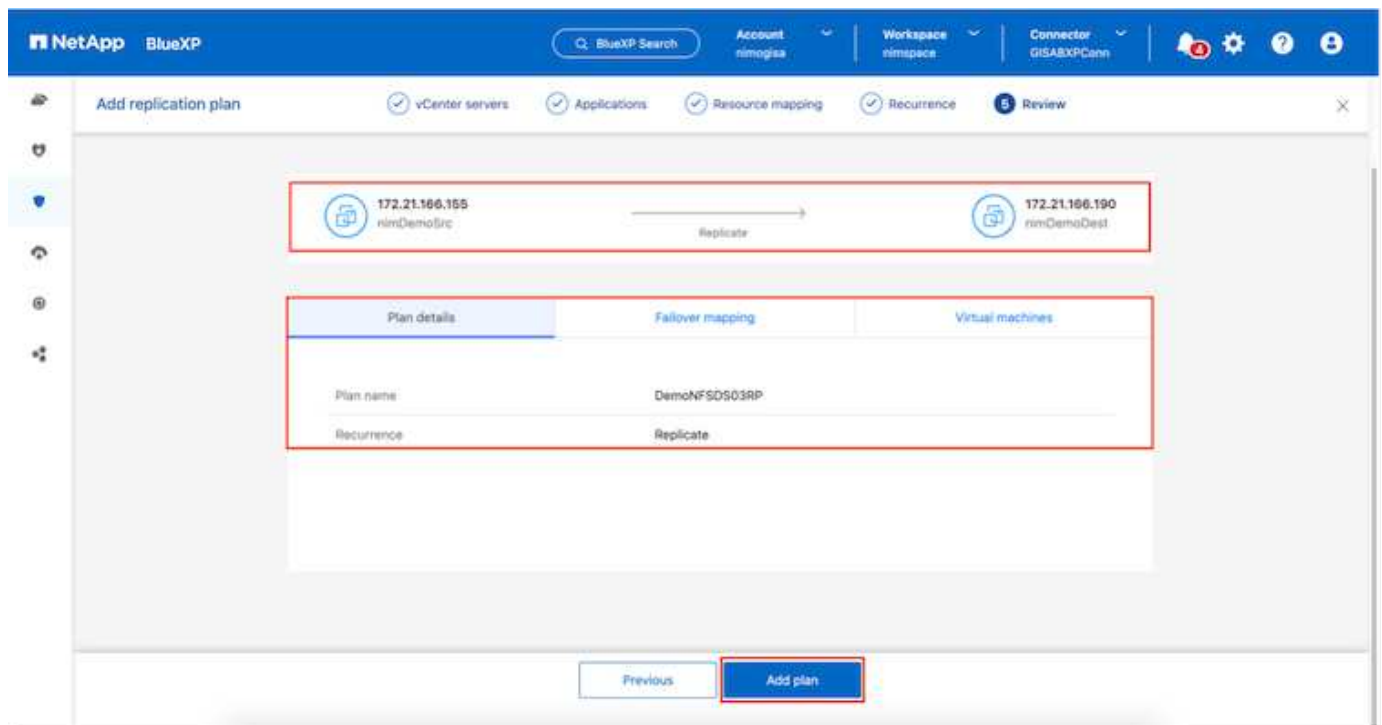
Vorgehensweise ist die Option „Replizieren“ ausgewählt.

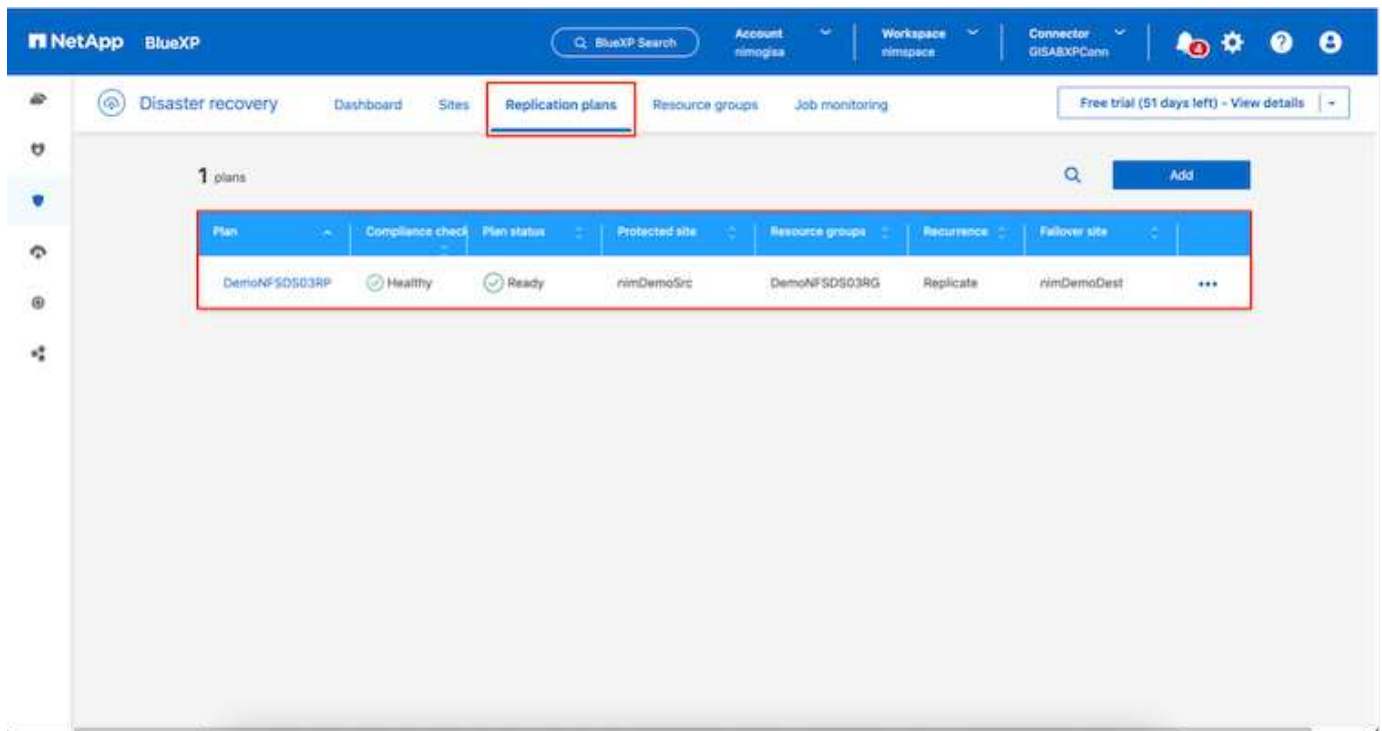


Überprüfen Sie anschließend die erstellten Zuordnungen und klicken Sie dann auf **Plan hinzufügen**.



VMs aus verschiedenen Volumes und SVMs können in einen Replikationsplan aufgenommen werden. Abhängig von der VM-Platzierung (sei es auf demselben Volume oder einem separaten Volume innerhalb derselben SVM, separate Volumes auf verschiedenen SVMs) erstellt die BlueXP disaster recovery einen Consistency Group Snapshot.



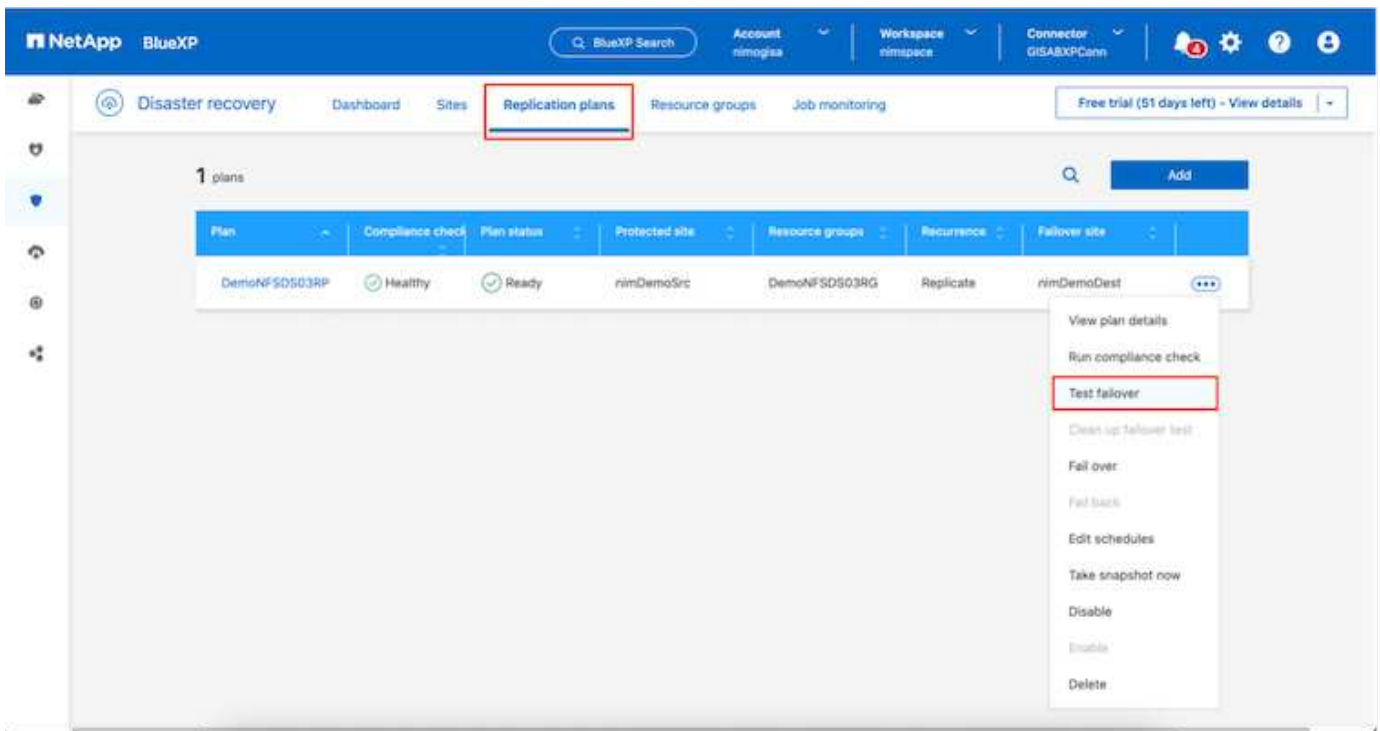


BlueXP DRaaS besteht aus den folgenden Workflows:

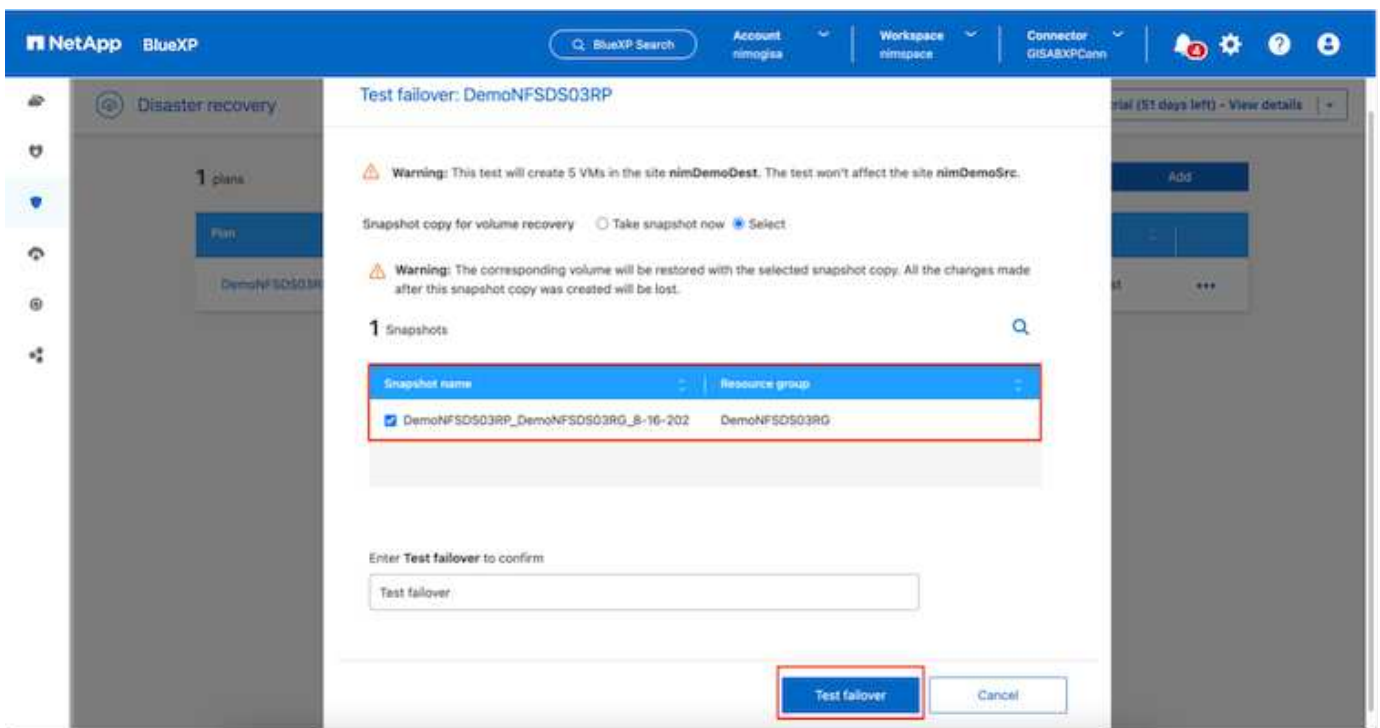
- Test-Failover (einschließlich regelmäßiger automatisierter Simulationen)
- Failovertest bereinigen
- Ausfallsicherung
- Failback

## Testen des Failovers

Test-Failover in BlueXP DRaaS ist ein Betriebsverfahren, das es VMware-Administratoren ermöglicht, ihre Wiederherstellungspläne vollständig zu validieren, ohne ihre Produktionsumgebungen zu stören.



BlueXP DRaaS bietet 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 auf die Zielsite repliziert werden und somit während des Tests vorhanden sind. Zu diesen Änderungen gehören Patches für das VM-Gastbetriebssystem



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

- Auslösen von SnapMirror -Beziehungen, um den Speicher am Zielstandort mit allen kürzlich am Produktionsstandort vorgenommenen Änderungen zu aktualisieren.

- Erstellen von NetApp FlexClone -Volumes der FlexVol -Volumes auf dem DR-Speicherarray.
- Verbinden der NFS-Datenspeicher 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 aller benutzerdefinierten Befehle, die im Replikationsplan gespeichert wurden.
- Einschalten der VMs in der im Replikationsplan festgelegten Reihenfolge.

