



## **Disaster recovery using BlueXP DRaaS**

NetApp public and hybrid cloud solutions

NetApp

February 04, 2026

# Table of Contents

Disaster recovery using BlueXP DRaaS .....	1
Overview .....	1
DR using BlueXP DRaaS for NFS Datastores .....	1
Getting started .....	2
BlueXP disaster recovery configuration .....	4
Configuring Storage replication between source site array and destination site array .....	5
How to set it up for VMware Disaster Recovery .....	6
What can BlueXP disaster recovery do for you? .....	7
Test failover .....	15
Cleanup failover test Operation .....	17
Planned Migration and Fail over .....	18
Fallback .....	20
Monitoring and Dashboard .....	21
DR using BlueXP DRaaS for VMFS Datastores .....	22
Getting started .....	23
BlueXP disaster recovery configuration .....	25
Configuring Storage replication between source and destination site .....	27
How to set it up for VMware Disaster Recovery .....	27
What can BlueXP disaster recovery do for you? .....	29
What happens during a failover or test failover operation? .....	37

# Disaster recovery using BlueXP DRaaS

## Overview

Disaster Recovery is foremost in the minds of every VMware administrator. Because VMware encapsulates entire servers into a series of files that make up the virtual machine; administrators take advantage of block storage-based techniques such as clones, snapshots and replicas to protect these VMs. ONTAP arrays offer built-in replication to transfer volume data, and therefore the virtual machines residing on the designated datastore LUNs, from one site to another. BlueXP DRaaS integrates with vSphere and automates the entire workflow for seamless failover and failback in the event of disaster. By combining storage replication with intelligent automation, administrators now have a manageable way to not only configure, automate, and test disaster recovery plans, but the means to easily run them in the case of a disaster.

Most time-consuming parts of a DR failover in a VMware vSphere environment is the execution of the steps necessary to inventory, register, reconfigure, and power up VMs at the DR site. An ideal solution has both a low RPO (as measured in minutes) and a low RTO (measured in minutes to hours). One factor that is often overlooked in a DR solution is the ability to test the DR solution efficiently on a periodic interval.

To architect a DR solution, keep the following factors in mind:

- The recovery time objective (RTO). The RTO is how quickly a business can recover from a disaster, or, more specifically, how long it takes to execute the recovery process to make business services available again.
- The recovery point objective (RPO). The RPO is how old the recovered data is after it has been made available, relative to the time that the disaster occurred.
- Scalability and adaptability. This factor includes the ability to grow storage resources incrementally as demand increases.

For more technical information on the available solutions, please see:

- [DR using BlueXP DRaaS for NFS Datastores](#)
- [DR using BlueXP DRaaS for VMFS Datastores](#)

## DR using BlueXP DRaaS for NFS Datastores

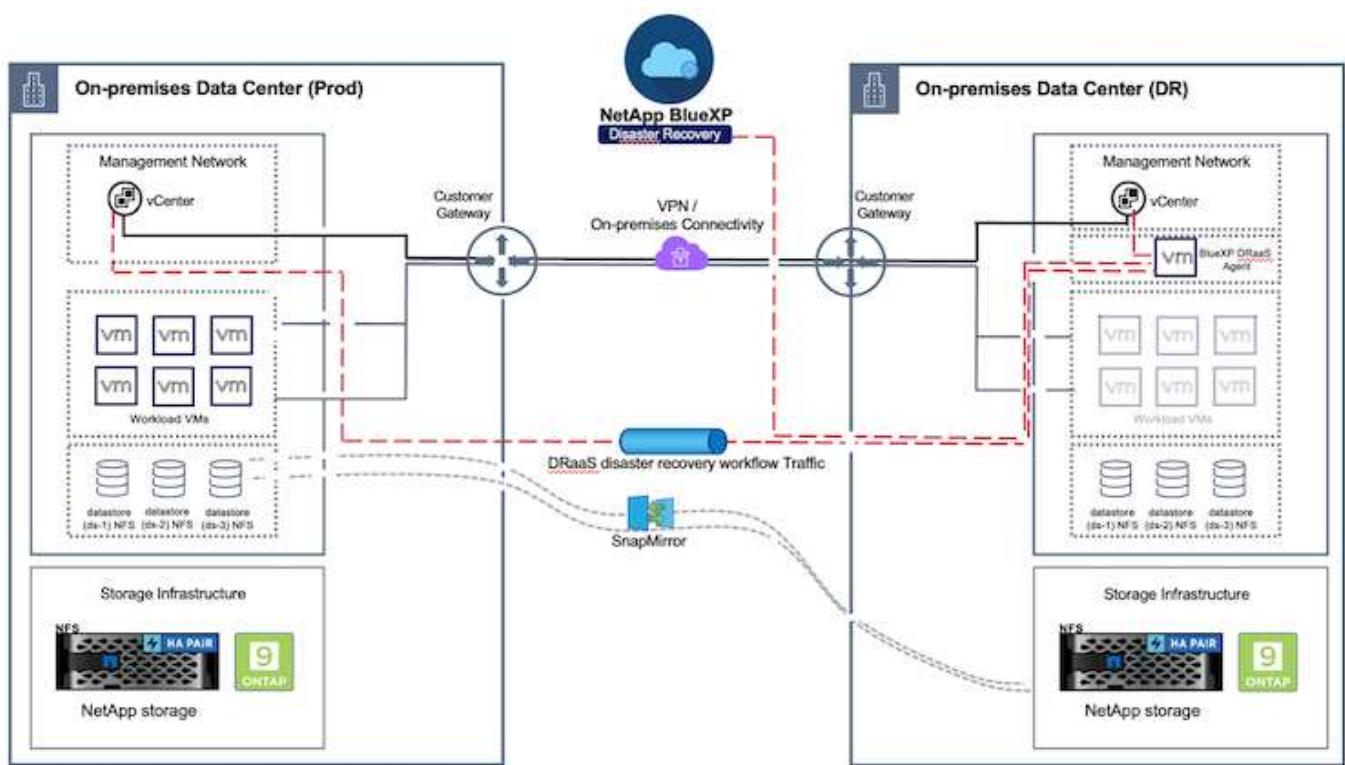
Implementing disaster recovery through block-level replication from the production site to the disaster recovery site is a resilient and cost-effective method for safeguarding workloads against site outages and data corruption events, such as ransomware attacks. Using NetApp SnapMirror replication, VMware workloads running on on-premises ONTAP systems with NFS datastore can be replicated to another ONTAP storage system located in a designated recovery datacenter where VMware is also deployed.

This section of the document describes the configuration of BlueXP DRaaS to set up disaster recovery for on-premises VMware VMs to another designated site. As part of this setup, the BlueXP account, BlueXP connector, the ONTAP arrays added within BlueXP workspace which is needed to enable communication from VMware vCenter to the ONTAP storage. In addition, this document details how to configure replication between

sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to failback when the primary site is recovered and brought online.

Utilizing the BlueXP disaster recovery service, integrated into the NetApp BlueXP console, companies can easily discover their on-premises VMware vCenters and ONTAP storage. Organizations can then create resource groupings, create a disaster recovery plan, associate it with resource groups, and test or execute failover and failback. SnapMirror provides storage-level block replication to keep the two sites up to date with incremental changes, resulting in a Recovery Point Objective (RPO) of up to 5 minutes. Additionally, it is possible to simulate disaster recovery procedures without affecting production or incurring additional storage costs.

BlueXP disaster recovery leverages ONTAP's FlexClone technology to create a space-efficient copy of the NFS datastore from the last replicated Snapshot on the disaster recovery site. After completing the disaster recovery test, customers can easily delete the test environment without impacting actual replicated production resources. In case of an actual failover, the BlueXP disaster recovery service orchestrates all the necessary steps to automatically bring up the protected virtual machines on the designated disaster recovery site with just a few clicks. The service will also reverse the SnapMirror relationship to the primary site and replicate any changes from the secondary to the primary for a failback operation, when needed. All these capabilities come at a fraction of the cost compared to other well-known alternatives.



## Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

1. Log in to BlueXP.
2. From the BlueXP left navigation, select Protection > Disaster recovery.
3. The BlueXP disaster recovery Dashboard appears.

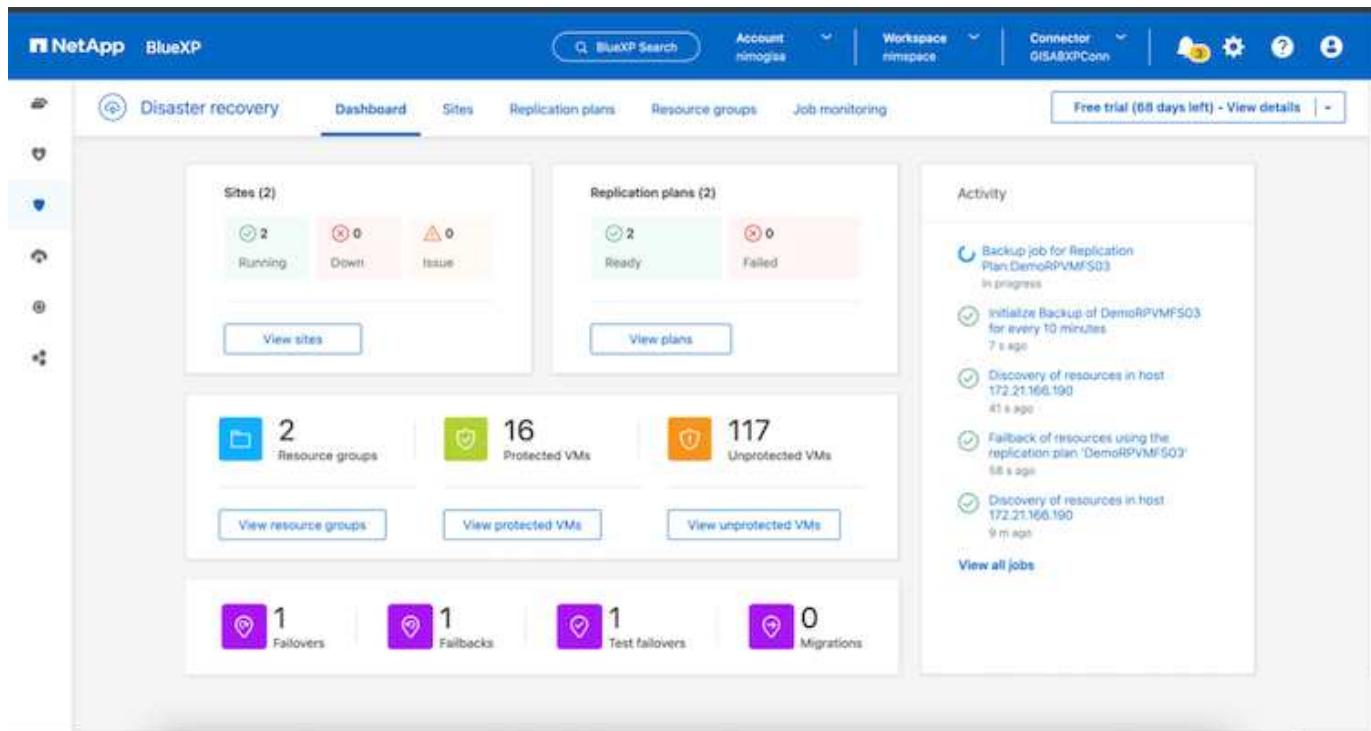
The screenshot shows the NetApp BlueXP interface. The left sidebar has a 'Disaster recovery' section highlighted with a red box. The main dashboard area includes a 'Replication plans (2)' section with 1 Ready and 2 Failed plans, and a 'Job monitoring' section with metrics for Protected VMs (21), Unprotected VMs (117), Failovers (1), Failbacks (1), Test failovers (2), and Migrations (0). On the right, there's an 'Activity' section listing recent backup jobs.

Before configuring disaster recovery plan, ensure the following pre-requisites are met:

- BlueXP Connector is set up in NetApp BlueXP.
- BlueXP connector instance have connectivity to the source and destination vCenter and storage systems.
- NetApp Data ONTAP cluster to provide storage NFS datastores.
- On-premises NetApp storage systems hosting NFS datastores for VMware are added in BlueXP.
- DNS resolution should be in place when using DNS names. Otherwise, use IP addresses for the vCenter.
- SnapMirror replication is configured for the designated NFS based datastore volumes.
- Make sure that the environment has supported versions of vCenter Server and ESXi servers.

Once the connectivity is established between the source and destination sites, proceed with configuration steps, which should take couple of clicks and about 3 to 5 minutes.

**i** NetApp recommends deploying the BlueXP connector in the destination site or in a third site, so that the BlueXP connector can communicate through the network with source and destination resources.

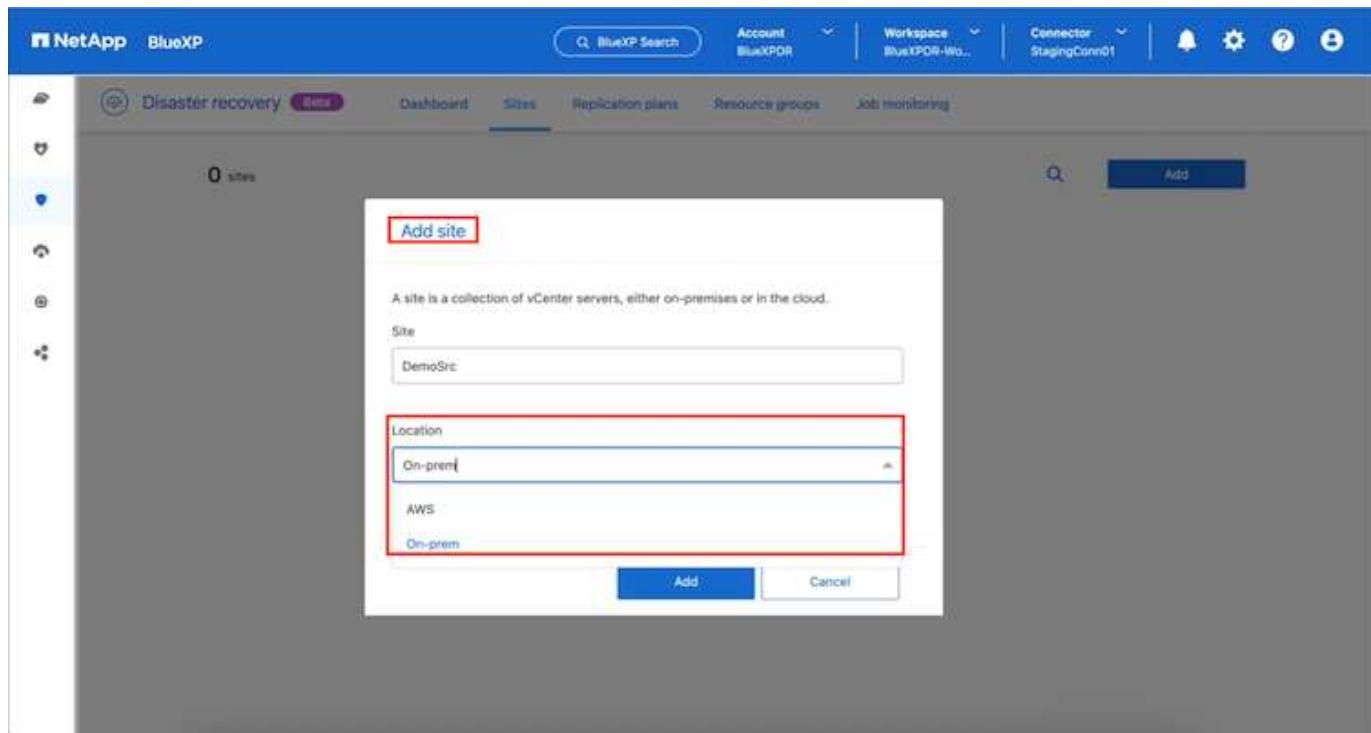


The screenshot shows the BlueXP Disaster Recovery dashboard. At the top, there are sections for 'Sites (2)' (2 Running, 0 Down, 0 Issues), 'Replication plans (2)' (2 Ready, 0 Failed), and 'Activity' (a list of recent events including backup jobs and resource discoveries). Below these are sections for 'Resource groups' (2), 'Protected VMs' (16), 'Unprotected VMs' (117), and 'Failovers' (1), 'Failbacks' (1), 'Test failovers' (1), and 'Migrations' (0).

## BlueXP disaster recovery configuration

The first step in preparing for disaster recovery is to discover and add the on-premises vCenter and storage resources to BlueXP disaster recovery.

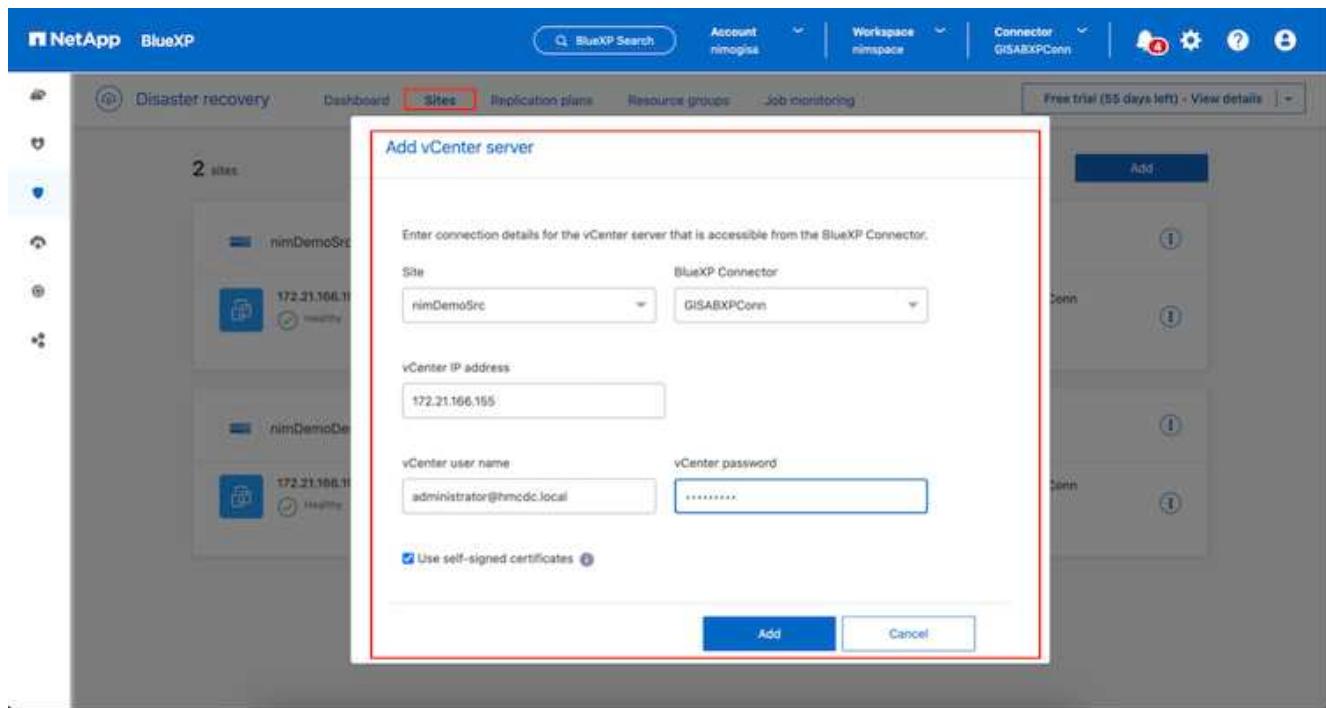
Open BlueXP console and select **Protection > Disaster Recovery** from left navigation. Select **Discover vCenter servers** or use top menu, Select **Sites > Add > Add vCenter**.



