



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
Fallback	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 Klonen, 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 Fallback 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

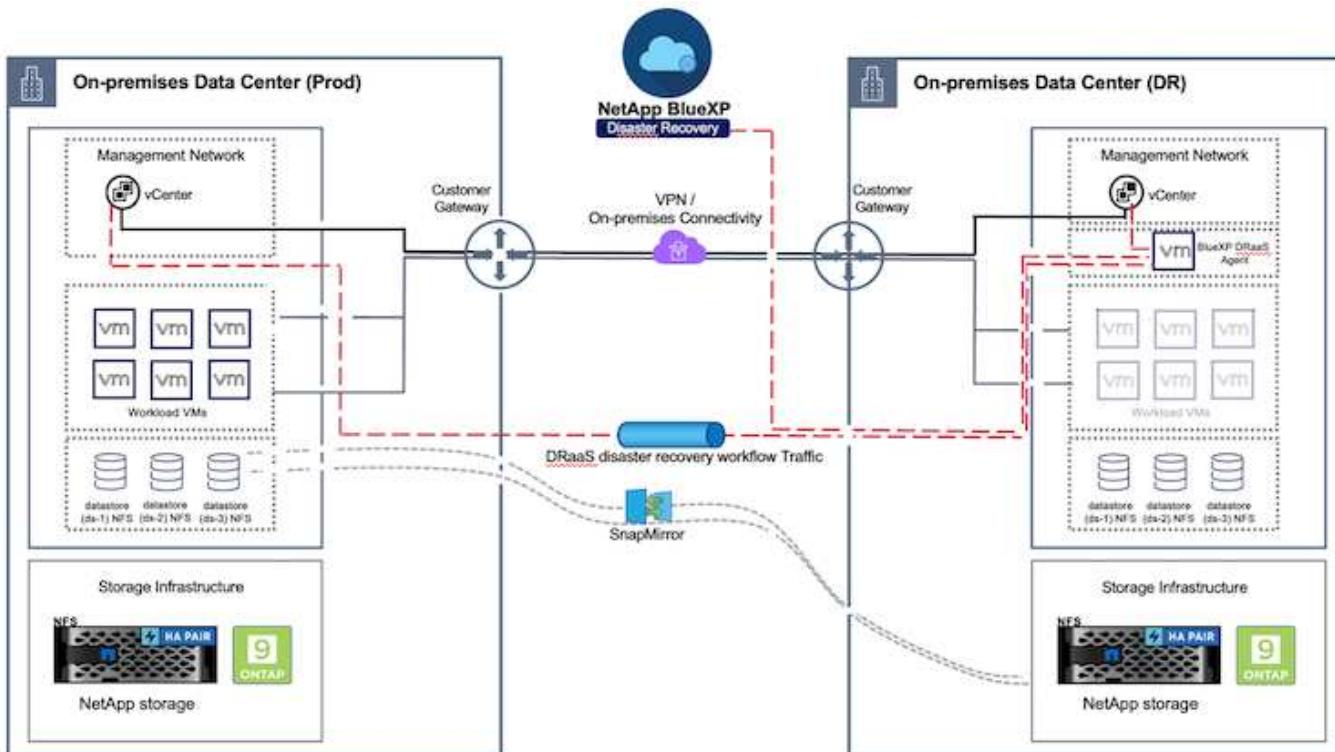
Die Implementierung einer Notfallwiederherstellung durch Blockreplikation vom Produktionsstandort zum Notfallwiederherstellungsstandort ist eine robuste und kostengünstige Methode zum Schutz von Workloads vor Standortausfällen und Datenbeschädigungen, wie beispielsweise Ransomware-Angriffen. Mithilfe 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 Specherebene, 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.

The screenshot shows the NetApp BlueXP dashboard. On the left, there is a navigation menu with several categories: Storage, Health, Protection, Backup and recovery (which has a sub-section for Disaster recovery highlighted with a red box), Replication, Ransomware protection, Governance, Mobility, and Extensions. The main content area is divided into several sections: a summary of issues (2 Unreached, 0 Down, 0 Issues), a list of replication plans (1 Ready, 2 Failed), a list of jobs (Backup job for Replication Plan DemoRP004, Initialize Backup of DemoRP004 for every 5 minutes, etc.), and metrics for protected (21) and unprotected (117) VMs, as well as failovers (1), fallbacks (1), test failovers (2), and migrations (0).

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 Datenspeichervolumes 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.



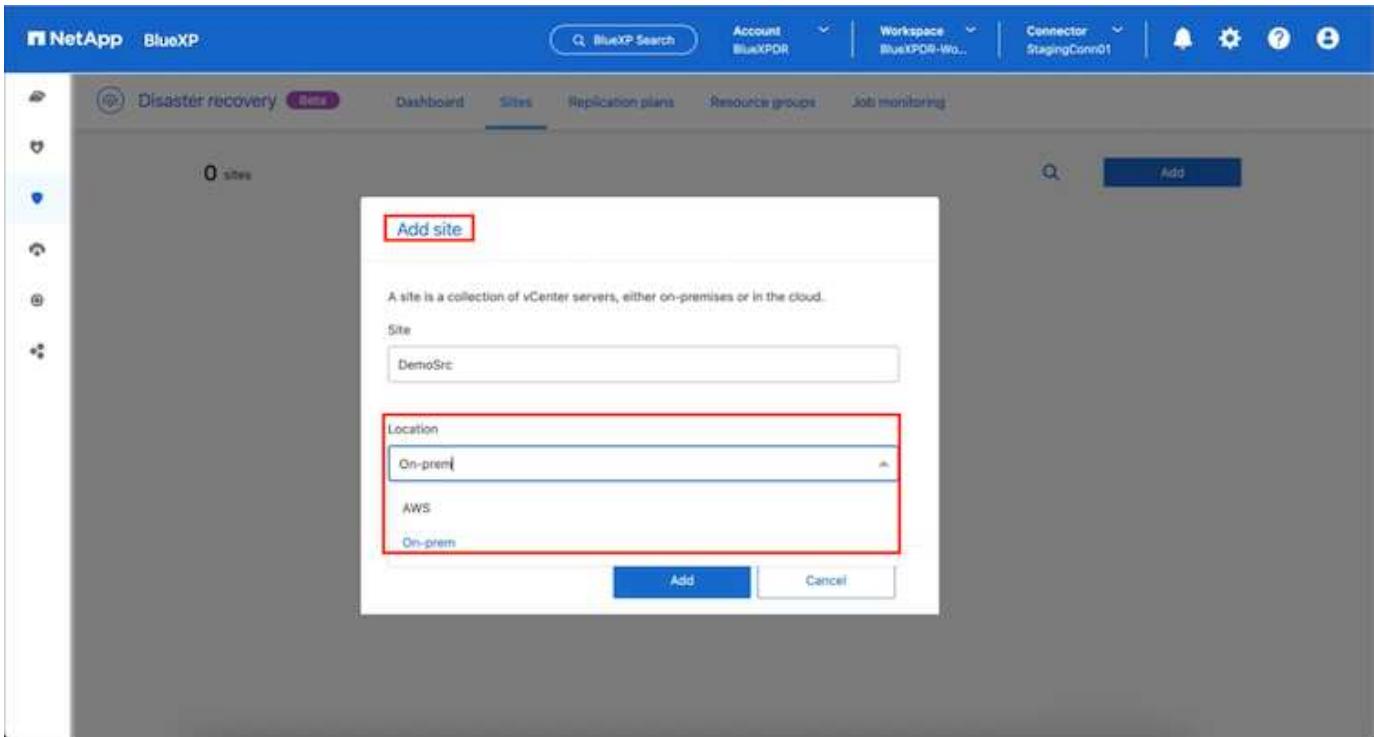
NetApp empfiehlt, den BlueXP Connector am Zielstandort oder an einem dritten Standort bereitzustellen, damit der BlueXP Connector über das Netzwerk mit Quell- und Zielressourcen kommunizieren kann.

The screenshot shows the NetApp BlueXP Disaster Recovery interface. At the top, there are tabs for Disaster recovery, Dashboard, Sites, Replication plans, Resource groups, and Job monitoring. A banner indicates a free trial with 68 days left. The main area displays various metrics: 2 Running sites, 0 Downt sites, 0 Issue sites; 2 Ready replication plans, 0 Failed replication plans; 2 Resource groups, 16 Protected VMs, 117 Unprotected VMs; and 1 Failovers, 1 Failbacks, 1 Test failovers, 0 Migrations. To the right, an 'Activity' section lists recent events: 'Backup job for Replication Plan DemoRPVMS03 in progress', 'Initialize Backup of DemoRPVMS03 for every 10 minutes 7 s ago', 'Discovery of resources in host 172.21.166.190 41 s ago', 'Failback of resources using the replication plan 'DemoRPVMS03' 0.6 s ago', and 'Discovery of resources in host 172.21.166.190 9 m ago'. A 'View all jobs' link is also present.

BlueXP disaster recovery

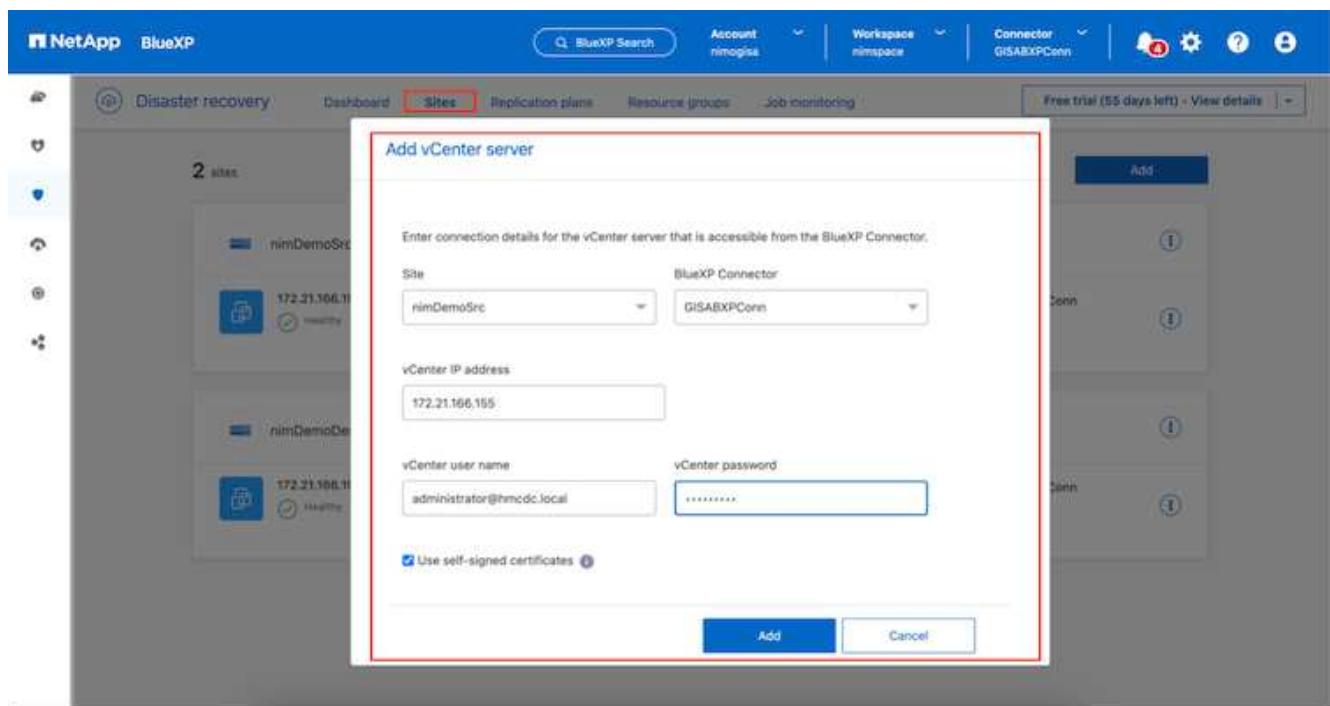
Der erste Schritt bei der Vorbereitung der Notfallwiederherstellung besteht darin, die lokalen vCenter- und Speicherressourcen zu ermitteln und zur BlueXP disaster recovery hinzuzufügen.

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**.

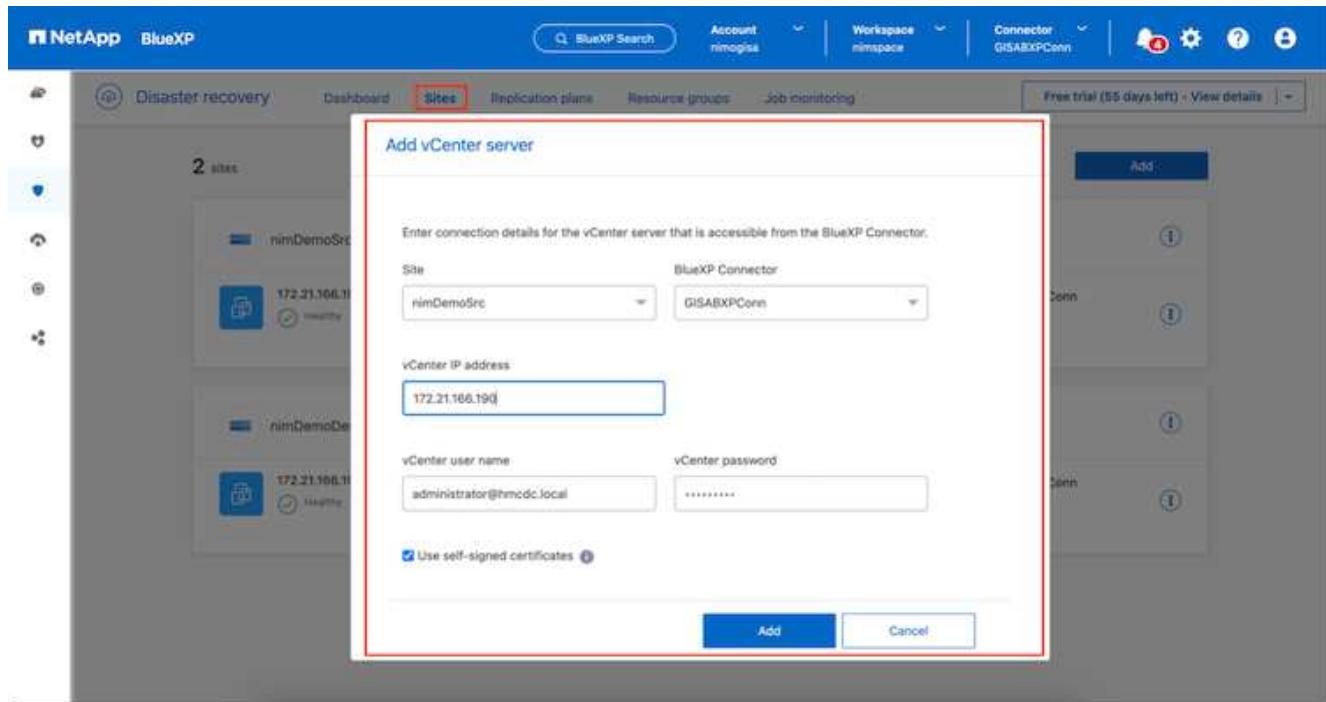


Fügen Sie die folgenden Plattformen hinzu:

- **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.

i 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?