The screenshot shows the vSphere Client interface. On the left, a tree view shows the hierarchy: **wkld04-vc01.hmcdc.local** > **wkld04-DC01** > **Src\_NFS\_DS03** (highlighted with a red box). The main panel displays the **Details** for **Src\_NFS\_DS03**, which is an NFS 3 volume. The details include:

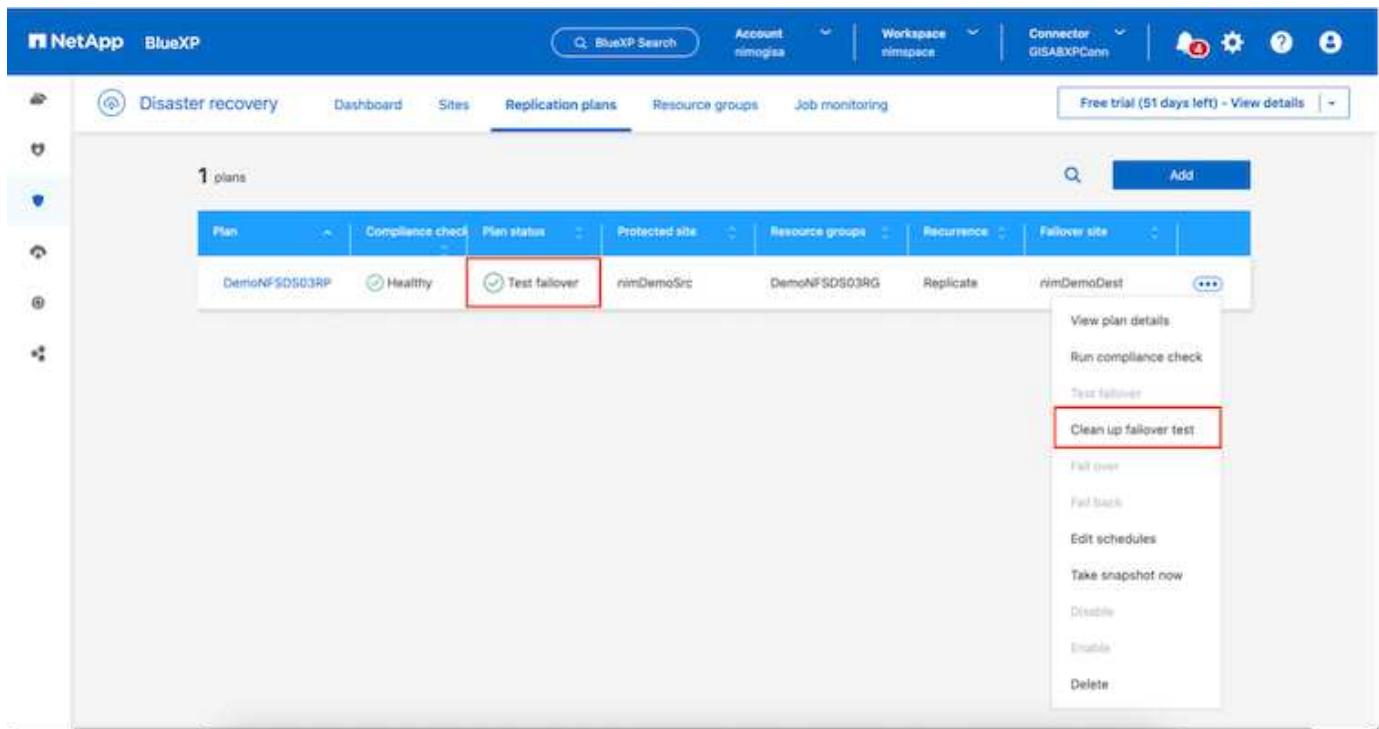
- Type: NFS 3
- Hosts: 2
- Virtual machines: 5
- VM templates: 0
- Server: 172.21.166.166
- Folder: /Src\_NFS\_DS03\_TEST
- Location: ds:///vmfs/volumes/b0c5bc3d-1a687494/

To the right, the **Capacity and Usage** section shows a storage bar chart with 71.22 GB free and 28.78 GB used, out of a 100 GB capacity. Below this, the **Recent Tasks** section shows a list of tasks:

Task Name	Target	Status	Details	Initiator	Outcome	Start Time	Completion Time
Reconfigure virtual machine	NFS-Demo-VM02	Completed		HMCDCLocal\Administrator	3 ms	08/16/2024, 6:53:59 A.M.	08/16/2024, 6:53:59 A.M.
Register virtual machine	..src04-DC01	Completed		System	6 ms	08/16/2024, 6:53:58 A.M.	08/16/2024, 6:53:59 A.M.
Register virtual machine	..src04-DC01	Completed		System	2 ms	08/16/2024, 6:53:58 A.M.	08/16/2024, 6:53:59 A.M.
Register virtual machine	..src04-DC01	Completed	Registering Virtual Machine 0 in destination host	System	2 ms	08/16/2024, 6:53:58 A.M.	08/16/2024, 6:54:00 A.M.

## Bereinigungs-Failover-Testvorgang

Der Bereinigungs-Failover-Testvorgang wird ausgeführt, nachdem der Replikationsplantest abgeschlossen wurde und der VMware-Administrator auf die Bereinigungsaufforderung reagiert.



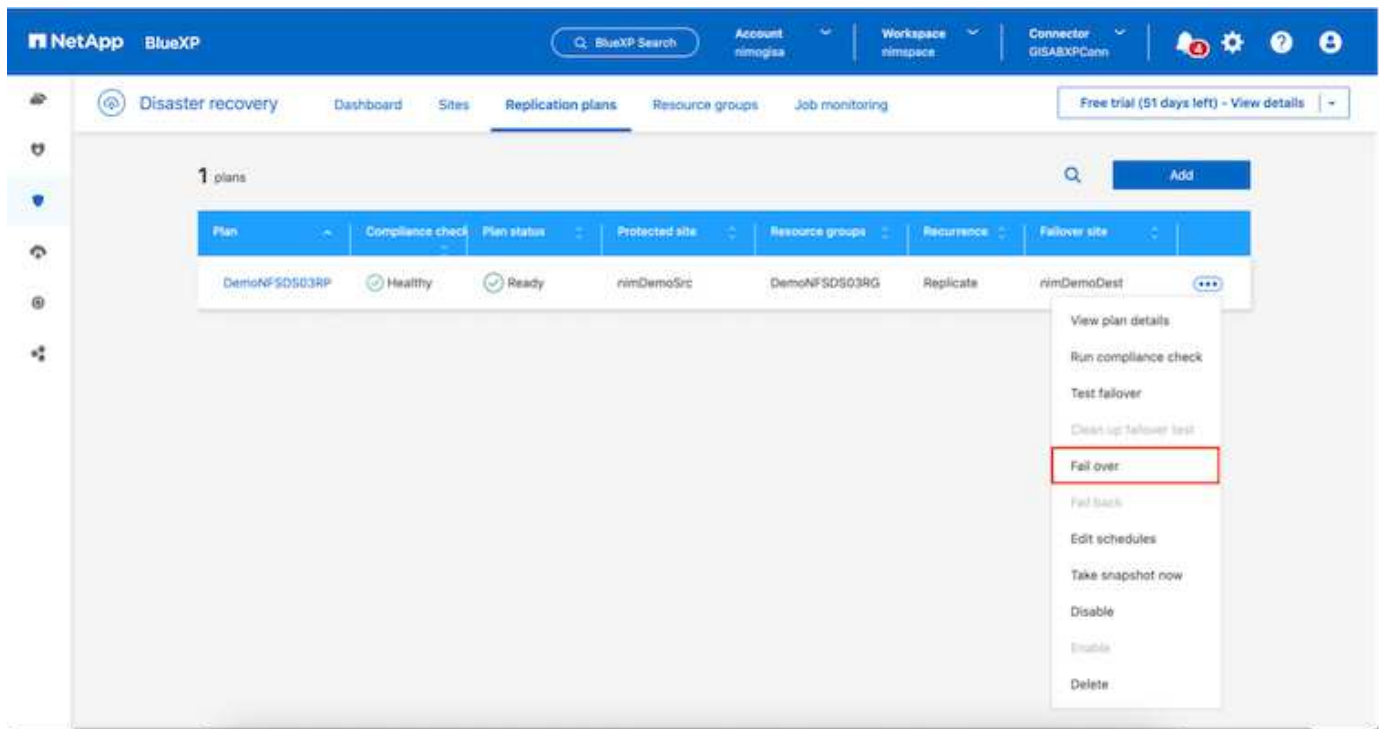
Durch diese Aktion werden die virtuellen Maschinen (VMs) und der Status des Replikationsplans auf den Bereitschaftszustand zurückgesetzt.

Wenn der VMware-Administrator einen Wiederherstellungsvorgang durchführt, führt BlueXP DRaaS den folgenden Prozess durch:

1. Es schaltet jede wiederhergestellte VM in der FlexClone -Kopie aus, die zum Testen verwendet wurde.
2. Es löscht das FlexClone Volume, das während des Tests zum Präsentieren der wiederhergestellten VMs verwendet wurde.

## Geplante Migration und Failover

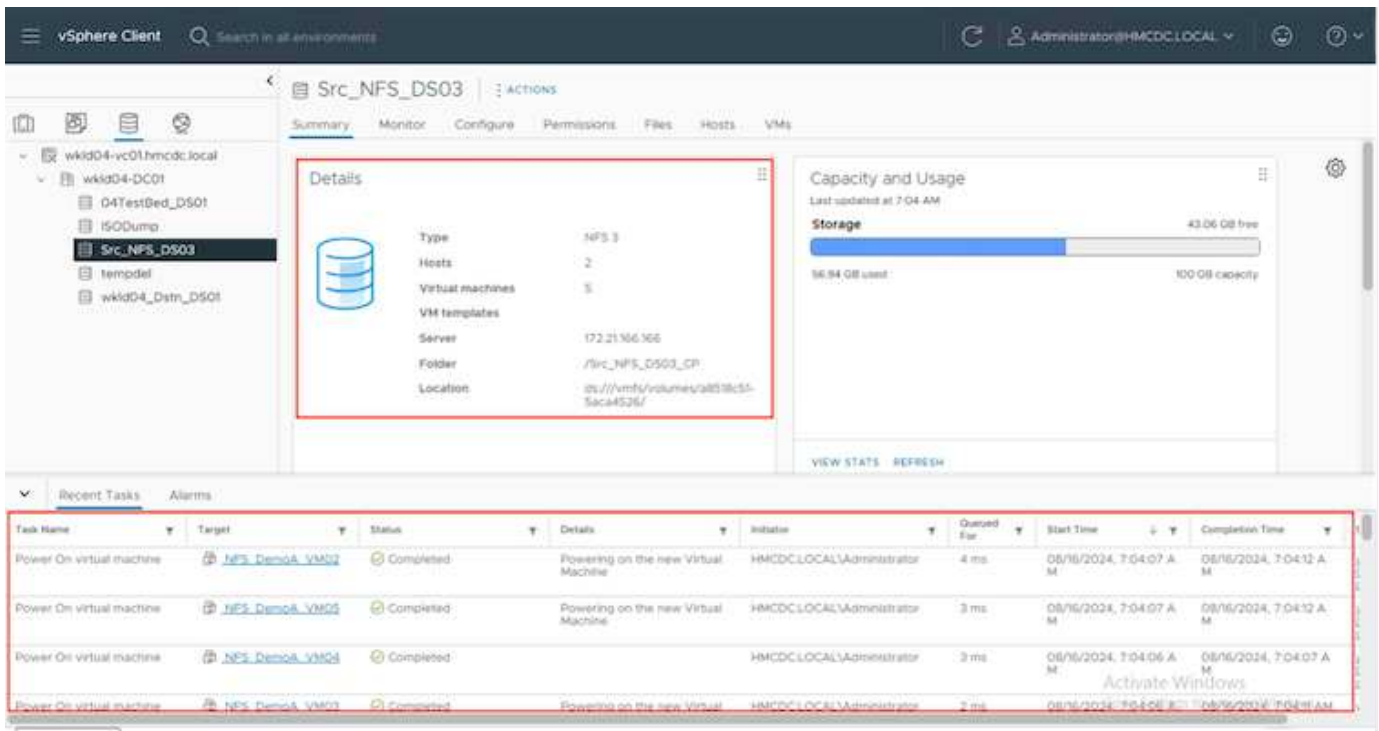
BlueXP DRaaS bietet zwei Methoden zur Durchführung eines echten Failovers: geplante Migration und Failover. Bei der ersten Methode, der geplanten Migration, werden das Herunterfahren der VM und die Synchronisierung der Speicherreplikation in den Prozess integriert, um die VMs wiederherzustellen oder effektiv an den Zielstandort zu verschieben. Für die geplante Migration ist Zugriff auf die Quellsite erforderlich. Die zweite Methode, Failover, ist ein geplantes/ungeplantes Failover, bei dem die VMs am Zielstandort aus dem letzten Speicherreplikationsintervall wiederhergestellt werden, das abgeschlossen werden konnte. Abhängig vom RPO, das in die Lösung integriert wurde, ist im DR-Szenario mit einem gewissen Datenverlust zu rechnen.



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

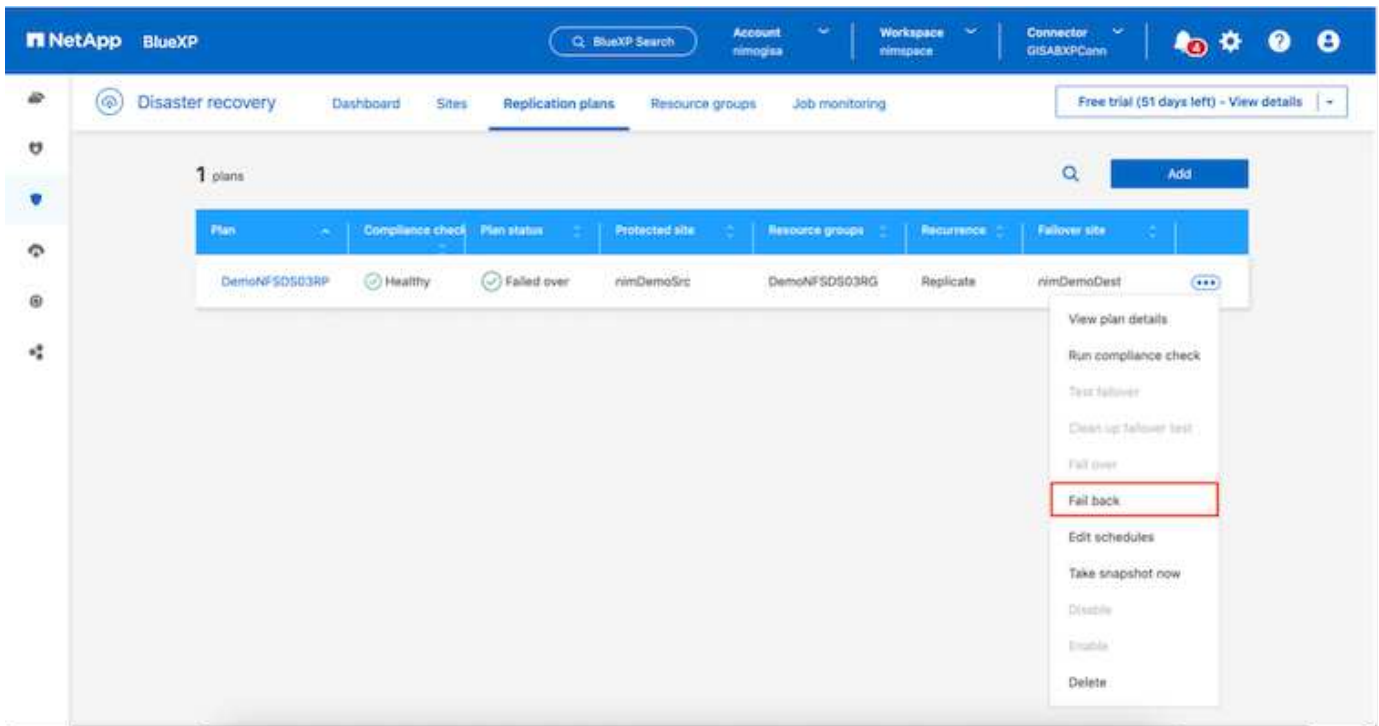
- Unterbrechen und Failover der NetApp SnapMirror -Beziehungen.
- Verbinden Sie die replizierten NFS-Datenspeicher mit den ESXi-Hosts am DR-Standort.
- Verbinden Sie die VM-Netzwerkadapter mit dem entsprechenden Zielstandortnetzwerk.
- Konfigurieren Sie die Netzwerkeinstellungen des VM-Gastbetriebssystems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





## Failback

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



VMware-Administratoren können ein Failback-Verfahren konfigurieren und ausführen, wenn sie bereit sind, die Dienste auf der ursprünglichen Quellsite wiederherzustellen.

**HINWEIS:** BlueXP DRaaS repliziert (resynchronisiert) alle Änderungen zurück zur ursprünglichen virtuellen Quellmaschine, bevor die Replikationsrichtung umgekehrt wird. Dieser Prozess beginnt mit einer Beziehung,

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

- Schalten Sie die virtuellen Maschinen aus und heben Sie die Registrierung auf. Die Volumes auf der Zielsite werden ausgehängt.
- Unterbrechen Sie die SnapMirror -Beziehung zur Originalquelle, um Lese-/Schreibzugriff zu ermöglichen.
- 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 zum Zugriff auf und zur Konfiguration von BlueXP DRaaS finden Sie im ["Erfahren Sie mehr über BlueXP Disaster Recovery für VMware"](#).