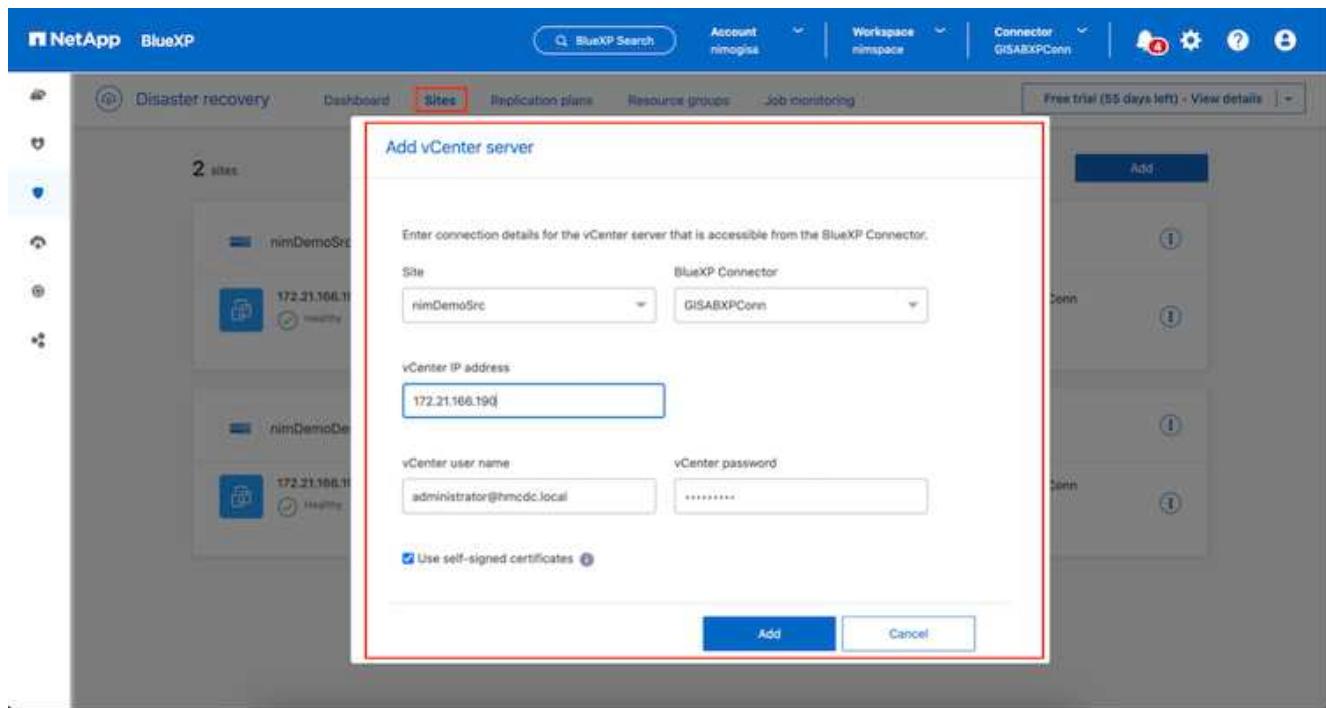
The screenshot shows the 'Add site' dialog box. It has fields for 'Site' (containing 'DemoSrc') and 'Location' (containing 'On-prem'). The 'Location' field is highlighted with a red box. At the bottom are 'Add' and 'Cancel' buttons.

Add the following platforms:

- **Source.** On-premises vCenter.



- **Destination.** VMC SDDC vCenter.



Once the vCenters are added, automated discovery is triggered.

## Configuring Storage replication between source site array and destination site array

SnapMirror provides data replication in a NetApp environment. Built on NetApp Snapshot technology,

SnapMirror replication is extremely efficient because it replicates only the blocks that have been changed or added since the previous update. SnapMirror is easily configured by using either NetApp OnCommand System Manager or the ONTAP CLI. BlueXP DRaaS also creates the SnapMirror relationship provided cluster and SVM peering is configured beforehand.

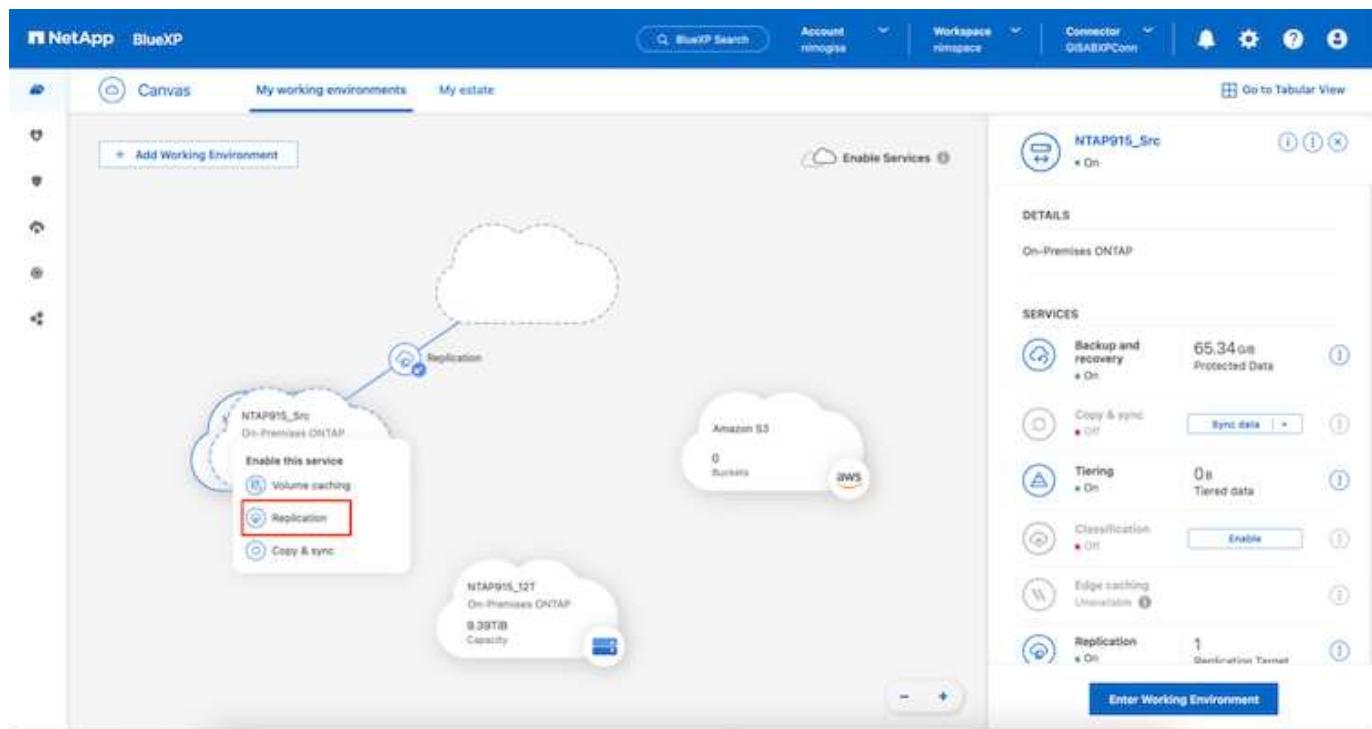
For cases in which the primary storage is not completely lost, SnapMirror provides an efficient means of resynchronizing the primary and DR sites. SnapMirror can resynchronize the two sites, transferring only changed or new data back to the primary site from the DR site by simply reversing the SnapMirror relationships. This means replication plans in BlueXP DRaaS can be resynchronized in either direction after a failover without recopying the entire volume. If a relationship is resynchronized in the reverse direction, only new data that was written since the last successful synchronization of the Snapshot copy is sent back to the destination.



If SnapMirror relationship is already configured for the volume via CLI or System Manager, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

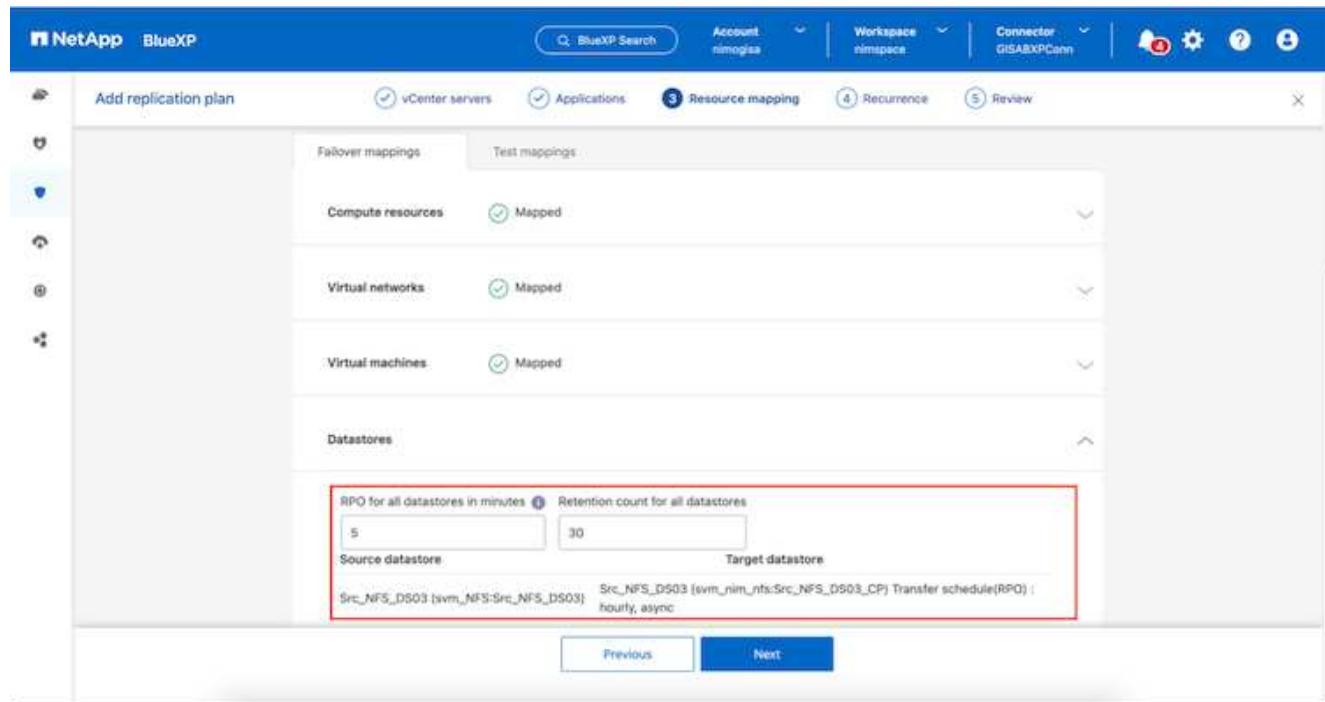
## How to set it up for VMware Disaster Recovery

The process to create SnapMirror replication remains the same for any given application. The process can be manual or automated. The easiest way is to leverage BlueXP to configure SnapMirror replication by using simple drag & drop of the source ONTAP system in the environment onto the destination to trigger the wizard that guides through the rest of the process.



BlueXP DRaaS can also automate the same provided the following two criteria's are met:

- Source and destination clusters have a peer relationship.
- Source SVM and destination SVM have a peer relationship.

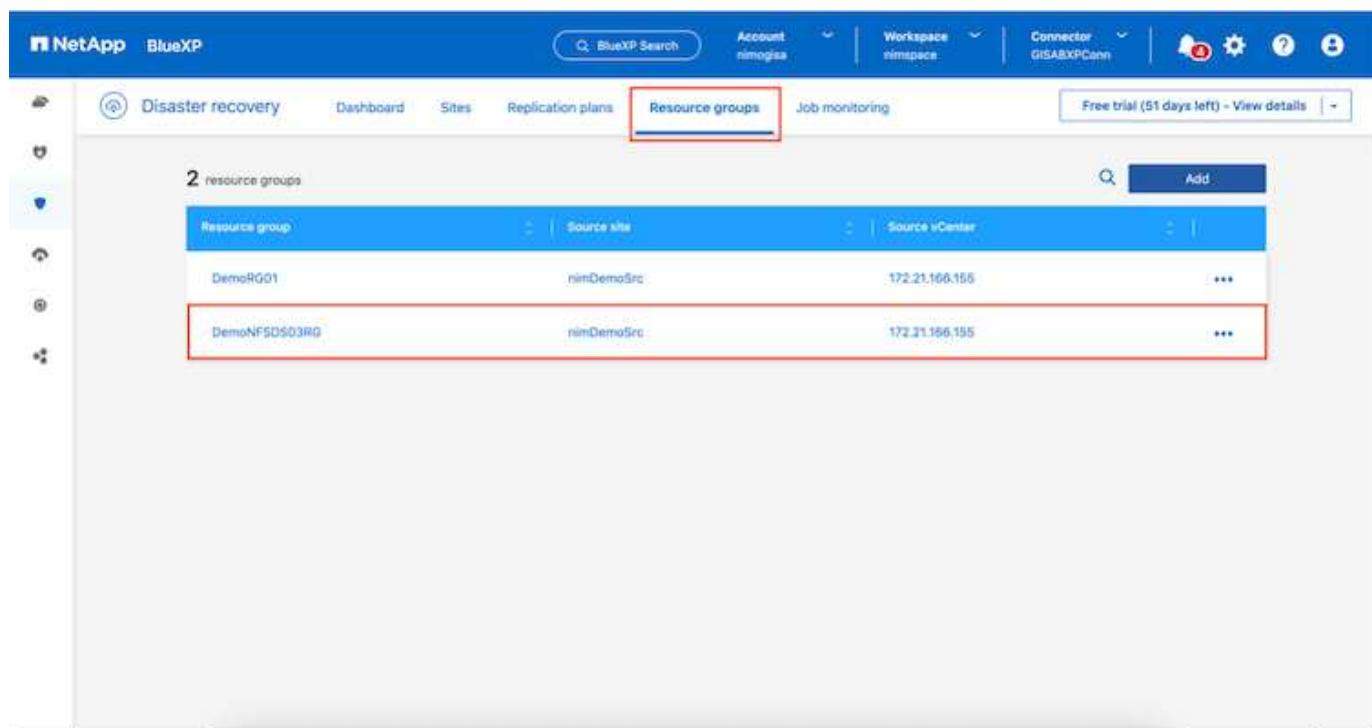
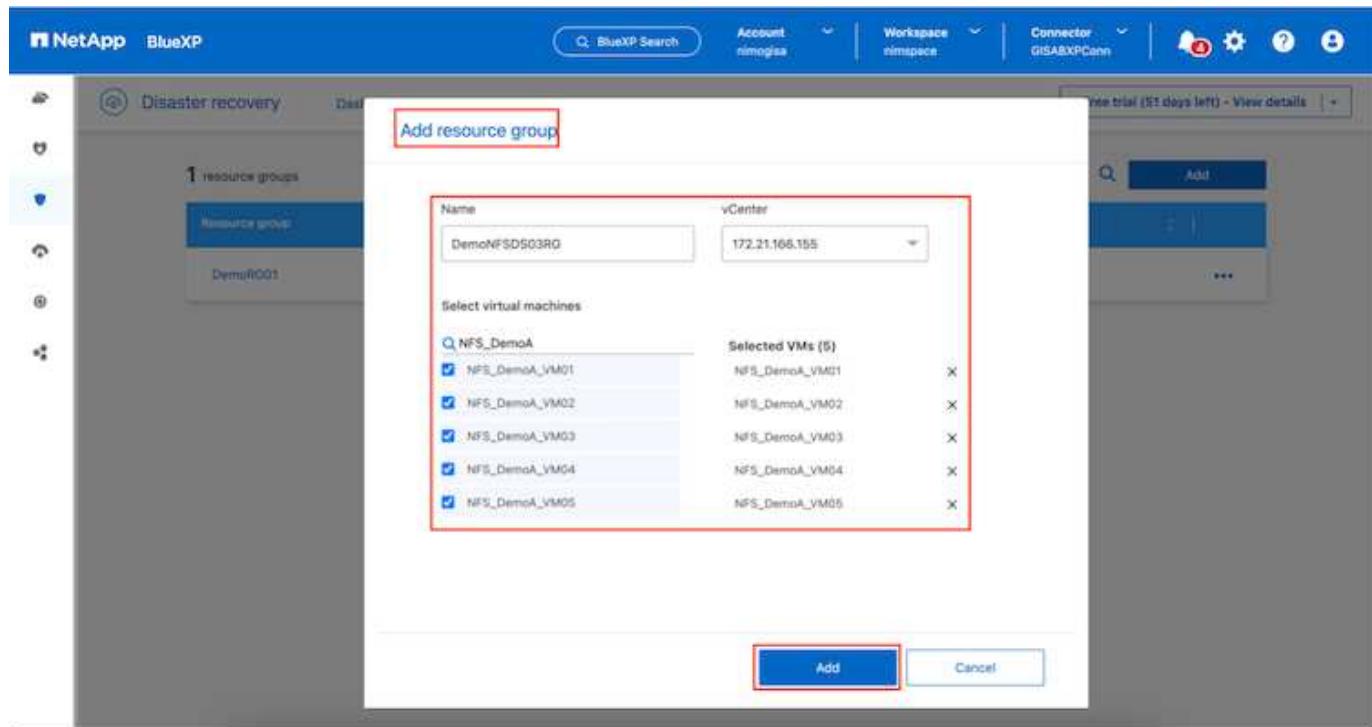


If SnapMirror relationship is already configured for the volume via CLI, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.

## What can BlueXP disaster recovery do for you?

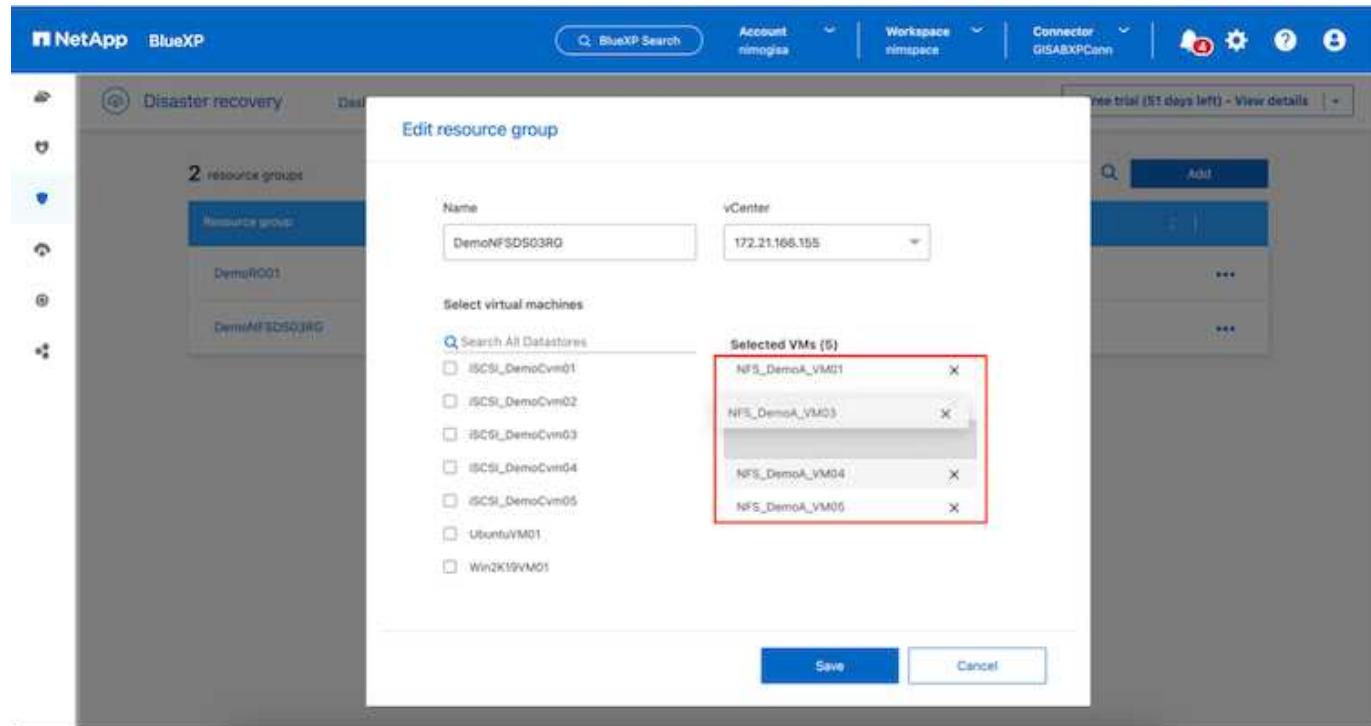
After the source and destination sites are added, BlueXP disaster recovery performs automatic deep discovery and displays the VMs along with associated metadata. BlueXP disaster recovery also automatically detects the networks and port groups used by the VMs and populates them.

After the sites have been added, VMs can be grouped into resource groups. BlueXP disaster recovery resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders and boot delays that can be executed upon recovery. To start creating resource groups, navigate to **Resource Groups** and click **Create New Resource Group**.

