BlueXP disaster recovery documentation

BlueXP disaster recovery

NetApp
August 08, 2025

Table of Contents

BlueXP disaster recovery documentation

Release notes

What's new in BlueXP disaster recovery

Learn what's new in BlueXP disaster recovery.

04 August 2025

Version 4.2.5P2

BlueXP disaster recovery updates

This release includes the following updates:

- Improved the VMFS support to handle the same LUN presented from multiple storage virtual machines.
- Improved the test teardown cleanup to handle the datastore already being unmounted and or deleted.
- Improved subnet mapping so that it now validates that the gateway entered is contained within the network provided.
- Corrected an issue that could cause the replication plan to fail if the VM name contains ".com".
- Removed a restriction preventing the destination volume from being the same as the source volume when creating the volume as part of the replication plan creation.
- Added support for a pay-as-you-go (PAYGO) subscription to NetApp Intelligent Services in the Azure Marketplace and added a link to the Azure Marketplace in the free trial dialog.

  For details, see BlueXP disaster recovery licensing and Set up licensing for BlueXP disaster recovery.

14 July 2025

Version 4.2.5

User roles in BlueXP disaster recovery

BlueXP disaster recovery now employs roles to govern the access that each user has to specific features and actions.

The service uses the following roles that are specific to BlueXP disaster recovery.

- **Disaster recovery admin**: Perform any actions in BlueXP disaster recovery.
- **Disaster recovery failover admin**: Perform failover and migrate actions in BlueXP disaster recovery.
- **Disaster recovery application admin**: Create and modify replication plans and start test failovers.
- **Disaster recovery viewer**: View information in BlueXP disaster recovery, but cannot perform any actions.

If you are clicking on the BlueXP disaster recovery service and configuring it for the first time, you must have the **SnapCenterAdmin** permission or have the **Organization Admin** role.

For details, see User roles and permissions in BlueXP disaster recovery.

Learn about BlueXP access roles for all services.

Other updates in BlueXP disaster recovery

- Enhanced network discovery
- Scalability improvements:
  - Filtering for the required metadata instead of all the details
  - Discovery improvements to retrieve and update VM resources faster
  - Memory optimization and performance optimization for data retrieval and data updates
  - vCenter SDK client creation and pool management improvements
- Stale data management on the next scheduled or manual discovery:
  - When a VM is deleted in the vCenter, BlueXP disaster recovery now automatically removes it from the replication plan.
  - When a datastore or network is deleted in the vCenter, BlueXP disaster recovery now deletes it from the replication plan and resource group.
  - When a cluster, host, or datacenter is deleted in the vCenter, BlueXP disaster recovery now deletes it from the replication plan and resource group.
- You can now access Swagger documentation in your browser's incognito mode. You can access it from within BlueXP disaster recovery from the Settings option > API Documentation or directly at the following URL in your browser's incognito mode: Swagger documentation.
- In some situations after a failback operation, the iGroup was left behind after the operation completed. This update removes the iGroup if it is stale.
- If the NFS FQDN was used in the replication plan, BlueXP disaster recovery now resolves it to an IP address. This update is useful if the FQDN is not resolvable in the disaster recovery site.
- UI alignment improvements
- Log improvements to capture the vCenter sizing details after the successful discovery

30 June 2025

Version 4.2.4P2

Discovery improvements

This update improves the discovery process, which reduces the time needed for discovery.

23 June 2025

Version 4.2.4P1

Subnet mapping improvements

This update enhances the Add and Edit Subnet Mapping dialog with a new search functionality. You can now quickly find specific subnets by entering search terms, making it easier to manage subnet mappings.

9 June 2025

Version 4.2.4

Windows Local Administrator Password Solution (LAPS) support

Windows Local Administrator Password Solution (Windows LAPS) is a Windows feature that automatically manages and backs up the password of a local administrator account on Active directory.

You can now select subnet mapping options and check the LAPS option by providing the domain controller details. Using this option, you don’t need to provide a password for each of your virtual machines.

For details, refer to Create a replication plan.

13 May 2025

Version 4.2.3

Subnet mapping

With this release, you can manage IP addresses on failover in a new way using subnet mapping, which enables you to add subnets for each vCenter. When you do so, you define the IPv4 CIDR, the default gateway, and the DNS for each virtual network.

Upon failover, BlueXP disaster recovery determines the appropriate IP address of each vNIC by looking at the CIDR provided for the mapped virtual network and uses it to derive the new IP address.

For example:

- NetworkA = 10.1.1.0/24
- NetworkB = 192.168.1.0/24

VM1 has a vNIC (10.1.1.50) that is connected to NetworkA.
NetworkA is mapped to NetworkB in the replication plan settings.

Upon failover, BlueXP disaster recovery replaces the Network portion of the original IP address (10.1.1) and keeps the host address (.50) of the original IP address (10.1.1.50). For VM1, BlueXP disaster recovery looks at the CIDR settings for NetworkB and uses that the NetworkB network portion 192.168.1 while keeping the host portion (.50) to create the new IP address for VM1. The new IP becomes 192.168.1.50.

In summary, the host address stays the same, while the network address is replaced with whatever is configured in the site subnet mapping. This enables you to manage IP address reassignment upon failover more easily, especially if you have hundreds of networks and thousands of VMs to manage.

For details about including subnet mapping in your sites, refer to Add vCenter server sites.

Skip protection

You can now skip protection so that the service does not automatically create a reverse protection relationship after a replication plan failover. This is useful if you want to perform additional operations on the restored site before you bring it back online within BlueXP disaster recovery.

When you initiate a failover, by default the service automatically creates a reverse protection relationship for each volume in the replication plan, if the original source site is online. This means that the service creates a SnapMirror relationship from the target site back to the source site. The service also automatically reverses the SnapMirror relationship when you initiate a failback.

When initiating a failover, you can now choose a **Skip protection** option. With this, the service does not automatically reverse the SnapMirror relationship. Instead, it leaves the writable volume on both sides of the

replication plan.

After the original source site is back online, you can establish reverse protection by selecting **Protect resources** from the Replication plan Actions menu. This attempts to create a reverse replication relationship for each volume in the plan. You can run this job repeatedly until protection is restored. When protection is restored, you can initiate a failback in the usual way.

For details skipping protection, refer to Fail over applications to a remote site.

SnapMirror schedule updates in the replication plan

BlueXP disaster recovery now supports the use of external snapshot management solutions such as the native ONTAP SnapMirror policy scheduler or third-party integrations with ONTAP. If every datastore (volume) in the replication plan already has a SnapMirror relationship that is being managed elsewhere, you can use those snapshots as recovery points in BlueXP disaster recovery.

To configure, in the Replication plan > Resource mapping section, check the **Use platform managed backups and retention schedules** checkbox when configuring the Datastores mapping.

When the option is selected, BlueXP disaster recovery does not configure a backup schedule. However, you still need to configure a retention schedule because snapshots might still be taken for testing, failover, and failback operations.

After this is configured, the service doesn't take any regularly scheduled snapshots, but instead relies on the external entity to take and update those snapshots.

For details about using external snapshot solutions in the replication plan, refer to Create a replication plan.

16 April 2025

Version 4.2.2

Scheduled discovery for VMs

BlueXP disaster recovery performs discovery once every 24 hours. With this release, you can now customize the discovery schedule to meet your needs and reduce impact on performance when you need it. For example, if you have a large number of VMs, you can set the discovery schedule to run every 48 hours. If you have a small number of VMs, you can set the discovery schedule to run every 12 hours.

If you don't wan to schedule discovery, you can disable the scheduled discovery option and refresh the discovery manually at any time.

For details, refer to Add vCenter server sites.

Resource group datastore support

Previously, you could create resource groups only by VMs. With this release, you can create a resource group by datastores. When you're creating a replication plan and creating a resource group for that plan, all the VMs in a datastore will be listed. This is useful if you have a large number of VMs and want to group them by datastore.

You can create a resource group with a datastore in the following ways:

- When you're adding a resource group using datastores, you can see a list of datastores. You can select one or more datastores to create a resource group.

- When you're creating a replication plan and creating a resource group within the plan, you can see the VMs in the datastores.

For details, refer to Create a replication plan.

Notifications of free trial or license expiration

This release provides notifications that the free trial will expire in 60 days to ensure you have time to get a license. This release also provides notifications on the day that the license expires.

Notification of service updates

With this release, a banner appears at the top to indicate that services are getting upgraded and that the service is placed in maintenance mode. The banner appears when the service is being upgraded and disappears when the upgrade is complete. While you can continue to work in the UI while the upgrade is in progress, you cannot submit new jobs. Scheduled jobs will run after the update is complete and the service returns to production mode.

10 March 2025

Version 4.2.1

Intelligent proxy support

The BlueXP Connector supports intelligent proxy. Intelligent proxy is a lightweight, secure, and efficient way to connect your on-premises environment to the BlueXP service. It provides a secure connection between your environment and the BlueXP service without requiring a VPN or direct internet access. This optimized proxy implementation offloads API traffic within the local network.

When a proxy is configured, BlueXP disaster recovery attempts to communicate directly with VMware or ONTAP and uses the configured proxy if direct communication fails.

BlueXP disaster recovery proxy implementation requires port 443 communication between the Connector and any vCenter Servers and ONTAP arrays using an HTTPS protocol. The BlueXP disaster recovery agent within the Connector communicates directly with VMware vSphere, the VC, or ONTAP when performing any actions.

For more information about the intelligent proxy for BlueXP disaster recovery, see Set up your infrastructure for BlueXP disaster recovery.

For more information about general proxy set up in BlueXP, see Configure a Connector to use a proxy server.

End the free trial any time

You can stop the free trial at any tine or you can wait until it expires.

See End the free trial.

19 February 2025

Version 4.2

ASA r2 support for VMs and datastores on VMFS storage

This release of BlueXP disaster recovery provides support for ASA r2 for VMs and datastores on VMFS

storage. On an ASA r2 system, ONTAP software supports essential SAN functionality while removes features not supported in SAN environments.

This release supports the following features for ASA r2:

- Consistency group provisioning for primary storage (flat consistency group only, meaning only one level without a hierarchical structure)
- Backup (consistency group) operations including SnapMirror automation

The support for ASA r2 in BlueXP disaster recovery uses ONTAP 9.16.1.

While datastores can be mounted on an ONTAP volume or an ASA r2 storage unit, a resource group in BlueXP disaster recovery cannot include both a datastore from ONTAP and one from ASA r2. You can select either a datastore from ONTAP or a datastore from ASA r2 in a resource group.