## Überwachung und Dashboard

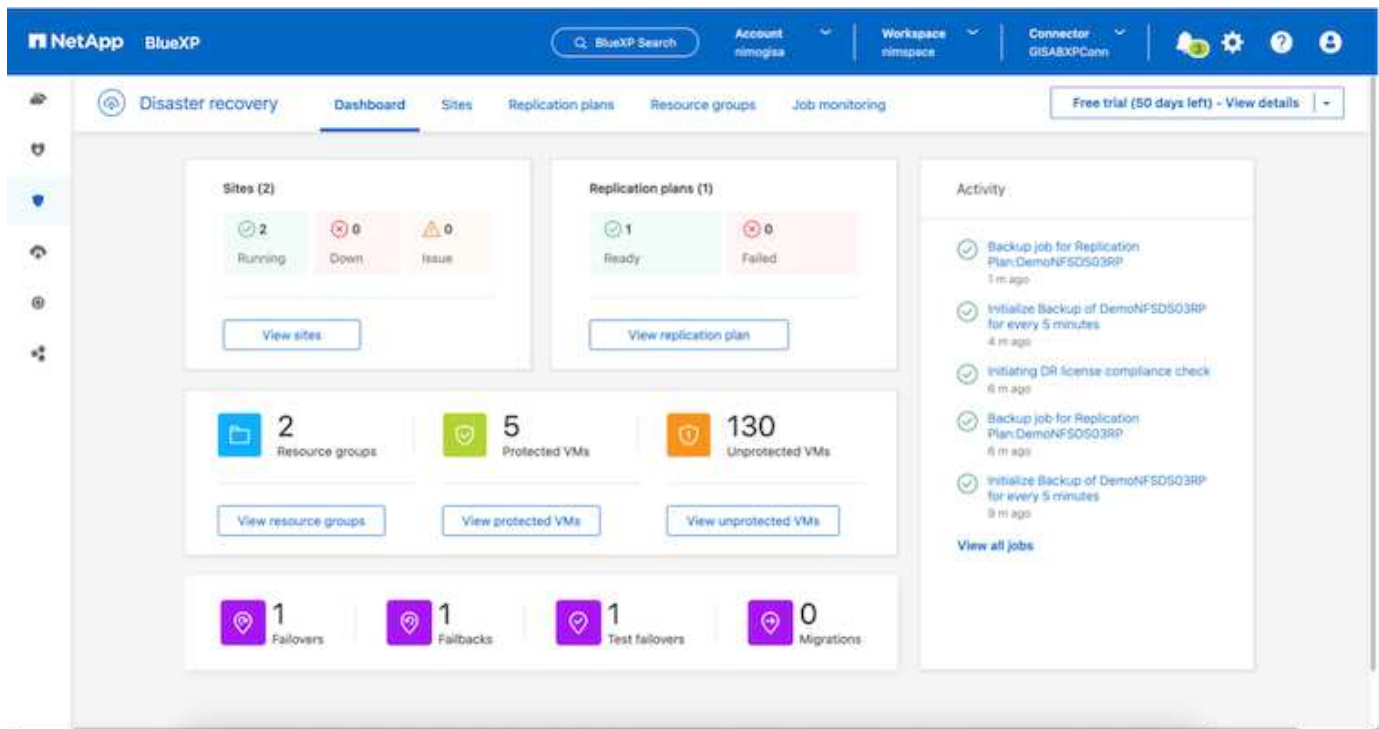
Von BlueXP oder der ONTAP CLI aus können Sie den Replikationszustand für die entsprechenden Datenspeichervolumen überwachen und den Status eines Failovers oder Testfailovers über die Jobüberwachung verfolgen.

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...	-
3549cc9c-aa4e-45e	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...
5cb01bcc-9ea6-4afl	Succe...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...
a2f225d9-b7be-4c2f	Succe...	Backup	Initialize Backup of DemoNFSDS03RP 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-afa8-48d	Succe...	Compliance	Initialize Compliance of DemoNFSDS03R...	08/16/2024, 04:4...	08/16/2024, 04:4...
97fdeb8-6f77-459	Succe...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...
bffc018e-ca3a-409d	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...
cde759a8-ebef-498	Succe...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...
a414daba-9630-4c5	Succe...	Backup	Initialize Backup of DemoNFSDS03RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...



Wenn ein Auftrag gerade ausgeführt wird oder sich in der Warteschlange befindet und Sie ihn stoppen möchten, können Sie ihn mit der Option „Abbrechen“ abbrechen.

Mit dem BlueXP disaster recovery können Sie den Status von Notfallwiederherstellungsstandorten und Replikationsplänen zuverlässig bewerten. Dadurch können Administratoren schnell fehlerfreie, nicht verbundene oder beeinträchtigte Sites und Pläne identifizieren.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Prozess zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen oder die "[Lösungssimulator](#)".

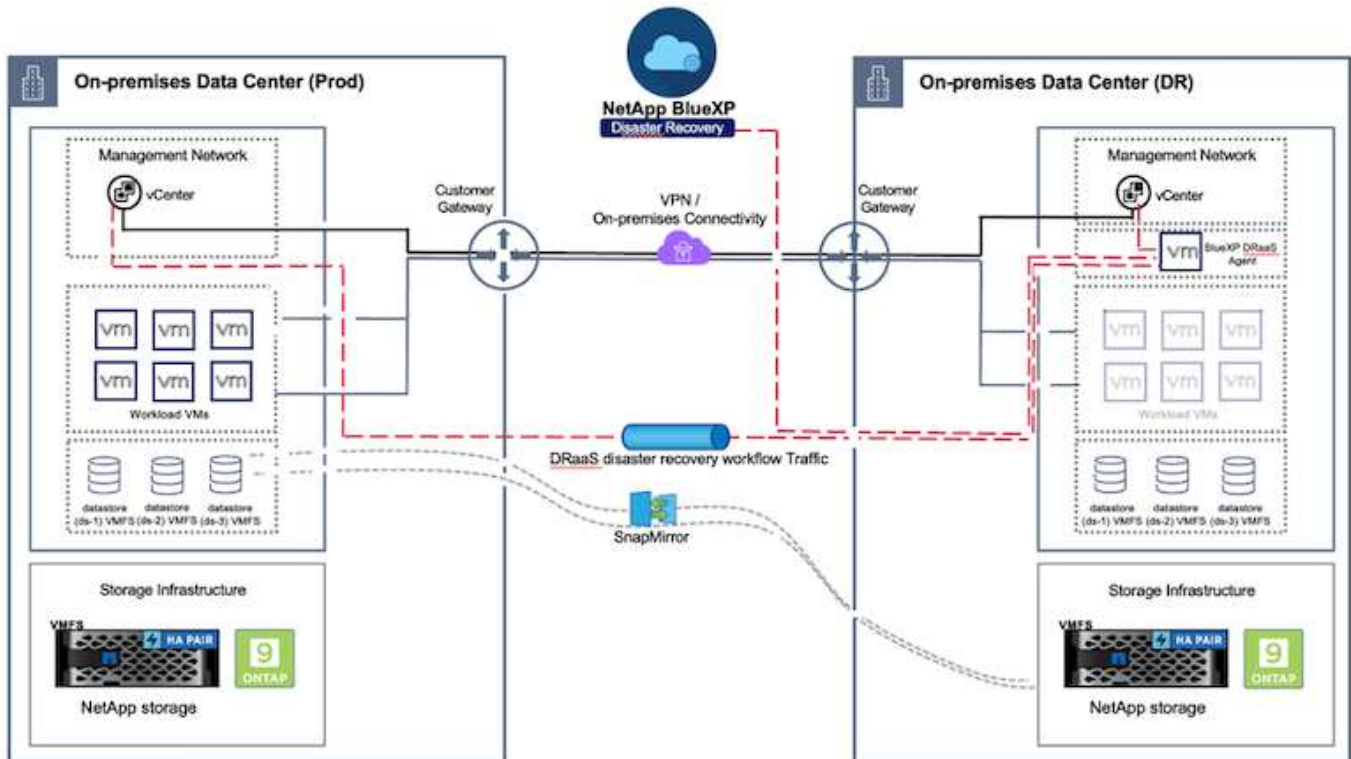
## DR mit BlueXP DRaaS für VMFS-Datenspeicher

Die Notfallwiederherstellung mithilfe der Blockebenenreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Möglichkeit, die Workloads vor Standortausfällen und Datenbeschädigungen wie Ransomware-Angriffen zu schützen. Mit der NetApp SnapMirror Replikation können VMware-Workloads, die auf lokalen ONTAP -Systemen mit VMFS-Datenspeicher ausgeführt werden, auf ein anderes ONTAP Speichersystem in einem dafür vorgesehenen Wiederherstellungs-Rechenzentrum repliziert werden, in dem sich VMware befindet.

In diesem Abschnitt des Dokuments wird die Konfiguration von BlueXP DRaaS zum Einrichten der Notfallwiederherstellung für lokale VMware-VMs an einem anderen bestimmten Standort beschrieben. Als Teil dieser Einrichtung werden das BlueXP -Konto, der BlueXP Connector und die ONTAP Arrays im BlueXP Arbeitsbereich hinzugefügt, die für die Kommunikation von VMware vCenter mit dem ONTAP Speicher erforderlich sind. Darüber hinaus wird in diesem Dokument detailliert beschrieben, wie die Replikation zwischen Standorten konfiguriert wird und wie ein Wiederherstellungsplan eingerichtet und getestet wird. Der letzte Abschnitt enthält Anweisungen zum Durchführen eines vollständigen Site-Failovers und zum Failback, wenn die primäre Site wiederhergestellt und online gestellt wurde.

Mithilfe des BlueXP disaster recovery -Dienstes, der in die NetApp BlueXP Konsole integriert ist, können Kunden ihre lokalen VMware vCenter zusammen mit ONTAP Speicher ermitteln, Ressourcengruppierungen erstellen, einen Disaster-Recovery-Plan erstellen, ihn mit Ressourcengruppen verknüpfen und Failover und Failback testen oder ausführen. SnapMirror bietet Blockreplikation auf Speicherebene, um die beiden Sites mit

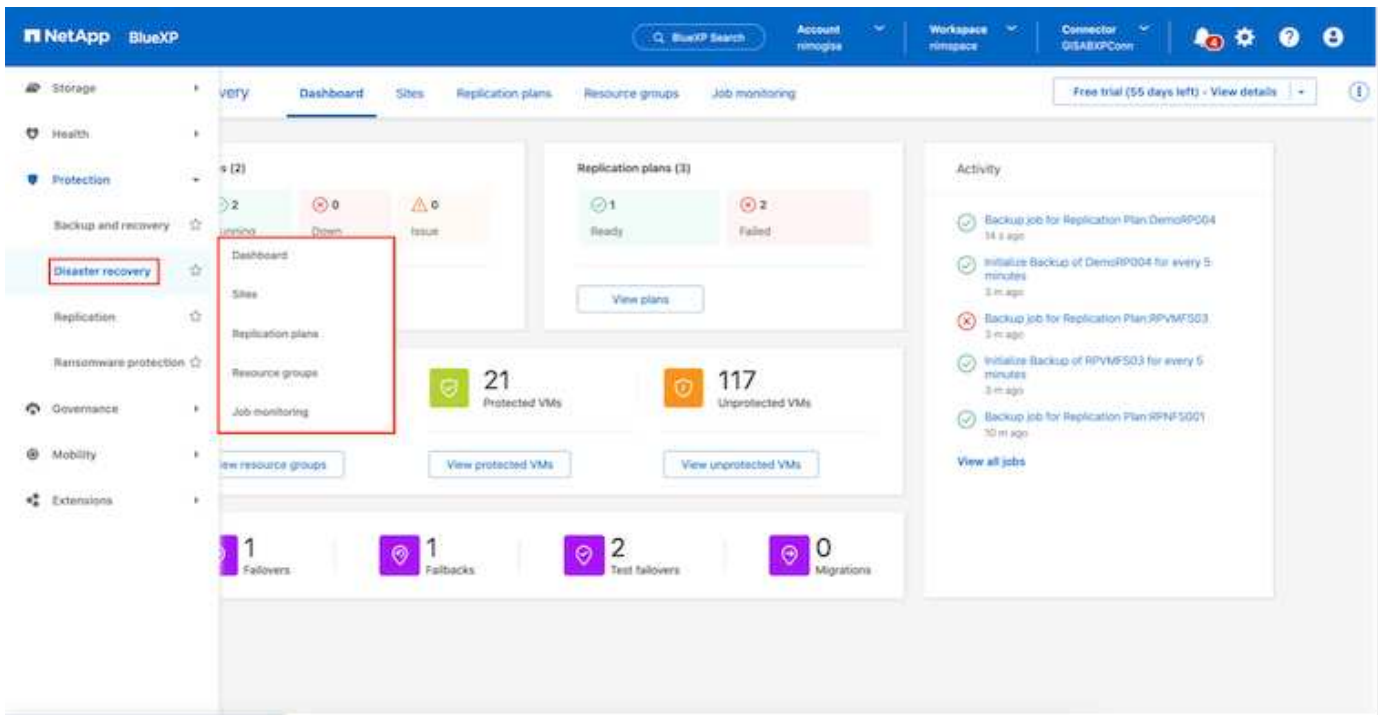
inkrementellen Änderungen auf dem neuesten Stand zu halten, was zu einem RPO von bis zu 5 Minuten führt. Darüber hinaus ist es möglich, DR-Verfahren als reguläre Übung zu simulieren, ohne die Produktion und die replizierten Datenspeicher zu beeinträchtigen oder zusätzliche Speicherkosten zu verursachen. Die BlueXP disaster recovery nutzt die FlexClone -Technologie von ONTAP, um eine platzsparende Kopie des VMFS-Datenspeichers aus dem letzten replizierten Snapshot auf der DR-Site zu erstellen. Sobald der DR-Test abgeschlossen ist, können Kunden die Testumgebung einfach löschen, wiederum ohne Auswirkungen auf die tatsächlich replizierten Produktionsressourcen. Wenn ein tatsächlicher Failover (geplant oder ungeplant) erforderlich ist, orchestriert der BlueXP disaster recovery mit wenigen Klicks alle erforderlichen Schritte, um die geschützten virtuellen Maschinen automatisch am vorgesehenen Notfallwiederherstellungsstandort hochzufahren. Der Dienst kehrt außerdem die SnapMirror -Beziehung zum primären Standort um und repliziert bei Bedarf alle Änderungen vom sekundären zum primären Standort für einen Failback-Vorgang. All dies kann im Vergleich zu anderen bekannten Alternativen zu einem Bruchteil der Kosten erreicht werden.



## Erste Schritte

Um mit der BlueXP disaster recovery zu beginnen, verwenden Sie die BlueXP -Konsole und greifen Sie dann auf den Dienst zu.

1. Melden Sie sich bei BlueXP an.
2. Wählen Sie in der linken Navigationsleiste von BlueXP „Schutz“ > „Notfallwiederherstellung“ aus.
3. Das BlueXP disaster recovery wird angezeigt.