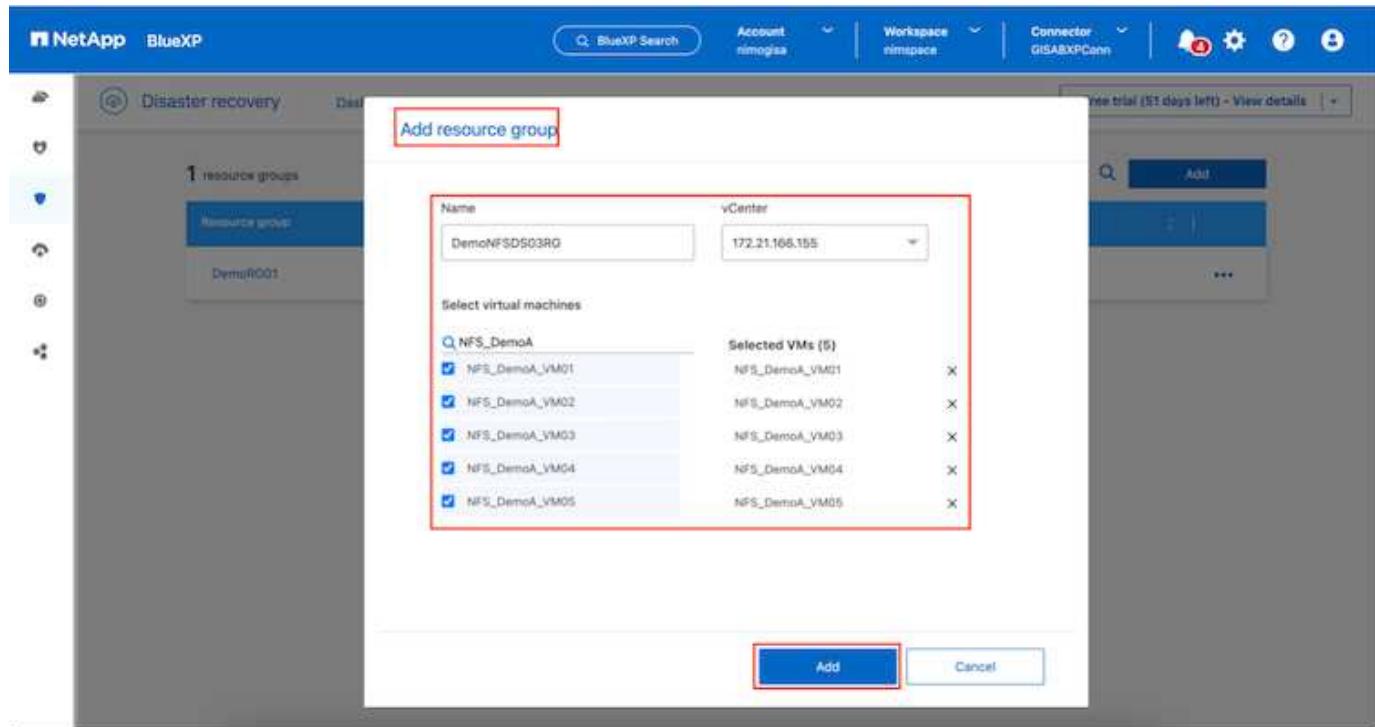
Nachdem die Quell- und Zielsites hinzugefügt wurden, führt die BlueXP disaster recovery eine automatische Tiefenerkennung durch und zeigt die VMs zusammen mit den zugehörigen Metadaten an. Die BlueXP disaster recovery erkennt außerdem automatisch die von den VMs verwendeten Netzwerke und Portgruppen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

The screenshot shows the NetApp BlueXP Disaster Recovery interface. At the top, there's a navigation bar with tabs: Disaster recovery, Dashboard, **Sites**, Replication plans, Resource groups, and Job monitoring. A search bar says "BlueXP Search". On the right, it shows "Account nimagis", "Workspace nimspace", "Connector GISABXPConn", and a "Free trial (83 days left) - View details" button. Below the navigation, it says "2 sites". There are two entries: "nimDemoSrc" and "nimDemoDest". Each entry has a summary table:

	172.21.166.155	72	13	1	GISABXPConn
VMs	Healthy	VMS	Datastores	Resource groups	Connector

Below each entry is a blue "Edit" icon.

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**.



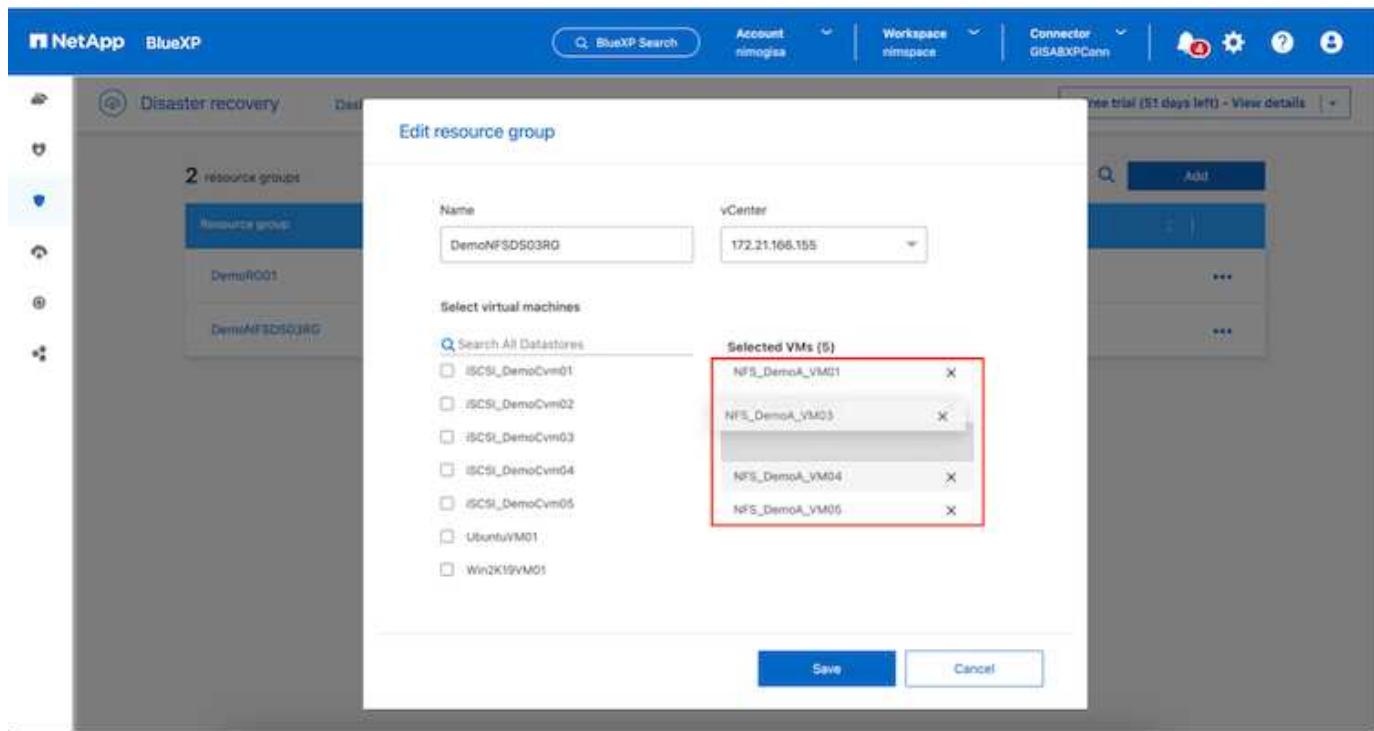
Resource groups

Resource group	Source site	Source vCenter
DemoRG01	nimDemoSrc	172.21.166.155
DemoNFSDS03RG	nimDemoSrc	172.21.166.155

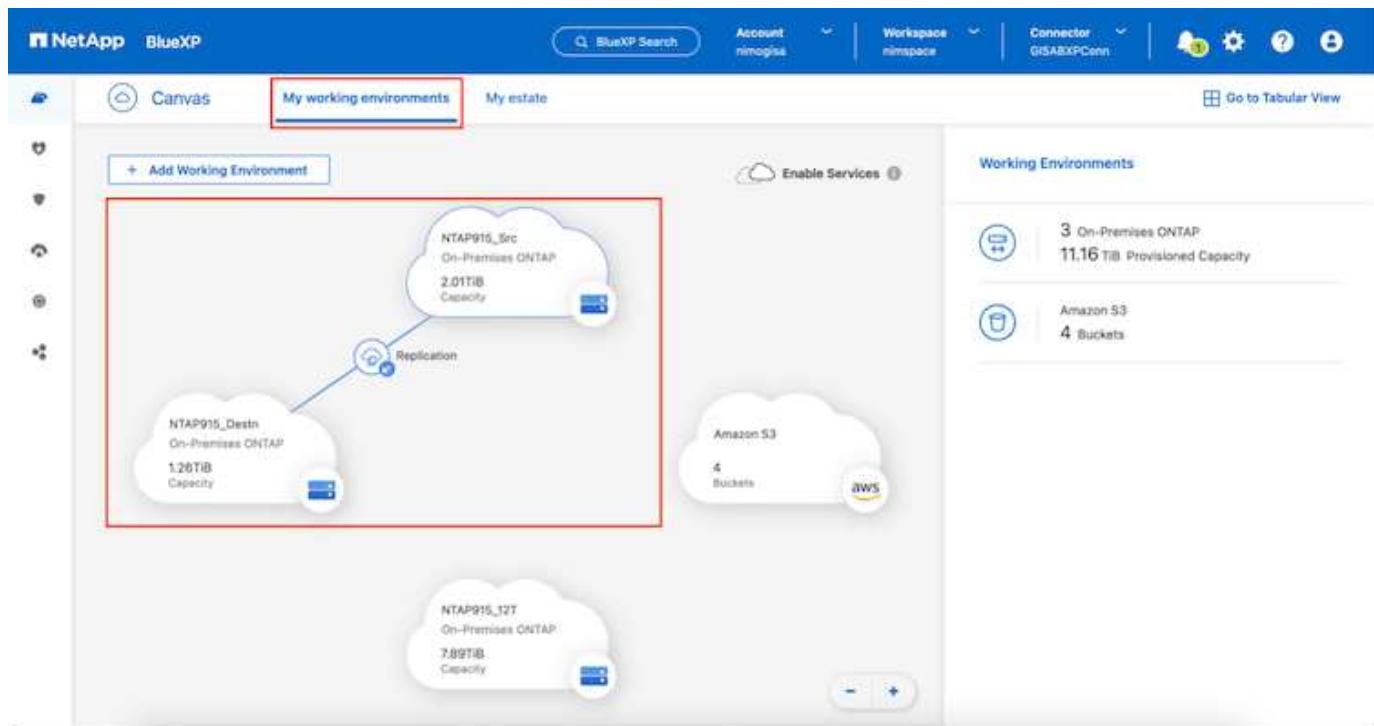


Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

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.



The screenshot shows the NetApp BlueXP interface with the 'Replication' tab selected. The main area displays a table titled 'Volume Relationships (8)'. The columns are: Health Status, Source Volume, Target Volume, Total Transfer Time, Status, Mirror State, and Last Successful Transfer. The table lists several replication pairs, with the fourth row (Src_NFS_DS03 to Src_NFS_DS03_Copy) highlighted by a red border.

Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful Transfer
Green	NTAP915_Src	NTAP915_Destn	24.5 min	idle	snapmirrored	
Green	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:16:38 386.63 MB
Green	Src_25G_Vol01 NTAP915_Src	Src_25G_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:23:59 79.23 MB
Green	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_Copy NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12:24:54 24.84 MB
Green	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_Copy NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12:47.38 MB
Green	Src_iSCSI_DS04 NTAP915_Src	Src_iSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:48.87 MB
Green	nimbra NTAP915_Src	nimbra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12:48.98 KIB

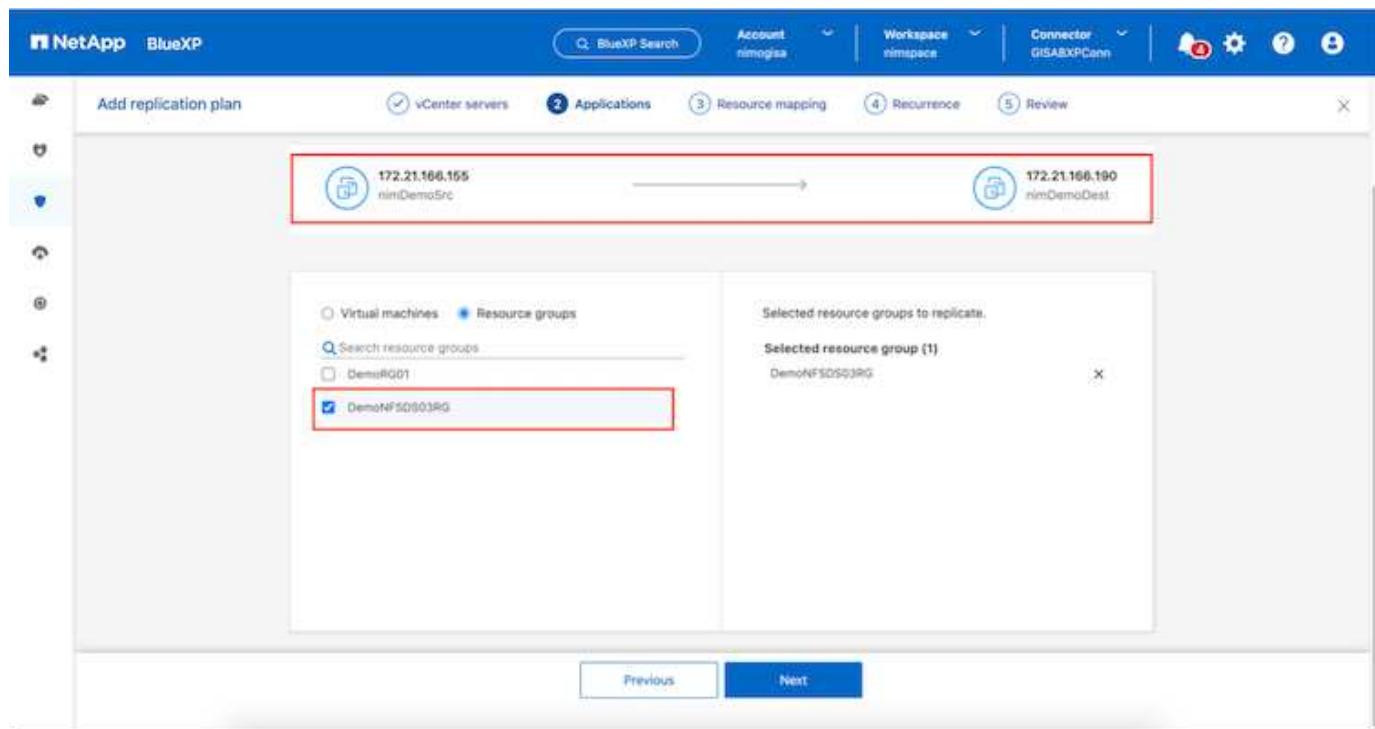
Konfigurieren Sie den Replikationsplan, indem Sie die Quell- und Ziel-vCenter-Plattformen aus der Dropdown-Liste auswählen und die Ressourcengruppen auswählen, die in den Plan aufgenommen werden sollen, zusammen mit der Gruppierung, wie Anwendungen wiederhergestellt und eingeschaltet werden sollen, und 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.

The screenshot shows the 'Add replication plan' wizard in step 1: vCenter servers. The interface includes tabs for 'vCenter servers', 'Applications', 'Resource mapping', 'Recurrence', and 'Review'. A red box highlights the 'Replication plan name' field, which contains 'DemoNFSDS03RP'. Another red box highlights the 'Source vCenter' and 'Target vCenter' selection fields, both set to '172.21.166.155'. The 'Next' button at the bottom right is also highlighted with a red box.

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.

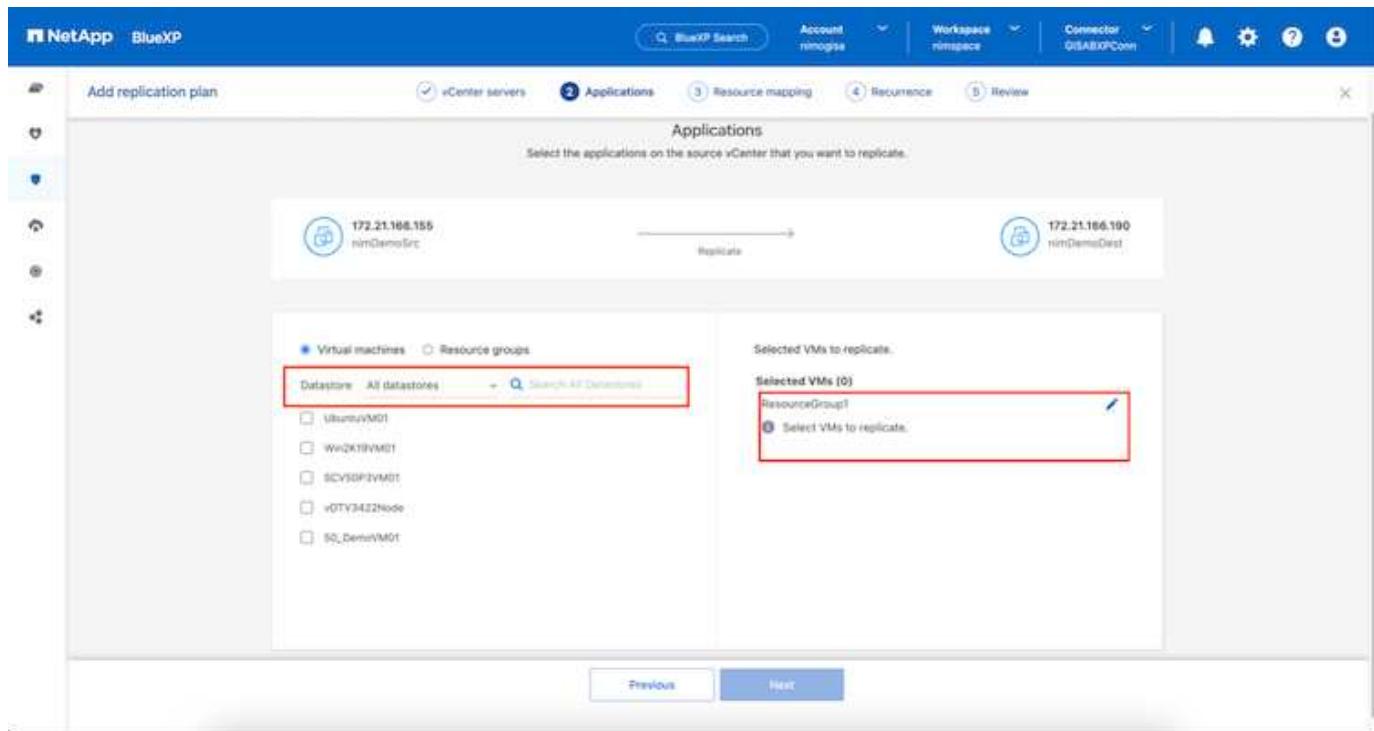


Die Ressourcengruppe ermöglicht das Festlegen der Startreihenfolge per Drag-and-Drop-Funktion. Damit lässt sich die Reihenfolge, in der die VMs während des Wiederherstellungsprozesses eingeschaltet werden, einfach ändern.

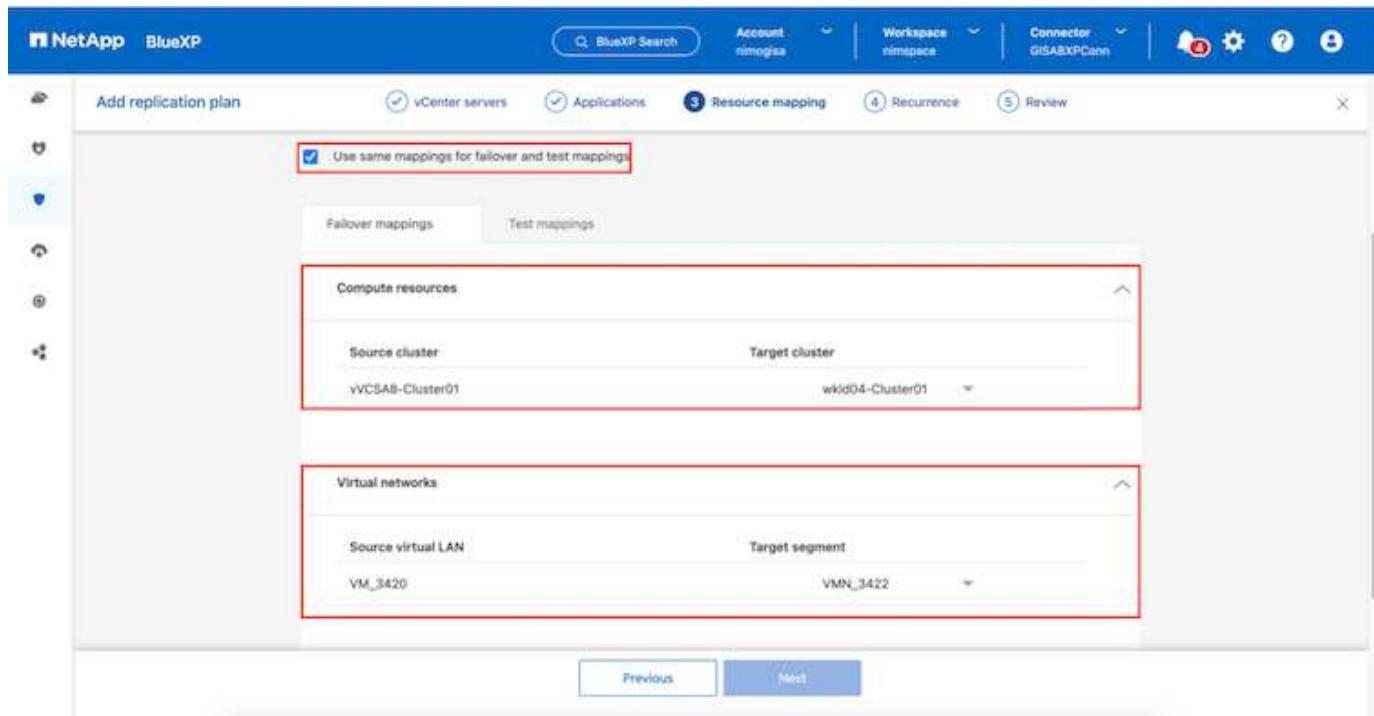


Jede virtuelle Maschine innerhalb einer Ressourcengruppe wird der Reihe nach basierend auf der Reihenfolge gestartet. Zwei Ressourcengruppen werden parallel gestartet.

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:

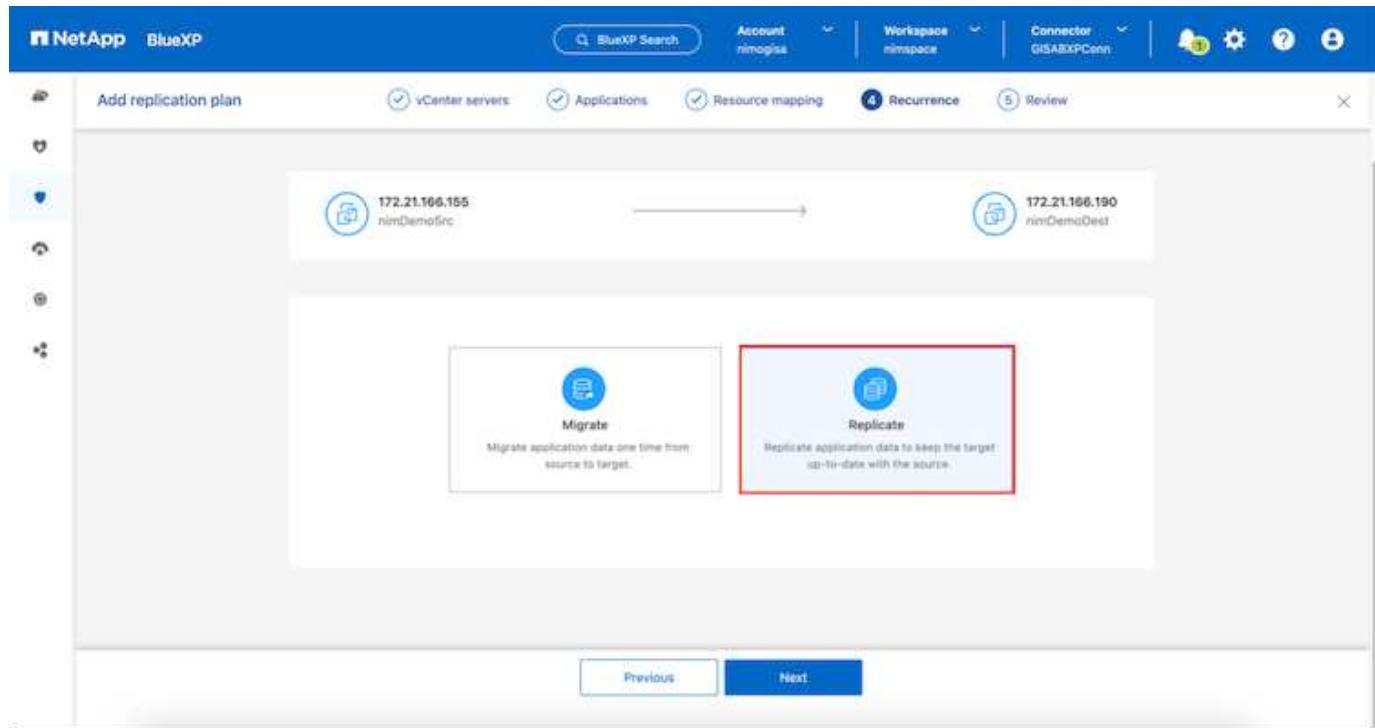
The screenshot shows the 'Add replication plan' wizard at step 3: Resource mapping. It displays a table of source VMs with their resource allocation details. The 'IP address type' and 'Target IP' settings are highlighted, showing 'Static' and 'Same as source' respectively. The 'Source VM' table includes columns for Source VM, CPUs, RAM, Boot delay(mins between 0 and 10), and Create application consistent replicas. Two specific VMs are listed: 'NFS_DemoA_VM01' and 'NFS_DemoA_VM02', each with its respective resource settings.

Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.

The screenshot shows the 'Add replication plan' wizard at step 3: Resource mapping. It displays a diagram showing the connection between 'nimDemoSrc' and 'nimDemoDest'. Below the diagram, a checkbox labeled 'Use same mappings for failover and test mappings' is checked. A red box highlights the 'Failover mappings' section, which contains three entries: 'Compute resources', 'Virtual networks', and 'Virtual machines', each with a 'Mapped' status indicator. Navigation buttons 'Previous' and 'Next' are visible at the bottom.

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

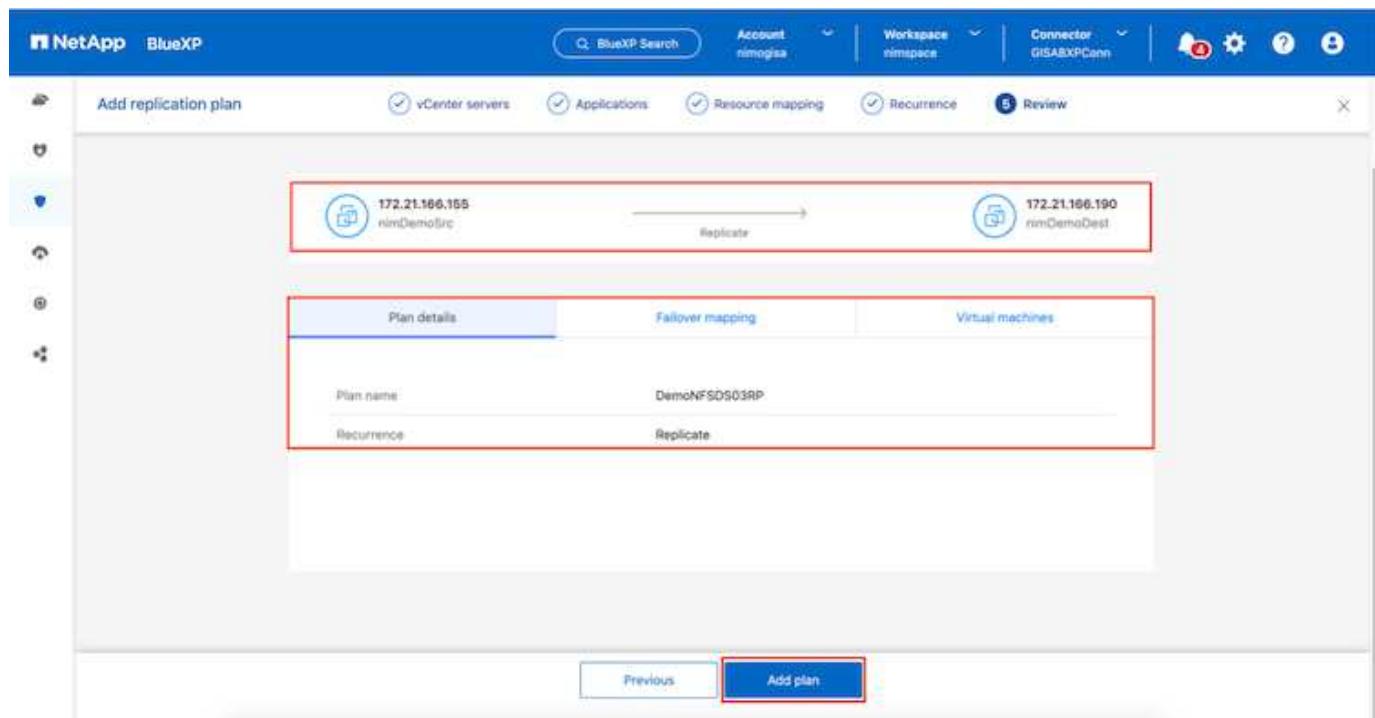
Vorgehensweise ist die Option „Replizieren“ ausgewählt.



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.



The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation links for Disaster recovery, Dashboard, Sites, and Replication plans (which is highlighted with a red box). To the right of these are Account, Workspace, and Connector dropdowns, along with various status icons. Below the navigation is a search bar and a 'Free trial (51 days left) - View details' button. The main content area displays a table titled '1 plans'. The table has columns for Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, Failover site, and an ellipsis button. The first row shows a plan named 'DemoNFS503RP' with a status of 'Healthy' and 'Ready'. The 'Protected site' is 'nimDemoSrc', 'Resource groups' is 'DemoNFS503RG', 'Recurrence' is 'Replicate', and 'Failover site' is 'nimDemoDest'.

BlueXP DRaaS besteht aus den folgenden Workflows:

- Test-Failover (einschließlich regelmäßiger automatisierter Simulationen)
- Failover-Test bereinigen
- Ausfallsicherung
- Fallback

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. In the left sidebar, under 'Storage', a folder named 'wklid04-vc01.hmccl.local' is expanded, showing sub-folders like '04TestBed_DS01', 'ISODump', and 'Src_NFS_DS03'. The 'Src_NFS_DS03' folder is highlighted with a red box. The main content area displays 'Details' for this volume, including its type (NFS 3), hosts (2), virtual machines (5), server (172.21.106.166), folder ('/src_NFS_DS03_TEST'), and location ('/s3://vmfs/volumes/b0cfc0c21-1ed87494/'). To the right, a 'Capacity and Usage' section shows 7122 GB free, 26.78 GB used, and 100 GB capacity. At the bottom, a table titled 'Recent Tasks' lists completed tasks for various hosts, such as 'Reconfigure virtual machine' and 'Register virtual machine'.

Task Name	Target	Status	Details	Owner	Ongoing For	Start Time	Completion Time
Reconfigure virtual machine	NFS_DemoA_VM02	Completed		HMCCL.LOCAL/Administrator	3 ms	06/16/2024, 6:53:59 A	06/16/2024, 6:53:59 A
Register virtual machine	wklid04-DC01	Completed	System		6 ms	06/16/2024, 6:53:58 A	06/16/2024, 6:53:59 A
Register virtual machine	wklid04-DC01	Completed	System		2 ms	06/16/2024, 6:53:58 A	06/16/2024, 6:53:59 A
Register virtual machine	wklid04-DC01	Completed	Registering Virtual Machine O... in destination host	System	3 ms	06/16/2024, 6:53:58 A	06/16/2024, 6:54:00 A

Bereinigungs-Failover-Testvorgang

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

The screenshot shows the NetApp BlueXP Disaster recovery interface. In the top navigation bar, 'Disaster recovery' is selected. Below it, there's a table with columns: Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, and Failover site. One row in the table is highlighted with a red box around the 'Test failover' status. A context menu is open on this row, with the 'Clean up failover test' option also highlighted with a red box.

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.

The screenshot shows the NetApp BlueXP web interface. At the top, there's a navigation bar with tabs for Disaster recovery, Dashboard, Sites, Replication plans (which is selected), Resource groups, and Job monitoring. On the right of the top bar, there are account and workspace dropdowns, a connector status, and various icons. Below the top bar, there's a search bar and a message about a free trial. The main content area has a header '1 plans' and a table with columns: Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, and Failover site. One row in the table is selected, showing 'DemoNFS03RP' under 'Plan', 'Healthy' under 'Compliance check', 'Ready' under 'Plan status', 'nimDemoSrc' under 'Protected site', 'DemoNFS03RG' under 'Resource groups', and 'Replicate' under 'Recurrence'. To the right of this table is a context menu with several options: View plan details, Run compliance check, Test failover, Clean up failover test, Fail over (which is highlighted with a red box), End backup, Edit schedules, Take snapshot now, Disable, Enable, and Delete.

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.

Task Name	Target	Status	Details	Initiator	Quoted For	Start Time	Completion Time
Power On virtual machine	NFS_DemoA_VM02	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	4 ms	05/16/2024, 7:04:07 A.M.	05/16/2024, 7:04:12 A.M.
Power On virtual machine	NFS_DemoA_VM05	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	3 ms	05/16/2024, 7:04:07 A.M.	05/16/2024, 7:04:12 A.M.
Power On virtual machine	NFS_DemoA_VM04	Completed		HMCDC.LOCAL\Administrator	3 ms	05/16/2024, 7:04:06 A.M.	05/16/2024, 7:04:07 A.M.
Power On virtual machine	NFS_DemoA_VM03	Completed	Powering on the new Virtual Machine	HMCDC.LOCAL\Administrator	2 ms	05/16/2024, 7:04:06 A.M.	05/16/2024, 7:04:07 A.M.

Fallback

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

VMware-Administratoren können ein Fallback-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,

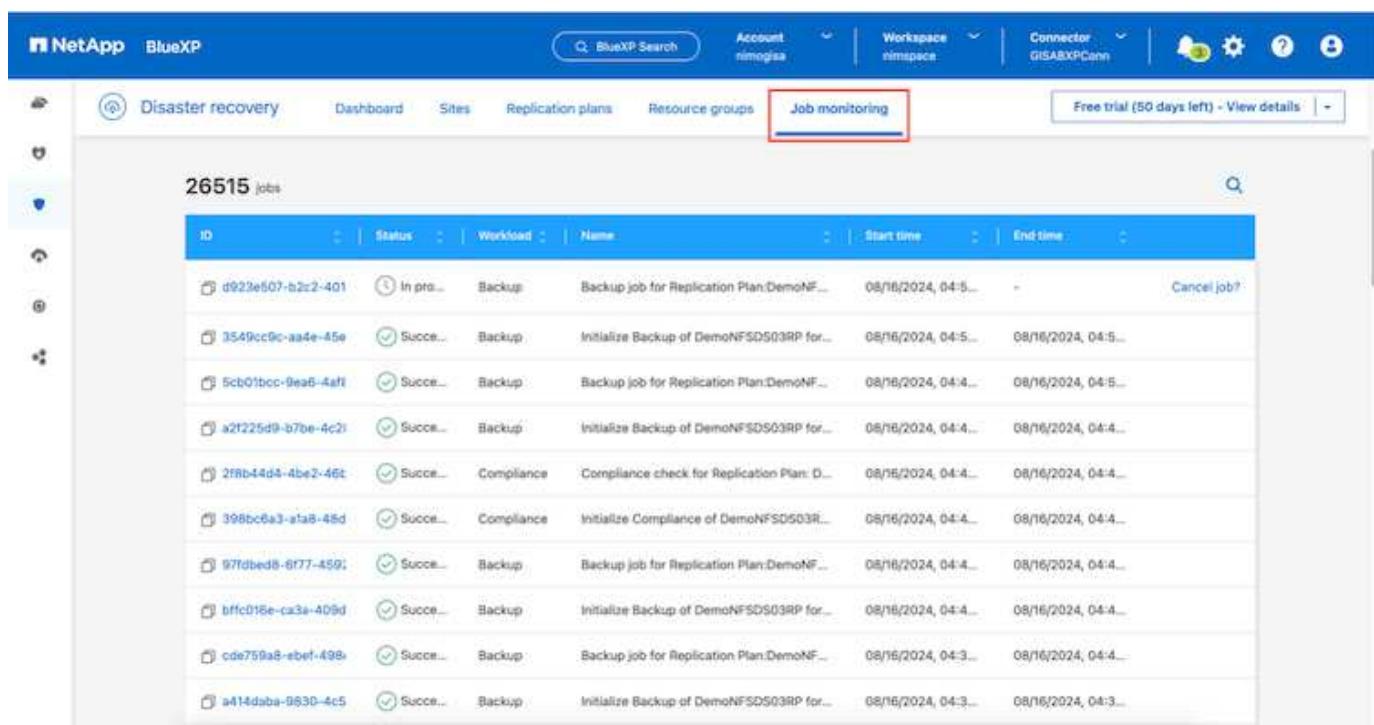
deren Failover zu einem Ziel abgeschlossen ist, und umfasst die folgenden Schritte:

- 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 Datenspeichervolumes überwachen und den Status eines Failovers oder Testfailovers über die Jobüberwachung verfolgen.



The screenshot shows the BlueXP Disaster recovery interface. At the top, there are tabs for Disaster recovery, Dashboard, Sites, Replication plans, Resource groups, and Job monitoring. The Job monitoring tab is highlighted with a red box. Below the tabs, it says "26515 jobs". A table lists 10 jobs, each with an ID, status (e.g., In pro..., Success...), workload (Backup or Compliance), name, start time, end time, and a "Cancel job?" link. The first job is "d923e507-b2c2-401".

ID	Status	Workload	Name	Start time	End time	Action
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc9c-aa4e-45e...	Success...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4af...	Success...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a2f225d9-b7be-4c2...	Success...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2ff8b44d4-4be2-46t...	Success...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-afa8-48d...	Success...	Compliance	Initialize Compliance of DemoNFS03RP...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-8f77-459...	Success...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bfffc016e-ca3a-409d...	Success...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebe1-498...	Success...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-8830-4c5...	Success...	Backup	Initialize Backup of DemoNFS03RP 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](#)" .