30 October 2024

Reporting

You can now generate and download reports to help you analyze your landscape. Predesigned reports summarize failovers and failbacks, show replication details on all sites, and show job details for the past seven days.

Refer to Create disaster recovery reports.

30-day free trial

You can now sign up for a 30-day free trial of BlueXP disaster recovery. Previously, free trials were for 90 days.

Refer to Set up licensing.

Disable and enable replication plans

A previous release included updates to the failover test schedule structure, which was needed to support daily and weekly schedules. This update required that you disable and re-enable all existing replication plans so that you will be able to use the new daily and weekly failover test schedules. This is a one-time requirement.

Here's how:

1. From the top menu, select **Replication plans**.
2. Select a plan and select the Actions icon to show the drop-down menu.
3. Select **Disable**.
4. After a few minutes, select **Enable**.

Folder mapping

When you create a replication plan and map compute resources, you can now map folders so that VMs are recovered in a folder you specify for datacenter, cluster, and host.

For details, refer to Create a replication plan.

VM details available for failover, failback, and test failover

When a failure occurs and you are starting a failover, performing a failback, or testing the failover, you can now see details of the VMs and identify which VMs did not restart.

Refer to Fail over applications to a remote site.

VM boot delay with ordered boot sequence

When you create a replication plan, you can now set a boot delay for each VM in the plan. This enables you to set a sequence for the VMs to start to ensure that all your priority one VMs are running before subsequent priority VMs are started.

For details, refer to Create a replication plan.

VM operating system information

When you create a replication plan, you can now see the operating system for each VM in the plan. This is helpful in deciding how to group VMs together in a resource group.

For details, refer to Create a replication plan.

VM name aliasing

When you create a replication plan, you can now add a prefix and suffix to the VM names on the disaster recovery sit. This enables you to use a more descriptive name for the VMs in the plan.

For details, refer to Create a replication plan.

Clean up old snapshots

You can delete any snapshots that are no longer needed beyond your specified retention count. Snapshots might accumulate over time when you lower your snapshot retention count, and you can now remove them to free up space. You can do this anytime on demand or when you delete a replication plan.

For details, refer to Manage sites, resource groups, replication plans, datastores, and virtual machines information.

Reconcile snapshots

You can now reconcile snapshots that are out of sync between the source and target. This might occur if snapshots are deleted on a target outside of BlueXP disaster recovery. The service deletes the snapshot on the source automatically every 24 hours. However, you can perform this on demand. This feature enables you to ensure that the snapshots are consistent across all sites.

For details, refer to Manage replication plans.

20 September 2024

Support for on-premises to on-premises VMware VMFS datastores

This release includes support for VMs mounted on VMware vSphere virtual machine file system (VMFS) datastores for iSCSI and FC protected to on-premises storage. Previously, the service provided a *technology preview* supporting VMFS datastores for iSCSI and FC.

Here are some additional considerations regarding both iSCSI and FC protocols:

- FC support is for client front-end protocols, not for replication.
- BlueXP disaster recovery supports only a single LUN per ONTAP volume. The volume should not have multiple LUNs.
- For any replication plan, the destination ONTAP volume should use the same protocols as the source ONTAP volume hosting the protected VMs. For example, if the source uses an FC protocol, the destination should also use FC.

2 August 2024

Support for on-premises to on-premises VMware VMFS datastores for FC

This release includes a *technology preview* of support for VMs mounted on VMware vSphere virtual machine file system (VMFS) datastores for FC protected to on-premises storage. Previously, the service provided a technology preview supporting VMFS datastores for iSCSI.

NetApp doesn't charge you for any previewed workload capacity.

Job cancel

With this release, you can now cancel a job in the Job Monitor UI.

Refer to Monitor jobs.

17 July 2024

Failover test schedules

This release includes updates to the failover test schedule structure, which was needed to support daily and weekly schedules. This update requires that you disable and re-enable all existing replication plans so that you will be able to use the new daily and weekly failover test schedules. This is a one-time requirement.

Here's how:

1. From the top menu, select **Replication plans**.
2. Select a plan and select the Actions icon to show the drop-down menu.
3. Select **Disable**.
4. After a few minutes, select **Enable**.

Replication plan updates

This release includes updates to replication plan data, which resolves a "snapshot not found" issue. This requires that you change the retention count in all replication plans to 1 and initiate an on-demand snapshot. This process creates a new backup and removes all older backups.

Here's how:

1. From the top menu, select **Replication plans**.
2. Select the replication plan, click the **Failover mapping** tab, and click the **Edit** pencil icon.

3. Click the **Datastores** arrow to expand it.
4. Note the value of the retention count in the replication plan. You will need to reinstate this original value when you're finished with these steps.
5. Reduce the count to 1.
6. Initiate an on-demand snapshot. To do so, on the Replication plan page, select the plan, click the Actions icon, and select **Take snapshot now**.
7. After the snapshot job completes successfully, increase the count in the replication plan back to its original value that you noted in the first step.
8. Repeat these steps for all existing replication plans.

5 July 2024

This BlueXP disaster recovery release includes the following updates:

Support for AFF A-series

This release supports the NetApp AFF A-series hardware platforms.

Support for on-premises to on-premises VMware VMFS datastores

This release includes a *technology preview* of support for VMs mounted on VMware vSphere virtual machine file system (VMFS) datastores protected to on-premises storage. With this release, disaster recovery is supported in a technology preview for on-premises VMware workloads to on-premises VMware environment with VMFS datastores.

NetApp doesn't charge you for any previewed workload capacity.

Replication plan updates

You can add a replication plan more easily by filtering VMs by datastore on the Applications page and by selecting more target details on the Resource mapping page.
Refer to Create a replication plan.

Edit replication plans

With this release, the Failover mappings page has been enhanced for better clarity.

Refer to Manage plans.

Edit VMs

With this release, the process for editing VMs in the plan included some minor UI improvements.

Refer to Manage VMs.

Fail over updates

Before you initiate a failover, you can now determine the status of VMs and whether they are powered on or off. The failover process now enables you to take a snapshot now or choose the snapshots.

Refer to Fail over applications to a remote site.

Failover test schedules

You can now edit the failover tests and set daily, weekly, and monthly schedules for the failover test.

Refer to Manage plans.

Updates to prerequisite information

BlueXP disaster recovery prerequisites information has been updated.

Refer to BlueXP disaster recovery prerequisites.

15 May 2024

This BlueXP disaster recovery release includes the following updates:

Replicating VMware workloads from on-premises to on-premises

This is now released as a general availability feature. Previously, it was a technology preview with limited functionality.

Licensing updates

With BlueXP disaster recovery, you can sign up for a 90-day free trial, purchase a pay-as-you-go (PAYGO) subscription with Amazon Marketplace, or Bring Your Own License (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep or from the NetApp Support Site (NSS).

For details about setting up licensing for BlueXP disaster recovery, refer to Set up licensing.

Learn more about BlueXP disaster recovery.

5 March 2024

This is the General Availability release of BlueXP disaster recovery, which includes the following updates.

Licensing updates

With BlueXP disaster recovery, you can sign up for a 90-day free trial or Bring Your Own License (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep. You can use the license serial number to get the BYOL activated in BlueXP digital wallet. BlueXP disaster recovery charges are based on provisioned capacity of datastores.

For details about setting up licensing for BlueXP disaster recovery, refer to Set up licensing.

For details about managing licenses for **all** BlueXP services, refer to Manage licenses for all BlueXP services.

Edit schedules

With this release, you can now set up schedules to test compliance and failover tests so that you ensure that they will work correctly should you need them.

For details, refer to Create the replication plan.

1 February 2024

This BlueXP disaster recovery preview release includes the following updates:

Network enhancement

With this release, you can now resize the VM CPU and RAM values. You can also now select a network DHCP or static IP address for the VM.

- DHCP: If you choose this option, you provide credentials for the VM.
- Static IP: You can select the same or different information from the source VM. If you choose the same as the source, you do not need to enter credentials. On the other hand, if you choose to use different information from the source, you can provide the credentials, IP address, subnet mask, DNS, and gateway information.

For details, refer to Create a replication plan.

Custom scripts

Can now be included as post failover processes. With custom scripts, you can have BlueXP disaster recovery run your script after a failover process. For example, you can use a custom script to resume all database transactions after the failover is complete.

For details, refer to Fail over to a remote site.

SnapMirror relationship

You can now create a SnapMirror relationship while developing the replication plan. Previously, you had to create the relationship outside of BlueXP disaster recovery.

For details, refer to Create a replication plan.

Consistency groups

When you create a replication plan, you can include VMs that are from different volumes and different SVMs. BlueXP disaster recovery creates a Consistency Group Snapshot by including all the volumes and updates all the secondary locations.

For details, refer to Create a replication plan.

VM power-on delay option

When you create a replication plan, you can add VMs to a Resource Group. With Resource Groups, you can set a delay on each VM so that they power up on a delayed sequence.

For details, refer to Create a replication plan.

Application-consistent Snapshot copies

You can specify to create application-consistent Snapshot copies. The service will quiesce the application and then take a Snapshot to obtain a consistent state of the application.

For details, refer to Create a replication plan.

11 January 2024

This preview release of BlueXP disaster recovery includes the following updates:

Dashboard more quickly

With this release, you can access information on other pages from the Dashboard more quickly.

Learn about BlueXP disaster recovery.

20 October 2023

This preview release of BlueXP disaster recovery includes the following updates.

Protect on-premises, NFS-based VMware workloads

Now with BlueXP disaster recovery, you can protect your on-premises, NFS-based VMware workloads against disasters to another on-premises, NFS-based VMware environment in addition to the public cloud. BlueXP disaster recovery orchestrates the completion of the disaster recovery plans.

With this preview offering, NetApp reserves the right to modify offering details, contents and timeline before General Availability.

Learn more about BlueXP disaster recovery.

27 September 2023

This preview release of BlueXP disaster recovery includes the following updates:

Dashboard updates

You can now click into the options on the Dashboard, making it easier for you to review the information quickly. Also, the Dashboard now shows the status of failovers and migrations.

Refer to View the health of your disaster recovery plans on the Dashboard.

Replication plan updates

- **RPO**: You can now enter the Recovery Point Objective (RPO) and Retention count in the Datastores section of the Replication plan. This indicates the amount of data that must exist that is not older than the set time. If, for example, you set it at 5 minutes, the system can lose up to 5 minutes of data if there's a disaster without impacting business critical needs.