Stellen Sie vor der Konfiguration des Notfallwiederherstellungsplans sicher, dass die folgenden Voraussetzungen erfüllt sind:

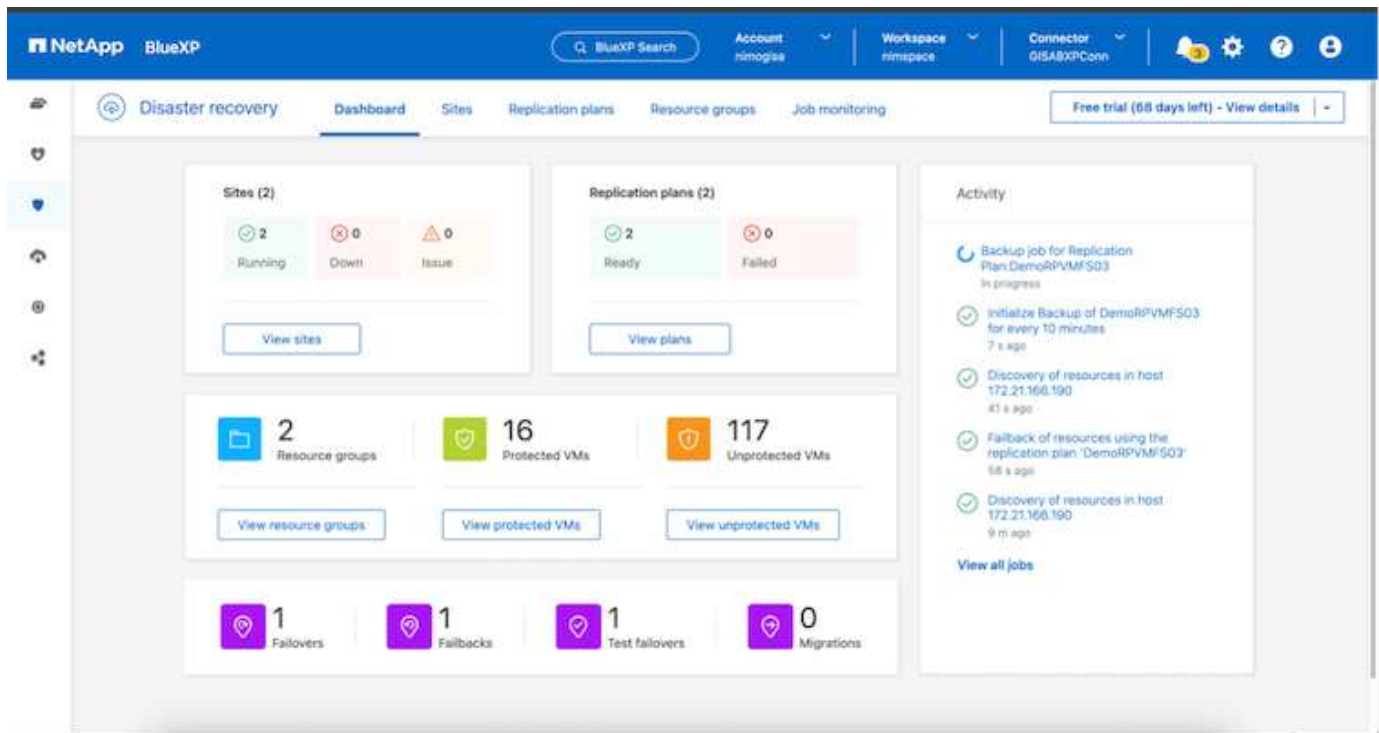
- BlueXP Connector wird in NetApp BlueXP eingerichtet. Der Connector sollte in AWS VPC bereitgestellt werden.
- Die BlueXP Connector-Instanz verfügt über eine Verbindung zum Quell- und Ziel-vCenter und den Speichersystemen.
- In BlueXP werden lokale NetApp -Speichersysteme hinzugefügt, die VMFS-Datenspeicher für VMware hosten.
- Bei der Verwendung von DNS-Namen sollte eine DNS-Auflösung vorhanden sein. Andernfalls verwenden Sie IP-Adressen für das vCenter.
- Die SnapMirror Replikation ist für die angegebenen VMFS-basierten Datenspeichervolumen konfiguriert.

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



NetApp empfiehlt, den BlueXP Connector am Disaster-Recovery-Standort oder an einem dritten Standort bereitzustellen, damit der BlueXP Connector bei tatsächlichen Ausfällen oder Naturkatastrophen über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.





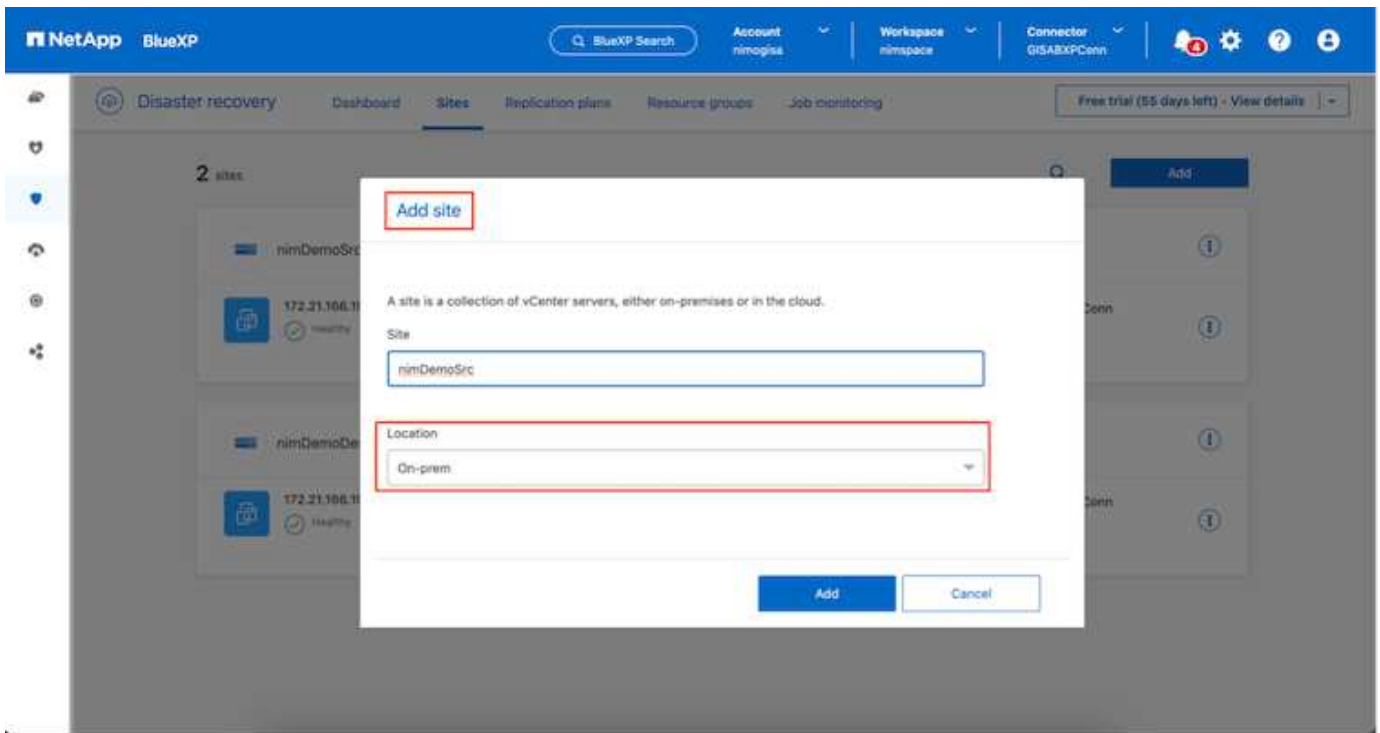
Die Unterstützung für lokale VMFS-Datenspeicher befindet sich beim Schreiben dieses Dokuments in der Technologievorschau. Die Funktion wird sowohl mit FC- als auch mit ISCSI-Protokoll-basierten VMFS-Datenspeichern unterstützt.

## BlueXP disaster recovery

Der erste Schritt bei der Vorbereitung der Notfallwiederherstellung besteht darin, die lokalen vCenter- und Speicherressourcen zu ermitteln und zur BlueXP disaster recovery hinzuzufügen.

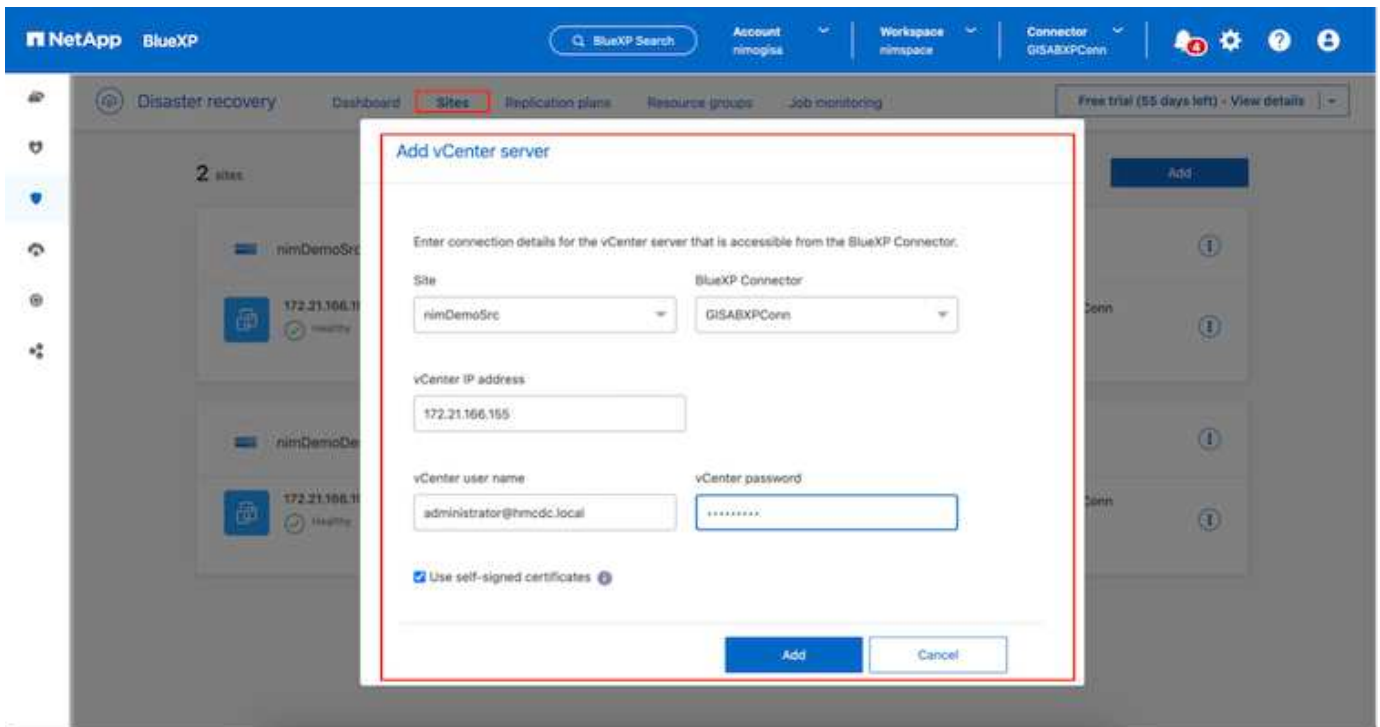


Stellen Sie sicher, dass die ONTAP Speichersysteme der Arbeitsumgebung innerhalb des Canvas hinzugefügt werden. Öffnen Sie die BlueXP -Konsole und wählen Sie in der linken Navigation **Schutz > Notfallwiederherstellung**. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü. Wählen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



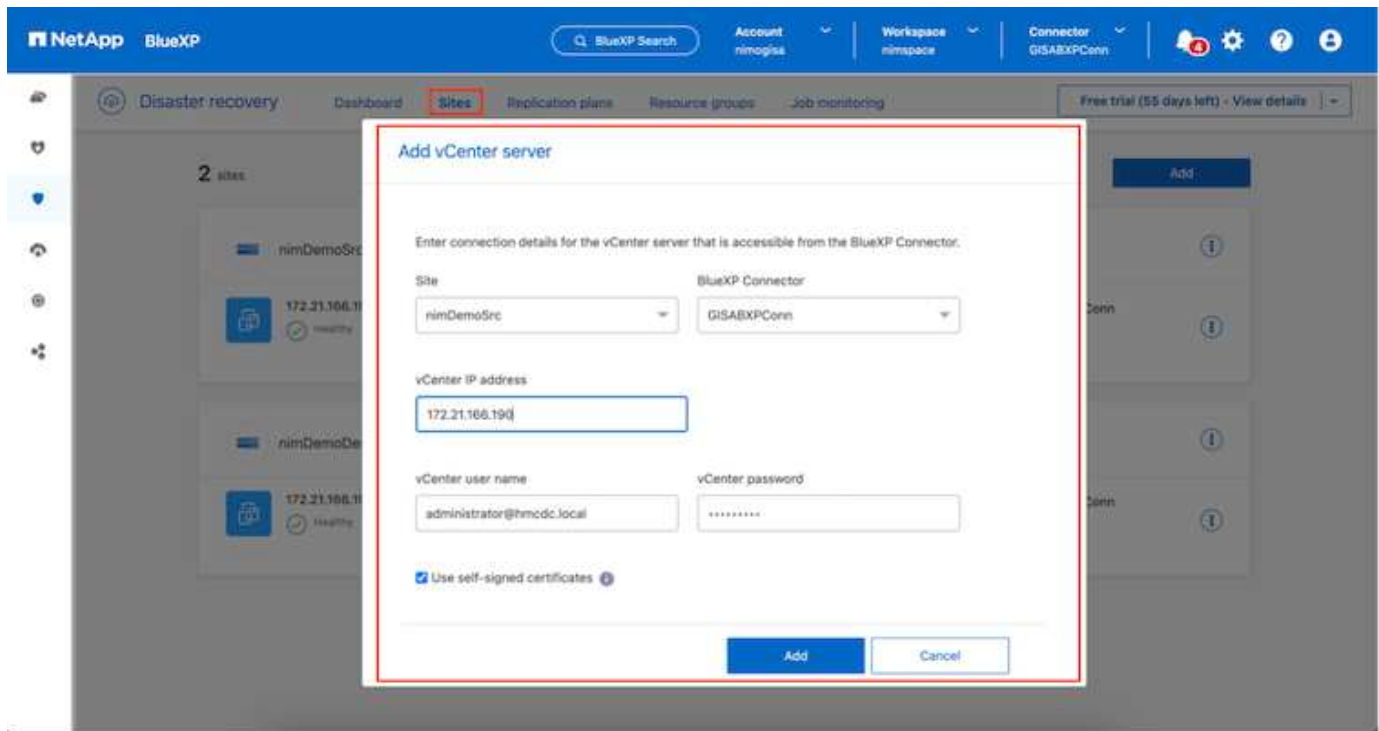
Fügen Sie die folgenden Plattformen hinzu:

- **Quelle.** Lokales vCenter.



- **Ziel.** VMC SDDC vCenter.





Sobald die vCenter hinzugefügt wurden, wird die automatische Erkennung ausgelöst.

## Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort

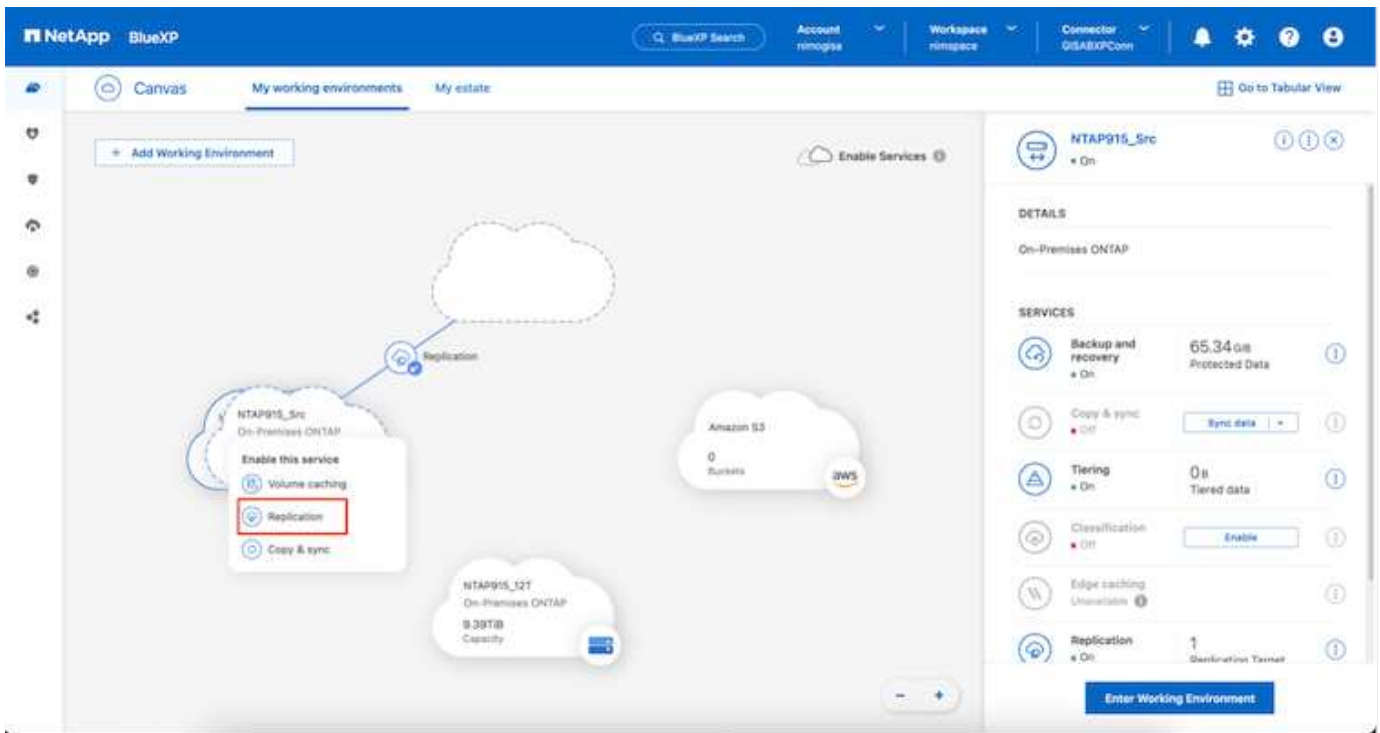
SnapMirror nutzt ONTAP -Snapshots, um die Datenübertragung von einem Ort zum anderen zu verwalten. Zunächst wird eine vollständige Kopie basierend auf einem Snapshot des Quellvolumes auf das Ziel kopiert, um eine Basissynchronisierung durchzuführen. Wenn an der Quelle Datenänderungen auftreten, wird ein neuer Snapshot erstellt und mit dem Basis-Snapshot verglichen. Die Blöcke, bei denen Änderungen festgestellt wurden, werden dann zum Ziel repliziert, wobei der neuere Snapshot zur aktuellen Basislinie oder zum neuesten gemeinsamen Snapshot wird. Dadurch kann der Vorgang wiederholt und inkrementelle Updates an das Ziel gesendet werden.