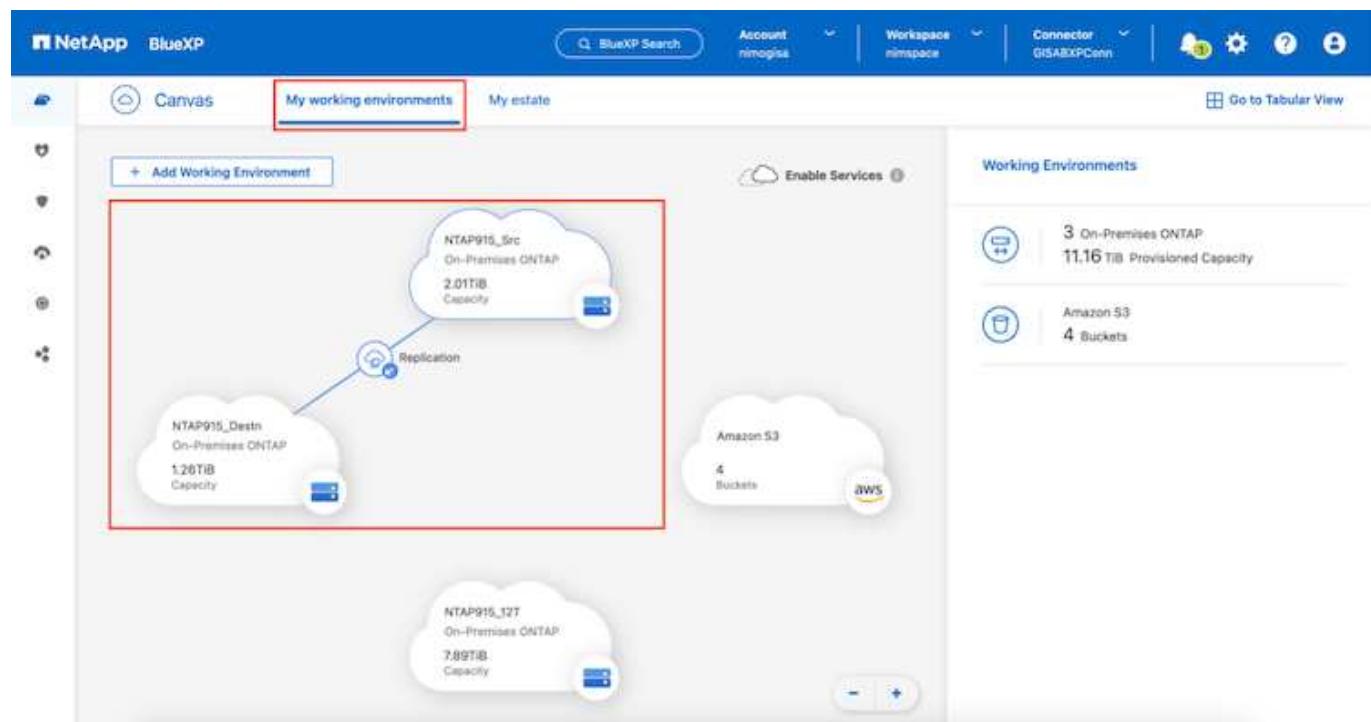


The resource group can also be created while creating a replication plan.

The boot order of the VMs can be defined or modified during the creation of resource groups by using simple drag and drop mechanism.



Once the resource groups are created, the next step is to create the execution blueprint or a plan to recover virtual machines and applications in the event of a disaster. As mentioned in the prerequisites, SnapMirror replication can be configured beforehand or DRaaS can configure it using the RPO and retention count specified during creation of the replication plan.



Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful
Green	NTAP915_Src	NTAP915_Destn	24.5 MB	idle	snapmirrored	
Green	Demo_TPS_DS01 NTAP915_Src	Demo_TPS_DS01_Copy NTAP915_Destn	13 seconds	idle	snapmirrored	Aug 5, 2024, 6:16 386.63 MB
Green	Src_25G_Vol01 NTAP915_Src	Src_25G_Vol01_Copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:3 79.23 MB
Green	Src_NFS_DS03 NTAP915_Src	Src_NFS_DS03_Copy NTAP915_Destn	12 seconds	idle	snapmirrored	Aug 16, 2024, 12:3 24.84 MB
Green	Src_NFS_DS04 NTAP915_Src	Src_NFS_DS04_Copy NTAP915_Destn	3 seconds	idle	snapmirrored	Aug 16, 2024, 12:3 47.38 MB
Green	Src_iSCSI_DS04 NTAP915_Src	Src_iSCSI_DS04_copy NTAP915_Destn	4 seconds	idle	snapmirrored	Aug 16, 2024, 12:3 108.87 MB
Green	nimbra NTAP915_Src	nimbra_dest NTAP915_Destn	2 seconds	idle	snapmirrored	Aug 16, 2024, 12:3 3.48 KB

Configure the replication plan by selecting the source and destination vCenter platforms from the drop down and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and networks. To define the recovery plan, navigate to the **Replication Plan** tab and click **Add Plan**.

First, select the source vCenter and then select the destination vCenter.

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

Replication plan name  
DemoNFSDS03RP

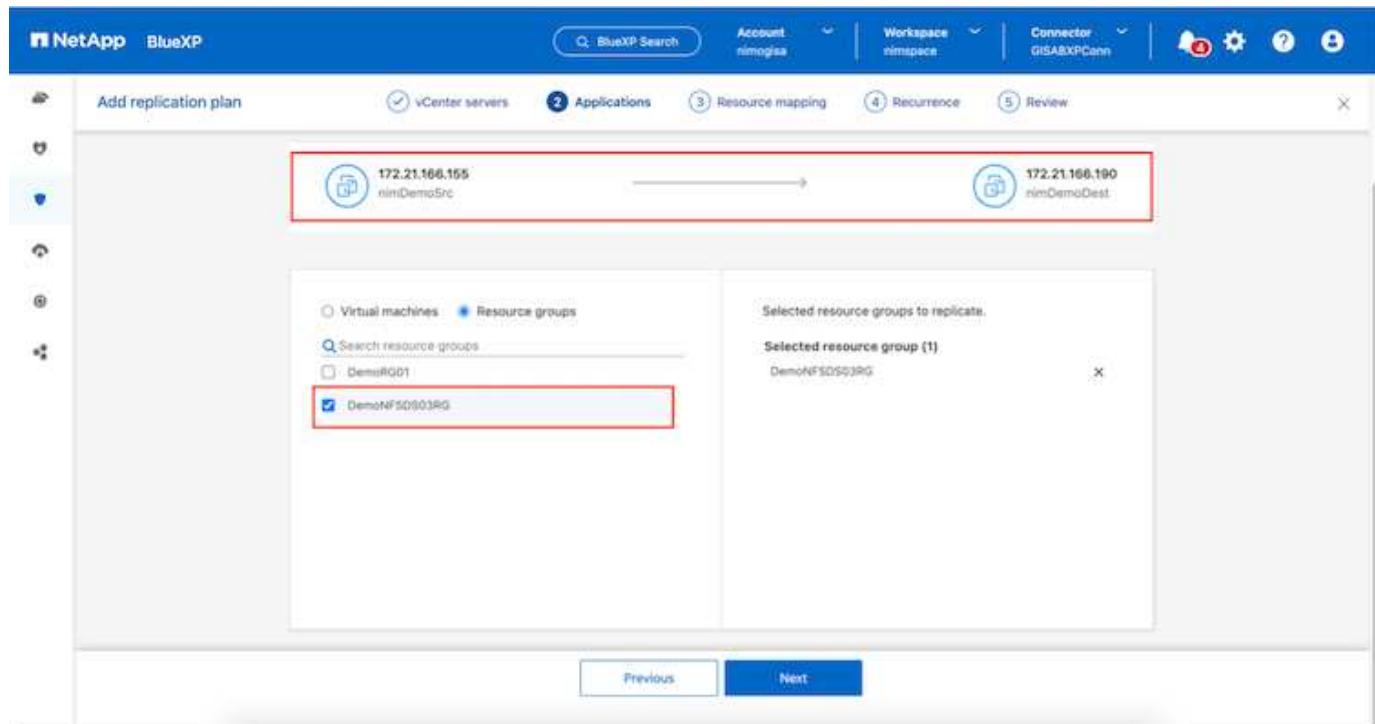
Select a source vCenter where your data exists, to replicate to the selected target vCenter.

Source vCenter: 172.21.106.155 Target vCenter: 172.21.106.190

Cancel Next

The next step is to select existing resource groups. If no resource groups created, then the wizard helps to group the required virtual machines (basically create functional resource groups) based on the recovery objectives. This also helps define the operation sequence of how application virtual machines should be

restored.

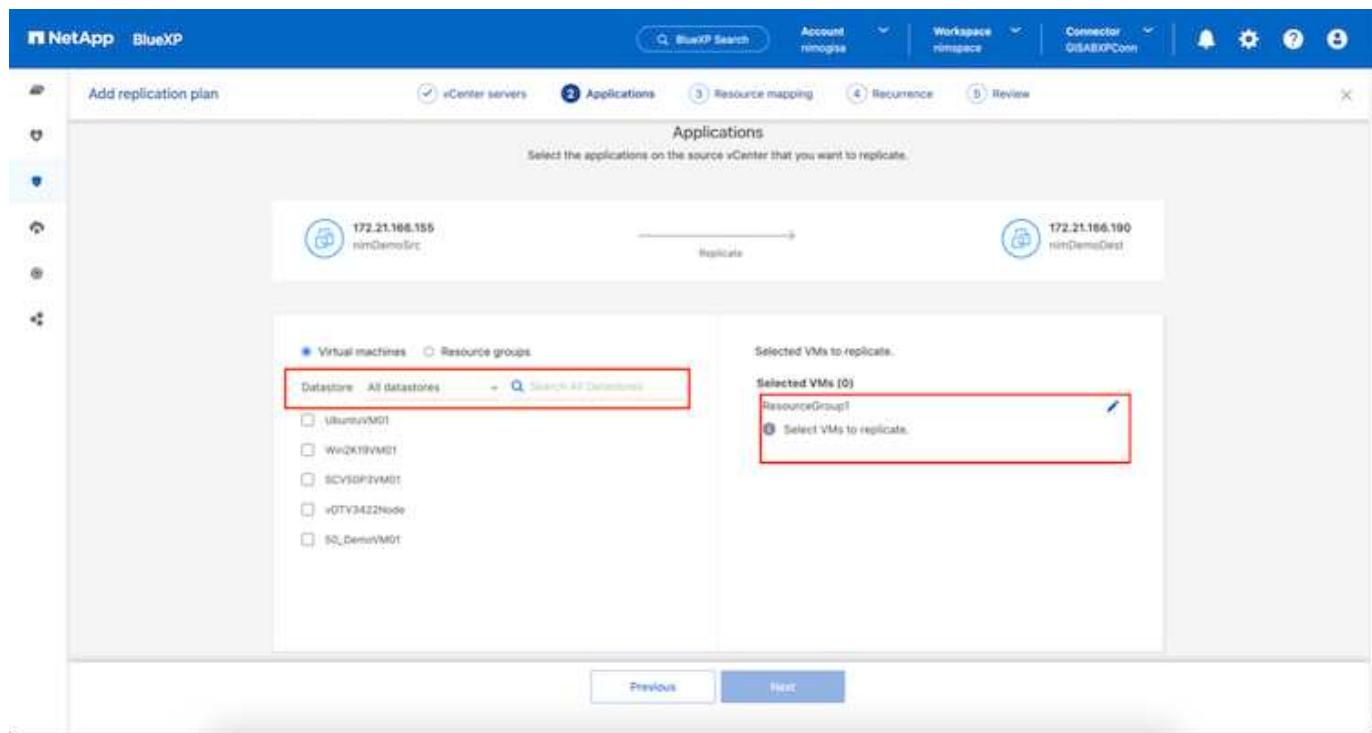


Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.

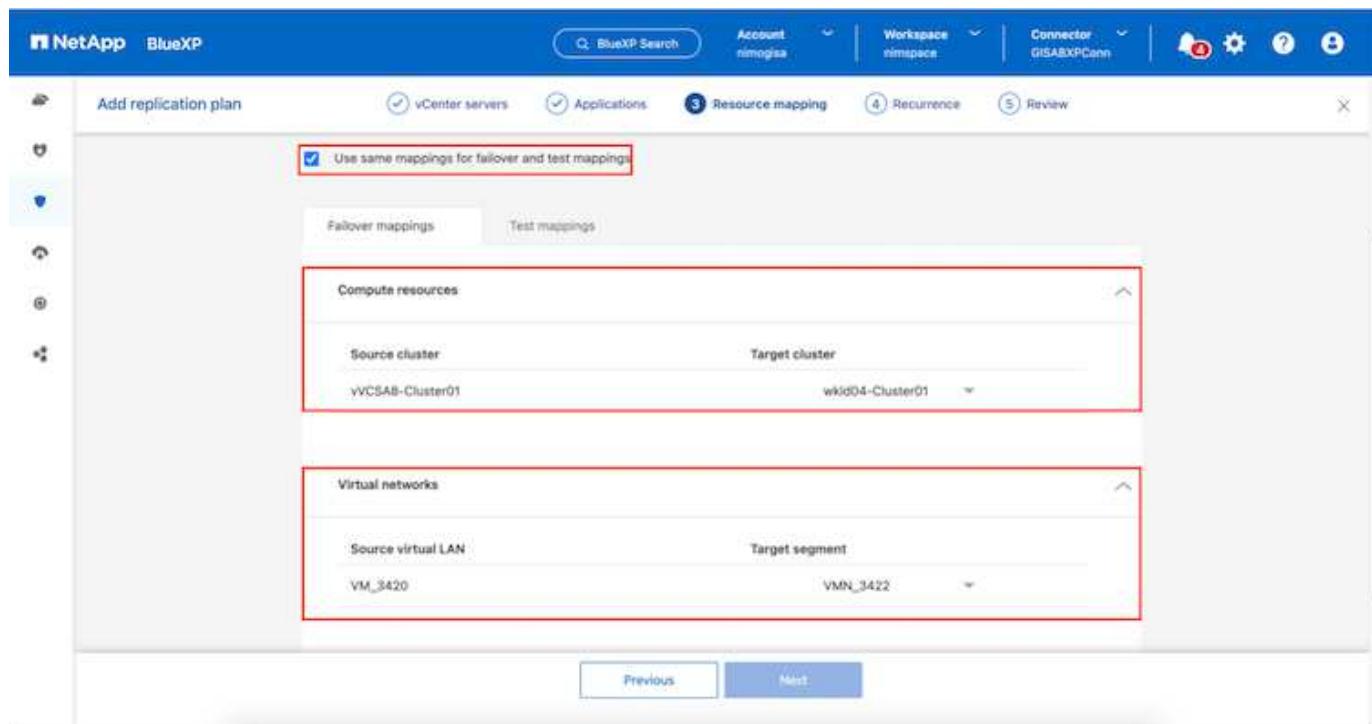


Each virtual machine within a resource group is started in sequence based on the order. Two resource groups are started in parallel.

The below screenshot shows the option to filter virtual machines or specific datastores based on organizational requirements if resource groups are not created beforehand.



Once the resource groups are selected, create the failover mappings. In this step, specify how the resources from the source environment maps to the destination. This includes compute resources, virtual networks. IP customization, pre- and post-scripts, boot delays, application consistency and so on. For detailed information, refer to [Create a replication plan](#).



 By default, same mapping parameters are used for both test and failover operations. To set different mappings for test environment, select the Test mapping option after unchecking the checkbox as shown below:

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
NFS_DemoA_VM01	2	4 GB	0	<input type="checkbox"/>
NFS_DemoA_VM02	2	4 GB	0	<input type="checkbox"/>

Once the resource mapping is complete, click Next.

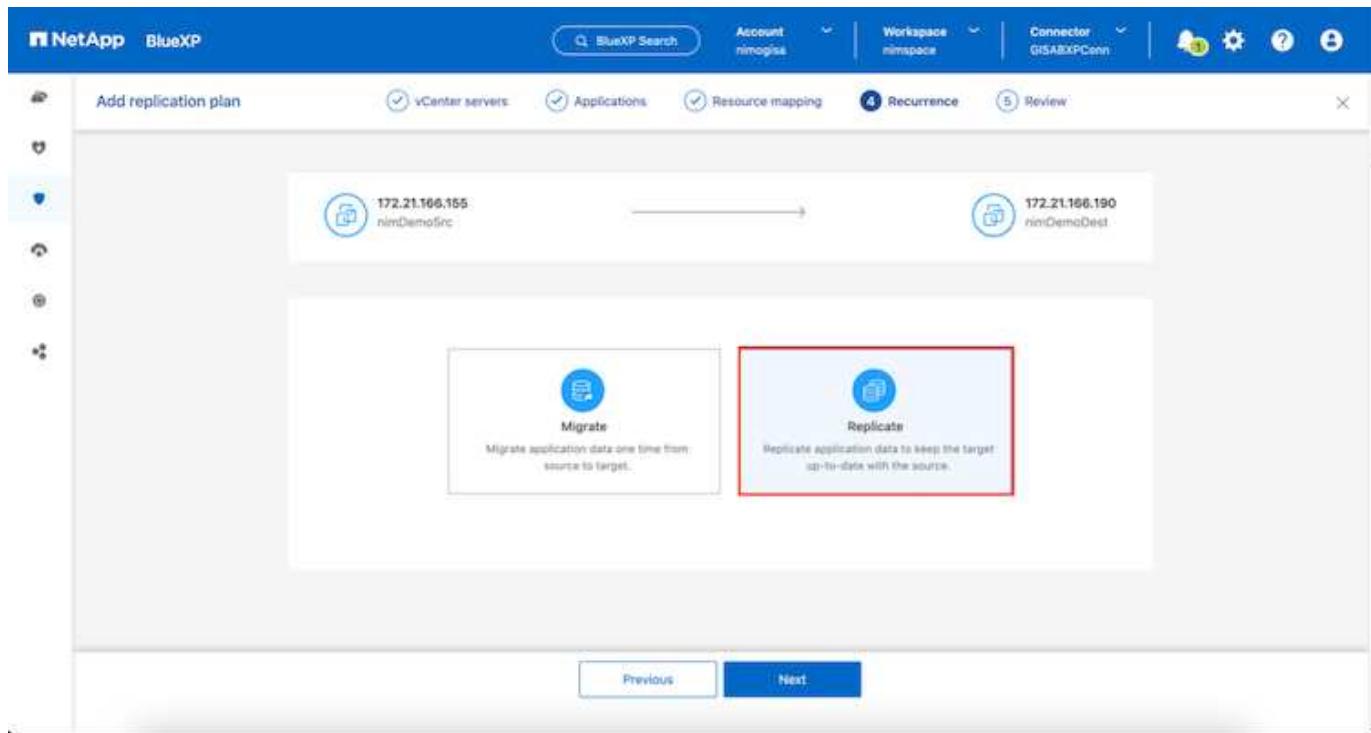
172.21.166.165  
nimDemoSrc

172.21.166.190  
nimDemoDest

Use same mappings for failover and test mappings

Failover mappings	Test mappings
Compute resources	<input checked="" type="checkbox"/> Mapped
Virtual networks	<input checked="" type="checkbox"/> Mapped
Virtual machines	<input checked="" type="checkbox"/> Mapped

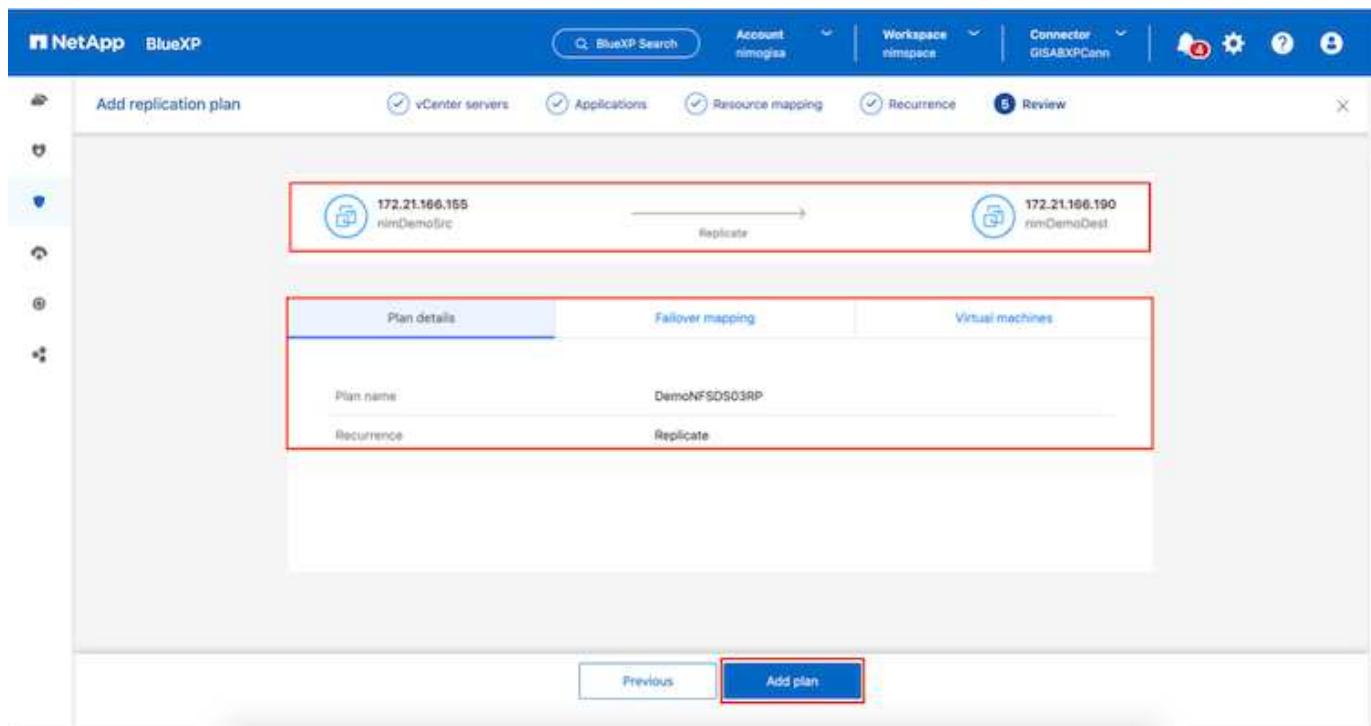
Select the recurrence type. In simple words, select Migrate (one time migration using failover) or recurring continuous replication option. In this walkthrough, Replicate option is selected.