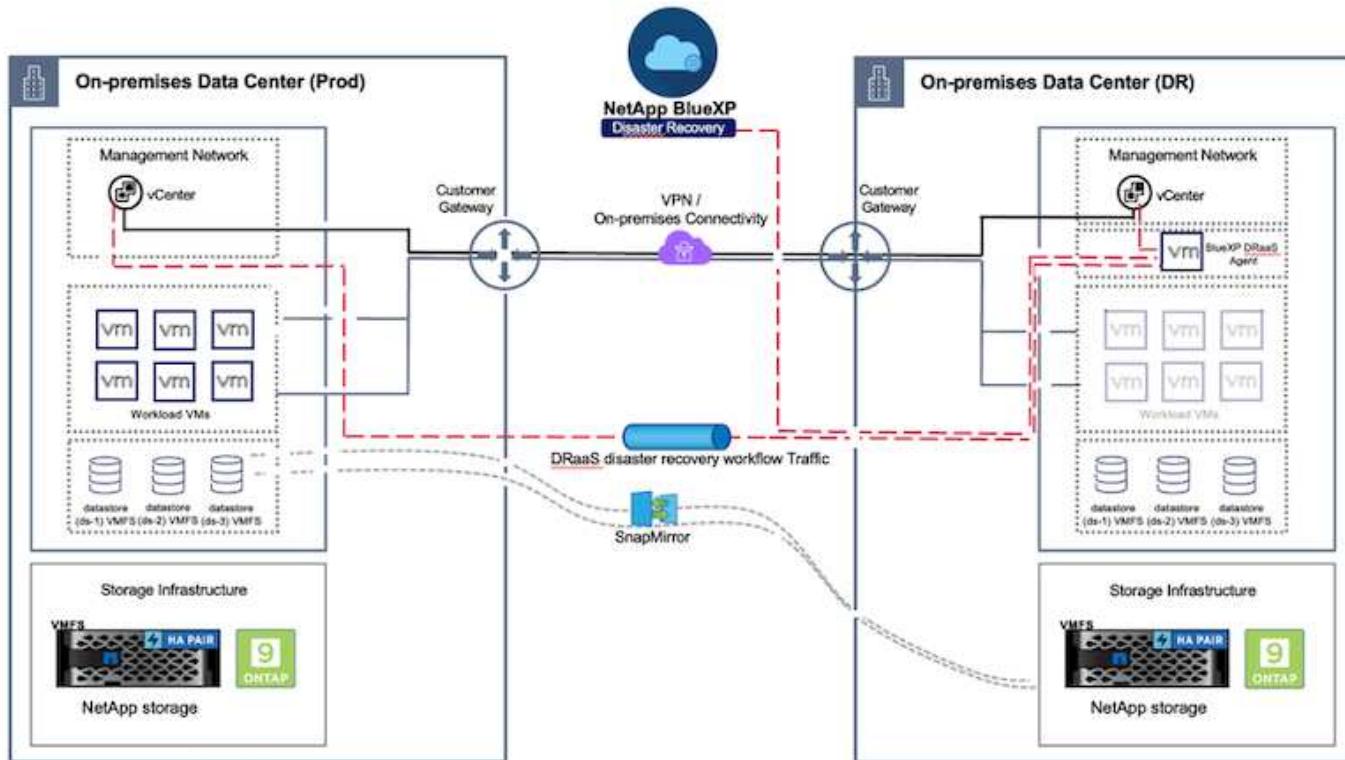
DR mit BlueXP DRaaS für VMFS-Datenspeicher

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 Specherebene, 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.

The screenshot shows the NetApp BlueXP interface. The left sidebar has categories like Storage, Health, Protection, Backup and recovery (with Disaster recovery highlighted), Replication, Ransomware protection, Governance, Mobility, and Extensions. The main area has tabs for very, Dashboard, Sites, Replication plans, Resource groups, and Job monitoring. The Dashboard tab is selected. It displays a summary of replication plans (1 Ready, 2 Failed), protected VMs (21), unprotected VMs (117), failovers (1), fallbacks (1), test failovers (2), and migrations (0). A red box highlights the 'Disaster recovery' section in the sidebar.

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 Datenspeichervolumes 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.

The screenshot shows the NetApp BlueXP Disaster recovery interface. The top navigation bar includes 'NetApp BlueXP', 'BlueXP Search', 'Account: nimogis', 'Workspace: nimospace', 'Connector: G1SA&XPConn', and various system icons. The main dashboard area has three main sections: 'Sites (2)' (Running: 2, Down: 0, Issue: 0), 'Replication plans (2)' (Ready: 2, Failed: 0), and 'Activity'. The 'Activity' section lists recent events such as backup initialization, resource discovery, and failback operations.



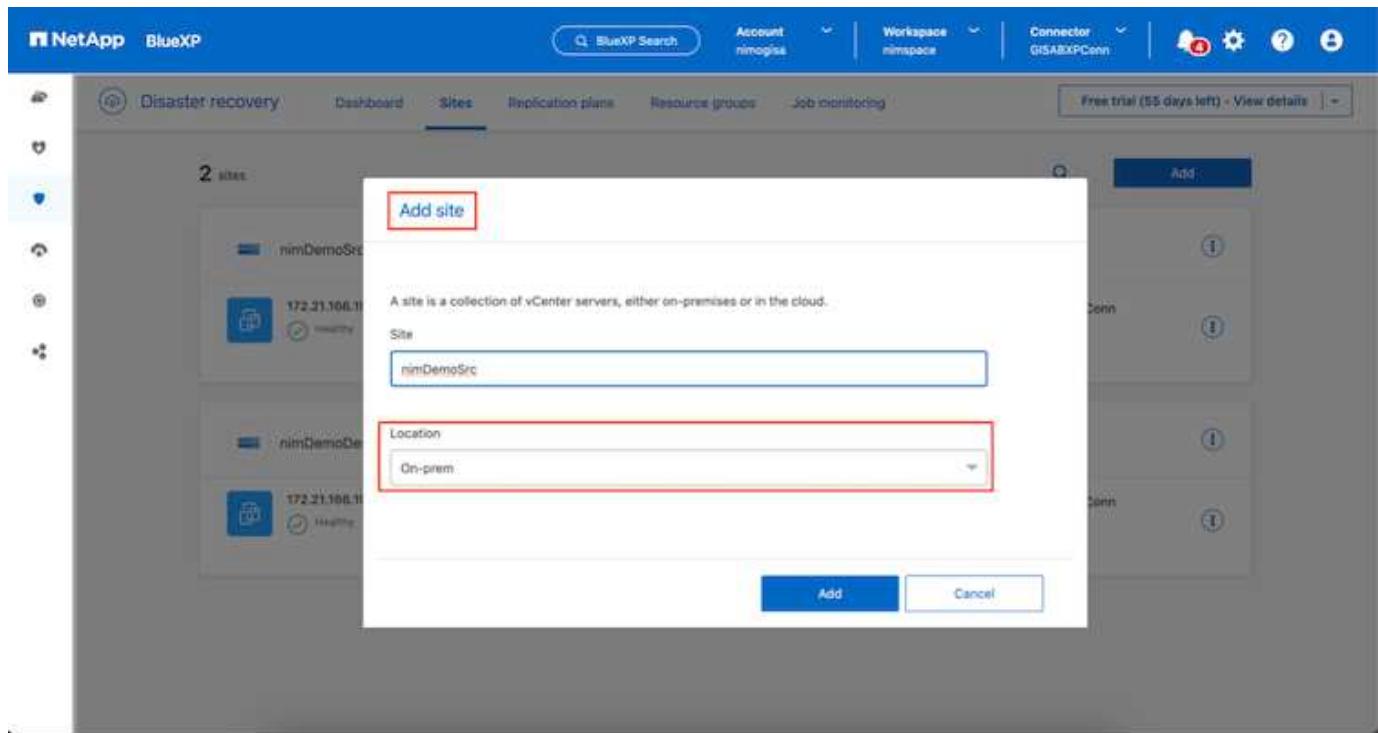
Die Unterstützung für lokale VMFS-Datenspeicher befindet sich beim Schreiben dieses Dokuments in der Technologievorschau. Die Funktion wird sowohl mit FC- als auch mit ISCSI-Protokoll-basierten VMFS-Datenspeichern unterstützt.

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.

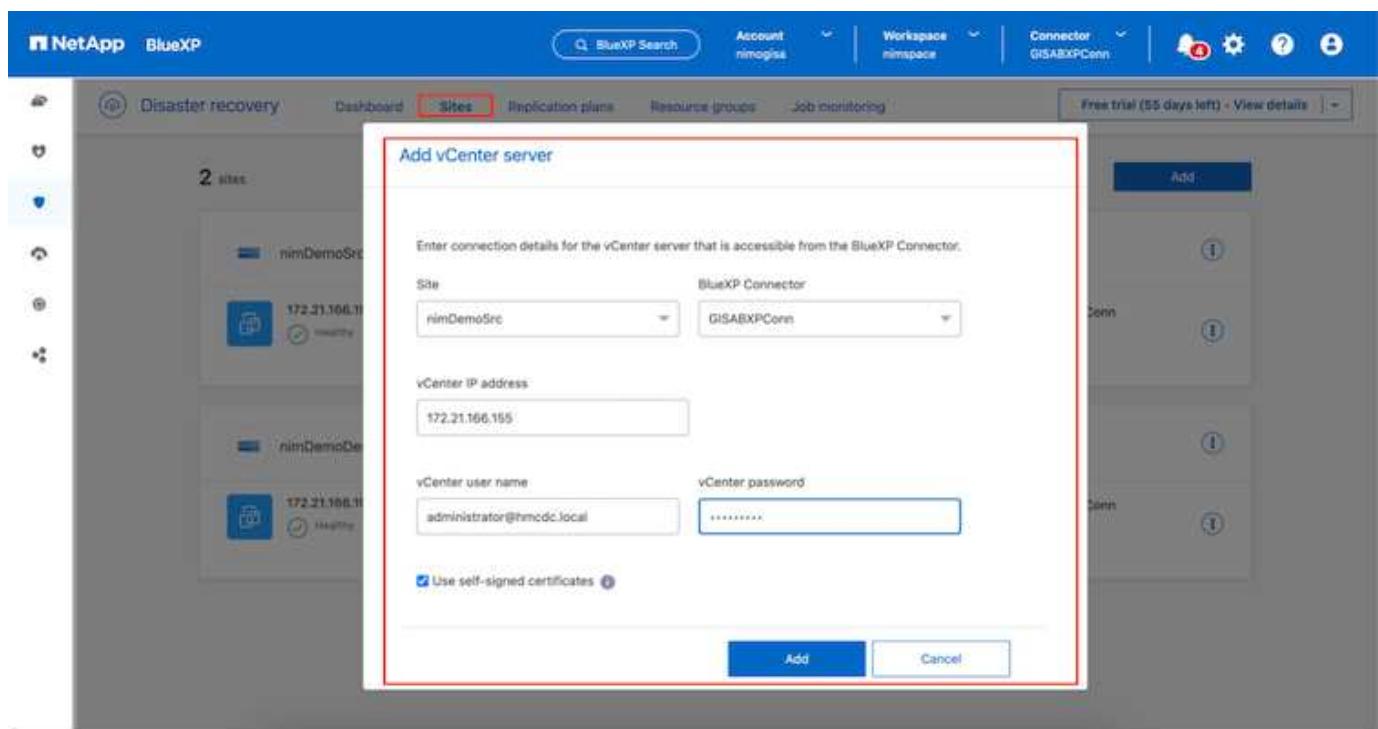


Stellen Sie sicher, dass die ONTAP Speichersysteme der Arbeitsumgebung innerhalb des Canvas hinzugefügt werden. Öffnen Sie die BlueXP -Konsole und wählen Sie in der linken Navigation **Schutz > Notfallwiederherstellung**. Wählen Sie **vCenter-Server ermitteln** oder verwenden Sie das Hauptmenü. Wählen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

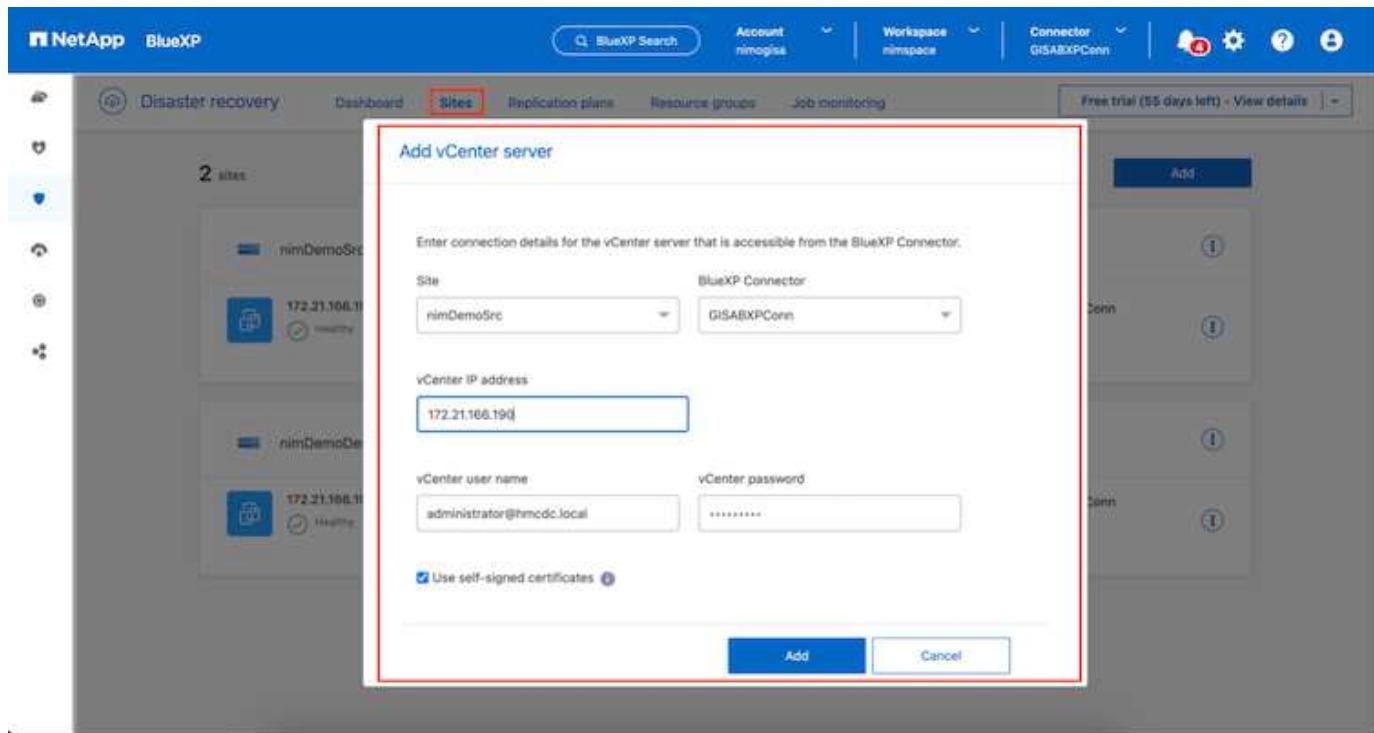


Fügen Sie die folgenden Plattformen hinzu:

- **Quelle.** Lokales vCenter.