Wenn eine SnapMirror -Beziehung hergestellt wurde, befindet sich das Zielvolume in einem schreibgeschützten Online-Zustand und ist daher weiterhin zugänglich. SnapMirror arbeitet mit physischen Speicherblöcken und nicht auf Datei- oder anderer logischer Ebene. Dies bedeutet, dass das Zielvolume eine identische Replik des Quellvolumes ist, einschließlich Snapshots, Volumeeinstellungen usw. Wenn ONTAP Speicherplatzeffizienzfunktionen wie Datenkomprimierung und Datendeduplizierung vom Quellvolume verwendet werden, behält das replizierte Volume diese Optimierungen bei.

Durch das Aufheben der SnapMirror Beziehung wird das Zielvolume beschreibbar und wird normalerweise zum Durchführen eines Failovers verwendet, wenn SnapMirror zum Synchronisieren von Daten mit einer DR-Umgebung verwendet wird. SnapMirror ist so ausgereift, dass die am Failover-Standort geänderten Daten effizient mit dem primären System resynchronisiert werden können, falls dieses später wieder online geht. Anschließend kann die ursprüngliche SnapMirror Beziehung wiederhergestellt werden.

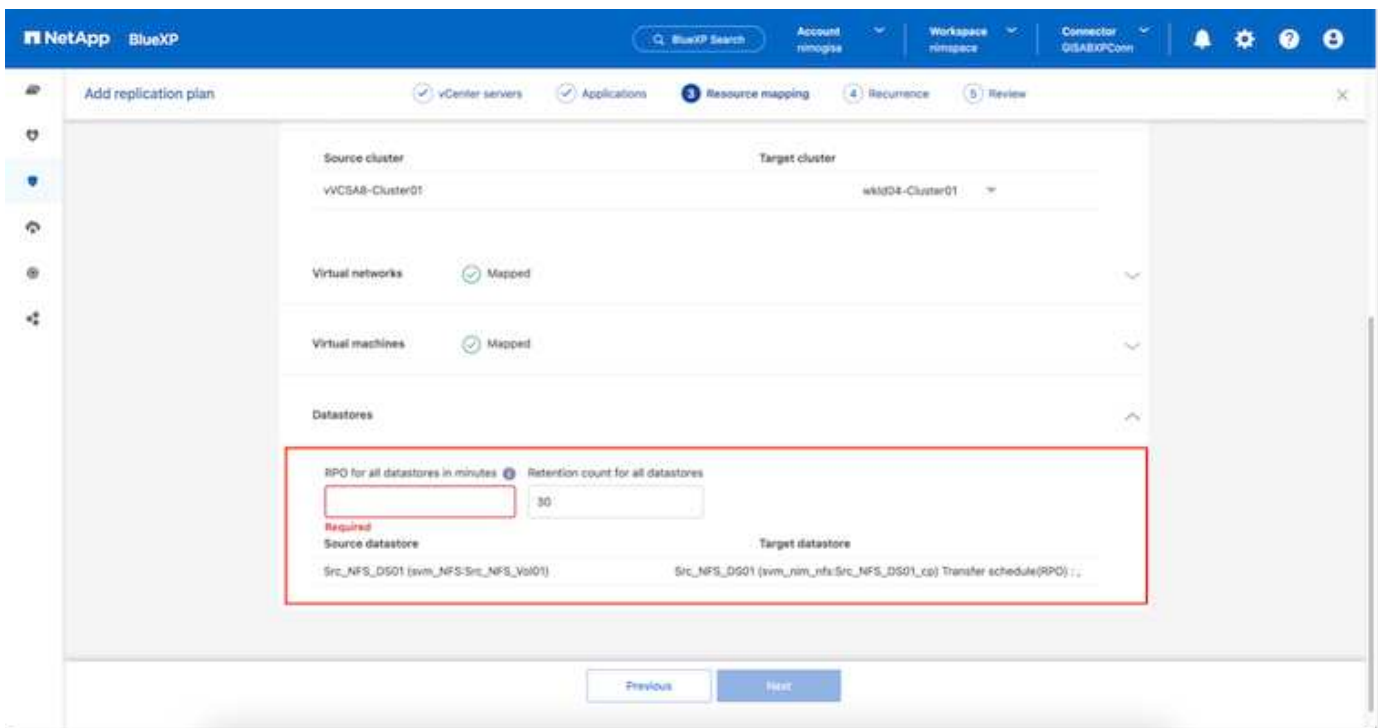
## So richten Sie es für VMware Disaster Recovery ein

Der Vorgang zum Erstellen der SnapMirror Replikation bleibt für jede Anwendung derselbe. Der Vorgang kann manuell oder automatisiert erfolgen. Am einfachsten ist es, BlueXP zu nutzen, um die SnapMirror -Replikation zu konfigurieren. Dazu ziehen Sie das Quell ONTAP -System in der Umgebung einfach per Drag & Drop auf das Ziel, um den Assistenten zu starten, der Sie durch den Rest des Prozesses führt.



BlueXP DRaaS kann dies auch automatisieren, sofern die folgenden beiden Kriterien erfüllt sind:

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



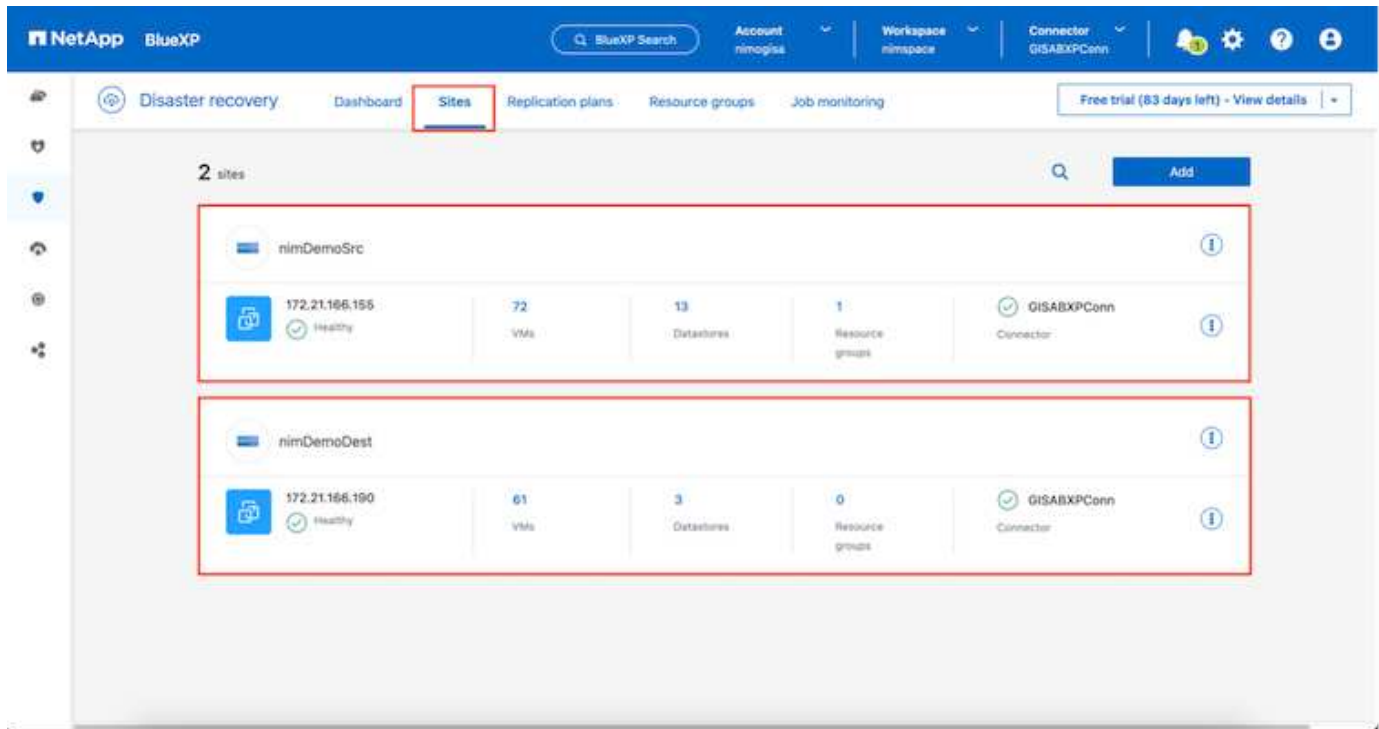
Wenn die SnapMirror -Beziehung für das Volume bereits über die CLI konfiguriert ist, übernimmt BlueXP DRaaS die Beziehung und fährt mit den restlichen Workflow-Vorgängen fort.



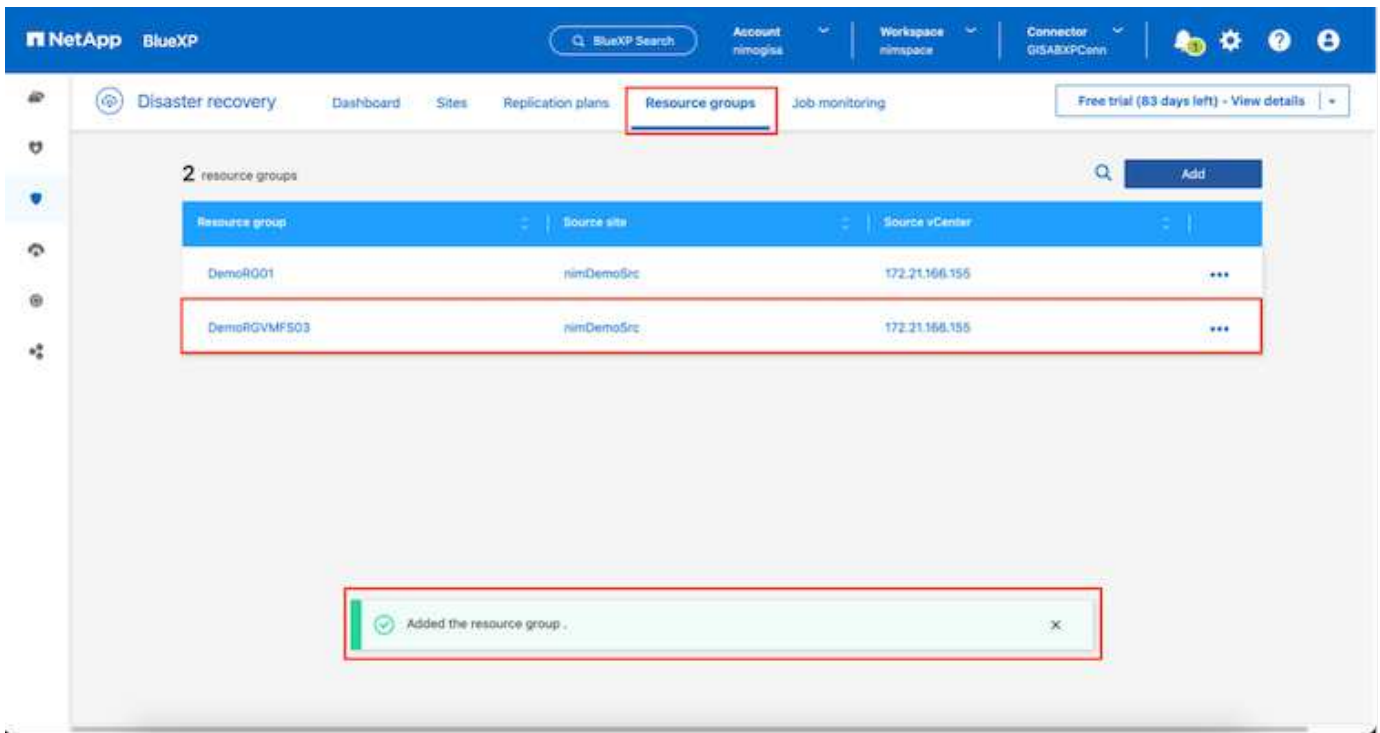
Abgesehen von den oben genannten Ansätzen kann die SnapMirror Replikation auch über ONTAP CLI oder System Manager erstellt werden. Unabhängig vom Ansatz, der zum Synchronisieren der Daten mit SnapMirror verwendet wird, orchestriert BlueXP DRaaS den Workflow für nahtlose und effiziente Disaster-Recovery-Vorgänge.

## Was kann BlueXP disaster recovery für Sie tun?

Nachdem die Quell- und Zielsites hinzugefügt wurden, führt die BlueXP disaster recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Die BlueXP disaster recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen und füllt sie.

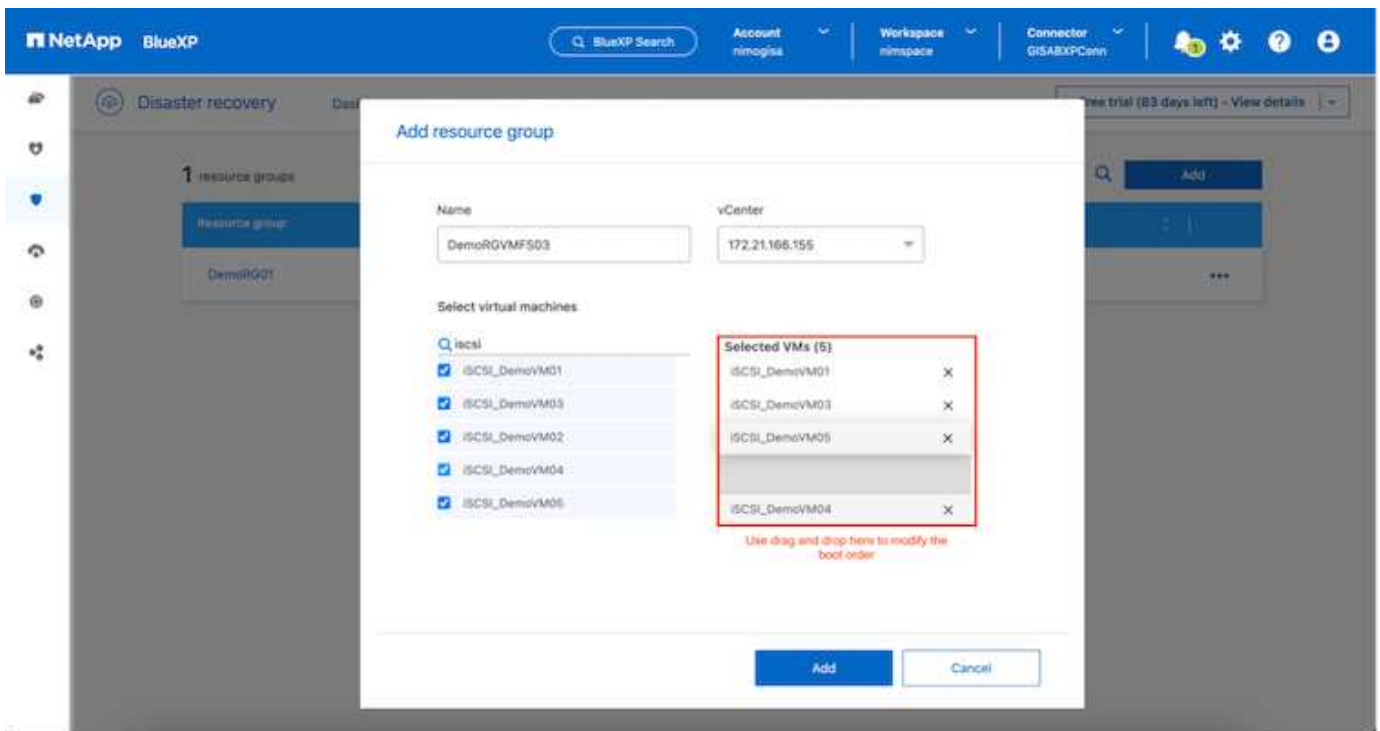


Nachdem die Sites hinzugefügt wurden, können VMs in Ressourcengruppen gruppiert werden. Mit den BlueXP disaster recovery können Sie eine Reihe abhängiger VMs in logische Gruppen gruppieren, die ihre Startreihenfolgen und Startverzögerungen enthalten, die bei der Wiederherstellung ausgeführt werden können. Um mit der Erstellung von Ressourcengruppen zu beginnen, navigieren Sie zu **Ressourcengruppen** und klicken Sie auf **Neue Ressourcengruppe erstellen**.