  Refer to Create a replication plan.

- **Networking enhancements**: When you are mapping networking between source and target locations in the virtual machines section of the replication plan, BlueXP disaster recovery now offers two options: DHCP or static IP. Previously, just DHCP was supported. For static IPs, you configure the subnet, gateway, and DNS servers. Additionally, you can now enter credentials for virtual machines.

  Refer to Create a replication plan.

- **Edit schedules**: You can now update replication plan schedules.

Refer to Manage resources.

- **SnapMirror automation**: While you are creating the replication plan in this release, you can define the SnapMirror relationship between source and target volumes in one of the following configurations:
  - 1 to 1
  - 1 to many in a fanout architecture
  - Many to 1 as a Consistency Group
  - Many to many

  Refer to Create a replication plan.

1 August 2023

BlueXP disaster recovery preview

BlueXP disaster recovery preview is a cloud-based disaster recovery service that automates disaster recovery workflows. Initially, with the BlueXP disaster recovery preview, you can protect your on-premises, NFS-based VMware workloads running NetApp storage to VMware Cloud (VMC) on AWS with Amazon FSx for ONTAP.

With this preview offering, NetApp reserves the right to modify offering details, contents and timeline before General Availability.

Learn more about BlueXP disaster recovery.

This release includes the following updates:

Resource groups update for boot order

When you create a disaster recovery or replication plan, you can add virtual machines into functional resource groups. Resource groups enable you to put a set of dependent virtual machines into logical groups that meet your requirements. For example, groups could contain boot order that can be executed upon recovery. With this release, each resource group can include one or more virtual machines. The virtual machines will power on based on the sequence in which you include them in the plan. Refer to Select applications to replicate and assign resource groups.

Replication verification

After you create the disaster recovery or replication plan, identify the recurrence in the wizard, and initiate a replication to a disaster recovery site, every 30 minutes BlueXP disaster recovery verifies that the replication is actually occurring according to the plan. You can monitor the progress in the Job Monitor page. Refer to Replicate applications to another site.

Replication plan shows recovery point objective (RPO) transfer schedules

When you create a disaster recovery or replication plan, you select the VMs. In this release, you can now view the SnapMirror associated with each of the volumes that are associated with the datastore or VM. You can also see the RPO transfer schedules that are associated with the SnapMirror schedule. RPO helps you determine whether your backup schedule is enough to recover after a disaster. Refer to Create a replication plan.

Job Monitor update

The Job Monitor page now includes a Refresh option so that you can get an up-to-date status of operations. Refer to Monitor disaster recovery jobs.

18 May 2023

This is the initial release of BlueXP disaster recovery.

Cloud-based disaster recovery service

BlueXP disaster recovery is a cloud-based disaster recovery service that automates disaster recovery workflows. Initially, with the BlueXP disaster recovery preview, you can protect your on-premises, NFS-based VMware workloads running NetApp storage to VMware Cloud (VMC) on AWS with Amazon FSx for ONTAP.

Learn more about BlueXP disaster recovery.

Limitations in BlueXP disaster recovery

Known limitations identify platforms, devices, or functions that are not supported by this release of the service, or that do not interoperate correctly with it.

Wait until failback completes before running discovery

After a failover has finished, do not initiate discovery on the source vCenter manually. Wait until the failback has finished and then initiate discovery on the source vCenter.

BlueXP might not discover Amazon FSx for NetApp ONTAP

Sometimes, BlueXP does not discover Amazon FSx for NetApp ONTAP clusters. This might be because the FSx credentials were not correct.

Workaround: Add the Amazon FSx for NetApp ONTAP cluster in BlueXP and periodically refresh the cluster to display any changes.

If you need to remove the ONTAP FSx cluster from BlueXP disaster recovery service, complete the following steps:

1. In the BlueXP Connector, use the connectivity options from your cloud provider, connect to the Linux VM that the Connector runs on, restart the "occm" service using the `docker restart occm` command.

   Refer to Manage existing Connectors.

2. In the BlueXP Canvas, add the Amazon FSx for ONTAP environment again and provide the FSx credentials.

   Refer to Create an Amazon FSx for NetApp ONTAP file system.

3. From BlueXP disaster recovery, select **Sites**, on the vCenter row select the **Actions** option  , and from the Actions menu, select **Refresh** to refresh the FSx discovery in BlueXP disaster recovery.

   This rediscovers the datastore, its virtual machines, and its destination relationship.

Get started

Learn about BlueXP disaster recovery for VMware

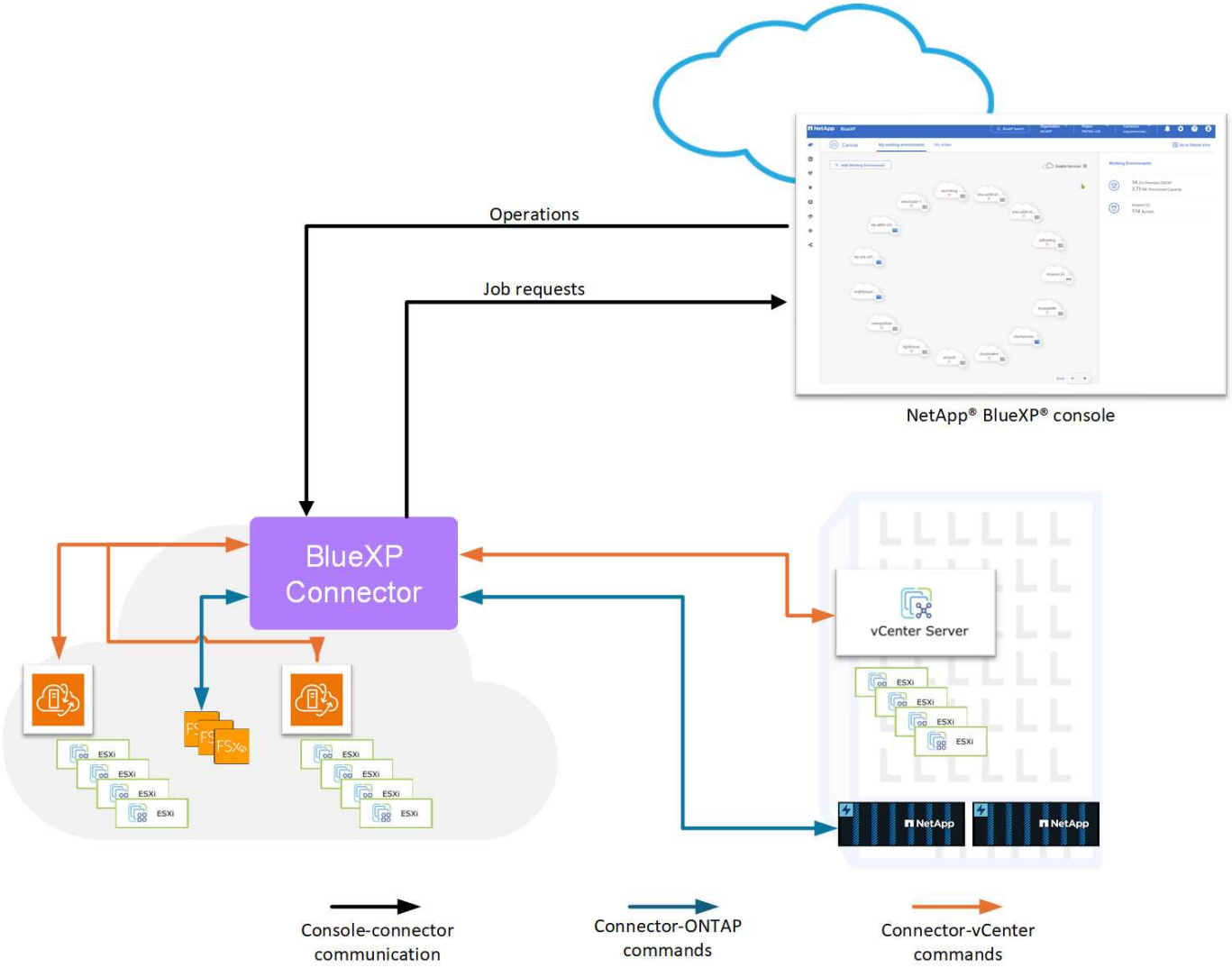
Disaster recovery to the cloud is a resilient and cost-effective way of protecting workloads against site outages and data corruption events. With BlueXP disaster recovery for VMware, you can replicate your on-premises VMware VM or datastore workloads running ONTAP storage to a VMware software-defined data center in a public cloud using NetApp cloud storage or to another on-premises VMware environment with ONTAP storage as a disaster recovery site.

BlueXP disaster recovery is a cloud-based disaster recovery service that automates disaster recovery workflows. With the BlueXP disaster recovery service you can protect your on-premises, NFS-based workloads and VMware vSphere virtual machine file system (VMFS) datastores for iSCSI and FC running NetApp storage to one of the following:

- VMware Cloud (VMC) on AWS with Amazon FSx for NetApp ONTAP or
- Another on-premises, NFS-based VMware environment with ONTAP storage

THIS DOCUMENTATION REGARDING AWS EVS IS PROVIDED AS A TECHNOLOGY PREVIEW. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability. For details, see Introduction of BlueXP disaster recovery using Amazon Elastic VMware Service and Amazon FSx for NetApp ONTAP.

BlueXP disaster recovery uses ONTAP SnapMirror technology as the replication transport to the disaster recovery site. This enables industry-best storage efficiency (compression and deduplication) on primary and secondary sites.