Once done, review the created mappings and then click on **Add plan**.



VMs from different volumes and SVMs can be included in a replication plan. Depending on the VM placement (be it on same volume or separate volume within the same SVM, separate volumes on different SVMs), the BlueXP disaster recovery creates a Consistency Group Snapshot.



1 plans

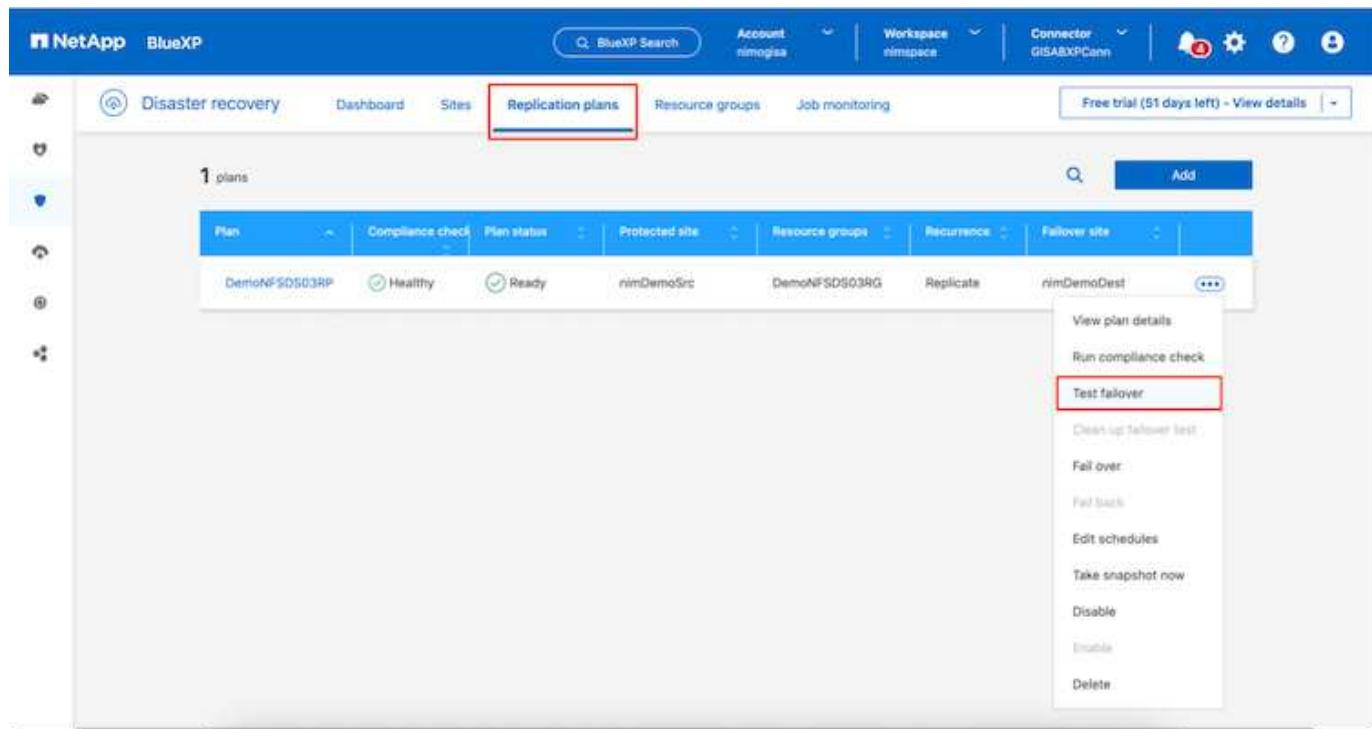
Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site
DemoNFS503RP	Healthy	Ready	nimDemoSrc	DemoNFS503RG	Replicate	nimDemoDest

BlueXP DRaaS consists of the following workflows:

- Test failover (including periodic automated simulations)
- Cleanup failover test
- Failover
- Failback

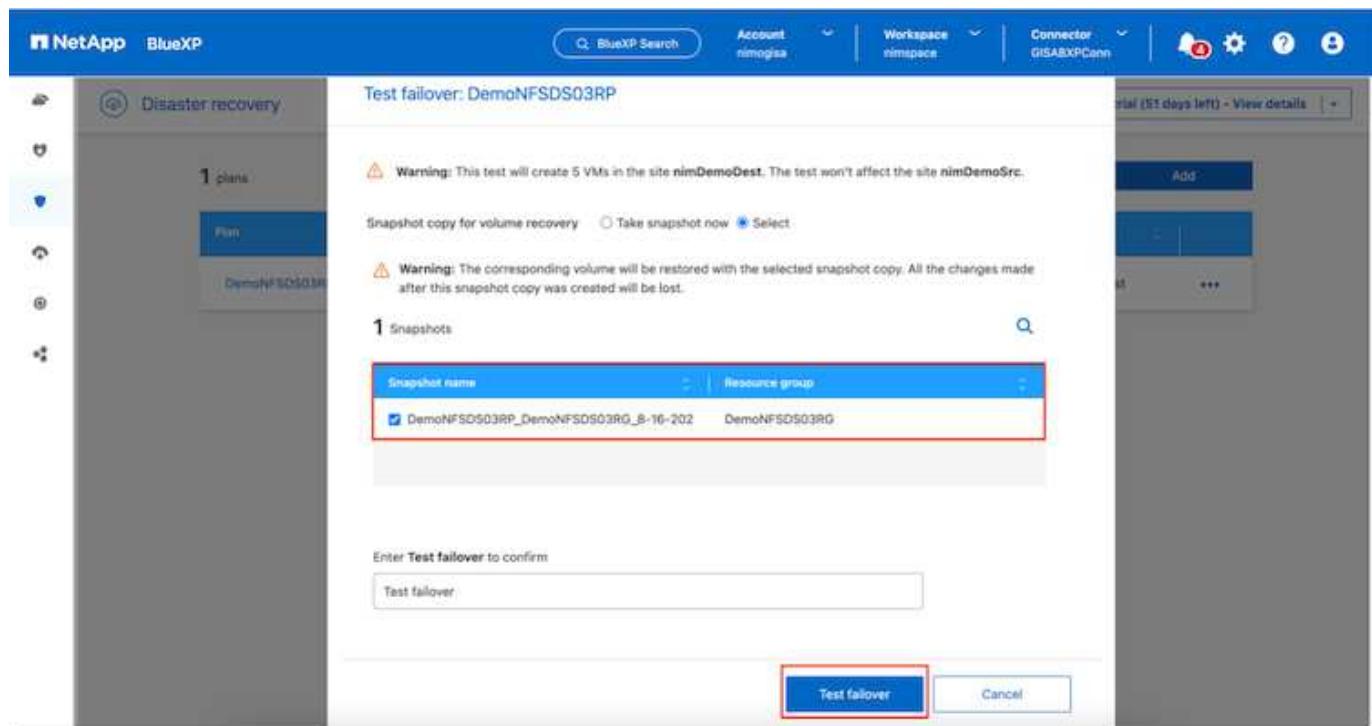
## Test failover

Test failover in BlueXP DRaaS is an operational procedure that allows VMware administrators to fully validate their recovery plans without disrupting their production environments.



The screenshot shows the NetApp BlueXP interface with the 'Replication plans' tab selected. A context menu is open for a plan named 'DemoNFSDS03RP', with the 'Test failover' option highlighted. Other options in the menu include 'View plan details', 'Run compliance check', 'Fail over', 'Edit schedules', 'Take snapshot now', 'Disable', 'Enable', and 'Delete'.

BlueXP DRaaS incorporates the ability to select the snapshot as an optional capability in the test failover operation. This capability allows the VMware administrator to verify that any changes that were recently made in the environment are replicated to the destination site and thus are present during the test. Such changes include patches to the VM guest operating system



The screenshot shows the 'Test failover: DemoNFSDS03RP' dialog box. It displays a warning that the test will create 5 VMs in the destination site and won't affect the source site. It also shows a radio button for 'snapshot copy for volume recovery' with 'Select' (radioed) and 'Take snapshot now' (unchecked). A warning message states that the corresponding volume will be restored with the selected snapshot copy, and all changes made after its creation will be lost. A table lists a single snapshot with the name 'DemoNFSDS03RP\_DemoNFSDS03RG\_B-16-202' and resource group 'DemoNFSDS03RG'. At the bottom, a text field 'Enter Test failover to confirm' contains 'Test failover', and the 'Test failover' button is highlighted with a red box.

When the VMware administrator runs a test failover operation, BlueXP DRaaS automates the following tasks:

- Triggering SnapMirror relationships to update storage at the destination site with any recent changes that were made at the production site.

- Creating NetApp FlexClone volumes of the FlexVol volumes on the DR storage array.
- Connecting the NFS datastores in the FlexClone volumes to the ESXi hosts at the DR site.
- Connecting the VM network adapters to the test network specified during the mapping.
- Reconfiguring the VM guest operating system network settings as defined for the network at the DR site.
- Executing any custom commands that have been stored in the replication plan.
- Powering on the VMs in the order that is defined in the replication plan.

The screenshot shows the vSphere Client interface. The left sidebar shows a tree view of datastores: 'wklid04-vc01.hmc0c.local' (selected), 'wklid04-DC01' (selected), '04Testbed\_DS01', '150Dumb', 'Src\_NFS\_DS03' (highlighted with a red box), 'tempdel', and 'wklid04\_Dstn\_DS01'. The main content area has two tabs: 'Details' and 'Capacity and Usage'. The 'Details' tab shows the following information for 'Src\_NFS\_DS03':
 

Type	NFS 3
Hosts	2
Virtual machines	5
VM templates	0
Server	172.21.10.6.166
Folder	/irc_NFS_DS03_TEST
Location	gs://vmfs/volume/10c80c2d-1e68749d/

 The 'Capacity and Usage' tab shows:
 

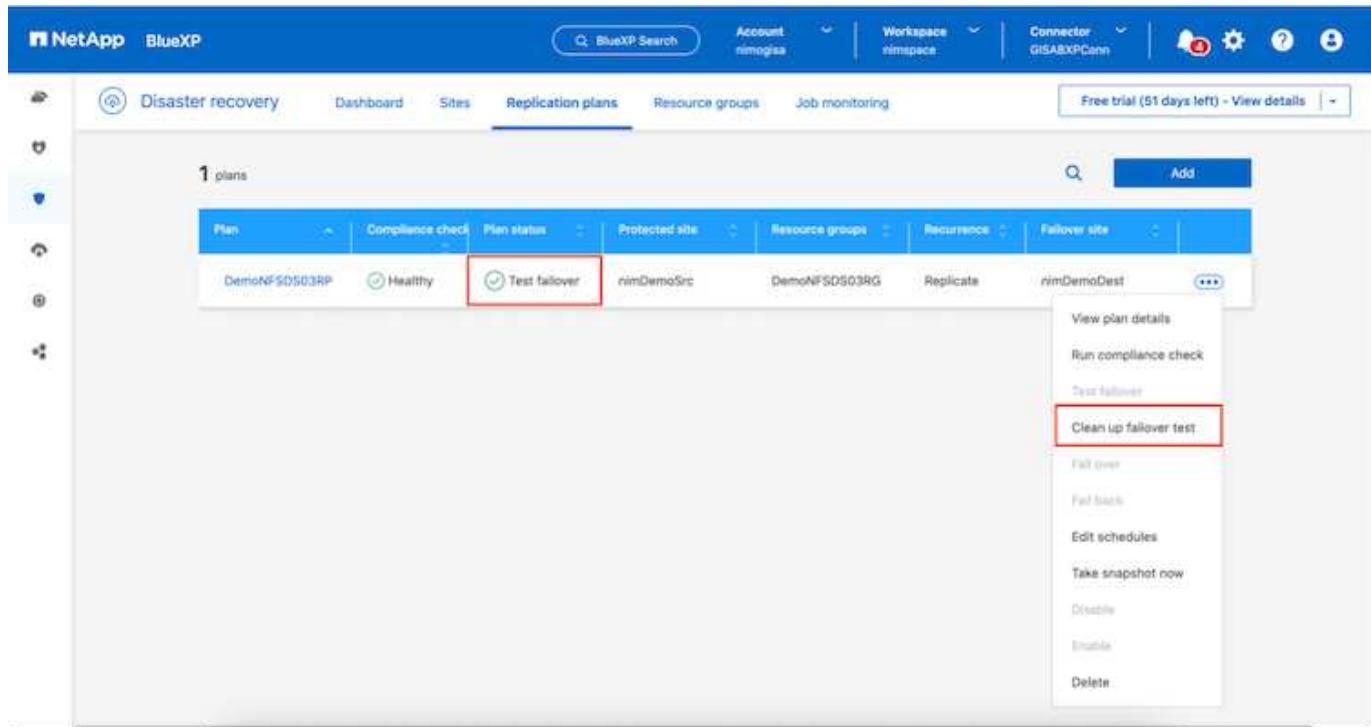
Storage	71.22 GB free
26.78 GB Used	100 GB capacity

 Below these tabs are 'VIEW STATS' and 'REFRESH' buttons. At the bottom of the screen, there is a table titled 'Recent Tasks' with the following data:
 

Task Name	Target	Status	Details	Owner	Queued For	Start Time	Completion Time	Set
Reconfigure virtual machine	ME5_DemoA_VM02	Completed		HMC0C.LOCAL\Administrator	3 ms	08/16/2024, 6:53:59 A	08/16/2024, 6:53:59 A	...
Register virtual machine	host04-DC01	Completed		System	6 ms	08/16/2024, 6:53:58 A	08/16/2024, 6:53:59 A	...
Register virtual machine	host04-DC01	Completed		System	2 ms	08/16/2024, 6:53:58 A	08/16/2024, 6:53:59 A	...
Register virtual machine	host04-DC01	Completed	Registering Virtual Machine on destination host	System	2 ms	08/16/2024, 6:53:58 A	08/16/2024, 6:54:00 A	...

## Cleanup failover test Operation

The cleanup failover test operation occurs after the replication plan test has been completed and the VMware administrator responds to the cleanup prompt.



The screenshot shows the NetApp BlueXP web interface. At the top, there are navigation tabs: Disaster recovery, Dashboard, Sites, Replication plans (which is the active tab), Resource groups, and Job monitoring. A search bar and account information are also at the top. The main content area shows a table with one plan entry. The columns in the table are: Plan, Compliance check, Plan status, Protected site, Resource groups, Recurrence, and Failover site. The 'Plan' column shows 'DemoNFSD503RP', 'Compliance check' shows 'Healthy', 'Plan status' shows a green checkmark and 'Test failover' (which is highlighted with a red box). The 'Protected site' column shows 'nimDemoSrc', 'Resource groups' shows 'DemoNFSD503RG', 'Recurrence' shows 'Replicate', and 'Failover site' shows 'nimDemoDest'. A context menu is open on the right side of the 'Test failover' button, listing options: View plan details, Run compliance check, Test failover (which is highlighted with a red box), Clean up failover test (which is also highlighted with a red box), Fail over, Fail back, Edit schedules, Take snapshot now, Disable, Enable, and Delete.

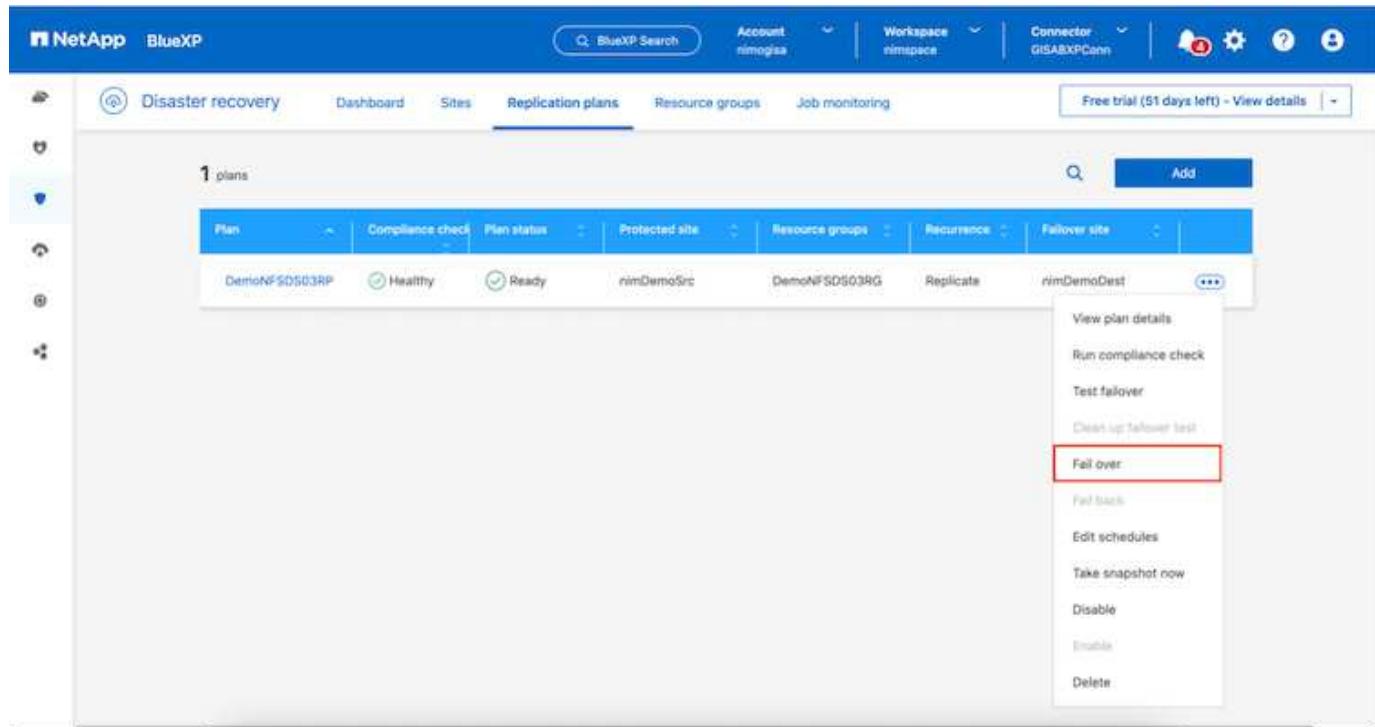
This action will reset the virtual machines (VMs) and the status of the replication plan to the ready state.

When the VMware administrator performs a recovery operation, BlueXP DRaaS completes the following process:

1. It powers off each recovered VM in the FlexClone copy that was used for testing.
2. It deletes the FlexClone volume that was used to present the recovered VMs during the test.

## Planned Migration and Fail over

BlueXP DRaaS has two methods for performing a real failover: planned migration and fail over. The first method, planned migration, incorporates VM shutdown and storage replication synchronization into the process to recover or effectively move the VMs to the destination site. Planned migration requires access to the source site. The second method, failover, is a planned/unplanned failover in which the VMs are recovered at the destination site from the last storage replication interval that was able to complete. Depending on the RPO that was designed into the solution, some amount of data loss can be expected in the DR scenario.



The screenshot shows the NetApp BlueXP Disaster recovery interface. The top navigation bar includes 'NetApp BlueXP', 'BlueXP Search' (with a search bar), 'Account nimgras', 'Workspace nimspace', 'Connector GISABXPConn', and various user icons. The main menu has tabs for 'Disaster recovery', 'Dashboard', 'Sites', 'Replication plans' (which is selected and highlighted in blue), 'Resource groups', and 'Job monitoring'. A banner at the top right indicates a 'Free trial (51 days left) - View details'. The 'Replication plans' section shows 1 plan: 'DemoNFS03RP'. The plan details are: 'Compliance check' (Healthy), 'Plan status' (Ready), 'Protected site' (nimDemoSrc), 'Resource groups' (DemoNFS03RG), 'Recurrence' (Replicate), and 'Failover site' (nimDemoDest). A context menu is open for this plan, listing options: 'View plan details', 'Run compliance check', 'Test failover', 'Clean up failover test', 'Fail over' (which is highlighted with a red box), 'Edit schedule', 'Take snapshot now', 'Disable', 'Enable', and 'Delete'.

When the VMware administrator performs a failover operation, BlueXP DRaaS automates the following tasks:

- Break and fail over the NetApp SnapMirror relationships.
- Connect the replicated NFS datastores to the ESXi hosts at the DR site.
- Connect the VM network adapters to the appropriate destination site network.
- Reconfigure the VM guest operating system network settings as defined for the network at the destination site.
- Execute any custom commands (if any) that have been stored in the replication plan.
- Power on the VMs in the order that was defined in the replication plan.

Recent Tasks

Task Name	Target	Status	Details	Initiator	Queried 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	Powering on the new Virtual Machine	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.

## Failback

A failback is an optional procedure that restores the original configuration of the source and destination sites after a recovery.