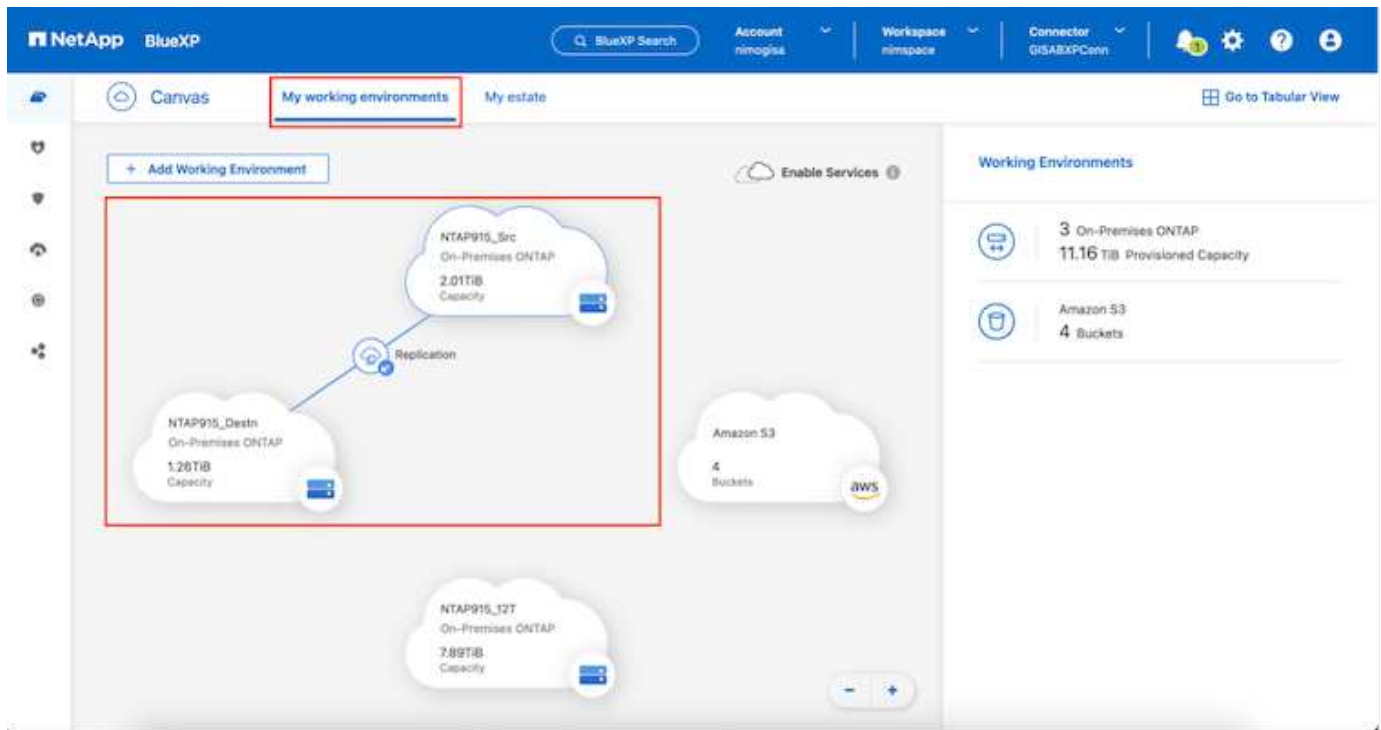
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

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



Sobald die Ressourcengruppen erstellt sind, besteht der nächste Schritt darin, den Ausführungsentwurf oder einen Plan zur Wiederherstellung virtueller Maschinen und Anwendungen im Katastrophenfall zu erstellen. Wie in den Voraussetzungen erwähnt, kann die SnapMirror Replikation im Voraus konfiguriert werden, oder DRaaS kann sie mithilfe des RPO und der Aufbewahrungsanzahl konfigurieren, die bei der Erstellung des

Replikationsplans angegeben wurden.



NetApp BlueXP

Replication

6 Volume Relationships

495.27 GiB Replicated Capacity

0 Currently Transferring

6 Healthy

0 Failed

Volume Relationships (6)

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_ISCSI_DS01 NTAP915_Src	Src_ISCSI_DS01_cp NTAP915_Destn	20 seconds	idle	snapmirrored	Jul 12, 2024, 4:24:34 22.35 MiB
✓	Src_ISCSI_DS03 NTAP915_Src	Src_ISCSI_DS03_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 254.89 MiB

Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und der Zuordnung von Clustern und Netzwerken. Um den Wiederherstellungsplan zu definieren, navigieren Sie zur Registerkarte **Replikationsplan** und klicken Sie auf **Plan hinzufügen**.

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

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPConn

Add replication plan 1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

Replication plan name  
DemoRPMFS03

Select a source vCenter where your data exists, to replicate to the selected target vCenter.

Source vCenter  
172.21.166.155

Target vCenter  
Select a target vCenter  
172.21.166.155 nimDemoSrc  
172.21.166.190 nimDemoDest

Cancel Next

Der nächste Schritt besteht darin, vorhandene Ressourcengruppen auszuwählen. Wenn keine Ressourcengruppen erstellt wurden, hilft der Assistent dabei, die erforderlichen virtuellen Maschinen basierend auf den Wiederherstellungszielen zu gruppieren (im Wesentlichen funktionale Ressourcengruppen zu erstellen). Dies hilft auch dabei, die Vorgangsreihenfolge für die Wiederherstellung virtueller Anwendungsmaschinen zu definieren.

NetApp BlueXP

BlueXP Search Account nimogisa Workspace nimspace Connector GISABXPConn

Add replication plan 1 vCenter servers 2 Applications 3 Resource mapping 4 Recurrence 5 Review

172.21.166.155 nimDemoSrc 172.21.166.190 nimDemoDest

Virtual machines Resource groups

Search resource groups  
DemoRG01  
DemoRGVMS03

Selected resource groups to replicate  
Selected resource group (1)  
DemoRGVMS03

Previous Next



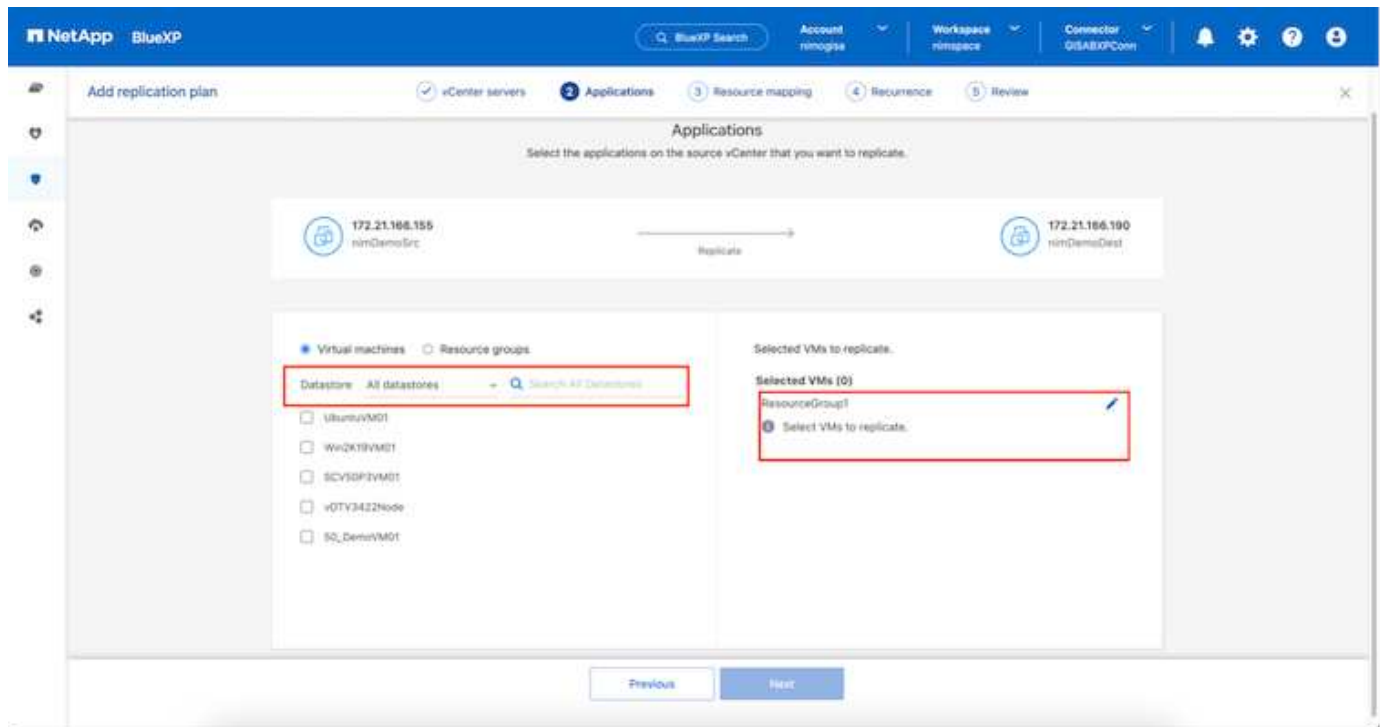
Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.





Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

Der folgende Screenshot zeigt die Option zum Filtern virtueller Maschinen oder bestimmter Datenspeicher basierend auf organisatorischen Anforderungen, wenn nicht zuvor Ressourcengruppen erstellt wurden.



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 und virtuelle Netzwerke. IP-Anpassung, Pre- und Post-Skripte, Boot-Verzögerungen, Anwendungskonsistenz und so weiter. Ausführliche Informationen finden Sie unter ["Erstellen eines Replikationsplans"](#).



**Virtual machines**

IP address type: Static Target IP: Same as source

☐ Use the same credentials for all VMs

☐ Use the same script for all VMs

Source VM	CPUs	RAM	Boot delay (mins between 0 and 10)	Create application consistent replicas	Scripts
DemoR001					
S0_DemoVM	2	4 GiB	0	<input type="checkbox"/>	None
S0_DemoVM01	2	4 GiB	0	<input type="checkbox"/>	None
S0_DemoVM02	2	4 GiB	0	<input type="checkbox"/>	None

Previous Next



Standardmäßig werden für Test- und Failovervorgänge dieselben Zuordnungsparameter verwendet. Um verschiedene Zuordnungen für die Testumgebung anzuwenden, wählen Sie die Option „Testzuordnung“ aus, nachdem Sie das Kontrollkästchen wie unten gezeigt deaktiviert haben:

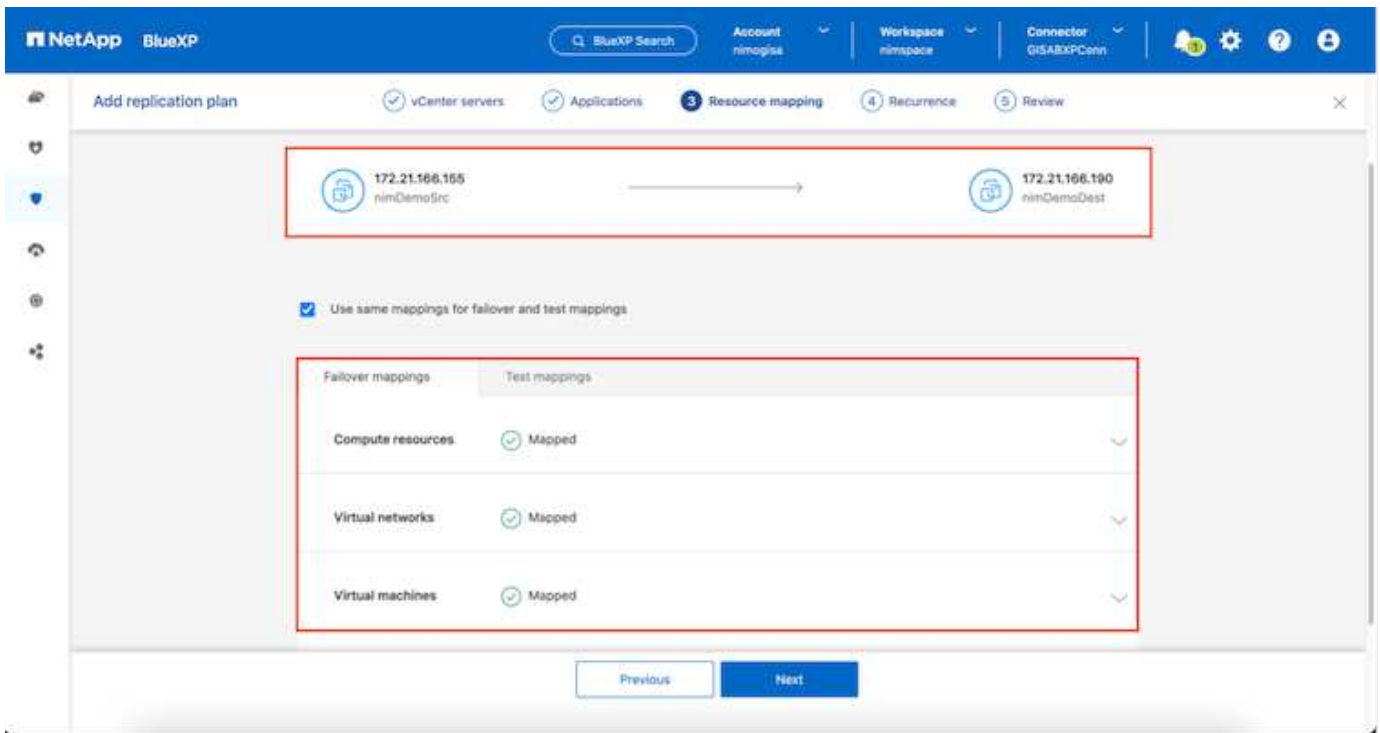
**Resource mapping**  
Specify how resources map from the source to the target.

172.21.166.155 nrmDemoSrc → 172.21.166.190 nrmDemoDest

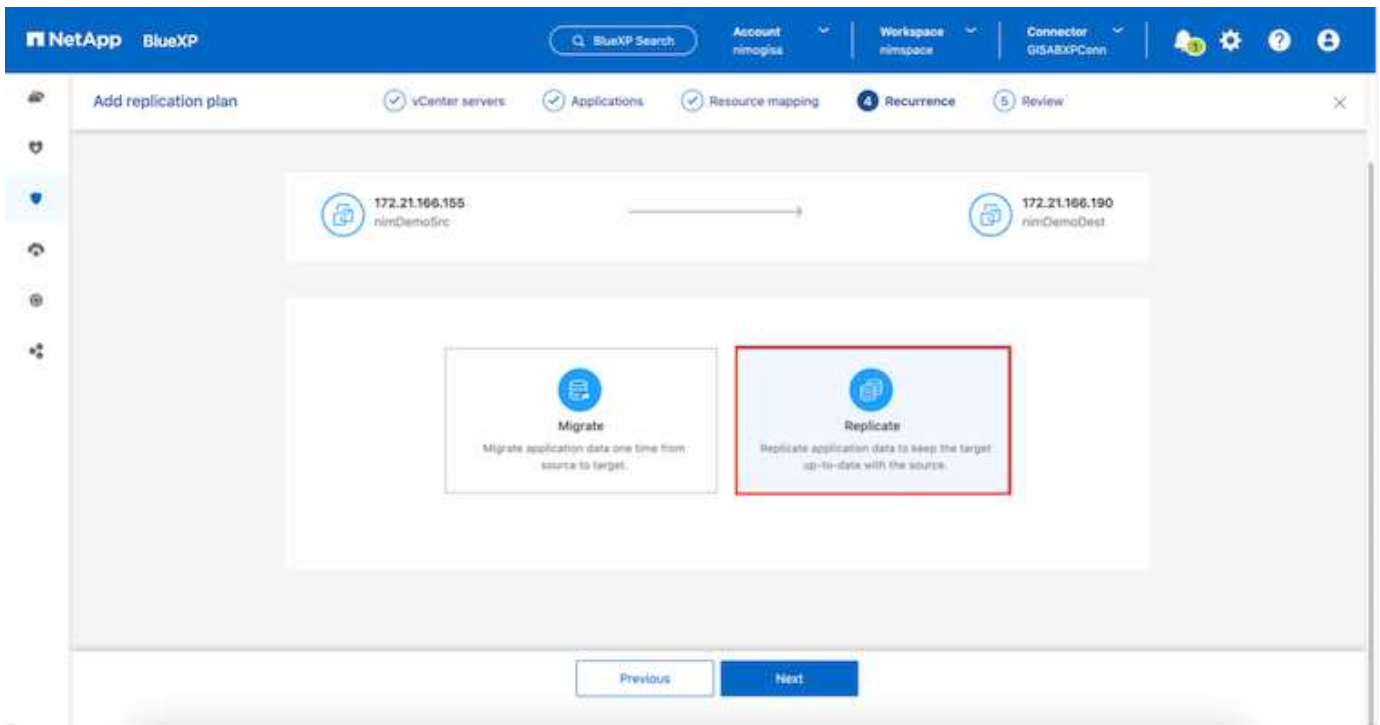
☒ Use same mappings for failover and test mappings

Failover mappings Test mappings

Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.