- **Ziel.** VMC SDDC vCenter.



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

Konfigurieren der Speicherreplikation zwischen Quell- und Zielstandort

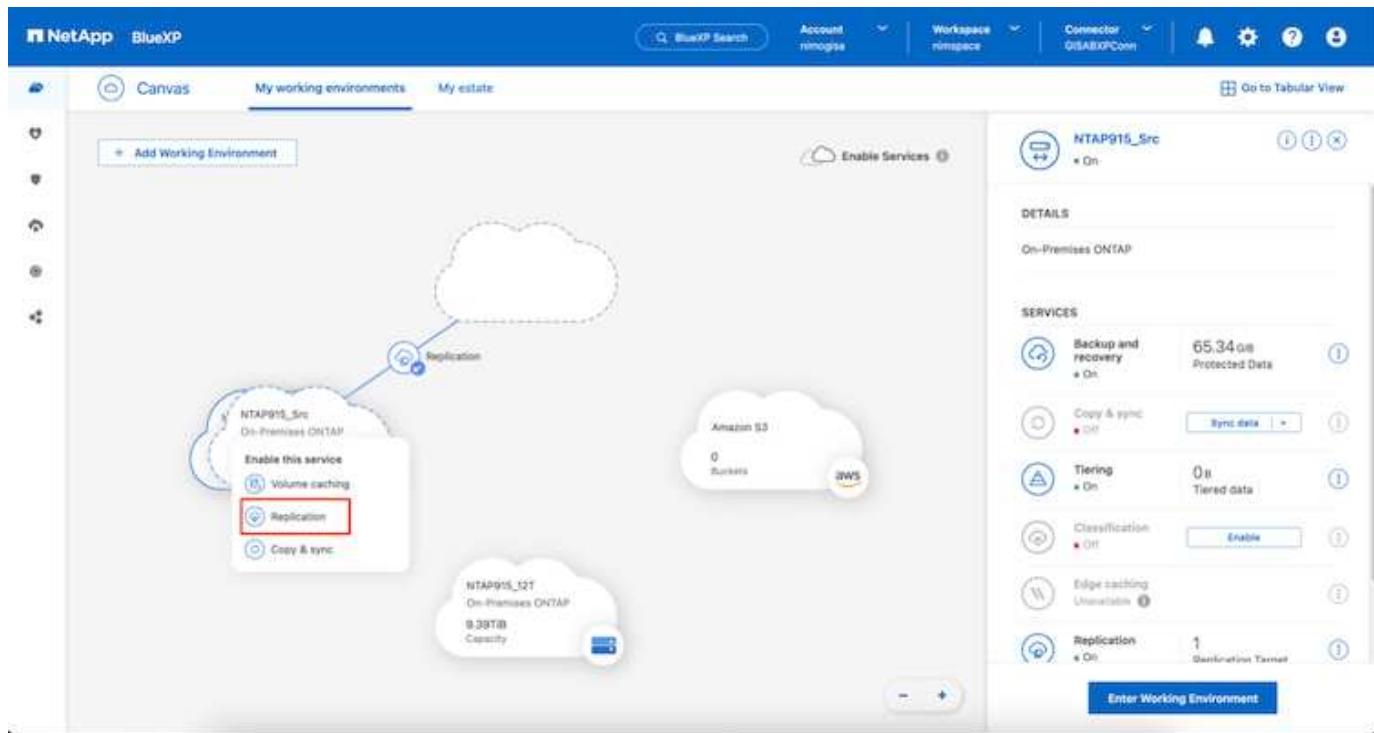
SnapMirror nutzt ONTAP -Snapshots, um die Datenübertragung von einem Ort zum anderen zu verwalten. Zunächst wird eine vollständige Kopie basierend auf einem Snapshot des Quellvolumes auf das Ziel kopiert, um eine Basissynchronisierung durchzuführen. Wenn an der Quelle Datenänderungen auftreten, wird 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.

The screenshot shows the "Add replication plan" wizard at step 4: Resource mapping. The configuration includes:

- Source cluster:** vVCSA8-Cluster01
- Target cluster:** wM0D4-Cluster01
- Virtual networks:** Mapped
- Virtual machines:** Mapped
- Datastores:**
 - RPO for all datastores in minutes: Required (30 minutes)
 - Retention count for all datastores: 30
 - Source datastore: Src_NFS_DS01 (svm_nim_nfsv3_src_NFS_Vol01)
 - Target datastore: Src_NFS_DS01 (svm_nim_nfsv3_src_NFS_DS01_c0) Transfer schedule(RPO) : ..



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.

The screenshot shows the BlueXP Disaster Recovery interface. At the top, there are tabs for Disaster recovery, Dashboard, Sites (which is highlighted with a red box), Replication plans, Resource groups, and Job monitoring. A banner at the top right indicates a free trial with 83 days left. Below the tabs, it says '2 sites'. There are two entries: 'nimDemoSrc' and 'nimDemoDest'. Each entry has a summary table:

	172.21.166.155	72	13	1	GISABXPConn
VMs	Healthy	VMs	Datastores	Resource groups	Connector

Each row has an 'Edit' button (blue circle with white 'i') on the far right.

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**.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', 'BlueXP Search', 'Account nimogis', 'Workspace nimspace', 'Connector GISABXPCnn', and various status icons. The left sidebar has icons for Disaster recovery, Dashboard, Sites, Replication plans, Resource groups (which is selected and highlighted in blue), and Job monitoring. The main content area displays '2 resource groups'. A table lists 'Resource group' (DemoRG01, DemoRGVMFS03), 'Source site' (nimDemoSrc), and 'Source vCenter' (172.21.166.155). Below the table, a green success message box says 'Added the resource group'.



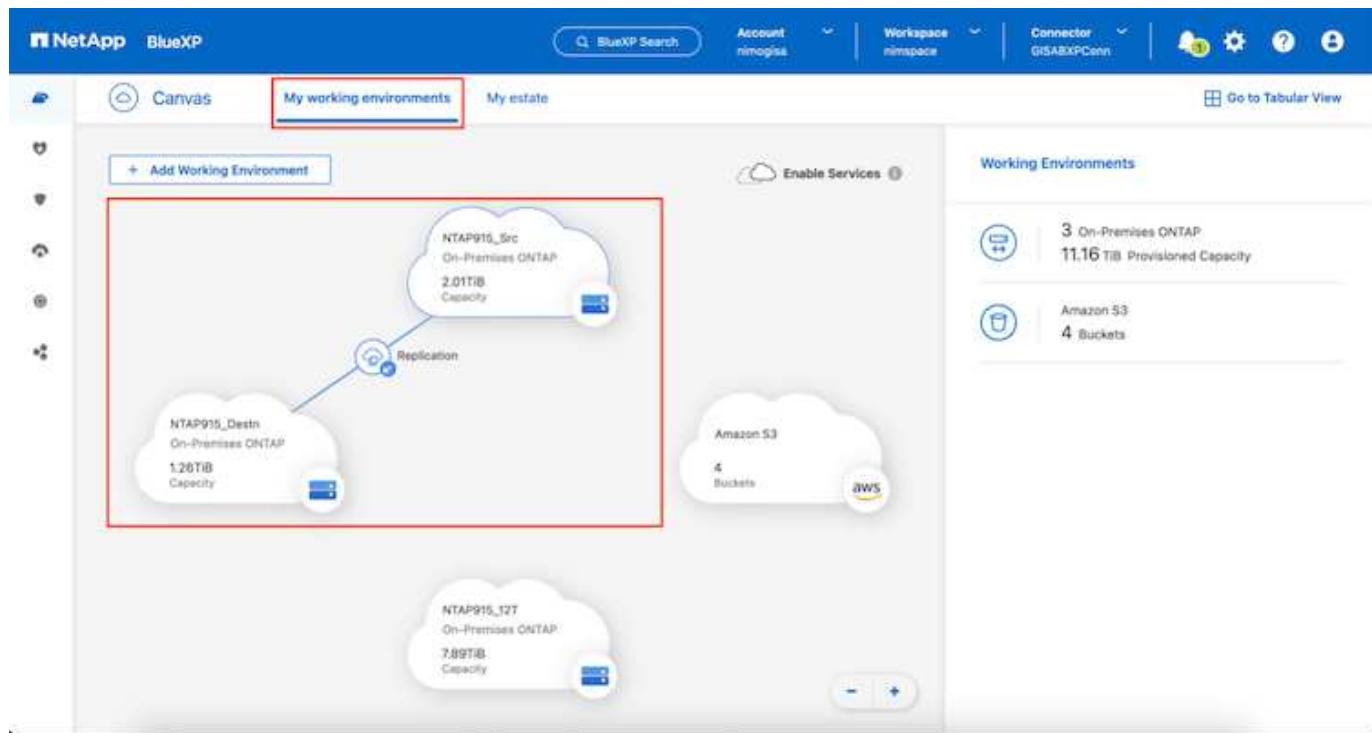
Die Ressourcengruppe kann auch beim Erstellen eines Replikationsplans erstellt werden.

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

The screenshot shows the 'Add resource group' dialog box. It has fields for 'Name' (DemoRGVMFS03) and 'vCenter' (172.21.166.155). Below these, there's a section titled 'Select virtual machines' with a search bar ('iSCSI') and a list of VMs: iSCSI_DemoVM01, iSCSI_DemoVM03, iSCSI_DemoVM02, iSCSI_DemoVM04, and iSCSI_DemoVM05. Each VM has a checkbox next to it. To the right, a box labeled 'Selected VMs (5)' lists the same five VMs, each with a red 'X' icon to their right. A note at the bottom says 'Use drag and drop here to modify the boot order'. At the bottom of the dialog are 'Add' and 'Cancel' buttons.

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

Replikationspläne angegeben wurden.



The screenshot shows the 'Replication' tab selected in the top navigation bar. The dashboard displays the following metrics:

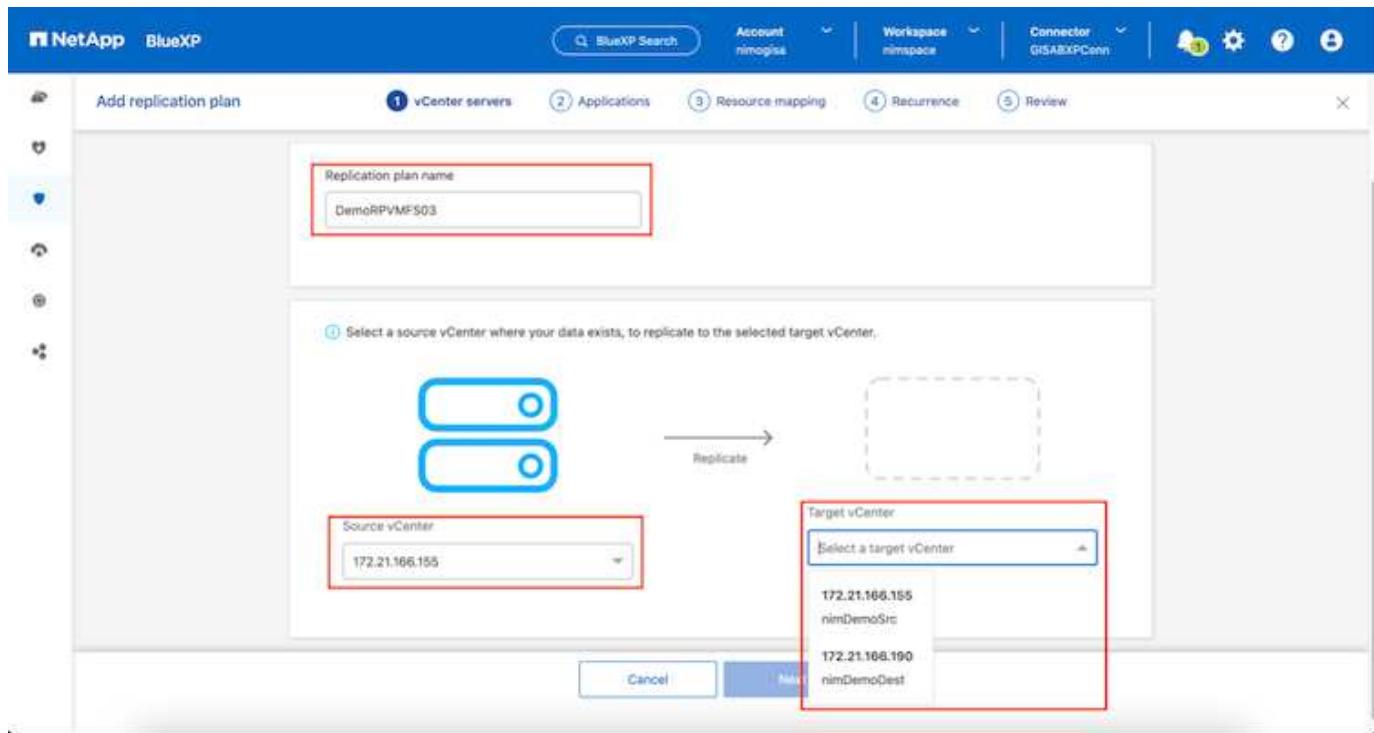
6 Volume Relationships	495.27 GiB Replicated Capacity	0 Currently Transferring	6 Healthy	0 Failed
------------------------	--------------------------------	--------------------------	-----------	----------