Replication plans

1 plans

Plan	Compliance check	Plan status	Protected site	Resource groups	Recurrence	Failover site
DemoNFS03RP	Healthy	Failed over	nimDemoSrc	DemoNFS03RG	Replicate	nimDemoDest

Fail back

VMware administrators can configure and run a failback procedure when they are ready to restore services to the original source site.

**NOTE:** BlueXP DRaaS replicates (resyncs) any changes back to the original source virtual machine before reversing the replication direction. This process starts from a relationship that has completed failing over to a

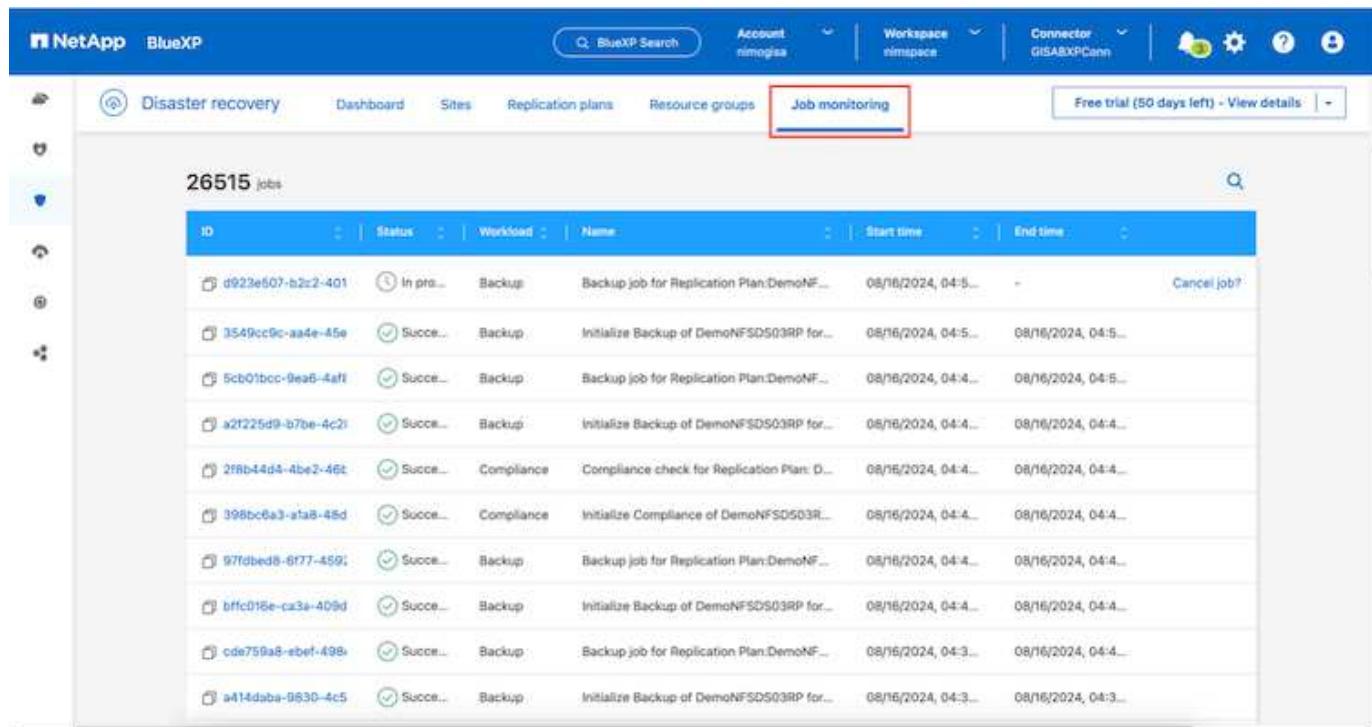
target and involves the following steps:

- Power off and unregister the virtual machines and volumes on the destination site are unmounted.
- Break the SnapMirror relationship on the original source is broken to make it read/write.
- Resynchronize the SnapMirror relationship to reverse the replication.
- Mount the volume on the source, power on and register the source virtual machines.

For more details about accessing and configuring BlueXP DRaaS, see the [Learn about BlueXP Disaster Recovery for VMware](#).

## Monitoring and Dashboard

From BlueXP or the ONTAP CLI, you can monitor the replication health status for the appropriate datastore volumes, and the status of a failover or test failover can be tracked via Job Monitoring.

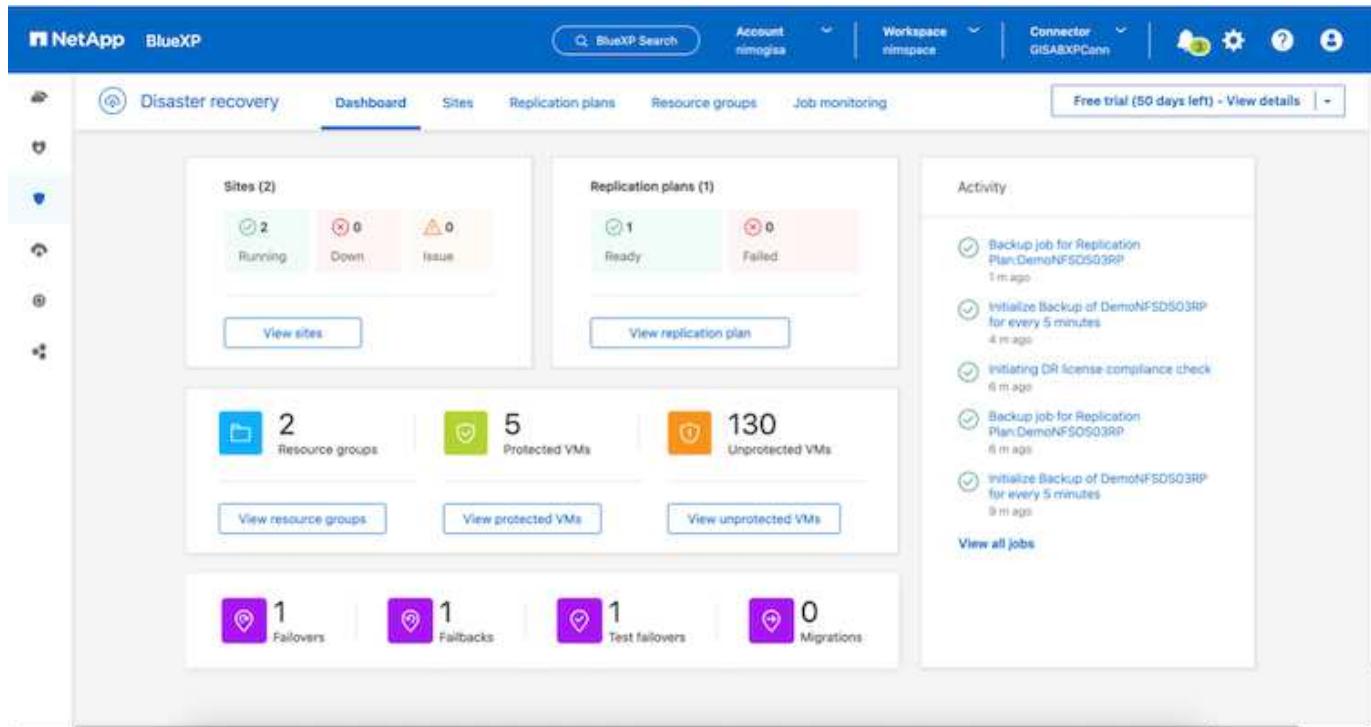


ID	Status	Workload	Name	Start time	End time	Cancel job?
d923e507-b2c2-401	In pro...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:5...	-	Cancel job?
3549cc0c-aa4e-45e	Succ...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:5...	08/16/2024, 04:5...	
5cb01bcc-9ea6-4aft	Succ...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:5...	
a2f225d9-b7be-4c2t	Succ...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
2f8b44d4-4be2-46t	Succ...	Compliance	Compliance check for Replication Plan: D...	08/16/2024, 04:4...	08/16/2024, 04:4...	
398bc6a3-ata8-45d	Succ...	Compliance	Initialize Compliance of DemoNFS03RP...	08/16/2024, 04:4...	08/16/2024, 04:4...	
97fdbed8-8f77-459t	Succ...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:4...	08/16/2024, 04:4...	
bff016e-ca3a-409d	Succ...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:4...	08/16/2024, 04:4...	
cde759a8-ebe1-498t	Succ...	Backup	Backup job for Replication Plan: DemoNF...	08/16/2024, 04:3...	08/16/2024, 04:4...	
a414daba-0830-4c5	Succ...	Backup	Initialize Backup of DemoNFS03RP for...	08/16/2024, 04:3...	08/16/2024, 04:3...	



If a job is currently in progress or queued, and you wish to stop it, there is an option to cancel it.

With the BlueXP disaster recovery dashboard, confidently evaluate the status of disaster recovery sites and replication plans. This enables administrators to swiftly identify healthy, disconnected, or degraded sites and plans.



This provides a powerful solution to handle a tailored and customized disaster recovery plan. Failover can be done as planned failover or failover with a click of a button when disaster occurs and decision is made to activate the DR site.

To learn more about this process, feel free to follow the detailed walkthrough video or use the [solution simulator](#).

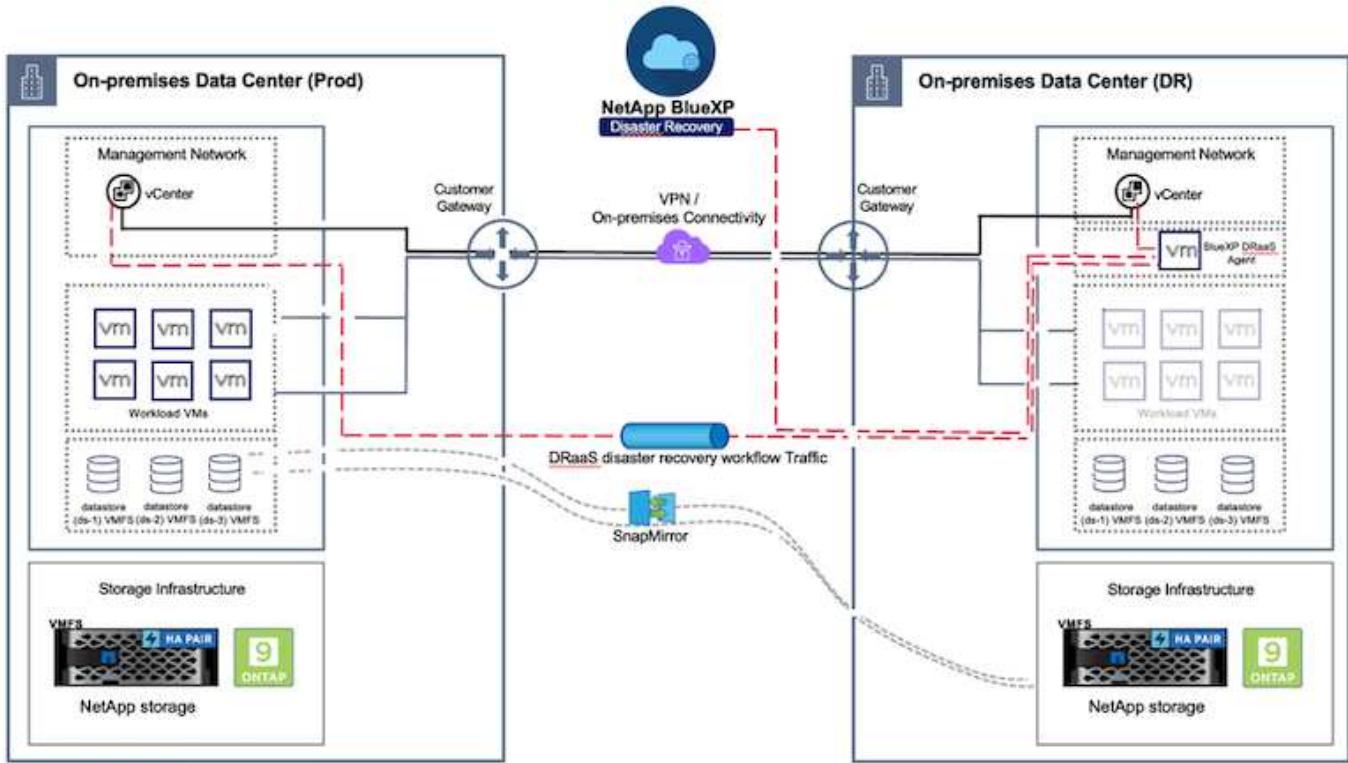
## DR using BlueXP DRaaS for VMFS Datastores

Disaster recovery using block-level replication from production site to disaster recovery site is a resilient and cost-effective way of protecting the workloads against site outages and data corruption events, like ransomware attacks. With NetApp SnapMirror replication, VMware workloads running on-premises ONTAP systems using VMFS datastore can be replicated to another ONTAP storage system in a designated recovery datacenter where VMware resides

This section of the document describes the configuration of BlueXP DRaaS to set up disaster recovery for on-premises VMware VMs to another designated site. As part of this setup, the BlueXP account, BlueXP connector, the ONTAP arrays added within BlueXP workspace which is needed to enable communication from VMware vCenter to the ONTAP storage. In addition, this document details how to configure replication between sites and how to setup and test a recovery plan. The last section has instructions for performing a full site failover and how to fallback when the primary site is recovered and brought online.

Using the BlueXP disaster recovery service, which is integrated into the NetApp BlueXP console, customers can discover their on-premises VMware vCenters along with ONTAP storage, create resource groupings, create a disaster recovery plan, associate it with resource groups, and test or execute failover and fallback. SnapMirror provides storage-level block replication to keep the two sites up to date with incremental changes, resulting in a RPO of up to 5 minutes. It is also possible to simulate DR procedures as a regular drill without impacting the production and replicated datastores or incurring additional storage costs. BlueXP disaster recovery takes advantage of ONTAP's FlexClone technology to create a space-efficient copy of the VMFS

datastore from the last replicated Snapshot on the DR site. Once the DR test is complete, customers can simply delete the test environment, again without any impact to actual replicated production resources. When there is a need (planned or unplanned) for actual failover, with a few clicks, the BlueXP disaster recovery service will orchestrate all the steps needed to automatically bring up the protected virtual machines on designated disaster recovery site. The service will also reverse the SnapMirror relationship to the primary site and replicate any changes from secondary to primary for a failback operation, when needed. All of these can be achieved with a fraction of cost compared to other well-known alternatives.



## Getting started

To get started with BlueXP disaster recovery, use BlueXP console and then access the service.

1. Log in to BlueXP.
2. From the BlueXP left navigation, select Protection > Disaster recovery.
3. The BlueXP disaster recovery Dashboard appears.

The screenshot shows the NetApp BlueXP interface. The left sidebar has a 'Disaster recovery' section highlighted with a red box. The main dashboard area shows various metrics: 21 Protected VMs, 117 Unprotected VMs, 1 Failovers, 1 Failbacks, 2 Test failovers, and 0 Migrations. The 'Replication plans' section shows 1 Ready and 2 Failed replication plans. The 'Activity' section lists recent backup jobs and their statuses.

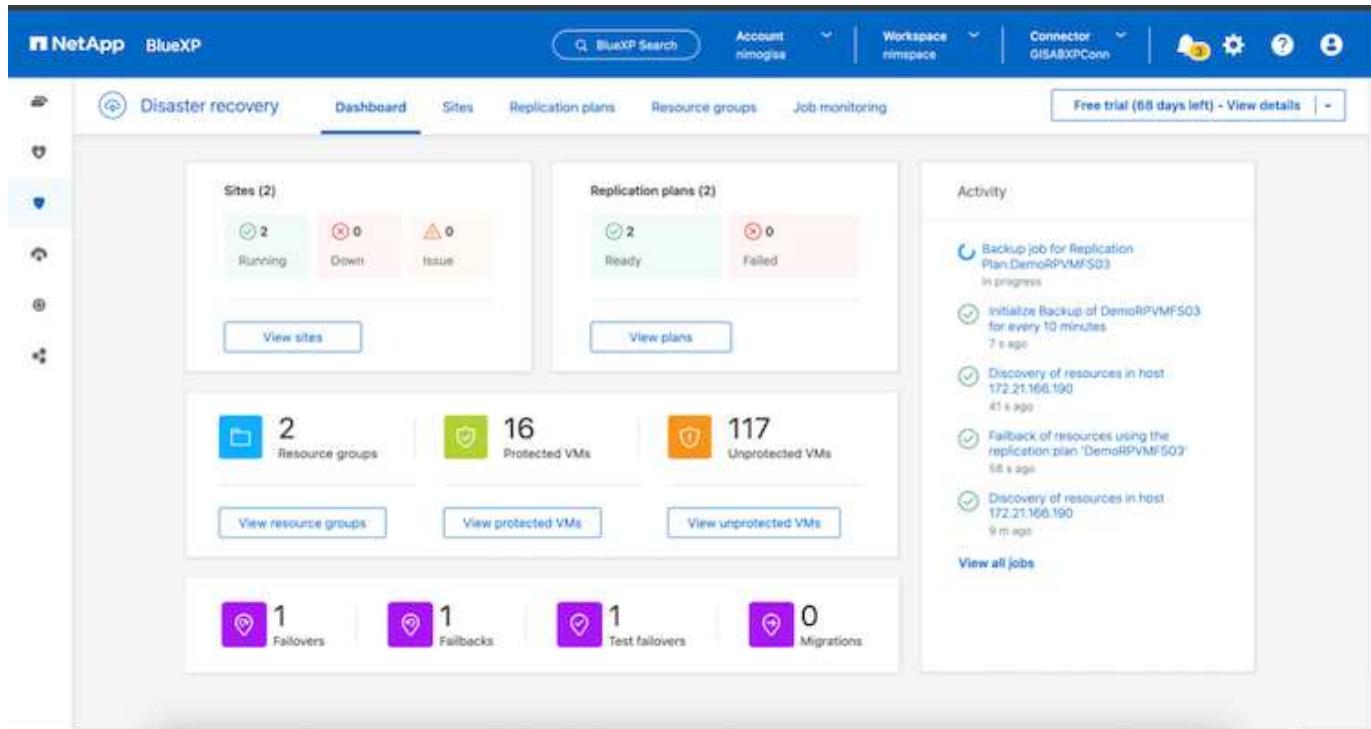
Before configuring disaster recovery plan, ensure the following pre-requisites are met:

- BlueXP Connector is set up in NetApp BlueXP. The connector should be deployed in AWS VPC.
- BlueXP connector instance have connectivity to the source and destination vCenter and storage systems.
- On-premises NetApp storage systems hosting VMFS datastores for VMware are added in BlueXP.
- DNS resolution should be in place when using DNS names. Otherwise, use IP addresses for the vCenter.
- SnapMirror replication is configured for the designated VMFS based datastore volumes.

Once the connectivity is established between the source and destination sites, proceed with configuration steps, which should take about 3 to 5 minutes.



NetApp recommends deploying the BlueXP connector in the disaster recovery site or in a third site, so that the BlueXP connector can communicate through the network with source and destination resources during real outages or natural disasters.

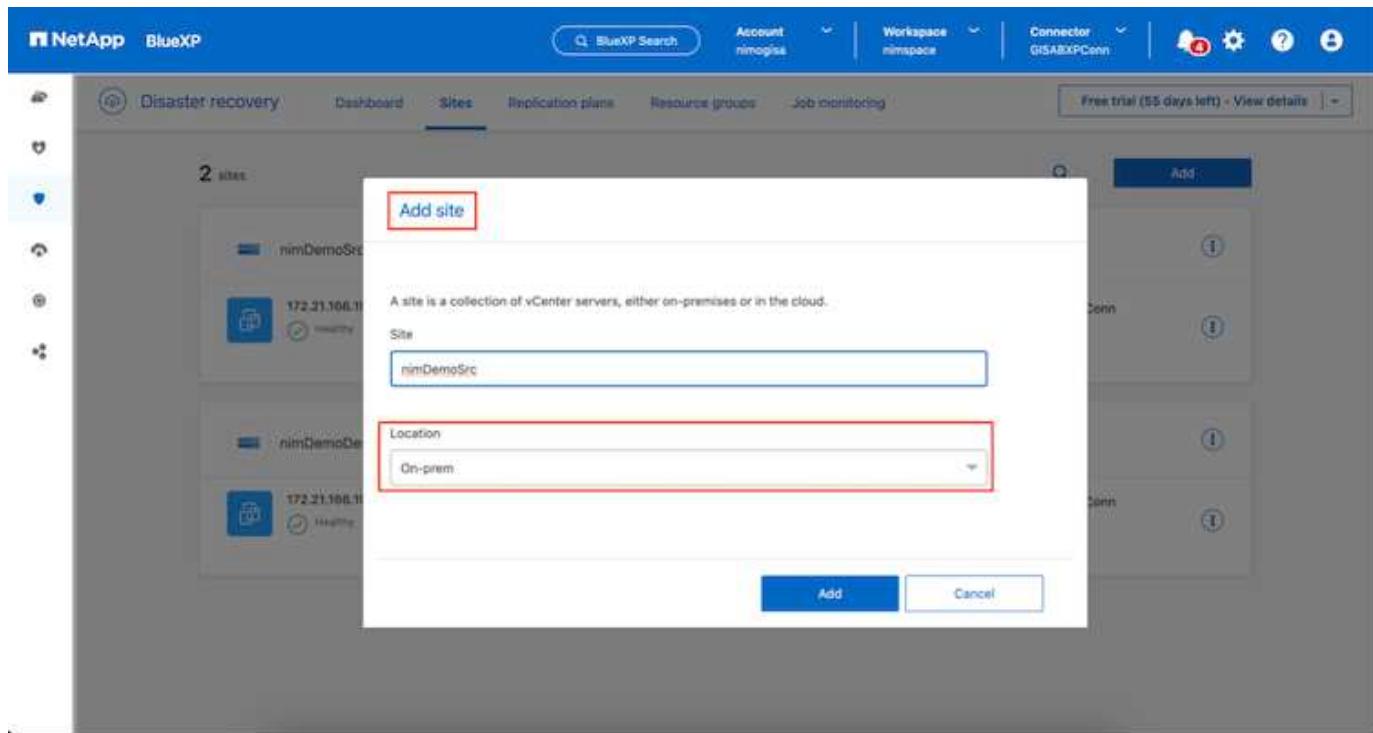


**i** Support for on-premises to on-premises VMFS datastores is in technology preview while writing this document. The capability is supported with both FC and iSCSI protocol based VMFS datastores.