Benefits of using BlueXP disaster recovery for VMware

BlueXP disaster recovery offers the following benefits:

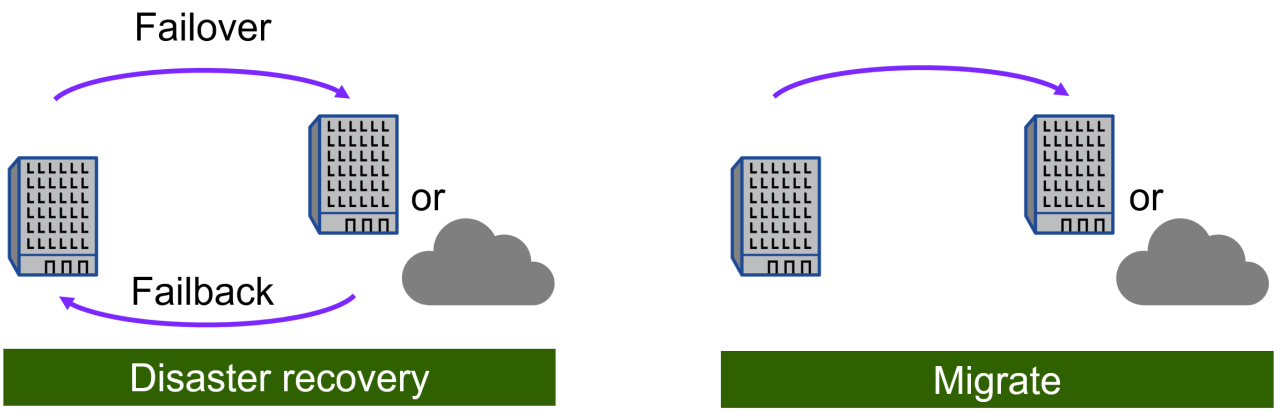
- Simplified user experience for vCenter discovery and recovery of applications with multiple point-in-time recovery operations
- Lower total cost of ownership with reduced cost of operations and ability to create and adjust disaster recovery plans with minimal resources
- Continuous disaster recovery readiness with virtual failover testing that does not disrupt operations
- Faster time to value with dynamic changes in your IT environment and ability to address it in your disaster recovery plans

What you can do with BlueXP disaster recovery for VMware

BlueXP disaster recovery provides you with full use of several NetApp technologies to accomplish the following goals:

- Replicate VMware apps on your on-premises production site to a disaster recovery remote site in the cloud or on-premises using SnapMirror replication.
- Migrate VMware workloads from your original site to another site.

- Conduct a failover test; virtual machines are temporarily created. BlueXP disaster recovery makes a new FlexClone volume from the selected snapshot, and a temporary datastore backing the FlexClone volume is mapped to the ESXi hosts. This process doesn't consume additional physical capacity on on-premises ONTAP storage or FSx for NetApp ONTAP storage in AWS. The original source volume is not modified and replica jobs can continue even during disaster recovery.
- In case of disaster, fail over your primary site on demand to the disaster recovery site, which can be VMware Cloud on AWS with Amazon FSx for NetApp ONTAP or an on-premises VMware environment with ONTAP.
- After the disaster has been resolved, fail back on demand from the disaster recovery site to the primary site.
  *Group VMs or datastores into logical resource groups for efficient management.



Configuration of vSphere server is done outside of BlueXP disaster recovery in vSphere Server.

Cost

NetApp doesn't charge you for using the trial version of BlueXP disaster recovery.

The BlueXP disaster recovery service can be used either with a NetApp license or an annual subscription-based plan through Amazon Web Services.

Some releases include a technology preview. NetApp doesn't charge you for any previewed workload capacity. See What's new in BlueXP disaster recovery for information about the latest technology previews.

Licensing

You can use the following license types:

- Sign up for a 30-day free trial.
- Purchase a pay-as-you-go (PAYGO) subscription to **NetApp Intelligent Services** with the Amazon Web Services (AWS) Marketplace and Microsoft Azure Marketplace.
- Bring your own license (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep. You can use the license serial number to get the BYOL activated in BlueXP digital wallet.

Licenses for all BlueXP services are managed by the BlueXP digital wallet service. After you set up your BYOL, you can see an active license for the service in the BlueXP digital wallet.

> BlueXP disaster recovery charges are based on used capacity of datastores on the source site when there is at least one VM that has a replication plan. Capacity for a failed over datastore is not included in the capacity allowance. For a BYOL, if the data exceeds the allowed capacity, operations in the service are limited until you obtain an additional capacity license or upgrade the license in BlueXP digital wallet.

For details about setting up licensing for BlueXP disaster recovery, refer to Set up BlueXP disaster recovery licensing.

30-day free trial

You can try out BlueXP disaster recovery by using a 30-day free trial.

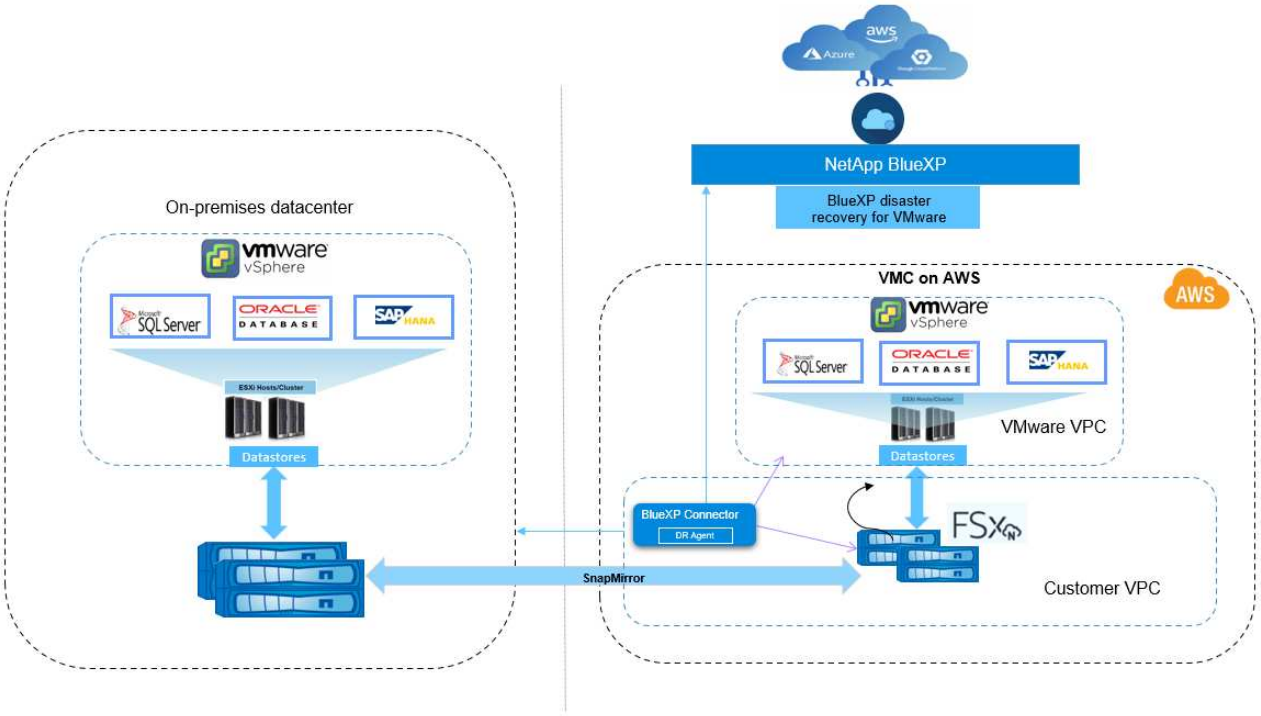
To continue after the 30-day trial, you'll need to obtain a Pay-as-you-go (PAYGO) subscription from your cloud provider or purchase a BYOL license from NetApp.

You can purchase a license at any time and you will not be charged until the 30-day trial ends.

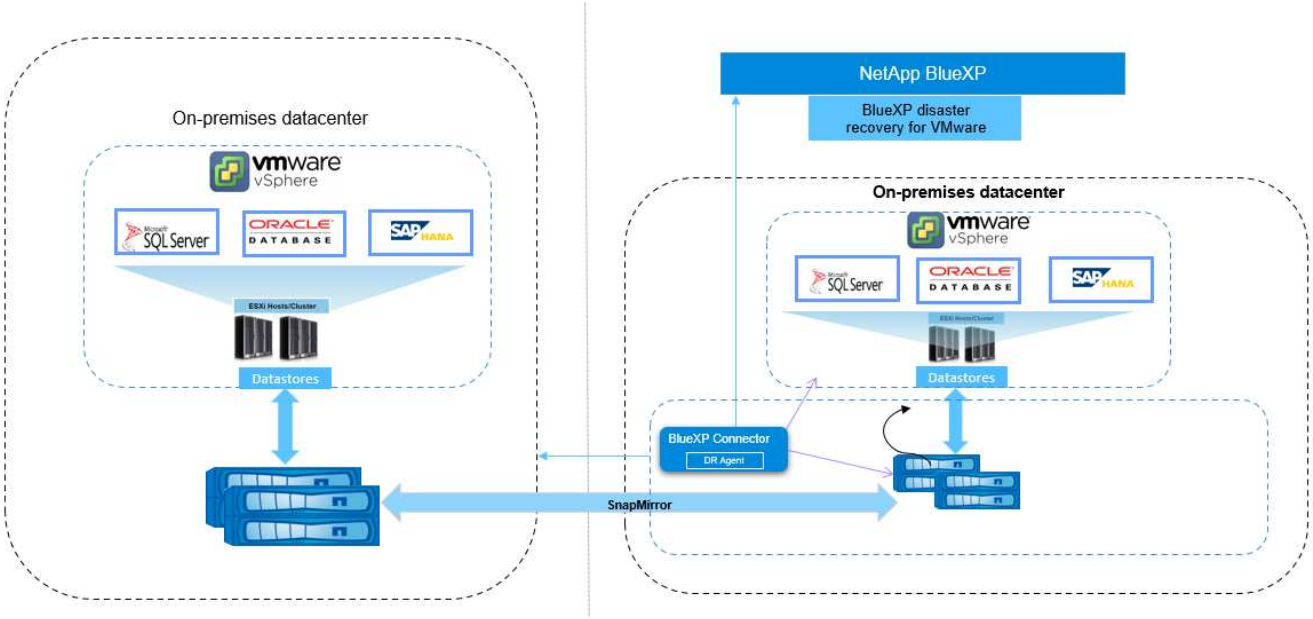
How BlueXP disaster recovery works

BlueXP disaster recovery can recover workloads replicated from an on-premises site to Amazon FSx for ONTAP or to another on-premises site. This service automates the recovery from the SnapMirror level, through virtual machine registration to Virtual Machine Cloud (VMC), and to network mappings directly on the VMware network virtualization and security platform, NSX-T. This feature is included with all Virtual Machine Cloud environments.

BlueXP disaster recovery uses ONTAP SnapMirror technology, which provides highly efficient replication and preserves the ONTAP incremental-forever snapshot efficiencies. SnapMirror replication ensures that application-consistent snapshot copies are always in sync and the data is usable immediately after a failover.



The following diagram shows the architecture of on-premises to on-premises disaster recovery plans.