Below the dashboard, the 'Volume Relationships (6)' table provides detailed information for each replication pair:

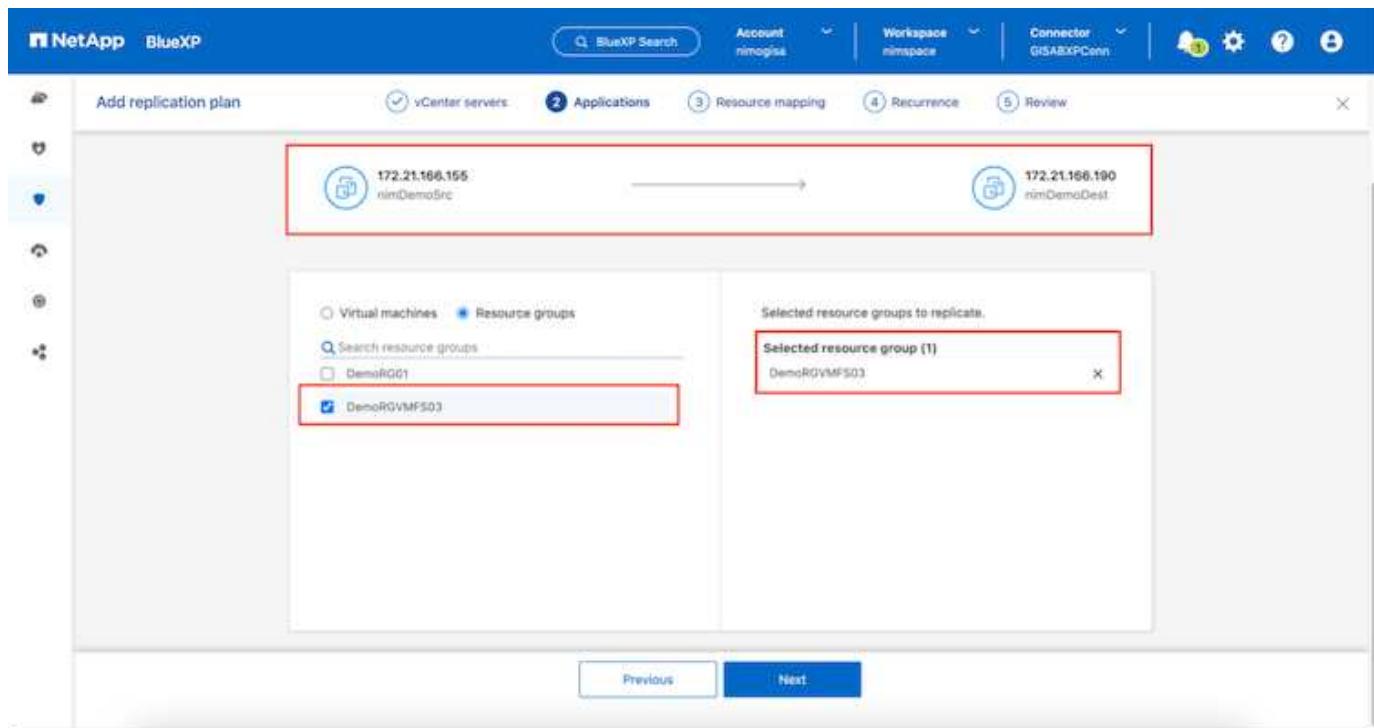
Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful
✓	DRaaS_src NTAP915_src	DRaaS_src_copy NTAP915_Destn	5 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 28.41 MiB
✓	Src_NFS_DS03 NTAP915_src	Src_NFS_DS03_Cp NTAP915_Destn	13 seconds	idle	snapmirrored	Jul 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, 8:05:06 183.38 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_D601 NTAP915_src	Src_iSCSI_D601_cp NTAP915_Destn	20 seconds	idle	snapmirrored	Jul 12, 2024, 4:24:34 22.35 MiB
✓	Src_iSCSI_D603 NTAP915_src	Src_iSCSI_D603_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.



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.

The screenshot shows the 'Add replication plan' wizard in NetApp BlueXP. The current step is 'Applications'. It shows two hosts: 'nimDemoSrc' (IP 172.21.108.155) and 'nimDemoDest' (IP 172.21.108.190). The 'nimDemoSrc' host has several virtual machines listed under 'Virtual machines': UbuntuVM01, Win2K19VM01, SCVSP02VM01, iOTV34Z2Node, and SQL_DemoVM01. The 'nimDemoDest' host has one entry: 'ResourceGroup1'. A red box highlights the 'Selected VMs (0)' section, which contains the instruction 'Select VMs to replicate.' Below the application selection are 'Previous' and 'Next' buttons.

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](#)".

Add replication plan

vCenter servers Applications Resource mapping Recurrence Review

Virtual machines

IP address type Target IP

Static Same as source

Use the same credentials for all VMs

Use the same script for all VMs

Source VM	CPU	RAM	Boot delay(mins between 0 and 10)	Create application consistent replicas	Scripts
S0_DemoVM1	2	4 GB	0	<input type="checkbox"/>	None
S0_DemoVM01	2	4 GB	0	<input type="checkbox"/>	None
S0_DemoVM02	2	4 GB	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:

Add replication plan vCenter servers Applications Resource mapping Recurrence Review

Replication plan > Add plan

Resource mapping

Specify how resources map from the source to the target.

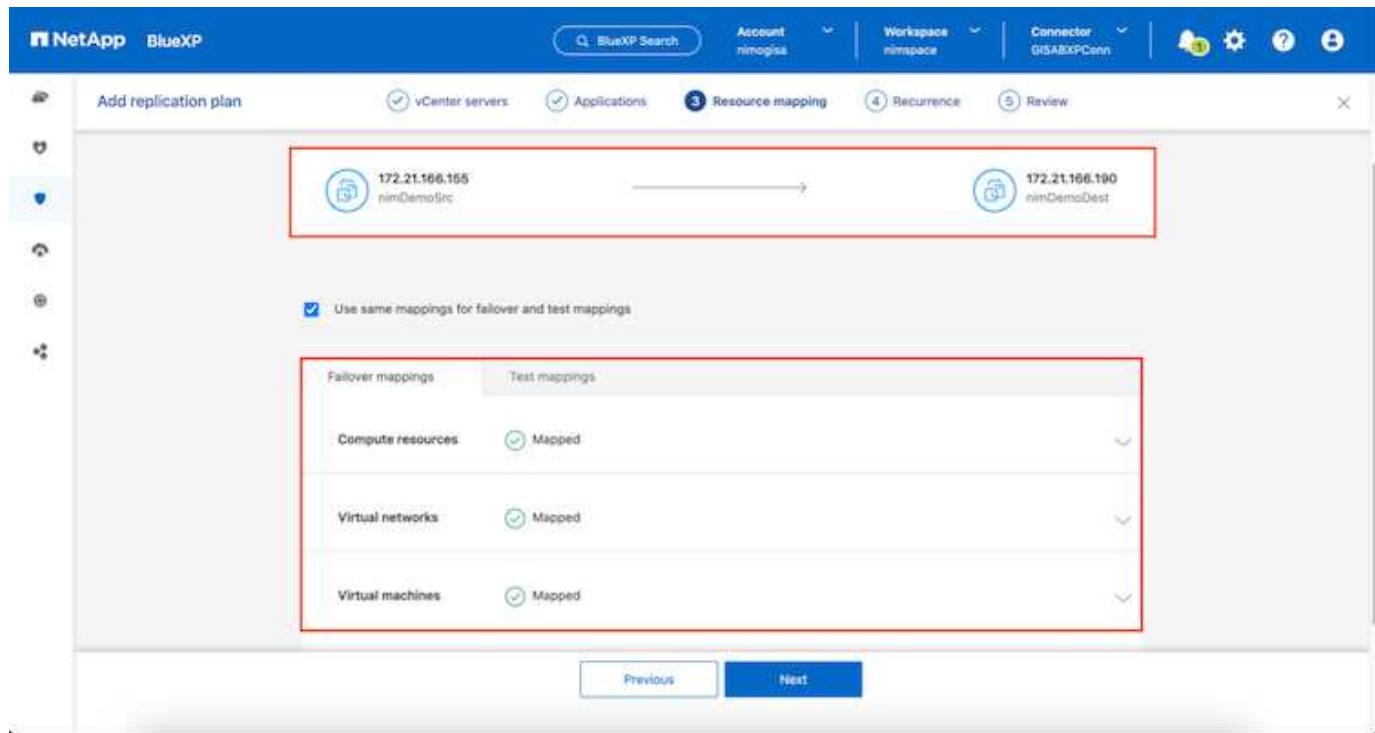
172.21.166.155
nmDemoSrc

172.21.166.190
nmDemoDest

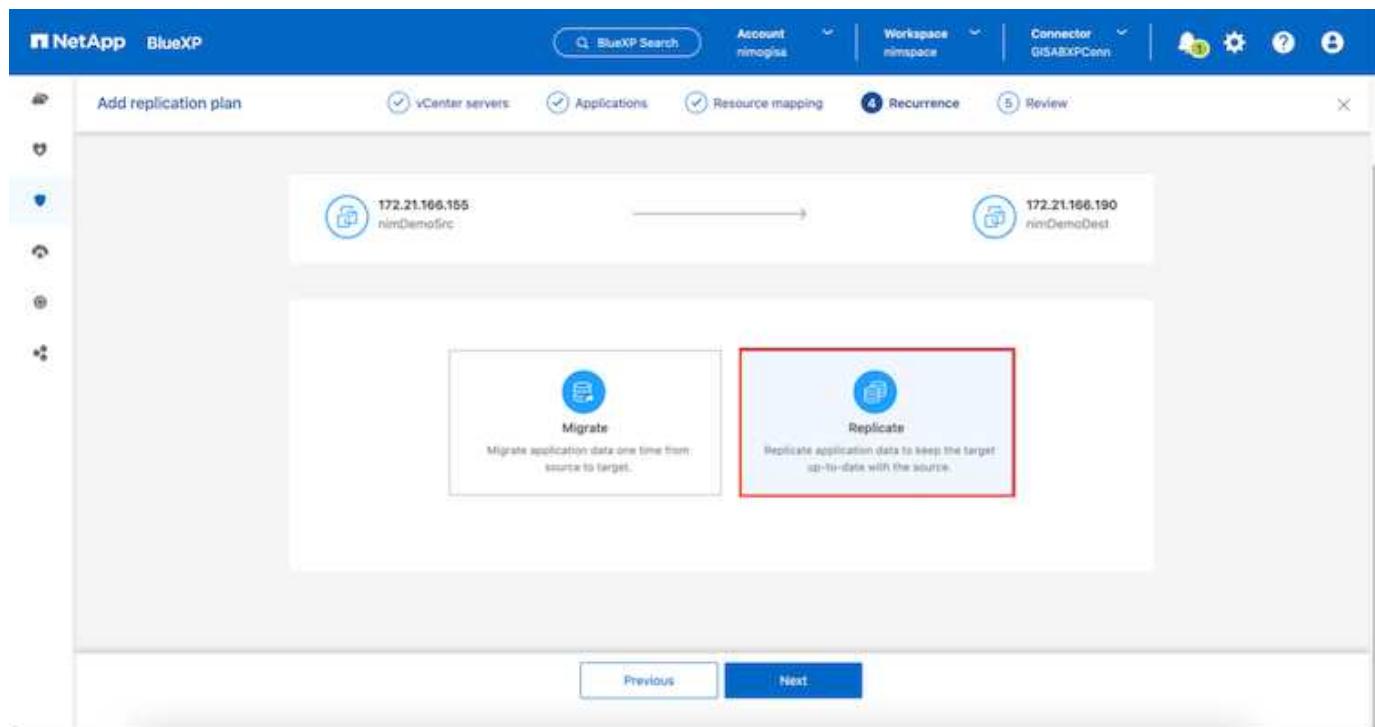
Use same mappings for failover and test mappings

Failover mappings Test mappings

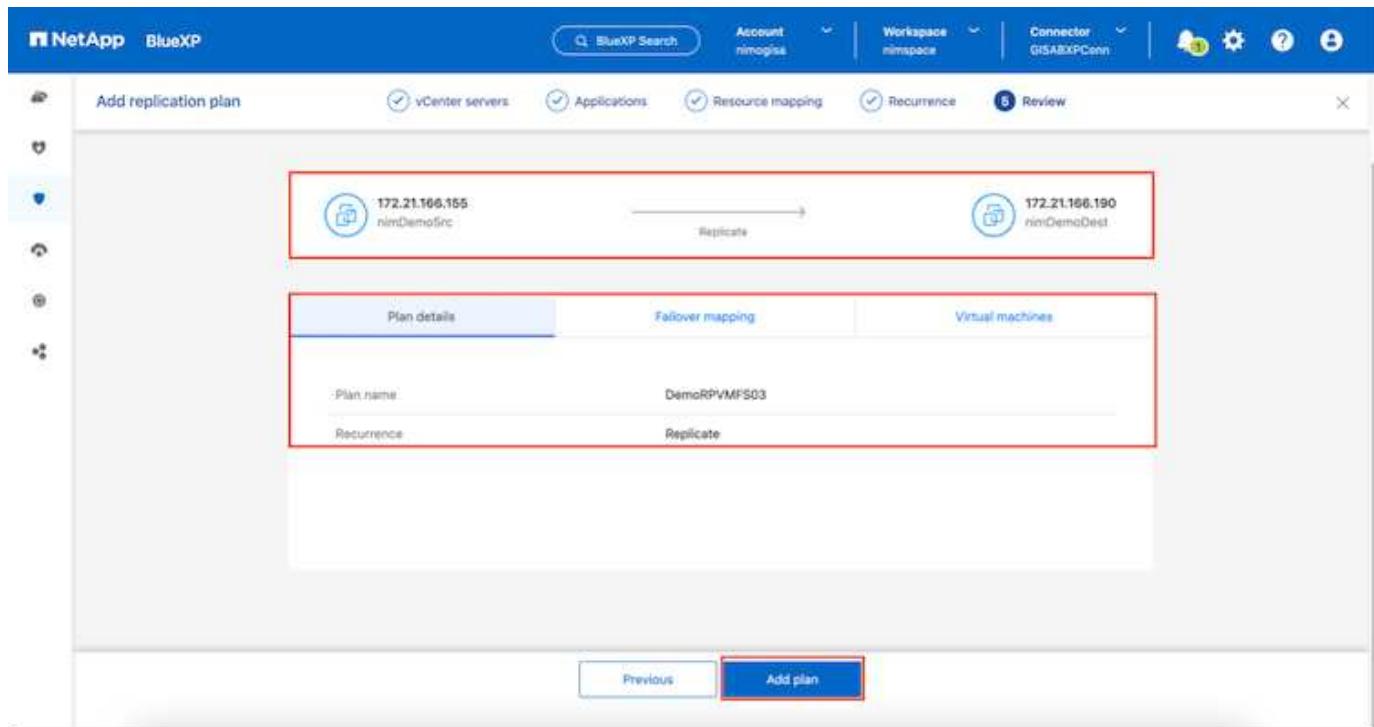
Klicken Sie nach Abschluss der Ressourcenzuordnung auf „Weiter“.