## BlueXP disaster recovery configuration

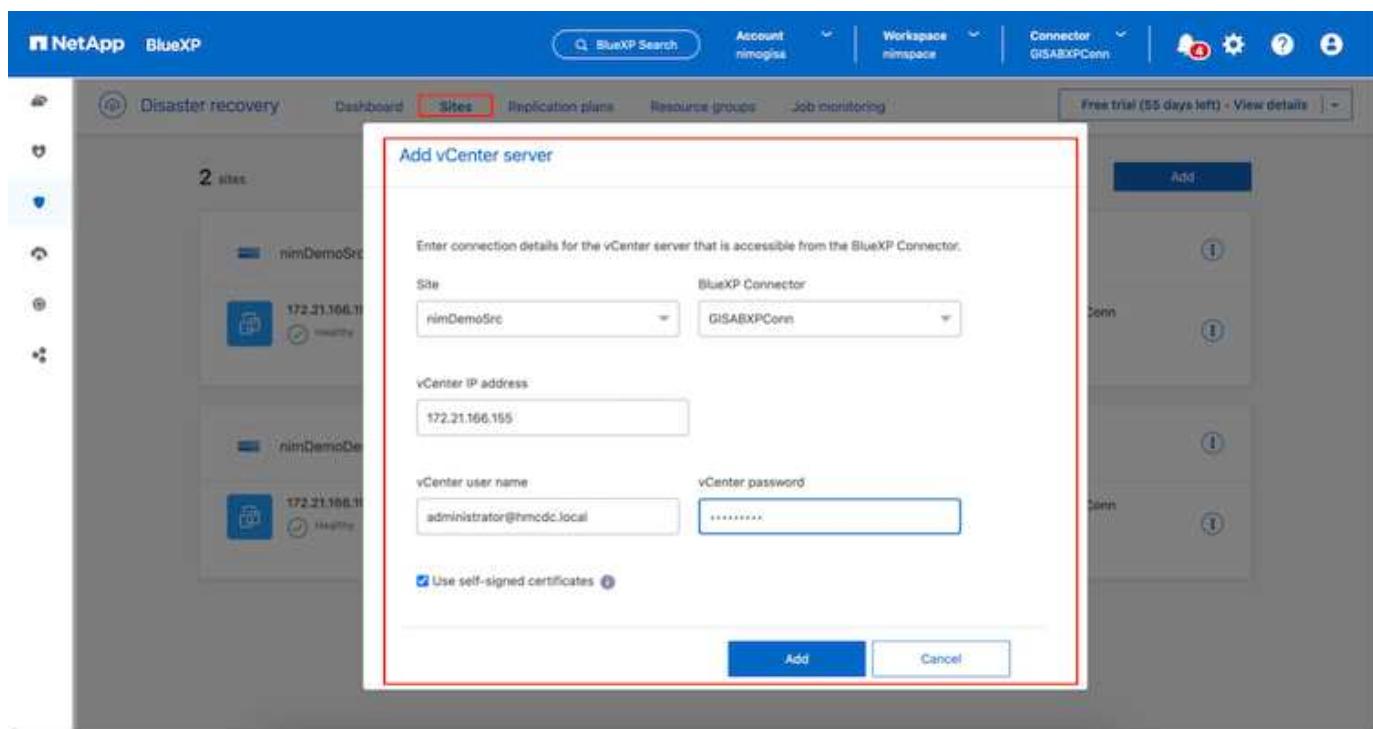
The first step in preparing for disaster recovery is to discover and add the on-premises vCenter and storage resources to BlueXP disaster recovery.

**i** Ensure the ONTAP storage systems are added to the working environment within the canvas. Open BlueXP console and select **Protection > Disaster Recovery** from left navigation. Select **Discover vCenter servers** or use top menu, Select **Sites > Add > Add vCenter**.

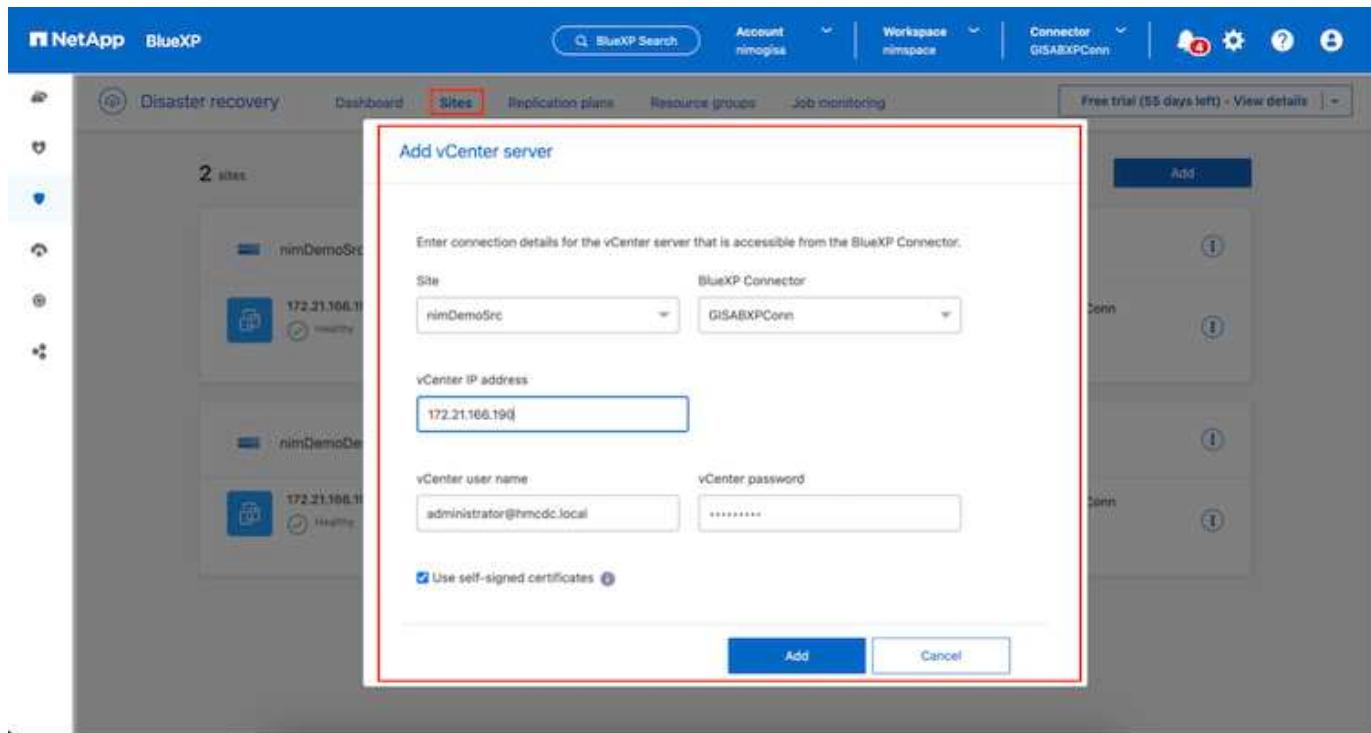


Add the following platforms:

- **Source.** On-premises vCenter.



- **Destination.** VMC SDDC vCenter.



Once the vCenters are added, automated discovery is triggered.

## Configuring Storage replication between source and destination site

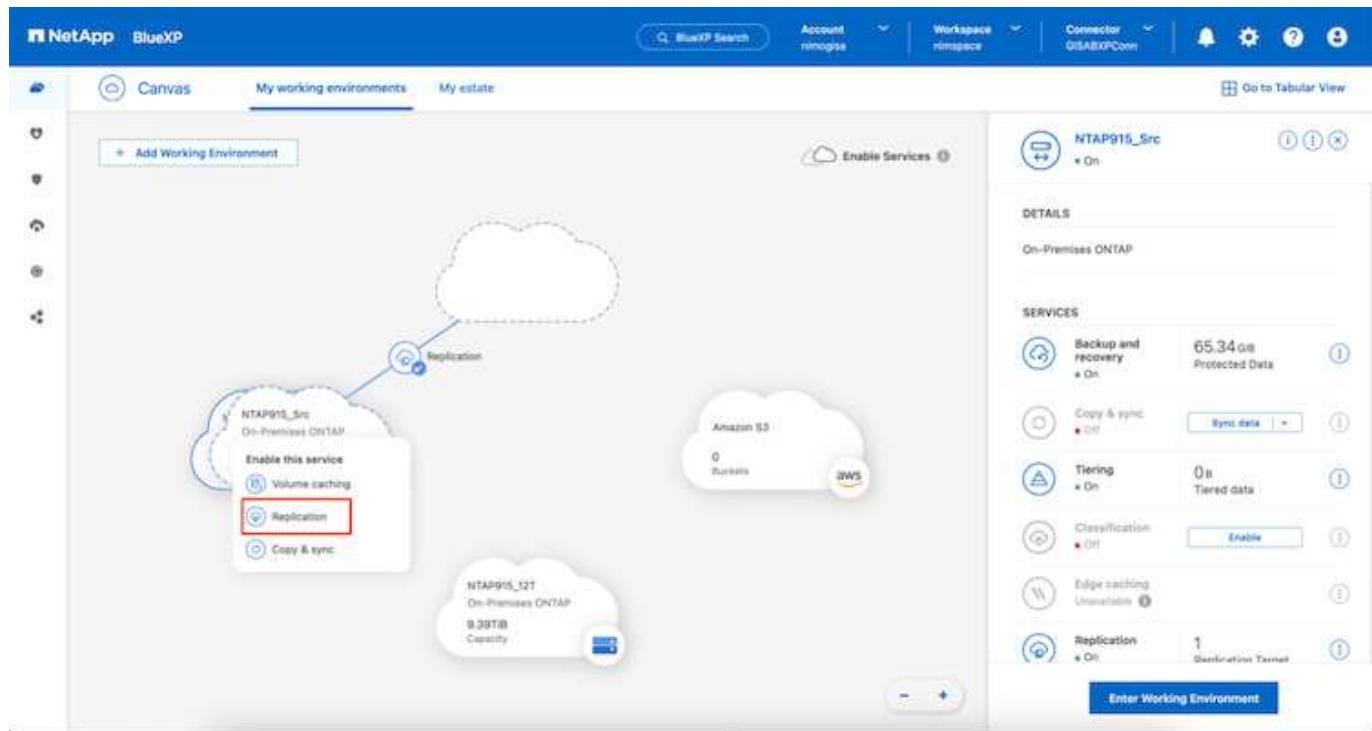
SnapMirror makes use of ONTAP snapshots to manage the transfer of data from one location to another. Initially, a full copy based on a snapshot of the source volume is copied over to the destination to perform a baseline synchronization. As data changes occur at the source, a new snapshot is created and compared to the baseline snapshot. The blocks found to have changed are then replicated to the destination, with the newer snapshot becoming the current baseline, or newest common snapshot. This enables the process to be repeated and incremental updates to be sent to the destination.

When a SnapMirror relationship has been established, the destination volume is in an online read-only state, and so is still accessible. SnapMirror works with physical blocks of storage, rather than at a file or other logical level. This means that the destination volume is an identical replica of the source, including snapshots, volume settings, etc. If ONTAP space efficiency features, such as data compression and data deduplication, are being used by the source volume, the replicated volume will retain these optimizations.

Breaking the SnapMirror relationship makes the destination volume writable and would typically be used to perform a failover when SnapMirror is being used to synchronize data to a DR environment. SnapMirror is sophisticated enough to allow the data changed at the failover site to be efficiently resynchronized back to the primary system, should it later come back online, and then allow for the original SnapMirror relationship to be re-established.

## How to set it up for VMware Disaster Recovery

The process to create SnapMirror replication remains the same for any given application. The process can be manual or automated. The easiest way is to leverage BlueXP to configure SnapMirror replication by using simple drag & drop of the source ONTAP system in the environment onto the destination to trigger the wizard that guides through the rest of the process.



BlueXP DRaaS can also automate the same provided the following two criteria's are met:

- Source and destination clusters have a peer relationship.
- Source SVM and destination SVM have a peer relationship.

NetApp BlueXP interface showing the 'Add replication plan' wizard. Step 4: Resource mapping. It shows a mapping between a Source cluster (vVCSA8-Cluster01) and a Target cluster (wM0D4-Cluster01). Under 'Datastores', it shows RPO and Retention settings, and a list of source and target datastores. A red box highlights the 'Source datastore' and 'Target datastore' fields.



If SnapMirror relationship is already configured for the volume via CLI, BlueXP DRaaS picks up the relationship and continues with the rest of the workflow operations.



Apart from the above approaches, SnapMirror replication can also be created via ONTAP CLI or System Manager. Irrespective of the approach used to synchronize the data using SnapMirror, BlueXP DRaaS orchestrates the workflow for seamless and efficient disaster recovery operations.

## What can BlueXP disaster recovery do for you?

After the source and destination sites are added, BlueXP disaster recovery performs automatic deep discovery and displays the VMs along with associated metadata. BlueXP disaster recovery also automatically detects the networks and port groups used by the VMs and populates them.

Site	IP Address	VMs	Datastores	Resource groups	Connector
nimDemoSrc	172.21.166.155	72	13	1	GISABXPConn
nimDemoDest	172.21.166.190	61	3	0	GISABXPConn

After the sites have been added, VMs can be grouped into resource groups. BlueXP disaster recovery resource groups allow you to group a set of dependent VMs into logical groups that contain their boot orders and boot delays that can be executed upon recovery. To start creating resource groups, navigate to **Resource Groups** and click **Create New Resource Group**.

The screenshot shows the NetApp BlueXP interface with the 'Resource groups' tab selected. There are two resource groups listed: 'DemoRG01' and 'DemoRGVMFS03'. A success message 'Added the resource group' is displayed in a toast notification at the bottom. The 'Add' button is visible in the top right corner of the table.

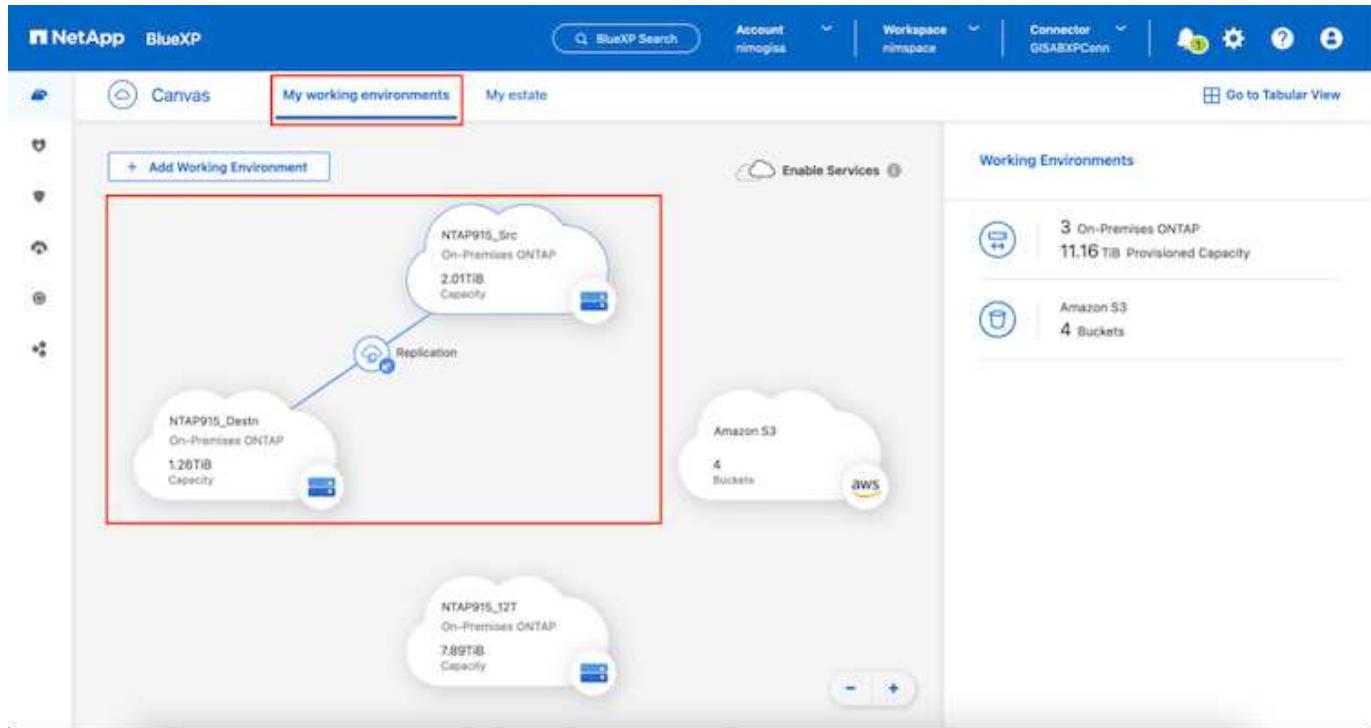


The resource group can also be created while creating a replication plan.

The boot order of the VMs can be defined or modified during the creation of resource groups by using simple drag and drop mechanism.

The screenshot shows the 'Add resource group' dialog. It includes fields for 'Name' (set to 'DemoRGVMFS03') and 'vCenter' (set to '172.21.166.155'). The 'Select virtual machines' section shows a list of VMs with checkboxes and a 'Selected VMs (5)' section containing five entries. A note at the bottom says 'Use drag and drop here to modify the boot order'.

Once the resource groups are created, the next step is to create the execution blueprint or a plan to recover virtual machines and applications in the event of a disaster. As mentioned in the prerequisites, SnapMirror replication can be configured beforehand or DRaaS can configure it using the RPO and retention count specified during creation of the replication plan.