When there is a disaster, this service helps you recover virtual machines in the other on-premises VMware environment or VMC by breaking the SnapMirror relationships and making the destination site active.

- The service also lets you fail back virtual machines to the original source location.
- You can test the disaster recovery failover process without disrupting the original virtual machines. The test recovers virtual machines to an isolated network by creating a FlexClone of the volume.
- For the failover or test failover process, you can choose the latest (default) or selected snapshot from which to recover your virtual machine.

Terms that might help you with BlueXP disaster recovery

You might benefit by understanding some terminology related to disaster recovery.

- **Site**: A logical container typically associated with a physical datacenter or cloud provider.
- **Resource group**: A logical container that enables you to manage multiple VMs as a single unit.
- **Replication plan**: A set of rules about how often backups occur and how to handle failover events. Plans are assigned to one or more resource groups.

BlueXP disaster recovery prerequisites

Before using BlueXP disaster recovery, you should ensure that your environment meets the ONTAP storage, VMware vCenter cluster, and BlueXP requirements.

ONTAP storage prerequisites

These prerequisites apply to either ONTAP or Amazon FSX for NetApp ONTAP instances.

- Source and destination clusters must have a peer relationship.
- The SVM that will host the disaster recovery volumes must exist on the destination cluster.
- The source SVM and destination SVM must have a peer relationship.

> Disaster recovery volumes in the destination SVM or SVMs should not be created ahead of time. BlueXP disaster recovery will create the destination volumes as needed for the replication plan.

- If deploying with Amazon FSx for NetApp ONTAP, the following prerequisite applies:
  - An Amazon FSx for NetApp ONTAP instance to host VMware DR datastores must exist in your VPC. Refer to Amazon FSx for ONTAP documentation on how to get started.

VMware vCenter clusters prerequisites

These prerequisites apply to both on-premises vCenter clusters and to VMware Cloud for AWS software-defined data center (SDDC).

- All VMware clusters that you want BlueXP disaster recovery to manage must be hosted on ONTAP volumes.
- All VMware datastores to be managed by BlueXP disaster recovery must use one of the following protocols:
  - NFS
  - VMFS using the iSCSI or FC protocol
- VMware vSphere version 7.0 Update 3 (7.0v3) or later
- If you are using VMware Cloud SDDC, these prerequisites apply.
  - In the VMware Cloud Console, use the service roles of Administrator and NSX Cloud Administrator. Also use the organization owner for the Organization role. Refer to Using VMware Cloud Foundations with AWS FSx for NetApp ONTAP documentation.
  - Link the VMware Cloud SDDC with Amazon FSx for NetApp ONTAP instance. Refer to VMware Cloud

on AWS integration with Amazon FSx for NetApp ONTAP deployment information.

BlueXP prerequisites

Get started with BlueXP

If you haven't already done so, sign up to BlueXP and create an organization

Gather credentials for ONTAP and VMware

- Amazon FSx for ONTAP and AWS credentials must be added to the working environment within the BlueXP project that will be used to manage BlueXP disaster recovery.
- BlueXP disaster recovery requires vCenter credentials. You enter the vCenter credentials when you're adding a site in BlueXP disaster recovery.

  For a list of vCenter privileges needed, refer to vCenter privileges needed for BlueXP disaster recovery. For instructions on how to add a site, refer to Add a site.

Create a BlueXP Connector

A BlueXP Connector must be set up in BlueXP. When you use the BlueXP Connector, it will include the appropriate capabilities for the disaster recovery service.

- BlueXP disaster recovery works only with the standard mode Connector deployment. See Getting started with BlueXP in standard mode.
- Ensure that both the source and destination vCenters use the same BlueXP Connector.
- Type of BlueXP Connector needed:
  - **On-premises to on-premises disaster recovery**: Install the BlueXP on-premises Connector in the disaster recovery site. Refer to Install and set up a Connector on premises.
  - **On-premises to AWS**: Install the BlueXP Connector for AWS in your AWS VPC. Refer to Connector installation options in AWS.

    For on-premises to on-premises, use the BlueXP on-premises Connector. For on-premises to AWS, use the BlueXP AWS Connector, which has access to the source on-premises vCenter and the destination on-premises vCenter.

  - The installed BlueXP Connector must be able to access any VMware cluster that BlueXP disaster recovery will manage.
- All ONTAP arrays to be managed by BlueXP disaster recovery must be added to any working environment within the BlueXP project that will be used to manage BlueXP disaster recovery.

  See Discover on-premises ONTAP clusters.

- For information about setting up an intelligent proxy for BlueXP disaster recovery, see Set up your infrastructure for BlueXP disaster recovery.

Workload prerequisites

To ensure that application-consistency processes are successful, apply these prerequisites:

- Ensure that VMware tools (or Open VM tools) are running on the VMs that will be protected.
- For Windows VMs running Microsoft SQL Server or Oracle Database or both, the databases should have their VSS Writers enabled.
- Oracle databases that are running on a Linux operating system should have the operating system user authentication enabled for the Oracle database SYSDBA role.

Quick start for BlueXP disaster recovery

Here's an overview of the steps needed to get started with BlueXP disaster recovery. The links within each step take you to a page that provides more details.

1 **Review prerequisites**

Ensure your environment meets these requirements.

2 **Set up the BlueXP disaster recovery service**

- Set up the infrastructure for the service.
- Set up licensing.

3 **What's next?**

After you set up the service, here's what you might do next.

- Add your vCenter sites to BlueXP disaster recovery.
- Create your first resource group.
- Create your first replication plan.
- Replicate applications to another site.
- Fail over applications to a remote site.
- Fail back applications to the original source site.
- Manage sites, resource groups, and replication plans.
- Monitor disaster recovery operations.

Set up your infrastructure for BlueXP disaster recovery

To use BlueXP disaster recovery, perform a few steps to set it up both in Amazon Web Services (AWS) and in BlueXP.

Review prerequisites to ensure that your environment is ready.

Get ready for BlueXP disaster recovery for on-premises-to-on-premises protection

Ensure that the following requirements are met before you set up BlueXP disaster recovery for on-premises-to-on-premises protection:

- ONTAP storage
  - Ensure that you have ONTAP credentials.
  - Create or verify your disaster recovery site.
  - Create or verify your destination ONTAP SVM.
  - Ensure that your source and destination ONTAP SVMs are peered.
- vCenter clusters
  - Ensure that the VMs you want to protect are hosted on NFS datastores (using ONTAP NFS volumes) or VMFS datastores (using NetApp iSCSI LUNs).
  - Review vCenter privileges required for BlueXP DR.
  - Create a disaster recovery user account (not the default vCenter admin account) and assign the vCenter privileges to the account.

Intelligent proxy support

The BlueXP Connector supports intelligent proxy. Intelligent proxy is a lightweight, secure, and efficient way to connect your on-premises environment to the BlueXP service. It provides a secure connection between your environment and the BlueXP service without requiring a VPN or direct internet access. This optimized proxy implementation offloads API traffic within the local network.

When a proxy is configured, BlueXP disaster recovery attempts to communicate directly with VMware or ONTAP and uses the configured proxy if direct communication fails.

BlueXP disaster recovery proxy implementation requires port 443 communication between the Connector and any vCenter Servers and ONTAP arrays using an HTTPS protocol. The BlueXP disaster recovery agent within the Connector communicates directly with VMware vSphere, the VC, or ONTAP when performing any actions.

For more information about general proxy set up in BlueXP, see Configure a Connector to use a proxy server.

Get ready for BlueXP disaster recovery for on-premises-to-cloud protection using AWS

To set up BlueXP disaster recovery for on-premises-to-cloud protection using AWS, you need to set up the following:

- Set up AWS FSx for NetApp ONTAP
- Set up VMware Cloud on AWS SDDC

Set up AWS FSx for NetApp ONTAP

- Create an Amazon FSx for NetApp ONTAP file system.
  - Provision and configure FSx for ONTAP. Amazon FSx for NetApp ONTAP is a fully managed service that provides highly reliable, scalable, high-performing, and feature-rich file storage, built on the NetApp ONTAP file system.
  - Follow the steps in Technical Report 4938: Mount Amazon FSx ONTAP as an NFS datastore with VMware Cloud on AWS and Quick start for Amazon FSx for NetApp ONTAP to provision and configure FSx for ONTAP.
- Add Amazon FSx for ONTAP to the working environment, and add AWS credentials for FSx for ONTAP.
- Create or verify your destination ONTAP SVM in AWS FSx for ONTAP instance.

- Configure replication between your source on-premises ONTAP cluster and your FSx for ONTAP instance in BlueXP.

Refer to how to set up an FSx for ONTAP working environment for detailed steps.

Set up VMware Cloud on AWS SDDC

VMware Cloud on AWS provides a cloud-native experience for VMware-based workloads in the AWS ecosystem. Each VMware software-defined data center (SDDC) runs in an Amazon Virtual Private Cloud (VPC) and provides a full VMware stack (including vCenter Server), NSX-T software-defined networking, vSAN software-defined storage, and one or more ESXi hosts that provide compute and storage resources to the workloads.

To configure a VMware Cloud environment on AWS, follow the steps in Deploy and configure the Virtualization Environment on AWS. A pilot-light cluster can also be used for disaster recovery purposes.

Access BlueXP disaster recovery

You use NetApp BlueXP to log in to the BlueXP disaster recovery service.

To log in to BlueXP, you can use your NetApp Support Site credentials or you can sign up for a NetApp cloud login using your email and a password. Learn more about logging in.