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“.



The screenshot shows the 'Replication plans' page in the NetApp BlueXP interface. The top navigation bar includes 'Disaster recovery', 'Dashboard', 'Sites', 'Replication plans' (which is selected and highlighted with a blue box), 'Resource groups', and 'Job monitoring'. A 'Free trial (83 days left) - View details' button is also present. The main area shows a table with two rows of replication plan details:

Plan	Compliance check	Plan status	Protected site	Resource group	Recurrence	Failover site	Actions
DemoRPVMS03	Healthy	Ready	nimDemoSrc	DemoRGVMS03	Replicate	nimDemoDest	...
RPNFS001	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.

The screenshot shows the 'Disaster recovery' section of the NetApp BlueXP interface. A modal window titled 'Failover: DemoRPVMS03' is open. It displays a warning that failing over will disrupt client access to the data in 'nimDemoSrc' during the transition to 'nimDemoDest DR Site'. Another warning states that all VMs are powered on. Below these, a section for 'Snapshot copy for volume recovery' shows four options, with the third one selected. A note says the corresponding volume will be restored with the selected snapshot copy, and changes made after its creation will be lost. At the bottom, there's a 'Force failover' button.

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

The screenshot shows the 'Replication plans' section of the NetApp BlueXP interface. It lists two replication plans: 'DemoRPVMS03' and 'RPNFS001'. The first plan is highlighted with a red box. A context menu is open for 'DemoRPVMS03', listing various actions: 'View plan details', 'Run compliance check', 'Test failover' (highlighted with a red box), 'Fail over' (also highlighted with a red box), 'Fail back', 'Edit schedules', 'Take snapshot now', 'Disable', 'Enable', and 'Delete'.

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.

The screenshot shows the NetApp BlueXP interface with the 'Disaster recovery' tab selected. A modal window titled 'Test failover: DemoRPVMS03' displays a list of validation steps:

- ✓ DR Test Failover Update Mirror
- ✓ SnapMirror relationship for volume :svm_iSCSI:Src_iSCSI_D503
- ✓ Destination volume 'Src_iSCSI_D503_CP' size is less than source volume 'Src_iSCSI_D503' size
- ✓ SnapMirror relationship is healthy for volume :svm_iSCSI:Src_iSCSI_D503
- ✓ Destination storage environment found for volume :svm_iSCSI:Src_iSCSI_D503
- ✓ Take snapshot now option is not selected, primary backup & snapmirror update not performed.

At the bottom right of the modal is a blue button labeled 'Run in background'.

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.

The screenshot shows the vSphere Client interface with the vCenter server 'wkld04-vc01.hmc当地' selected. The 'Summary' tab is active, displaying the following details:

- vCenter Details:**
 - Version: 8.0.2
 - Build: 22385739
 - Last Updated: May 20, 2024, 3:21 AM
 - Last File-Based Backup: Not scheduled
 - Clusters: 1
 - Hosts: 2
 - Virtual Machines: 61
- Capacity and Usage:**
 - CPU: 72.12 GHz free
 - Memory: 73.44 GHz capacity, 485.84 GB free
 - Storage: 59.99 GB capacity, 3.91 TB free
 - Network: 94.28 GB used, 4 TB capacity

Below the summary are sections for 'Recent Tasks' and 'Alarms'. The 'Recent Tasks' table lists two completed tasks:

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Rescan VMFS	wkld04-esx01.hmc	Completed		HMCDCLLOCAL\Administrator	2 ms	07/30/2024, 3:22:47 AM	07/30/2024, 3:22:47 AM
Rescan all HBAs	wkld04-esx01.hmc	Completed		HMCDCLLOCAL\Administrator	3 ms	07/30/2024, 3:22:47 AM	07/30/2024, 3:22:47 AM

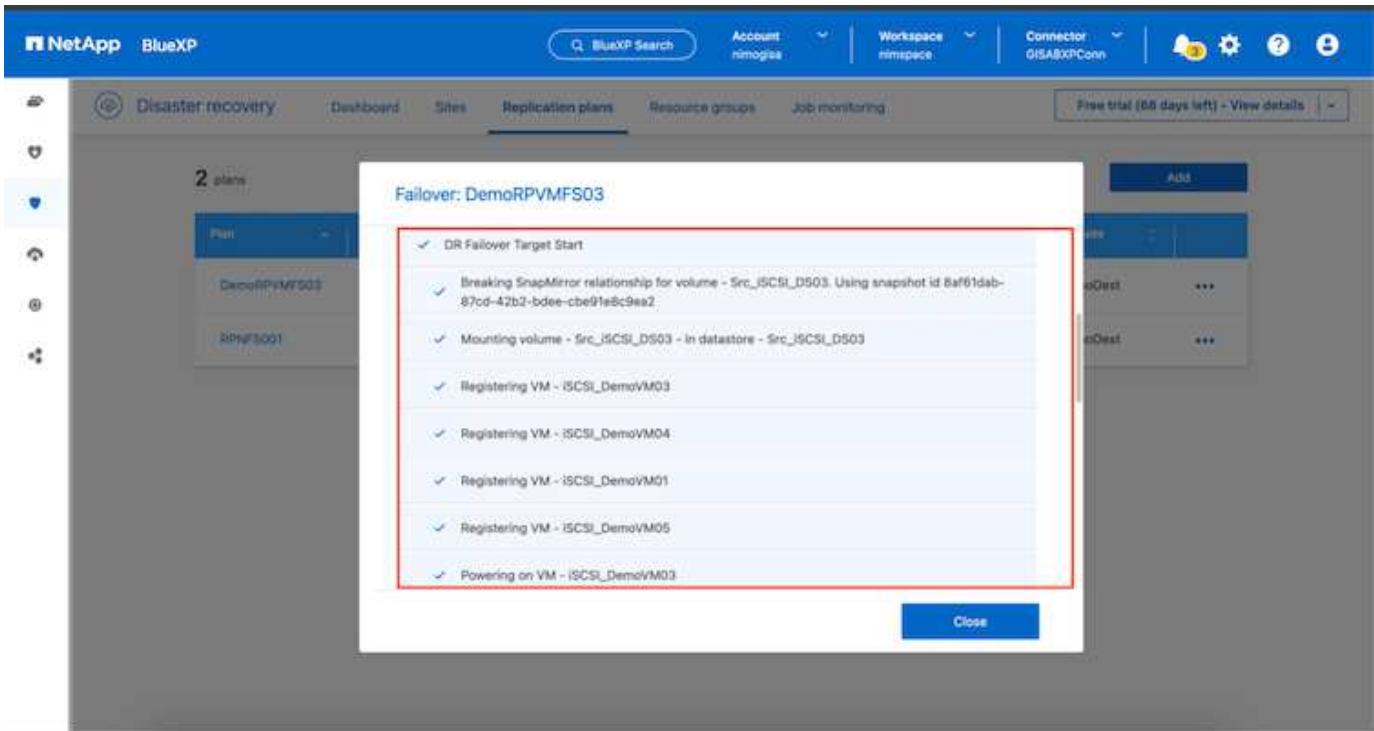
The screenshot shows the vSphere Client interface. In the left sidebar, the tree view shows 'wkld04-vc01.hmc当地' selected. Underneath, 'wkld04-DC01' is expanded, showing '04TestBed_DS01', 'ISOdump', and 'Src_iSCSI_DS03'. The 'Src_iSCSI_DS03' item is highlighted with a red border. The main content area displays 'vCenter Details' and 'Capacity and Usage' information. The 'Capacity and Usage' panel provides a summary of system resources. Below this, a table titled 'Recent Tasks' lists two entries:

Task Name	Target	Status	Details	Initiator	Queued For	Start Time	Completion Time
Register virtual machine	wkld04-DC01	20%	Registering Virtual Machine o... in destination host	System	20 ms	07/30/2024, 3:23:43 AM	
Register virtual machine	wkld04-DC01	20%	Registering Virtual Machine o... in destination host	System	17 ms	07/30/2024, 3:23:43 AM	Windows

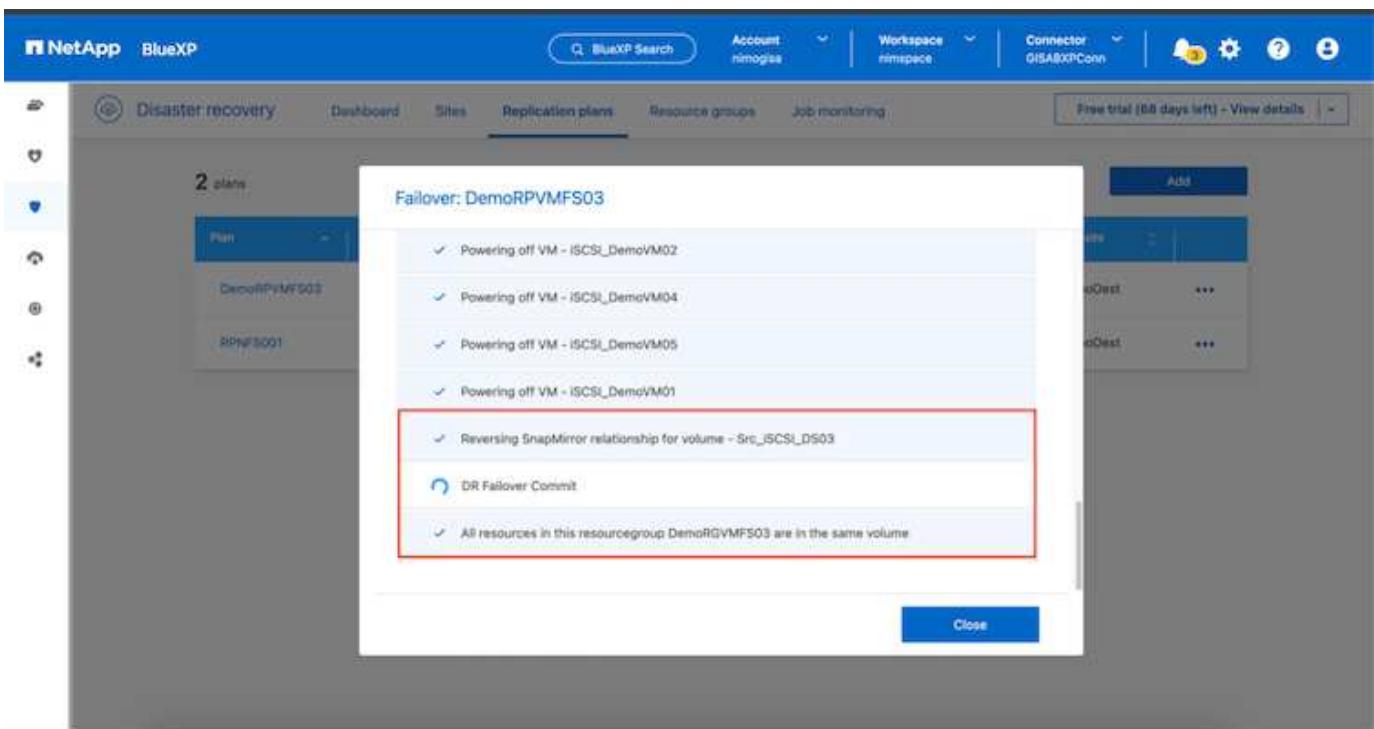
Wenn der Test-Failover-Vorgang abgeschlossen ist, kann der Bereinigungsvorgang mit "**Failover-Test bereinigen**" ausgelöst werden. Während dieses Vorgangs zerstört die BlueXP disaster recovery das FlexClone -Volume, das bei diesem Vorgang verwendet wurde.

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 Fallback, 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 Datenspeichervolumes überwachen und den Status eines Failovers oder Testfailovers über die

Jobüberwachung verfolgen.

The screenshot shows the NetApp BlueXP interface with the 'Job monitoring' tab selected. At the top, there are five summary metrics: 0 Jobs (Success), 0 In progress, 0 Queued, 0 Warning, and 0 Failed. Below this, a table lists 11102 jobs, with three specific entries highlighted in red boxes:

ID	Status	Workload	Name	Start time	End time	...
2963d7f3-7eb0-475d	Success	Discovery	Discovery of resources in host 172.21.166...	07/30/2024, 11:52:...	07/30/2024, 11:52:...	...
f7ea7c0c-90d8-49b2	Success	DRFallback	Fallback of resources using the replication...	07/30/2024, 11:49:...	07/30/2024, 11:52:...	...
471f5cf2-1e97-48ca	Success	Discovery	Discovery of resources in host 172.21.166...	07/30/2024, 11:43:...	07/30/2024, 11:44:...	...

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 BESCHRÄNKKT 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, BEISPIELHAFFE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 IRGENDERINER 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.