Wählen Sie den Wiederholungstyp aus. Einfach ausgedrückt: Wählen Sie „Migrieren“ (einmalige Migration mit Failover) oder die Option „Wiederkehrende kontinuierliche Replikation“. In dieser exemplarischen Vorgehensweise ist die Option „Replizieren“ ausgewählt.



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

**NetApp BlueXP**

BlueXP Search Account nimoglas Workspace nimspace Connector GISABXPConn

Add replication plan vCenter servers Applications Resource mapping Recurrence **5 Review**

172.21.166.155 nimDemoSrc Replicate 172.21.166.190 nimDemoDest

Plan details Failover mapping Virtual machines

Plan name: DemoRPVMFS03

Recurrence: Replicate

Previous Add plan

**NetApp BlueXP**

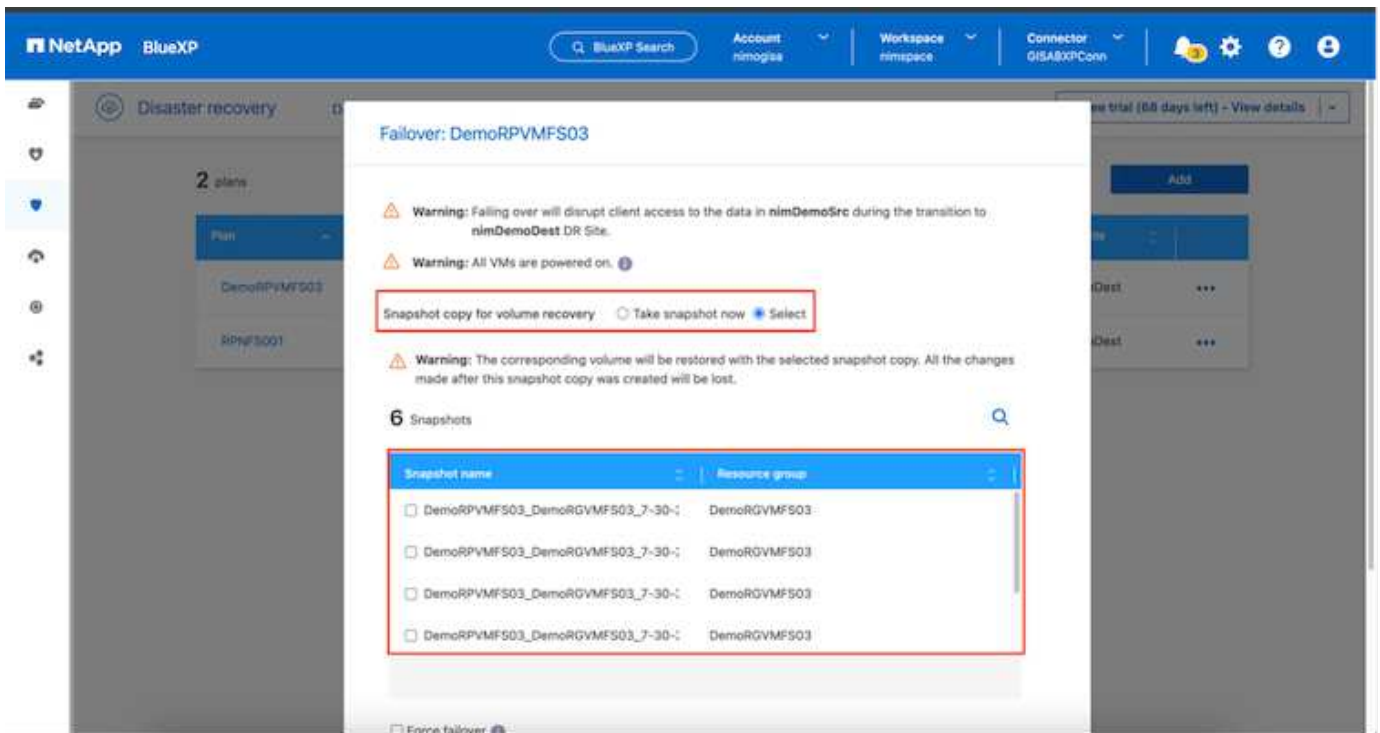
BlueXP Search Account nimoglas Workspace nimspace Connector GISABXPConn

Disaster recovery Dashboard Sites **Replication plans** Resource groups Job monitoring Free trial (63 days left) - View details

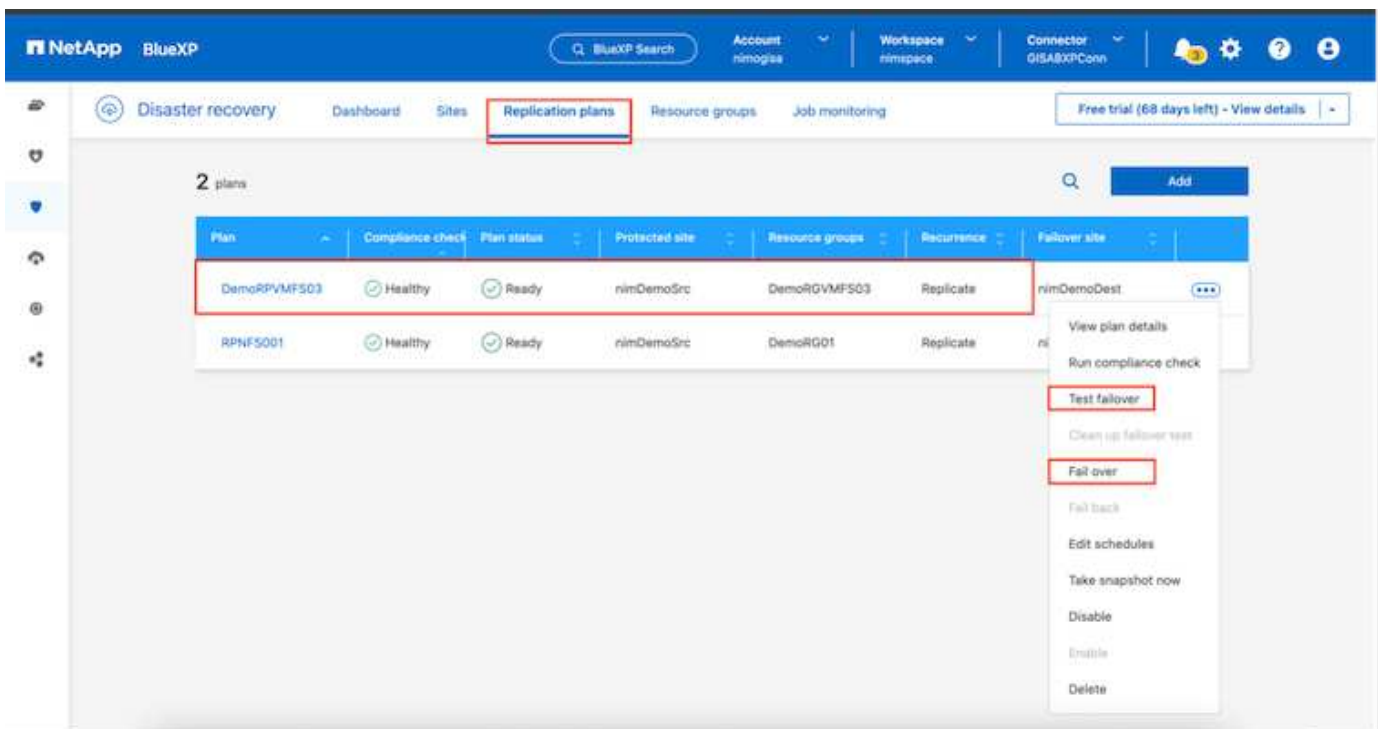
2 plans

Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site	
DemoRPVMFS03	Healthy	Ready	nimDemoSrc	DemoRGVMFS03	Replicate	nimDemoDest	...
RPHFS001	Healthy	Ready	nimDemoSrc	DemoRG01	Replicate	nimDemoDest	...

Sobald der Replikationsplan erstellt ist, kann je nach Bedarf ein Failover durchgeführt werden, indem die Failover-Option, die Test-Failover-Option oder die Migrationsoption ausgewählt wird. BlueXP disaster recovery stellt sicher, dass der Replikationsprozess planmäßig alle 30 Minuten ausgeführt wird. Während der Failover- und Test-Failover-Optionen können Sie die aktuellste SnapMirror -Snapshot-Kopie verwenden oder eine bestimmte Snapshot-Kopie aus einer Point-in-Time-Snapshot-Kopie auswählen (gemäß der Aufbewahrungsrichtlinie von SnapMirror). Die Point-in-Time-Option kann sehr hilfreich sein, wenn es zu einem Korruptionsereignis wie Ransomware kommt, bei dem die aktuellsten Replikate bereits kompromittiert oder verschlüsselt sind. BlueXP disaster recovery zeigt alle verfügbaren Wiederherstellungspunkte an.



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



## Was passiert während eines Failovers oder Test-Failover-Vorgangs?

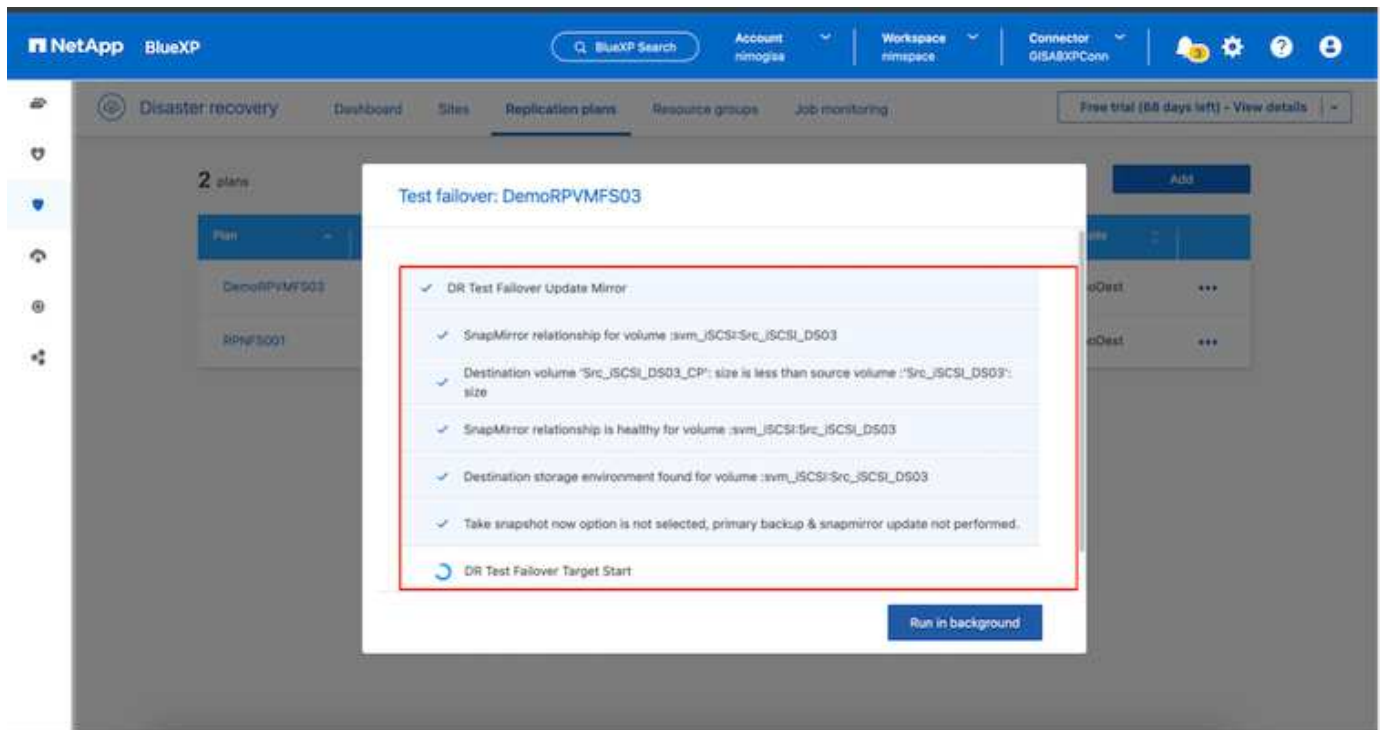
Während eines Test-Failover-Vorgangs erstellt die BlueXP disaster recovery mithilfe der neuesten Snapshot-Kopie oder eines ausgewählten Snapshots des Ziel-Volumes ein FlexClone -Volume auf dem Ziel ONTAP -Speichersystem.



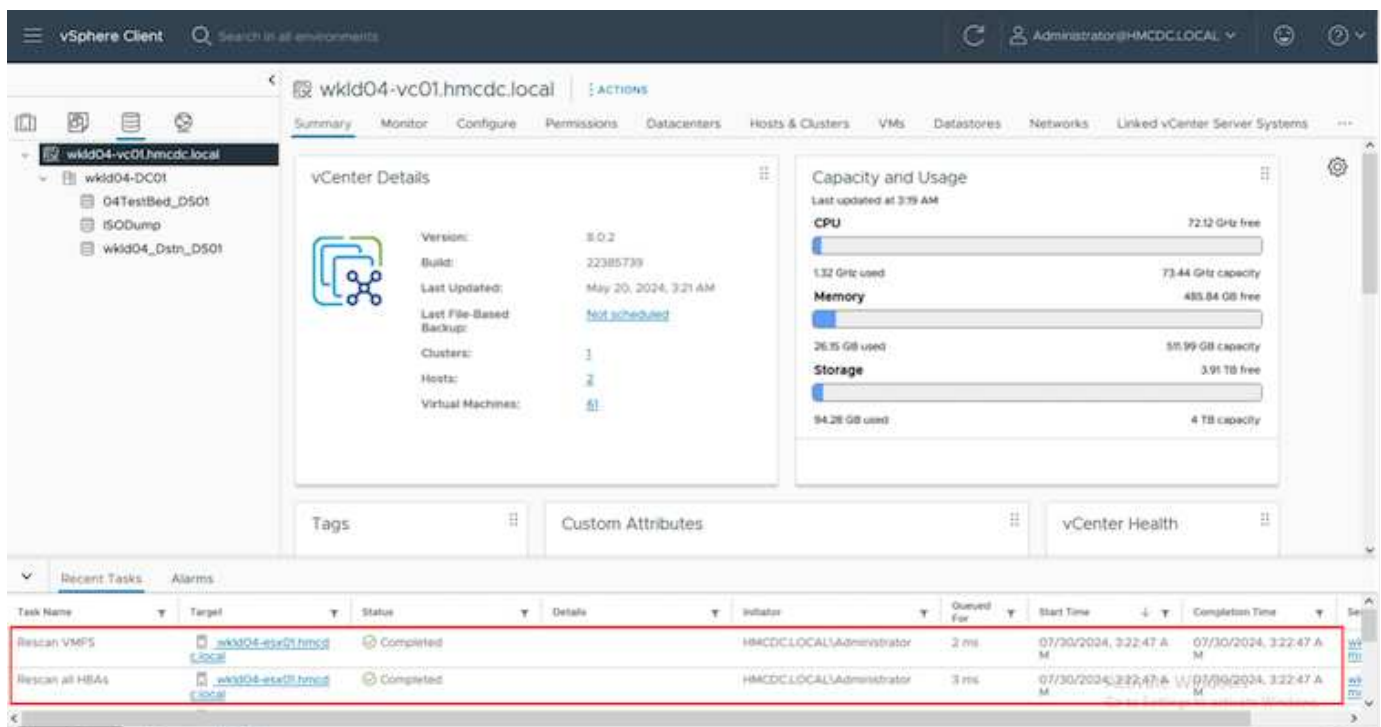
Ein Test-Failover-Vorgang erstellt ein geklontes Volume auf dem Ziel ONTAP -Speichersystem.