Specific tasks require specific BlueXP user roles.
Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

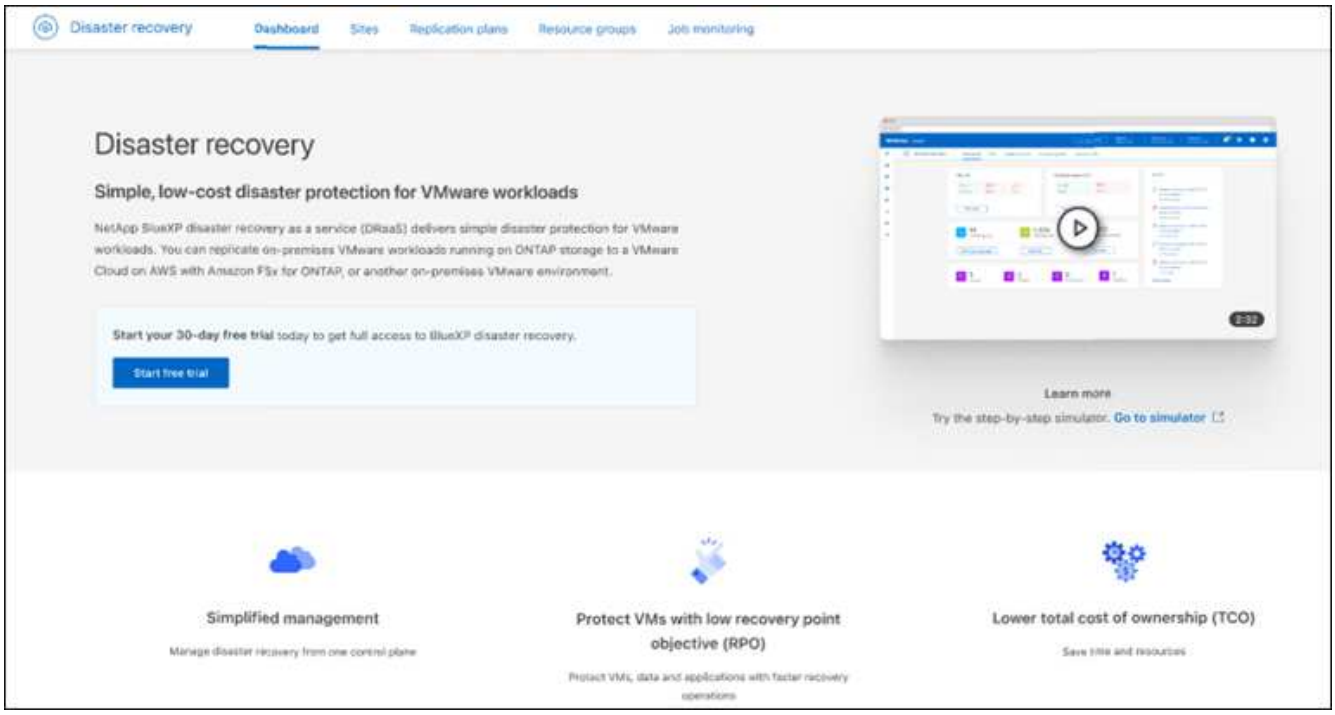
Steps

1. Open a web browser and go to the BlueXP console.

   The NetApp BlueXP login page appears.

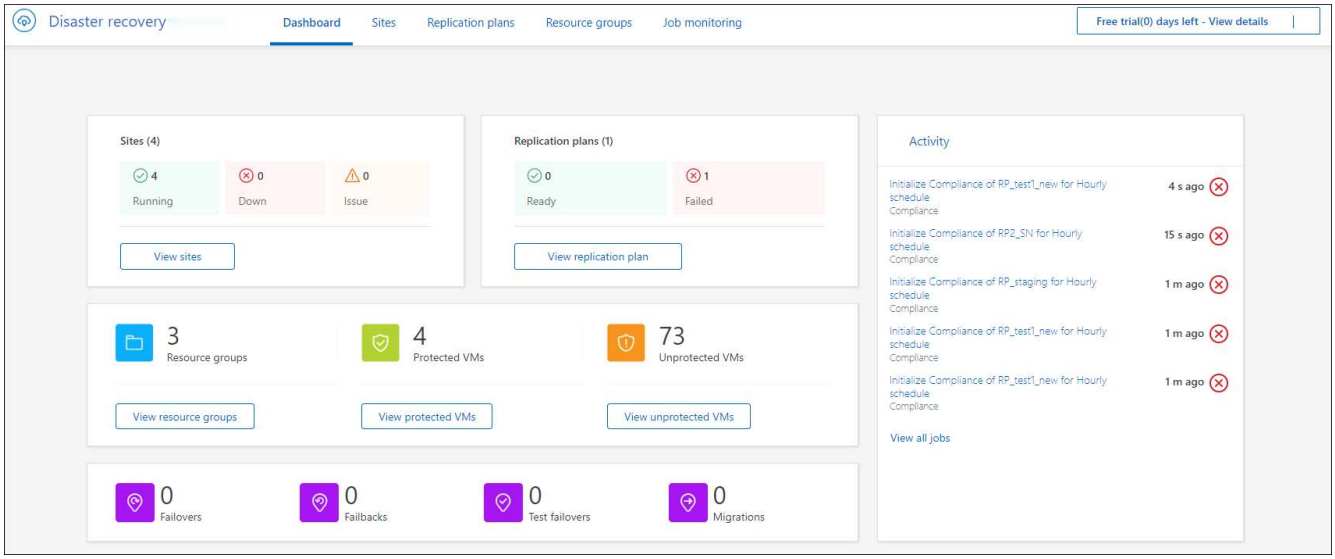
2. Log in to BlueXP.
3. From the BlueXP left navigation, select **Protection** > **Disaster recovery**.

   If this is your first time logging in to this service, the landing page appears and you can sign up for a free trial.



Otherwise, the BlueXP disaster recovery Dashboard appears.

- If you haven't yet added a BlueXP Connector, you'll need to add a Connector. To add a Connector, refer to Learn about Connectors.
- If you are a BlueXP user with an an existing Connector, when you select "Disaster recovery," a message appears about signing up.
- If you are already using the service, when you select "Disaster recovery," the Dashboard appears.



Set up licensing for BlueXP disaster recovery

With BlueXP disaster recovery, you can use different licensing plans including a free trial, a pay-as-you-go subscription, or bring your own license.

Required BlueXP role

Organization admin, Folder or project admin, Disaster recovery admin, or Disaster recovery application admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

Licensing options
You can use the following licensing options:

- Sign up for a 30-day free trial.
- Purchase a pay-as-you-go (PAYGO) subscription to **NetApp Intelligent Services** with Amazon Web Services (AWS) Marketplace or to Microsoft Azure Marketplace.
- Bring your own license (BYOL), which is a NetApp License File (NLF) that you obtain from your NetApp Sales Rep. You can use the license serial number to get the BYOL activated in BlueXP digital wallet.

> BlueXP disaster recovery charges are based on used capacity of datastores on the source site when there is at least one VM that has a replication plan. Capacity for a failed over datastore is not included in the capacity allowance. For a BYOL, if the data exceeds the allowed capacity, operations in the service are limited until you obtain an additional capacity license or upgrade the license in BlueXP digital wallet.

Learn more about digital wallet.

After the free trial ends or the license expires, you can still do the following in the service:

- View any resource, such as a workload or replication plan.
- Delete any resource, such as a workload or replication plan.
- Run all scheduled operations that were created during the trial period or under the license.

Try it out using a 30-day free trial

You can try BlueXP disaster recovery out by using a 30-day free trial.

> No capacity limits are enforced during the trial.

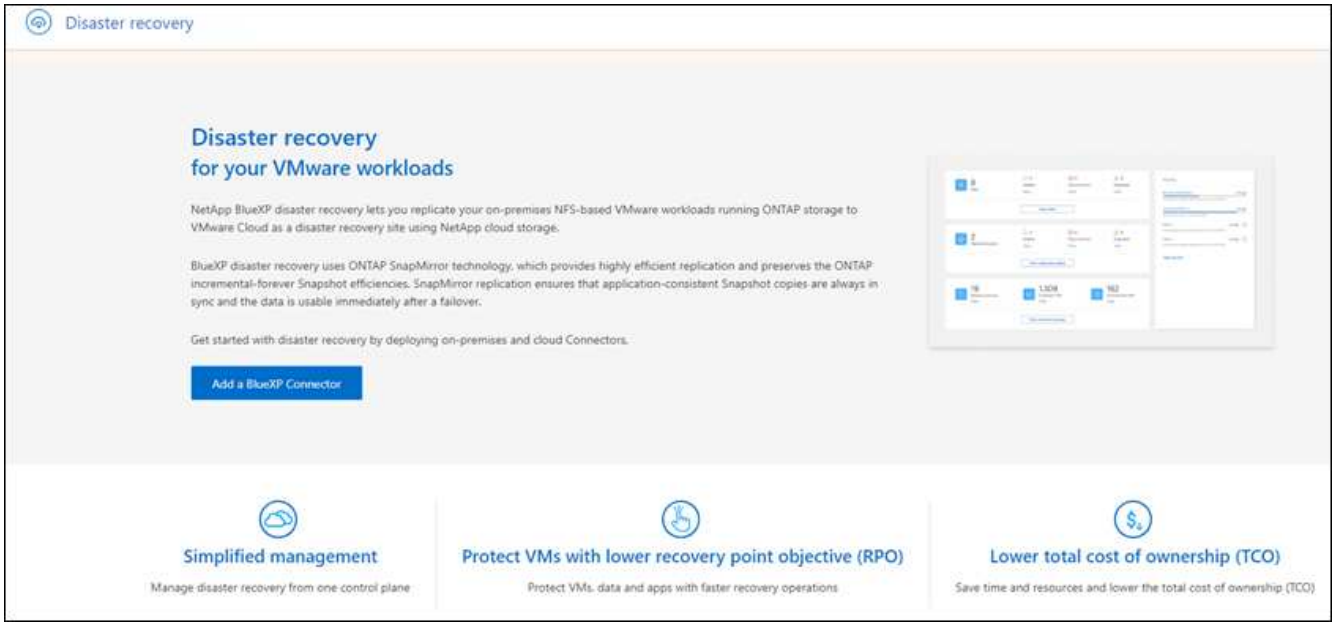
To continue after the trial, you'll need to purchase a BYOL license or PAYGO AWS subscription. You can get a license at any time and you will not be charged until the trial ends.

During the trial, you have full functionality.

Steps

1. Access the BlueXP console.
2. Log in to BlueXP.
3. From the BlueXP left navigation, select **Protection** > **Disaster recovery**.

   If this is your first time logging in to this service, the landing page appears.



4. If you haven't already added a Connector for other services, add one.

   To add a Connector, refer to Learn about Connectors.

5. After you set up a Connector, in the BlueXP disaster recovery landing page, the button to add a Connector changes to a button for starting a free trial. Select **Start free trial**.
6. Begin by adding vCenters.

   For details, see Add vCenter sites.