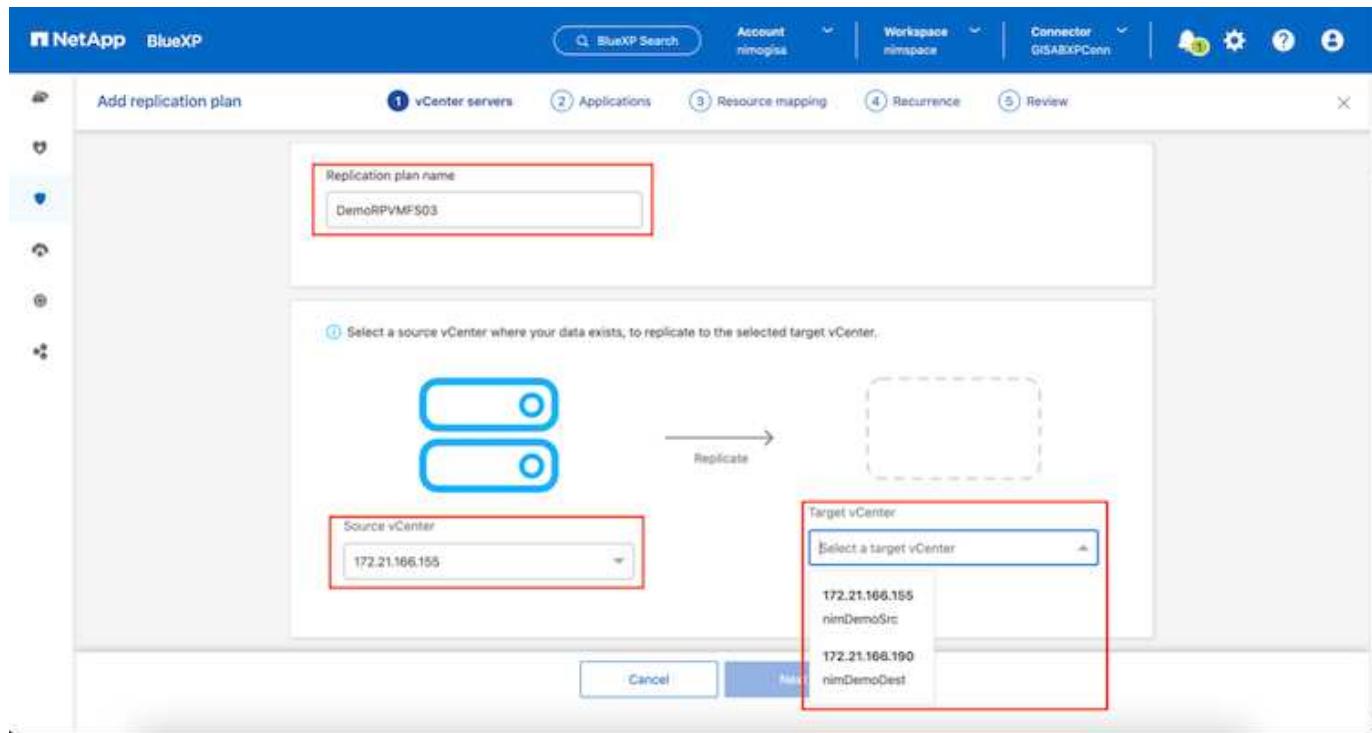
NetApp BlueXP

Replication

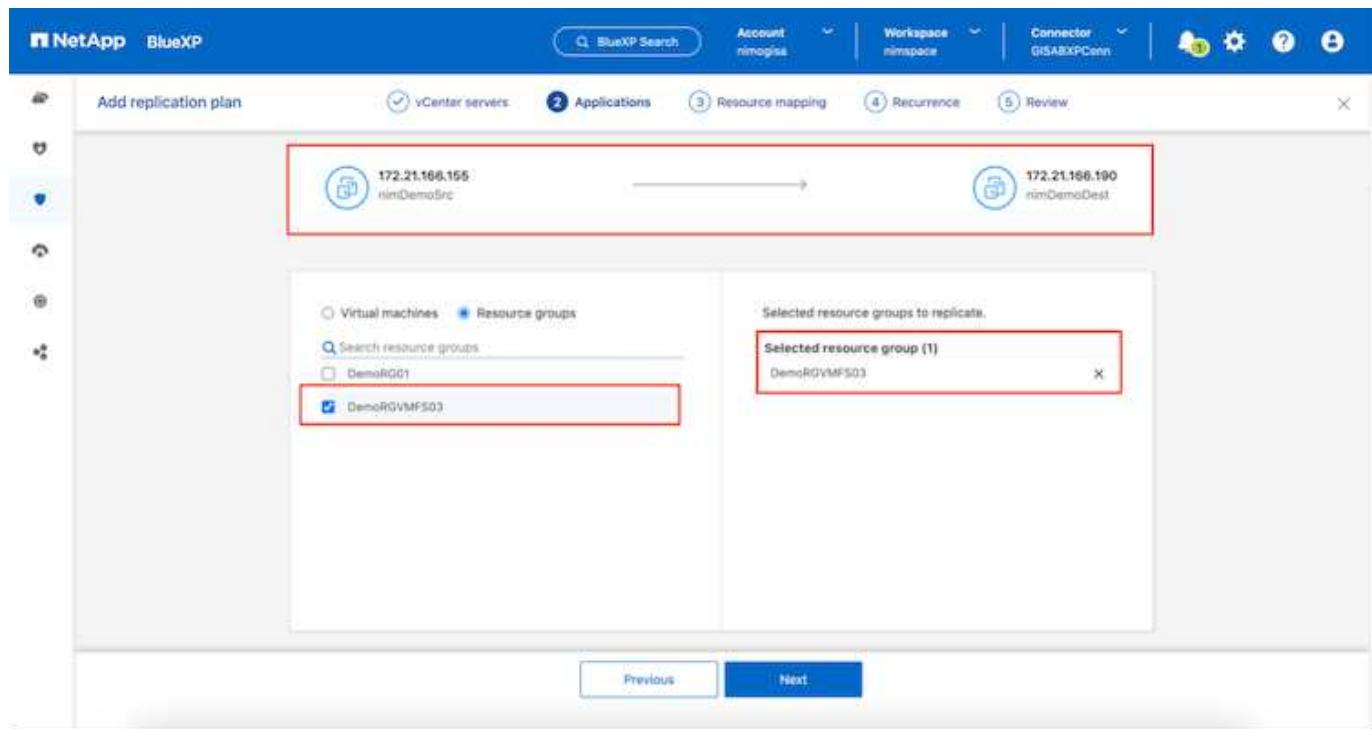
Health Status	Source Volume	Target Volume	Total Transfer Time	Status	Mirror State	Last Successful
✓	DRaaS_src NTAP915_Src	DRaaS_src_copy NTAP915_Destn	5 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:05 28.41 MiB
✓	Src_NFS_D503 NTAP915_Src	Src_NFS_D503_CP NTAP915_Destn	13 seconds	idle	snapmirrored	Jul 15, 2024, 8:07:13 183.41 MiB
✓	Src_NFS_D504 NTAP915_Src	Src_NFS_D504_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 183.58 MiB
✓	Src_NFS_Vol01 NTAP915_Src	Src_NFS_D501_cp NTAP915_Destn	14 seconds	idle	snapmirrored	Jul 15, 2024, 8:43:22 546.23 MiB
✓	Src_ISCSI_D501 NTAP915_Src	Src_ISCSI_D501_cp NTAP915_Destn	20 seconds	idle	snapmirrored	Jul 12, 2024, 4:24:34 22.35 MiB
✓	Src_ISCSI_D503 NTAP915_Src	Src_ISCSI_D503_CP NTAP915_Destn	6 seconds	idle	snapmirrored	Jul 15, 2024, 8:05:06 254.89 MiB

Configure the replication plan by selecting the source and destination vCenter platforms from the drop down and pick the resource groups to be included in the plan, along with the grouping of how applications should be restored and powered on and mapping of clusters and networks. To define the recovery plan, navigate to the **Replication Plan** tab and click **Add Plan**.

First, select the source vCenter and then select the destination vCenter.



The next step is to select existing resource groups. If no resource groups created, then the wizard helps to group the required virtual machines (basically create functional resource groups) based on the recovery objectives. This also helps define the operation sequence of how application virtual machines should be restored.

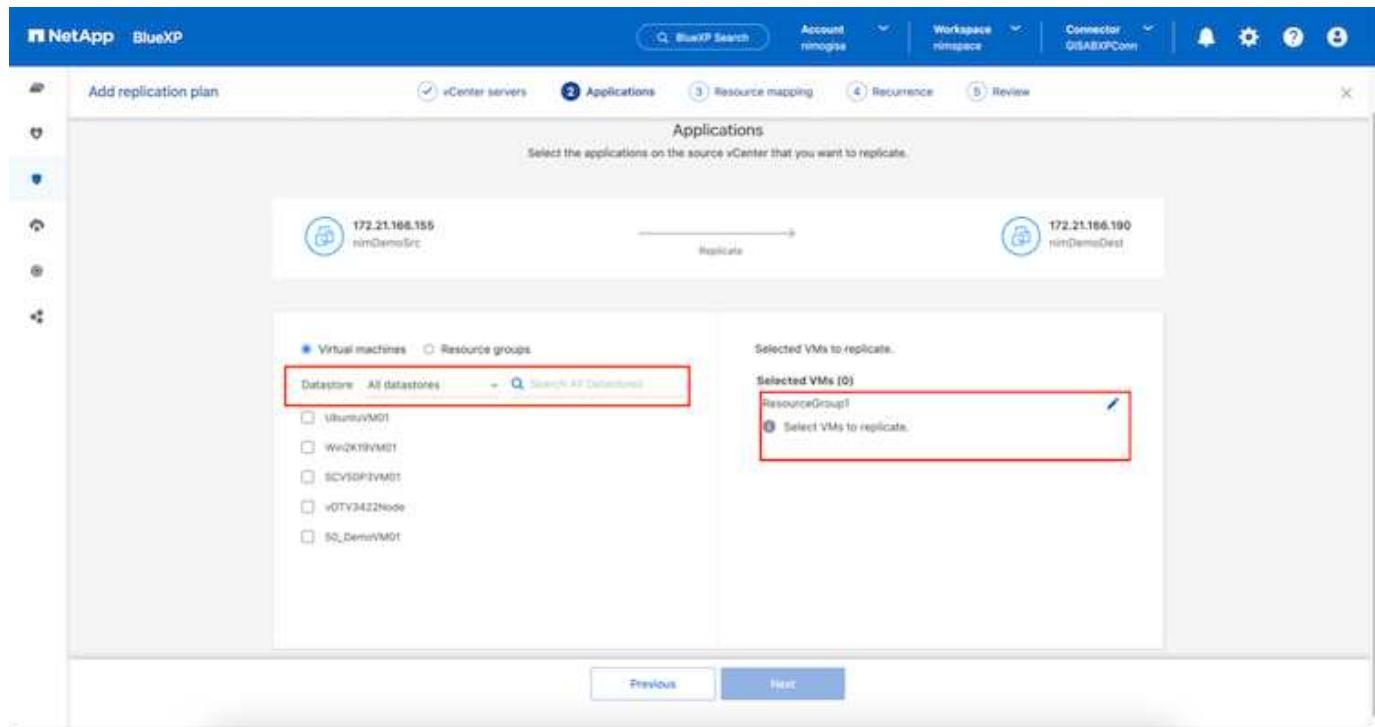


Resource group allows to set boot order using the drag and drop functionality. It can be used to easily modify the order in which the VMs would be powered on during the recovery process.



Each virtual machine within a resource group is started in sequence based on the order. Two resource groups are started in parallel.

The below screenshot shows the option to filter virtual machines or specific datastores based on organizational requirements if resource groups are not created beforehand.



Once the resource groups are selected, create the failover mappings. In this step, specify how the resources from the source environment maps to the destination. This includes compute resources, virtual networks. IP customization, pre- and post-scripts, boot delays, application consistency and so on. For detailed information, refer to [Create a replication plan](#).

Virtual machines

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



By default, same mapping parameters are used for both test and failover operations. To apply different mappings for test environment, select the Test mapping option after unchecking the checkbox as shown below:

Resource mapping

Specify how resources map from the source to the target.

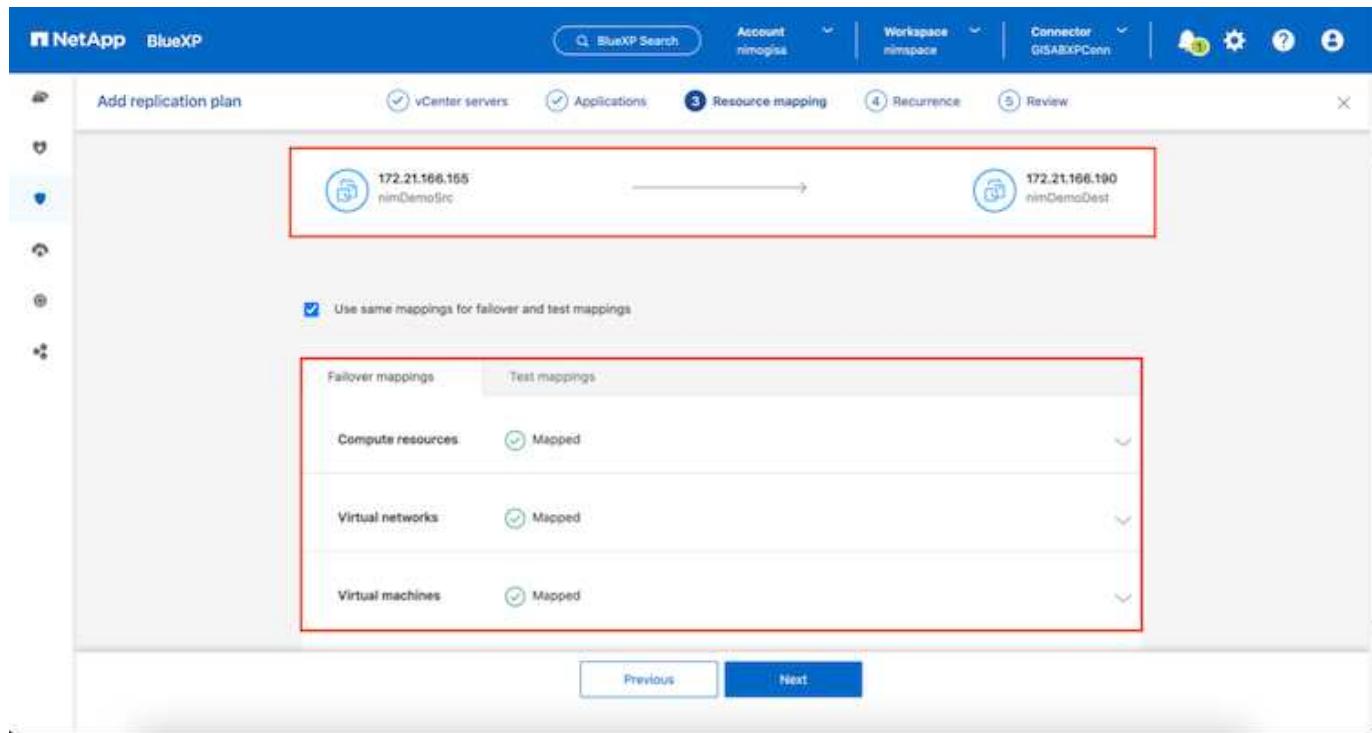
172.21.166.195  
nimDemoSrc

172.21.166.190  
nimDemoDest

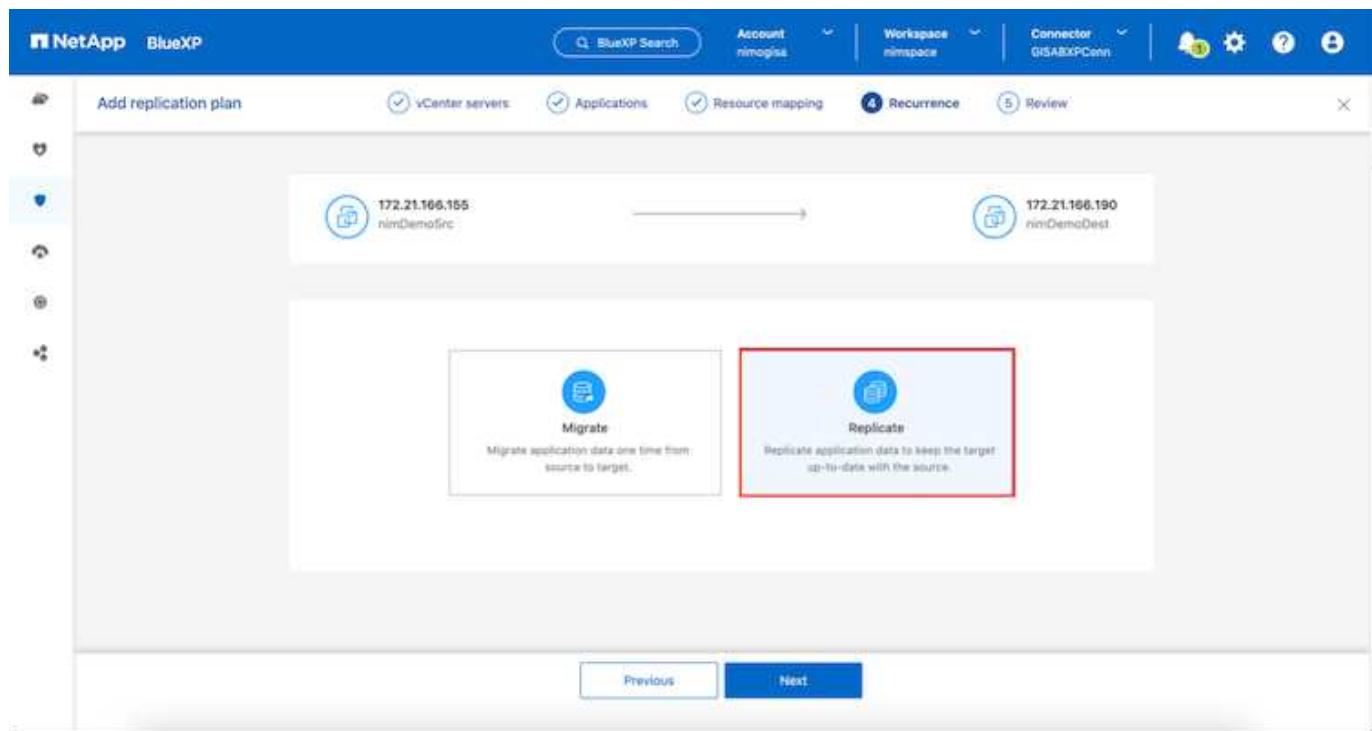
Use same mappings for failover and test mappings

Failover mappings Test mappings

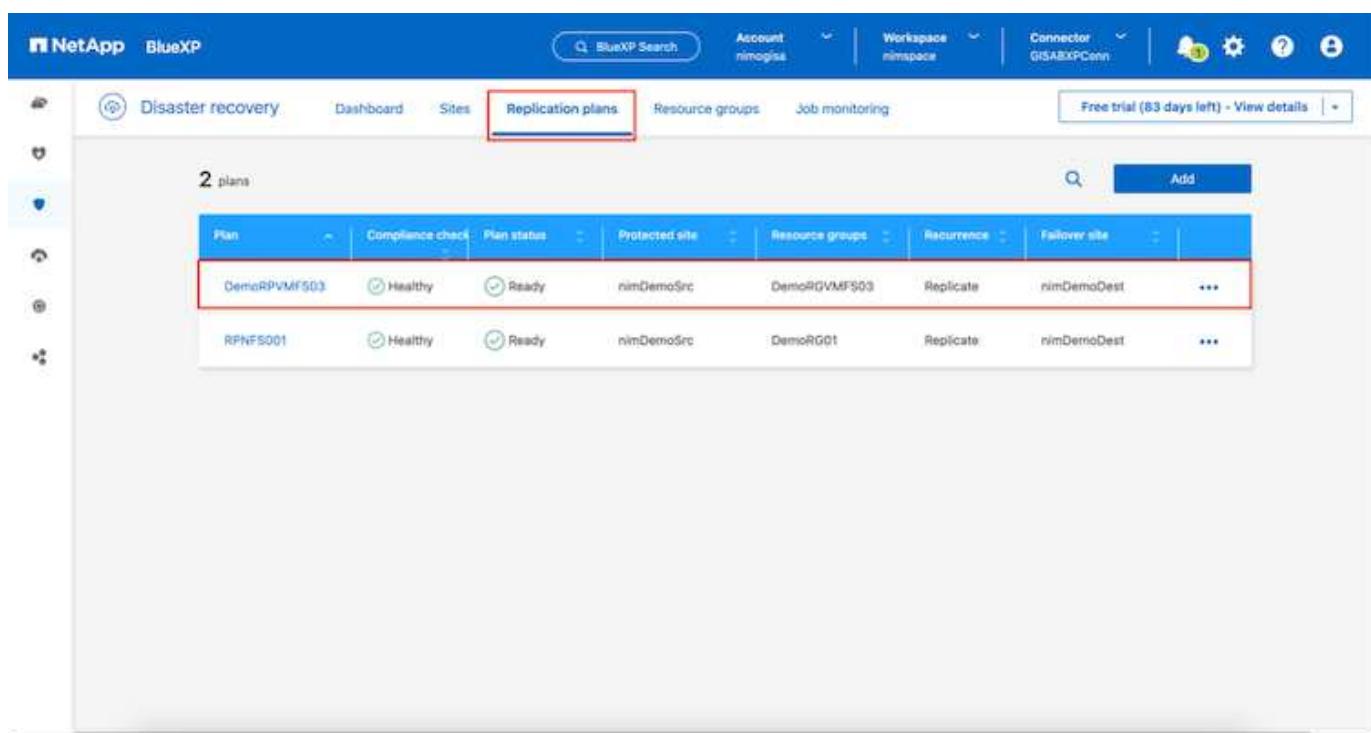
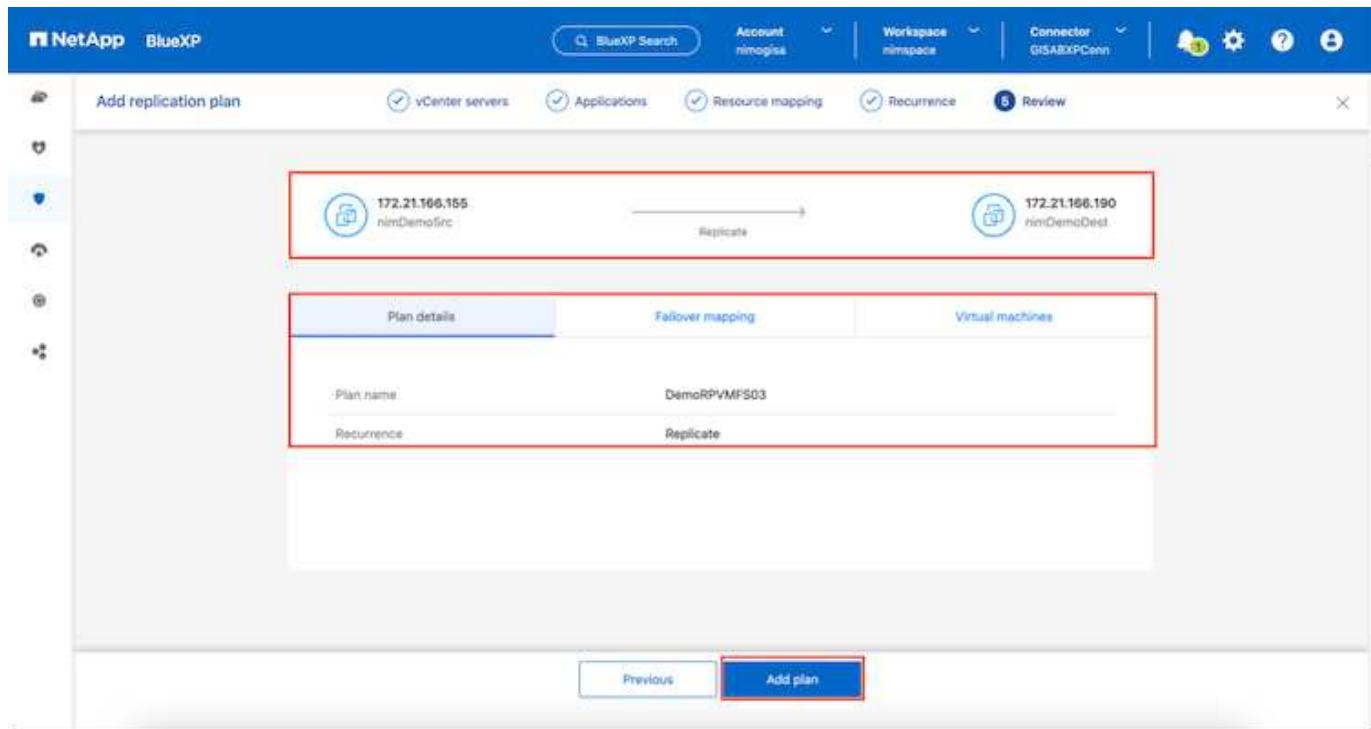
Once the resource mapping is complete, click Next.