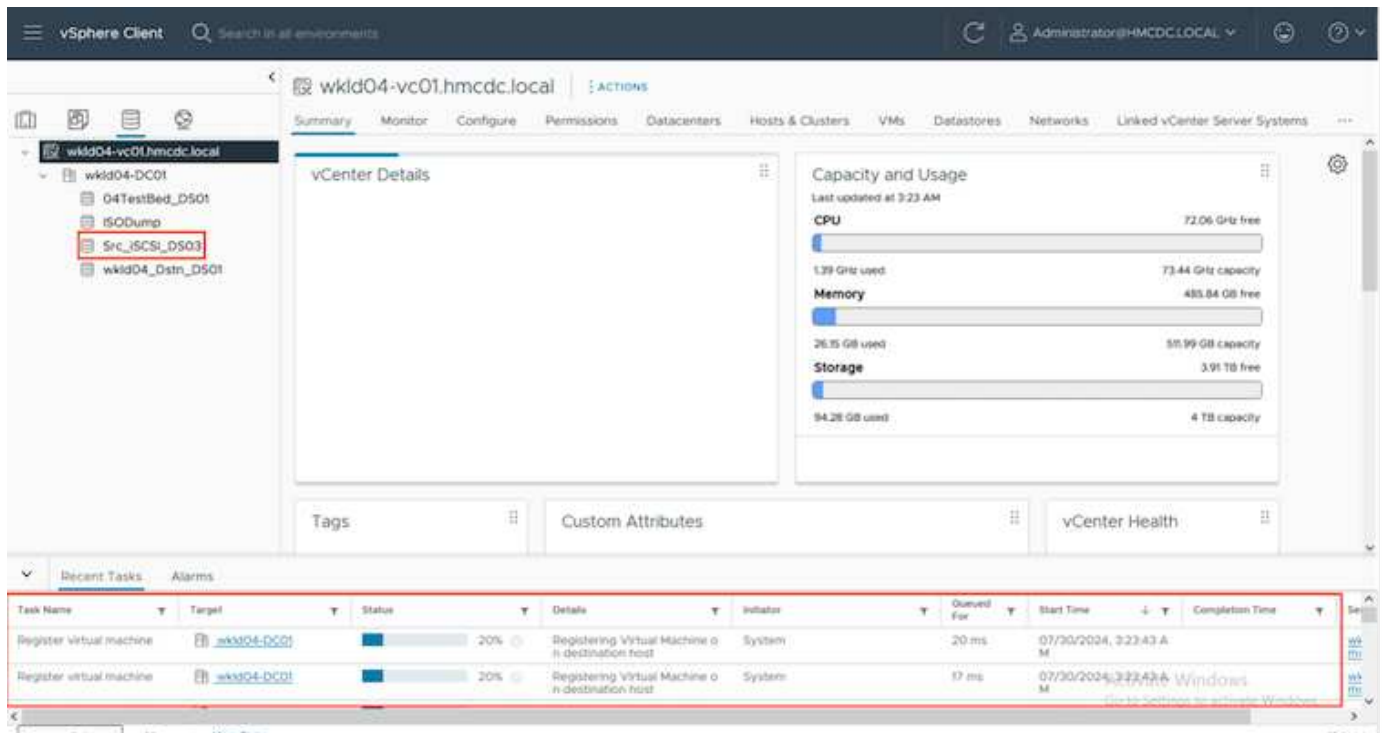


Das Ausführen eines Testwiederherstellungsvorgangs hat keine Auswirkungen auf die SnapMirror Replikation.



Während des Vorgangs ordnet BlueXP disaster recovery das ursprüngliche Zielvolume nicht zu. Stattdessen wird aus dem ausgewählten Snapshot ein neues FlexClone Volume erstellt und ein temporärer Datenspeicher, der das FlexClone Volume unterstützt, wird den ESXi-Hosts zugeordnet.



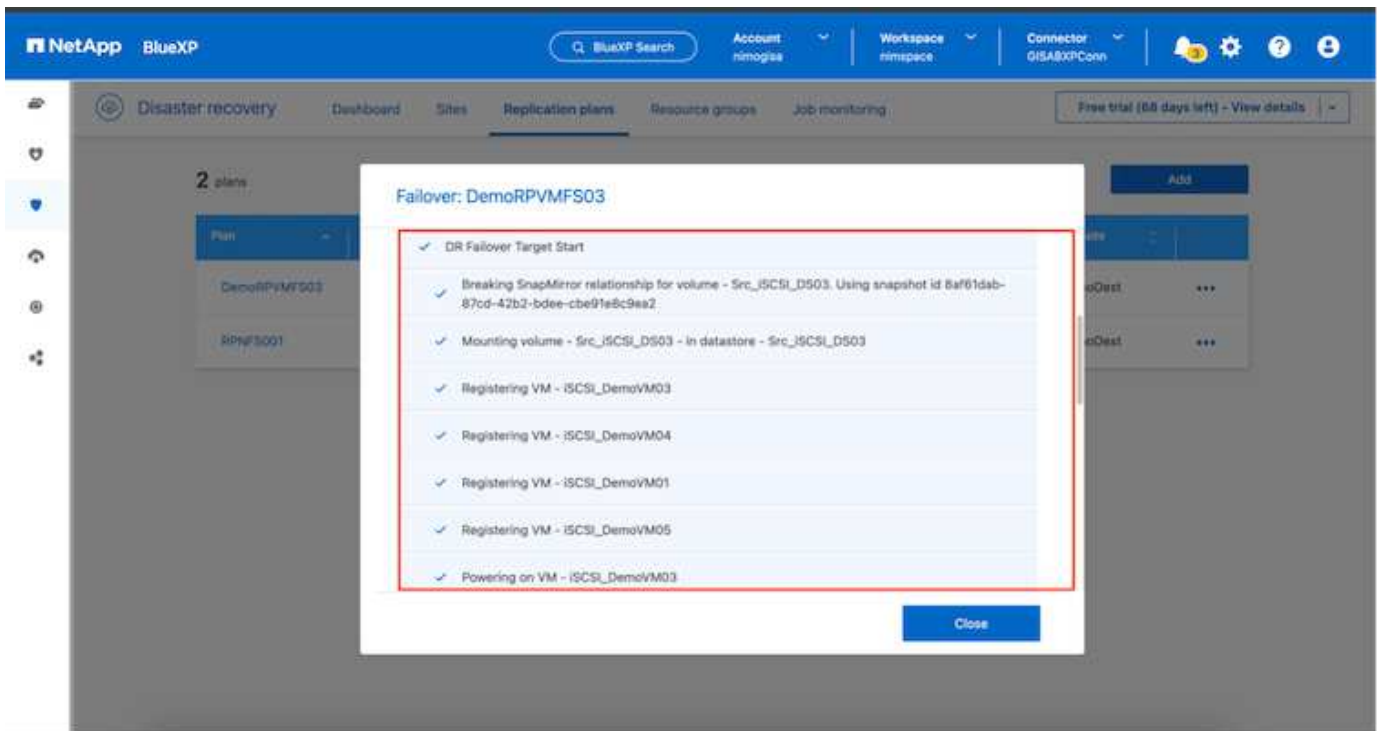


Wenn der Test-Failover-Vorgang abgeschlossen ist, kann der Bereinigungsverfahren mit **"Failover-Test bereinigen"** ausgelöst werden. Während dieses Vorgangs zerstört die BlueXP disaster recovery das FlexClone -Volume, das bei diesem Vorgang verwendet wurde.

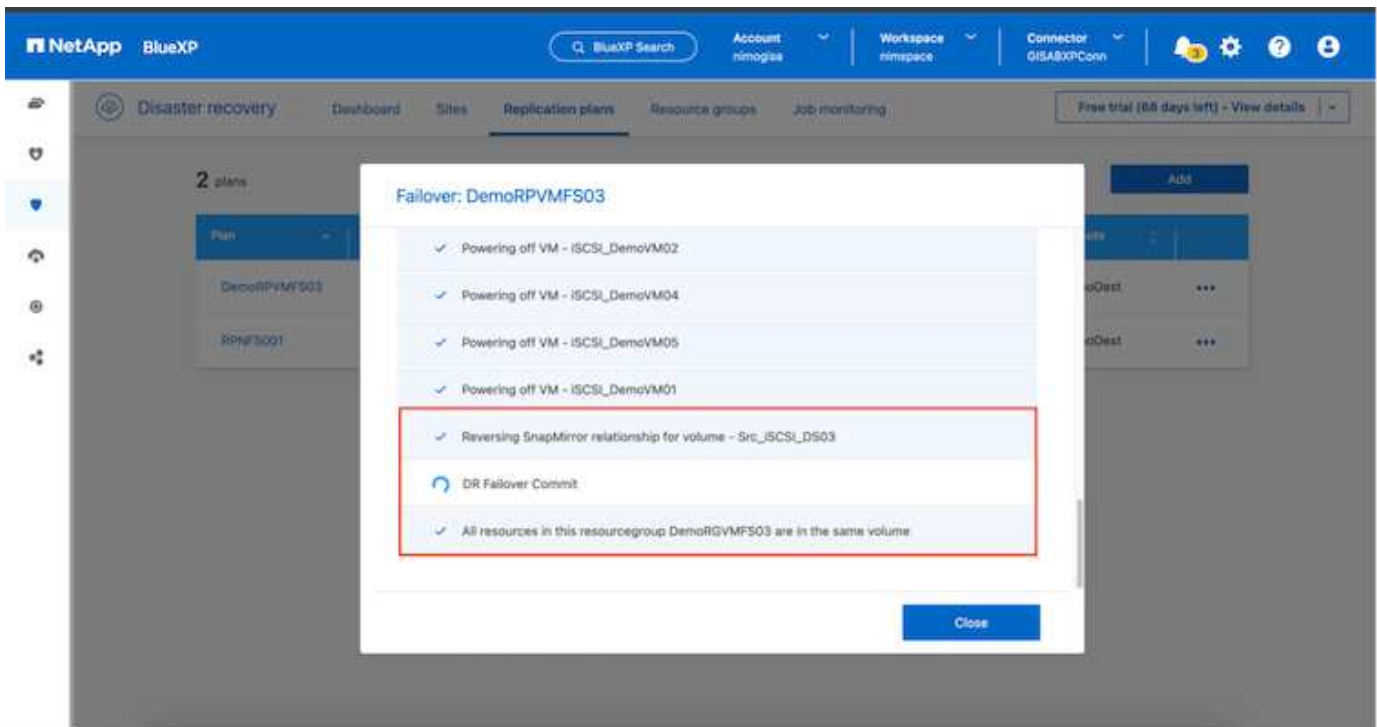
Im Falle eines echten Katastrophenfalls führt die BlueXP disaster recovery die folgenden Schritte aus:

1. Bricht die SnapMirror -Beziehung zwischen den Sites ab.
2. Mountet das VMFS-Datenspeichervolume nach der Neusignierung zur sofortigen Verwendung.
3. Registrieren der VMs
4. VMs einschalten





Sobald die primäre Site betriebsbereit ist, ermöglicht die BlueXP disaster recovery die umgekehrte Neusynchronisierung für SnapMirror und ermöglicht ein Failback, das ebenfalls per Mausklick ausgeführt werden kann.

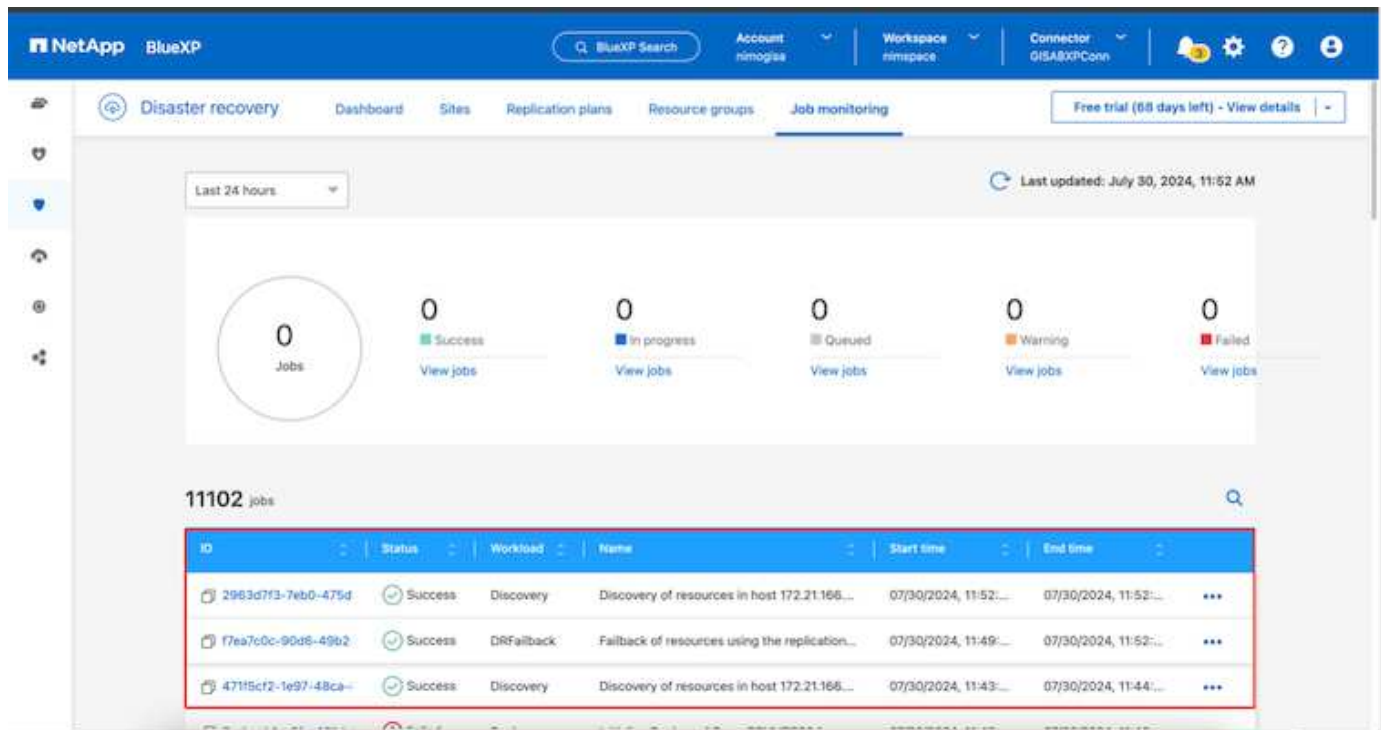


Und wenn die Migrationsoption gewählt wird, wird dies als geplantes Failover-Ereignis betrachtet. In diesem Fall wird ein zusätzlicher Schritt ausgelöst, der darin besteht, die virtuellen Maschinen am Quellstandort herunterzufahren. Die restlichen Schritte bleiben dieselben wie beim Failover-Ereignis.

Von BlueXP oder der ONTAP CLI aus können Sie den Replikationszustand für die entsprechenden Datenspeichervolumen überwachen und den Status eines Failovers oder Testfailovers über die



Jobüberwachung verfolgen.



Dies bietet eine leistungsstarke Lösung zur Handhabung eines maßgeschneiderten und individuellen Notfallwiederherstellungsplans. Das Failover kann als geplantes Failover oder per Mausklick erfolgen, wenn ein Notfall eintritt und die Entscheidung zur Aktivierung der DR-Site getroffen wird.

Um mehr über diesen Prozess zu erfahren, können Sie sich gerne das ausführliche Walkthrough-Video ansehen oder die "[Lösungssimulator](#)".

## Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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, BEISPIELHAFTE 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.