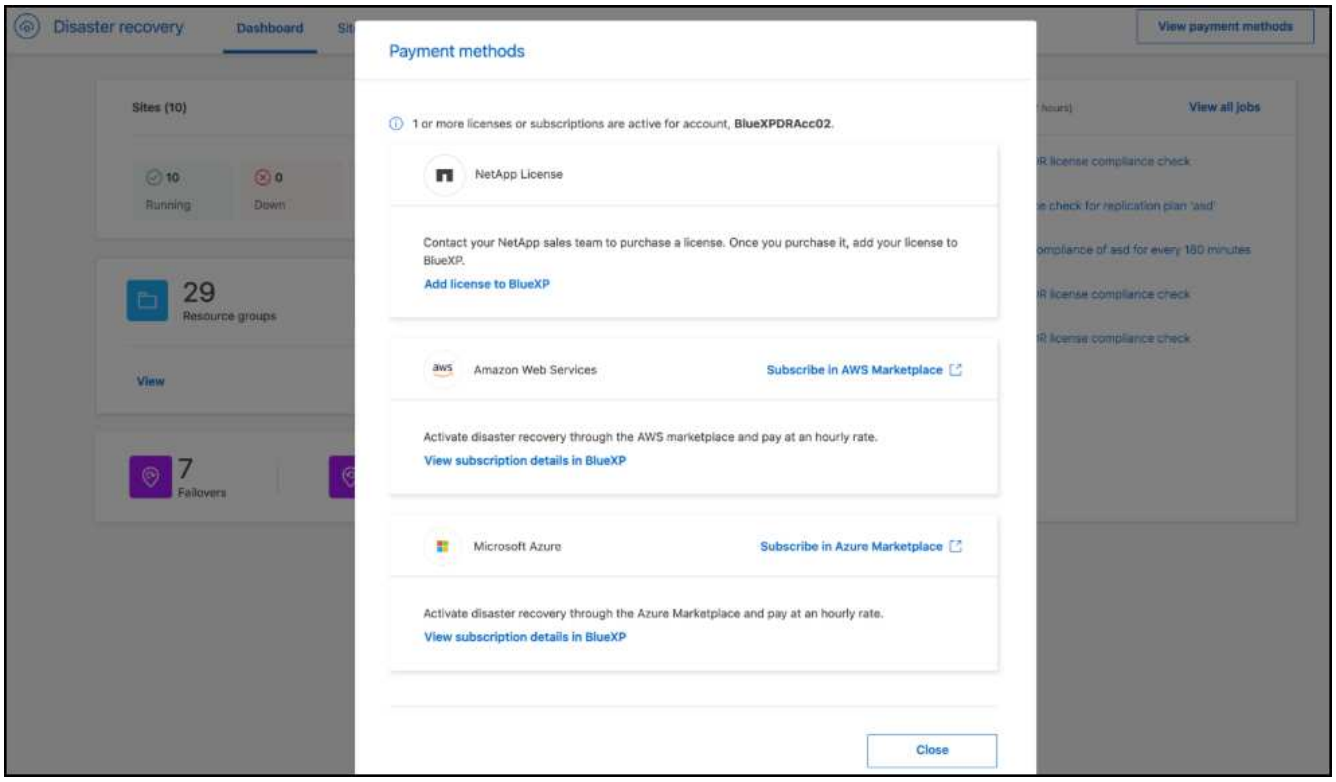
After the trial ends, subscribe through one of the Marketplaces

After the free trial ends, you can either purchase a license from NetApp or subscribe to **NetApp Intelligent Services** through AWS Marketplace or Microsoft Azure Marketplace. This procedure provides a high level overview of how to subscribe directly in one of the Marketplaces.

Steps

1. In the BlueXP disaster recovery, you see a message that the free trial is expiring. In the message, select **Subscribe or purchase a license**.

   Or, from the top right, select **View payment methods**.



2. Select **Subscribe in AWS Marketplace** or **Subscribe in Azure Marketplace**.
3. Use AWS Marketplace or Microsoft Azure Marketplaceto subscribe to **NetApp Intelligent Services** and **BlueXP disaster recovery**.
4. When you return to BlueXP disaster recovery, a message states that you are subscribed.

   You can view subscription details in BlueXP digital wallet. Learn more managing subscriptions with digital wallet.

After the trial ends, purchase a BYOL license through NetApp

After the trial ends, you can purchase a license through your NetApp Sales Rep.

If you bring your own license (BYOL), the set up includes purchasing the license, getting the NetApp License File (NLF), and adding the license to BlueXP digital wallet.

Add the license to BlueXP digital wallet*
After you've purchased your BlueXP disaster recovery license from your NetApp Sales Rep, you can manage the license in digital wallet.

Learn about adding licenses with digital wallet.

Update your BlueXP license when it expires

If your licensed term is nearing the expiration date, or if your licensed capacity is reaching the limit, you'll be notified in the BlueXP disaster recovery UI. You can update your BlueXP disaster recovery license before it expires so that there is no interruption in your ability to access your scanned data.

This message also appears in BlueXP digital wallet and in Notifications.

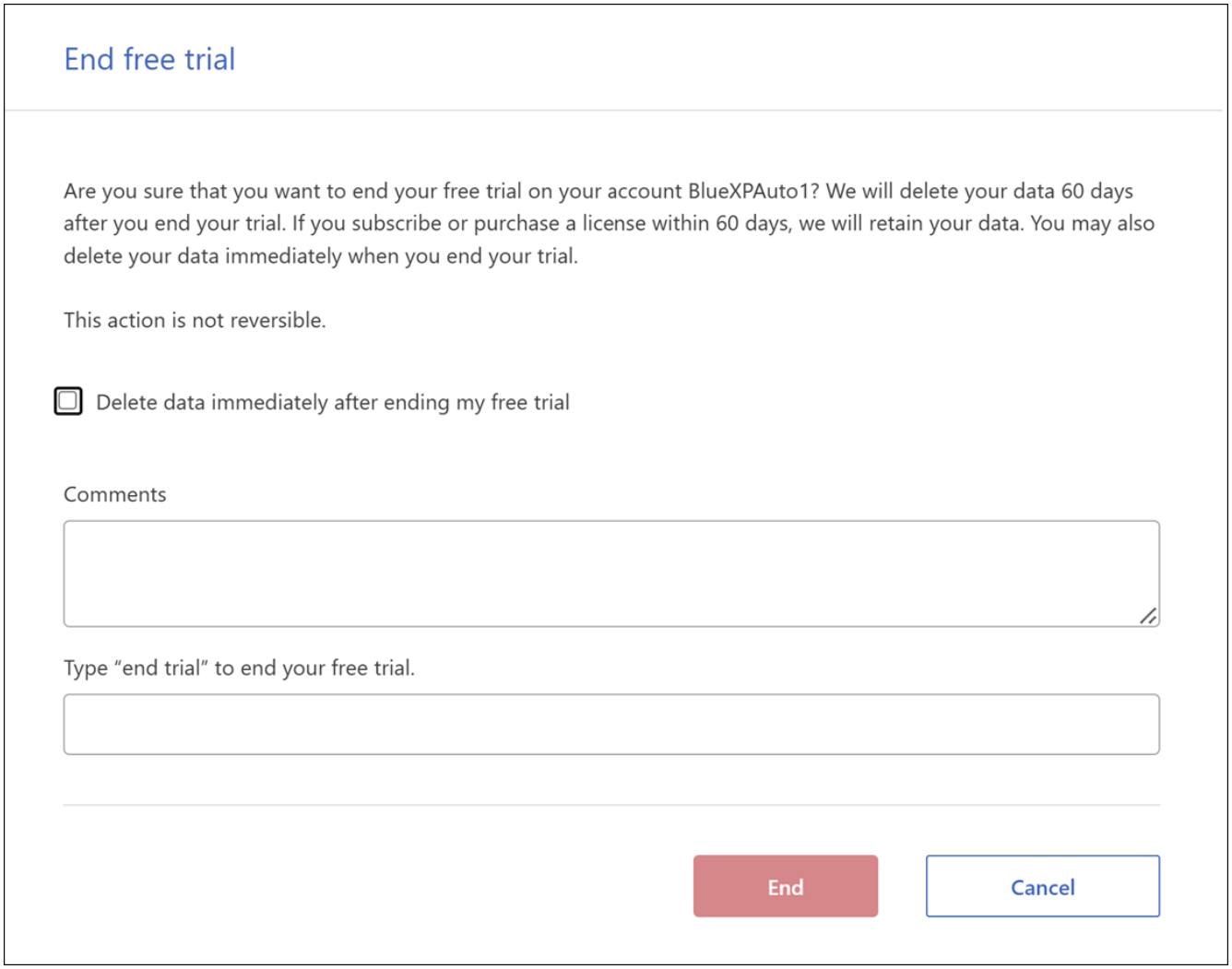
Learn about updating licenses with digital wallet.

End the free trial

You can stop the free trial at any time or you can wait until it expires.

Steps

1. In BlueXP disaster recovery, at the top right, select **Free trial - View details**.
2. In the drop-down details, select **End free trial**.



3. If you want to delete all data, check **Delete data immediately after ending my free trial**.

   This will delete all schedules, replication plans, resource groups, vCenters, and sites. Audit data, operation logs, and jobs history are retained until the end of the life of the product.

   If you end the free trial, did not request to delete data and don’t purchase a license or subscription, then BlueXP disaster recovery deletes all of your data 60 days after the free trial ends.

4. Type "end trial" in the text box.
5. Select **End**.

Frequently asked questions for BlueXP disaster recovery

This FAQ can help if you're just looking for a quick answer to a question.

What's the BlueXP disaster recovery URL?
For the URL, in a browser, enter: https://console.bluexp.netapp.com/ to access the BlueXP console.

Do you need a license to use BlueXP disaster recovery?
A BlueXP disaster recovery license is required for complete access. However, you can try it out with the free trial.

For details about setting up licensing for BlueXP disaster recovery, refer to Set up BlueXP disaster recovery licensing.

How do you access BlueXP disaster recovery?
BlueXP disaster recovery does not require any enablement. The disaster recovery option automatically appears on the BlueXP left navigation.

Use BlueXP disaster recovery

Use BlueXP disaster recovery overview

Using BlueXP disaster recovery, you can accomplish the following goals:

- View the health of your disaster recovery plans.
- Add vCenter sites.
- Create resource groups to organize VMs together
- Create a disaster recovery plan.
- Replicate VMware apps on your primary site to a disaster recovery remote site in the cloud using SnapMirror replication.
- Migrate VMware apps on your primary site to another site.
- Test the fail over without disrupting the original virtual machines.
- In case of disaster, fail over your primary site to VMware Cloud on AWS with FSx for NetApp ONTAP.
- After the disaster has been resolved, fail back from the disaster recovery site to the primary site.
- Monitor disaster recovery operations on the Job Monitoring page.