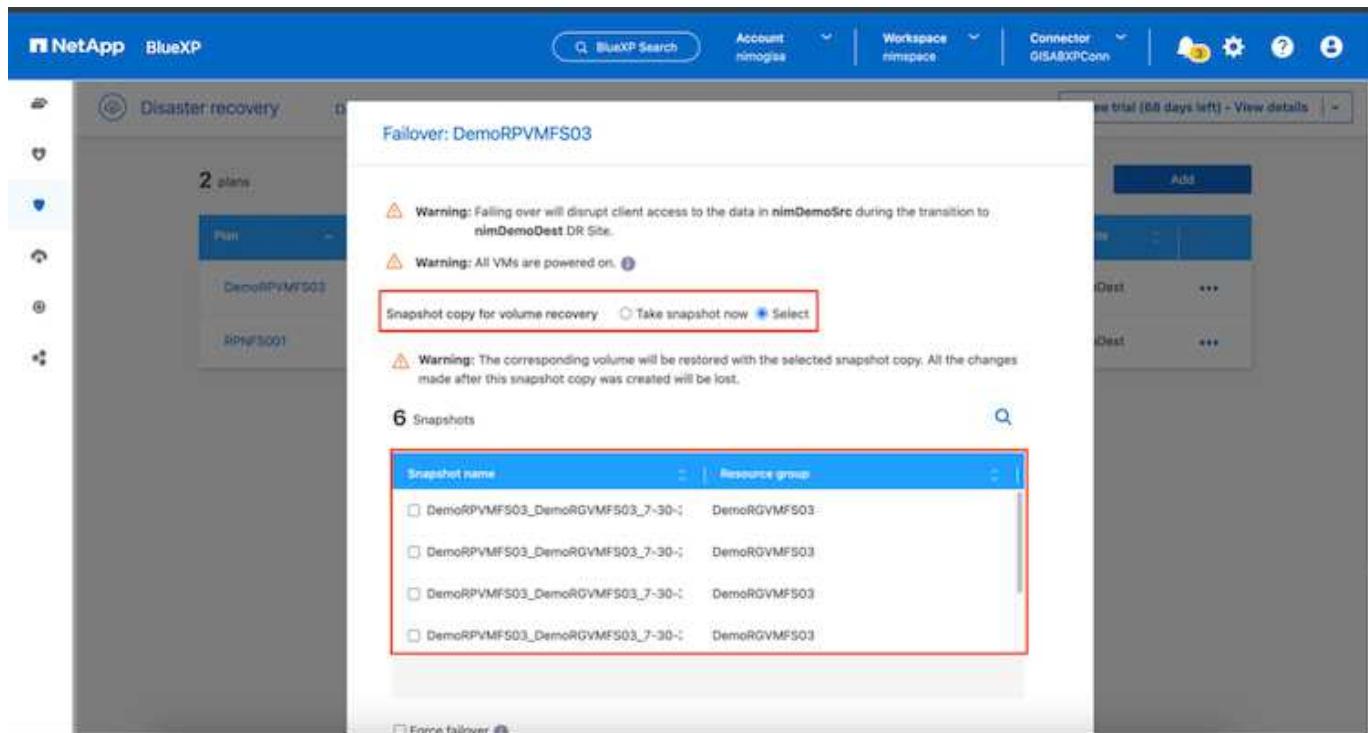
Select the recurrence type. In simple words, select Migrate (one time migration using failover) or recurring continuous replication option. In this walkthrough, Replicate option is selected.



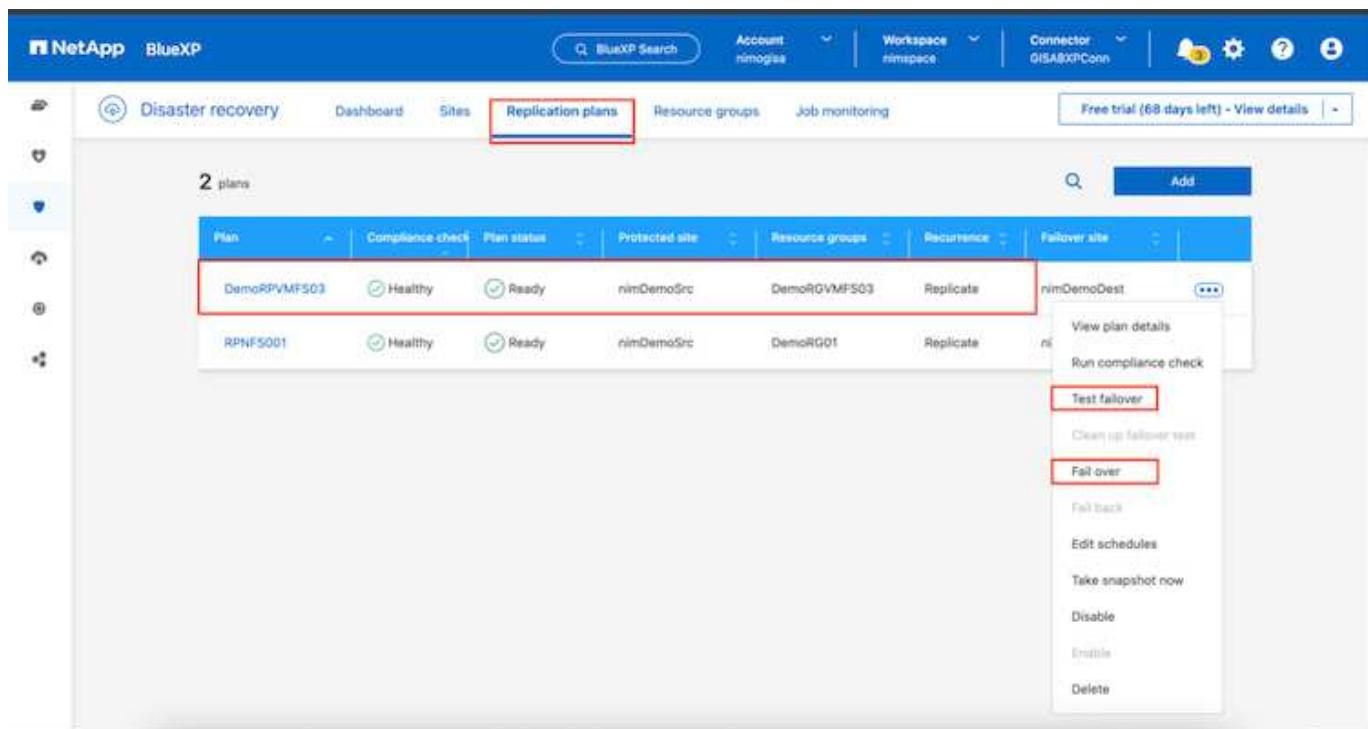
Once done, review the created mappings and then click on Add plan.



Once the replication plan is created, failover can be performed depending on the requirements by selecting the failover option, test-failover option, or the migrate option. BlueXP disaster recovery ensures that the replication process is being executed according to the plan every 30 minutes. During the failover and test-failover options, you can use the most recent SnapMirror Snapshot copy, or you can select a specific Snapshot copy from a point-in-time Snapshot copy (per the retention policy of SnapMirror). The point-in-time option can be very helpful if there is a corruption event like ransomware, where the most recent replicas are already compromised or encrypted. BlueXP disaster recovery shows all available recovery points.



To trigger failover or test failover with the configuration specified in the replication plan, click on **Failover** or **Test failover**.



## What happens during a failover or test failover operation?

During a test failover operation, BlueXP disaster recovery creates a FlexClone volume on the destination ONTAP storage system using the latest Snapshot copy or a selected snapshot of the destination volume.



A test failover operation creates a cloned volume on the destination ONTAP storage system.



Running a test recovery operation does not affect the SnapMirror replication.

The screenshot shows the NetApp BlueXP interface. The top navigation bar includes 'NetApp BlueXP', 'BlueXP Search', 'Account: nimogas', 'Workspace: nimospace', 'Connector: GHSA8XPConn', and various status icons. The main menu has tabs for 'Disaster recovery', 'Dashboard', 'Sites', 'Replication plans', 'Resource groups', and 'Job monitoring'. A 'Free trial (0.8 days left) - View details' button is in the top right. The left sidebar shows '2 plans' with 'DemoRPVMS03' and 'RPMS001' listed. The central area is titled 'Test failover: DemoRPVMS03' and contains a list of validation steps with checkmarks, some of which are highlighted with a red border. The steps include: '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', and 'Take snapshot now option is not selected, primary backup & snapmirror update not performed.' A 'DR Test Failover Target Start' button is at the bottom. A 'Run in background' button is also present.

During the process, BlueXP disaster recovery does not map the original target volume. Instead, it makes a new FlexClone volume from the selected Snapshot and a temporary datastore backing the FlexClone volume is mapped to the ESXi hosts.

The screenshot shows the vSphere Client interface. The top navigation bar includes 'vSphere Client', 'Search in all environments', and 'Administrators@HMCDC.LOCAL'. The main content area shows 'vCenter Details' for 'wklid04-vc01.hmc当地'. It displays the following information: 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. To the right is a 'Capacity and Usage' section with metrics for CPU, Memory, Storage, and Network. Below these are 'Tags', 'Custom Attributes', and 'vCenter Health'. At the bottom, a 'Recent Tasks' table lists completed tasks: 'Rescan VMFS' and 'Rescan all HBAs'. The 'Rescan VMFS' task was initiated by 'HMCDC.LOCAL\Administrator' and completed in 2 ms on 07/30/2024, 3:22:47 AM. The 'Rescan all HBAs' task was initiated by 'HMCDC.LOCAL\Administrator' and completed in 3 ms on 07/30/2024, 3:22:47 AM.

Task Name	Target	Status	Initiator	Queued For	Start Time	Completion Time
Rescan VMFS	wklid04-esx01.hmc当地	Completed	HMCDC.LOCAL\Administrator	2 ms	07/30/2024, 3:22:47 AM	07/30/2024, 3:22:47 AM
Rescan all HBAs	wklid04-esx01.hmc当地	Completed	HMCDC.LOCAL\Administrator	3 ms	07/30/2024, 3:22:47 AM	07/30/2024, 3:22:47 AM

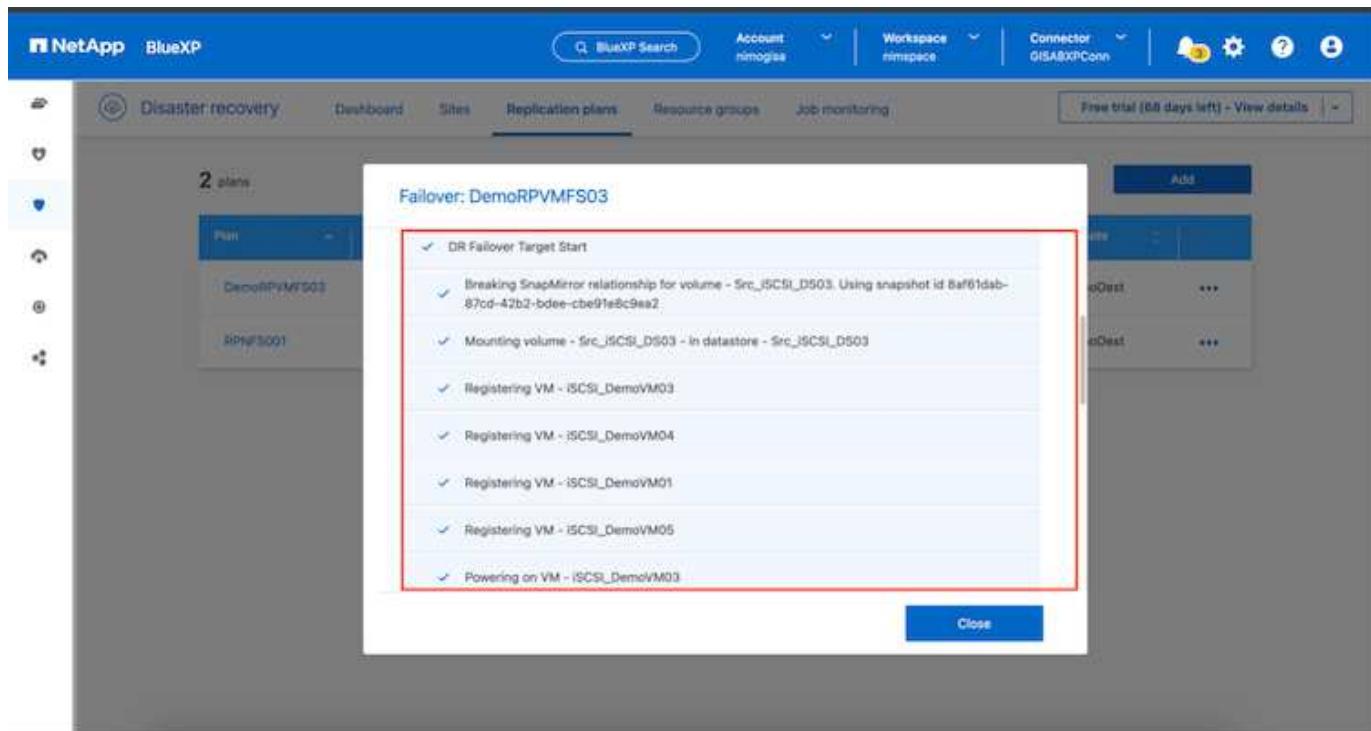
The screenshot shows the vSphere Client interface. The left sidebar shows the vCenter 'wkld04-vc01.hmc当地' with a tree view of its components. The 'Recent Tasks' section at the bottom shows two tasks in progress:

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

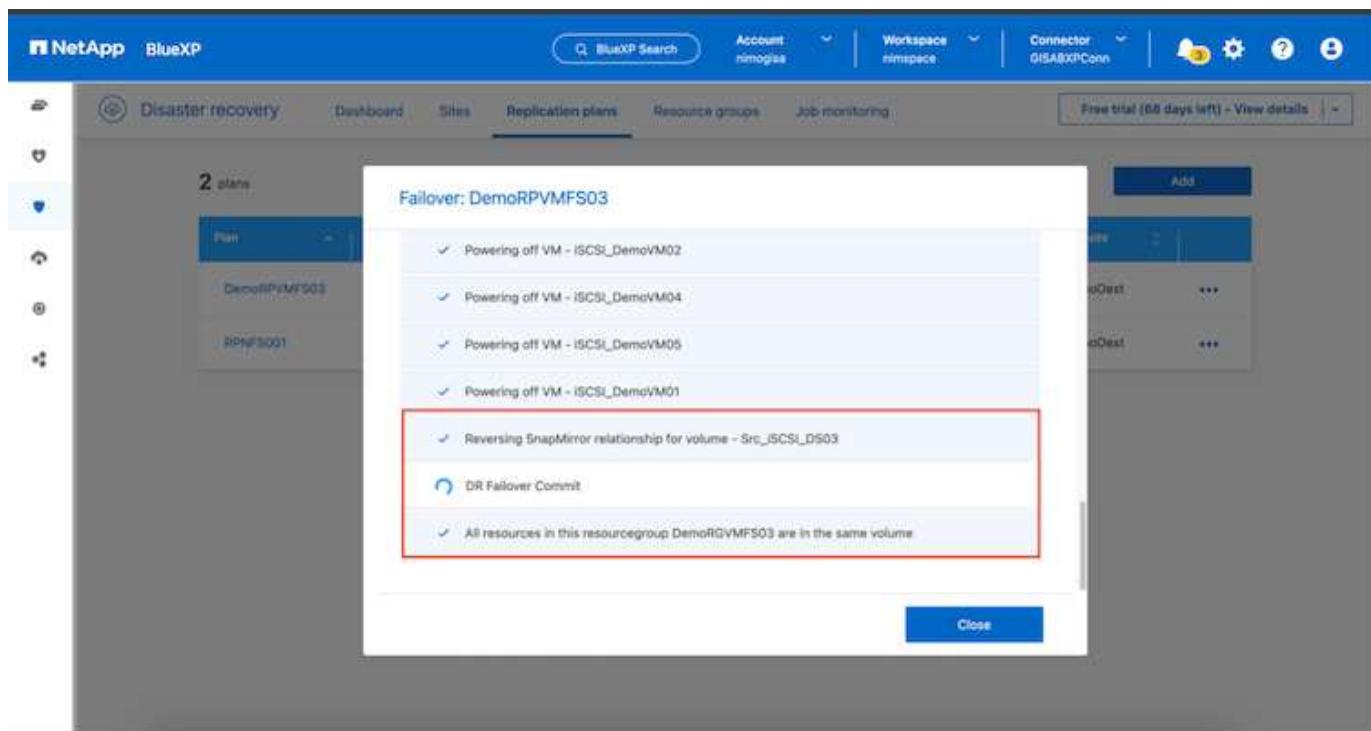
When the test failover operation completes, the cleanup operation can be triggered using "**Clean Up failover test**". During this operation, BlueXP disaster recovery destroys the FlexClone volume that was used in the operation.

In the event of real disaster event occurs, BlueXP disaster recovery performs the following steps:

1. Breaks the SnapMirror relationship between the sites.
2. Mounts the VMFS datastore volume after resignature for immediate use.
3. Register the VMs
4. Power on VMs



Once the primary site is up and running, BlueXP disaster recovery enables reverse resync for SnapMirror and enables fallback, which again can be performed with the click of a button.



And if migrate option is chosen, it is considered as a planned failover event. In this case, an additional step is triggered which is to shut down the virtual machines at the source site. The rest of the steps remains the same as failover event.

From BlueXP or the ONTAP CLI, you can monitor the replication health status for the appropriate datastore volumes, and the status of a failover or test failover can be tracked via Job Monitoring.

The screenshot shows the NetApp BlueXP interface with the 'Job monitoring' tab selected. At the top, there are navigation links for 'Disaster recovery', 'Dashboard', 'Sites', 'Replication plans', 'Resource groups', and 'Job monitoring'. A search bar and account information are also present. A banner at the top right indicates a 'Free trial (68 days left) - View details'.

The main area displays job statistics for the last 24 hours:

- 0 Jobs (Total)
- 0 Success (View jobs)
- 0 In progress (View jobs)
- 0 Queued (View jobs)
- 0 Warning (View jobs)
- 0 Failed (View jobs)

Below this, a table lists 11102 jobs. The columns are: ID, Status, Workload, Name, Start time, and End time. The first three rows are highlighted with a red border:

ID	Status	Workload	Name	Start time	End time
2983d7f3-7eb0-475d	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:...

This provides a powerful solution to handle a tailored and customized disaster recovery plan. Failover can be done as planned failover or failover with a click of a button when disaster occurs and decision is made to activate the DR site.

To learn more about this process, feel free to follow the detailed walkthrough video or use the [solution simulator](#).

## Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—with prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

**LIMITED RIGHTS LEGEND:** Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.