View the health of your BlueXP disaster recovery plans on the Dashboard

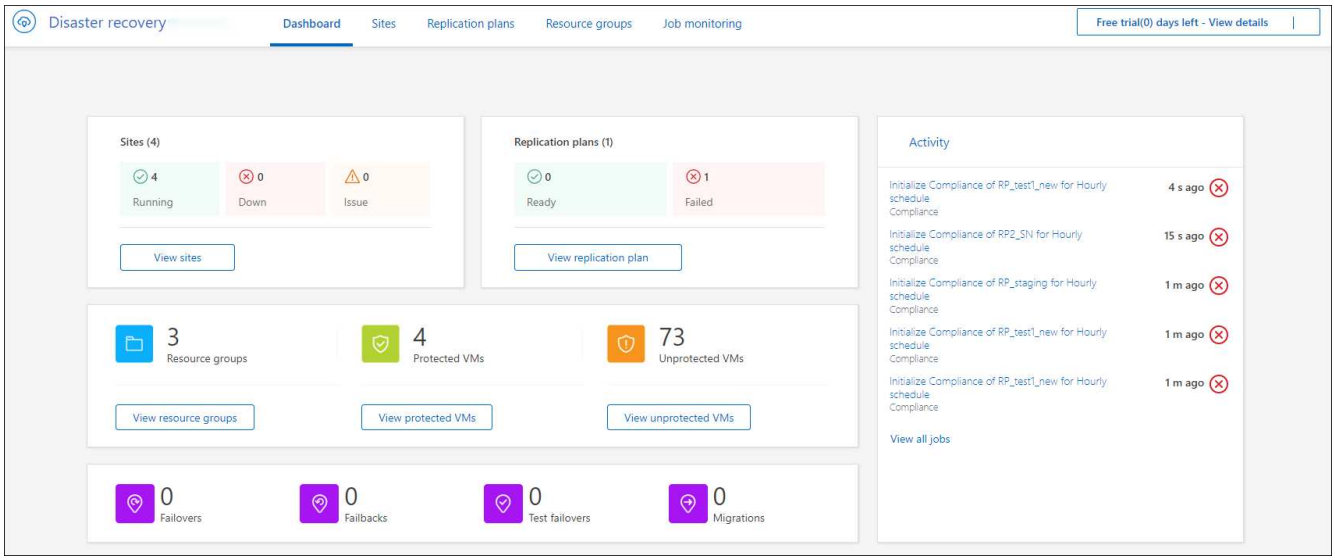
Using the BlueXP disaster recovery Dashboard, you can determine the health of your disaster recovery sites and replication plans. You can quickly ascertain which sites and plans are healthy, disconnected, or degraded.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery application admin, or Disaster recovery viewer role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the BlueXP disaster recovery top menu, select **Dashboard**.



3. Review the following information on the Dashboard:
   - **Sites**: View the health of your sites. A site can have one of the following statuses:
     - **Running**: The vCenter is connected, healthy, and running.
     - **Down**: The vCenter is not reachable or having connectivity issues.
     - **Issue**: The vCenter is not reachable or having connectivity issues.

     To see site details, select **View all** for a status or **View sites** to see them all.
   - **Replication plans**: View the health of your plans. A plan can have one of the following statuses:
     - **Ready**
     - **Failed**

     To review replication plan details, select **View all** for a status or **View replication plans** to see them all.
   - **Resource groups**: View the health of your resource groups. A resource group can have one of the following statuses:
   - **Protected VMs**: The VMs are part of a resource group.
   - **Unprotected VMs**: The VMs are not part of a resource group.

     To review details, select the **View** link below each.
   - The number of failovers, test failovers, and migrations. For example, if you created two plans and migrated to the destinations, the migration count appears as "2."
4. Review all operations in the Activity pane. To view all operations on the Job Monitor, select **View all jobs**.

Add vCenters to a site in BlueXP disaster recovery

Before you can create a disaster recovery plan, you need to add a primary vCenter server to a site and a target vCenter disaster recovery site in BlueXP.

Ensure that both the source and destination vCenters use the same BlueXP Connector.

After vCenters are added, BlueXP disaster recovery performs a deep discovery of the vCenter environments, including vCenter clusters, ESXi hosts, datastores, storage foot print, virtual machine details, SnapMirror replicas, and virtual machine networks.

Required BlueXP role
Organization admin, Folder or project admin, or Disaster recovery admin.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

If you added vCenters in previous releases and want to customize the discovery schedule, you must edit the vCenter server site and set the schedule.

BlueXP disaster recovery performs discovery once every 24 hours. After setting up a site, you can later edit the vCenter to customize the discovery schedule that meets your needs. For example, if you have a large number of VMs, you can set the discovery schedule to run every 23 hours and 59 minutes. If you have a small number of VMs, you can set the discovery schedule to run every 12 hours. The minimum interval is 30 minutes and the maximum is 24 hours.

You should first do a few manual discoveries to get the most up-to-date information about your environment. After that, you can set the schedule to run automatically.

Newly added or deleted VMs are recognized in the next scheduled discovery or during an immediate manual discovery.

VMs can be protected only if the replication plan is in one of the following states:

- Ready
- Failback committed
- Test failover committed

Steps

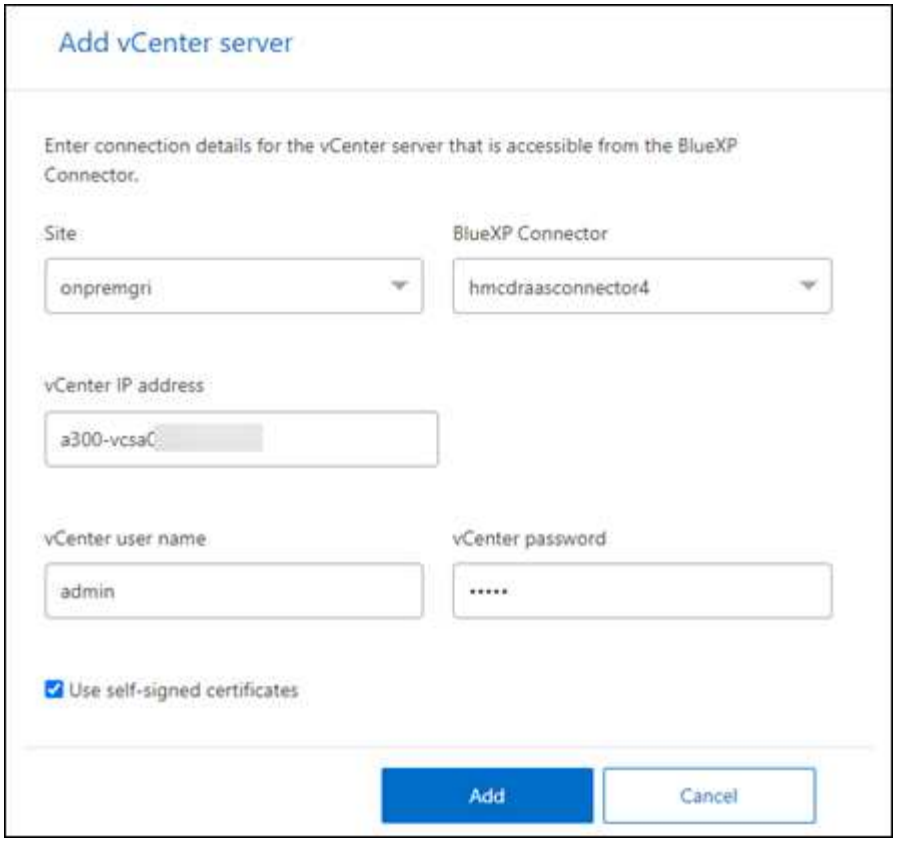
1. Log in to BlueXP and from the left navigation menu, select **Protection** > **Disaster recovery**.

   You'll land on BlueXP disaster recovery Dashboard page. When you first start with the service, you need to add vCenter information. Later, the Dashboard displays data about your sites and replication plans.

   Different fields appear depending on the type of site you are adding.

2. **Source**: Select **Discover vCenter servers** to enter information about the source vCenter site.

   If some vCenter sites already exist and you want to add more, from the top menu, select **Sites** and then select **Add**.



- Add a site, select the BlueXP Connector, and provide vCenter credentials.
- (Applies only to on-premises sites) To accept self-signed certificates for the source vCenter, check the box.

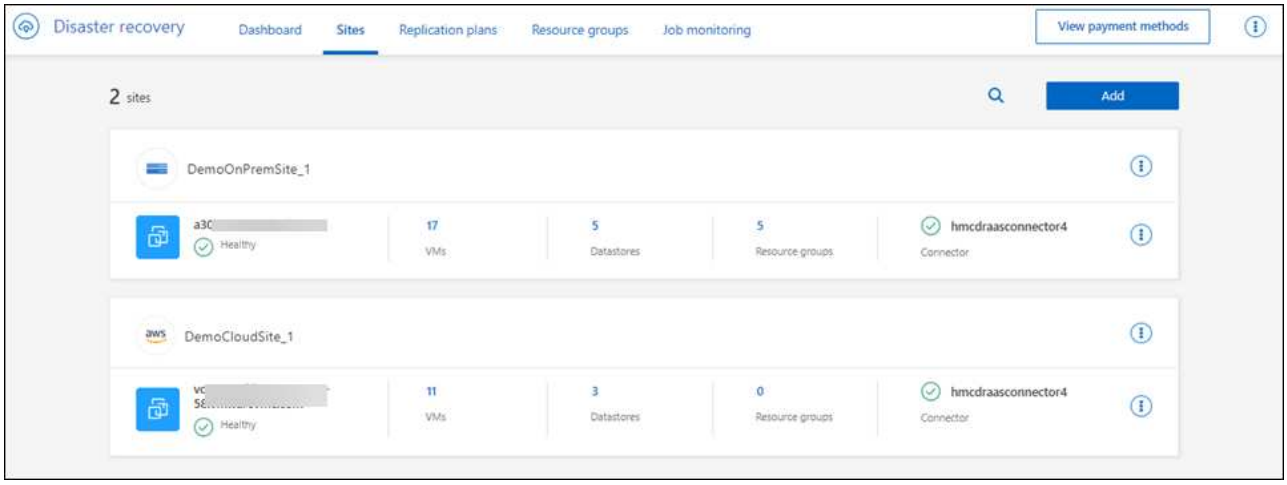
> Self-signed certificates are not as secure as other certificates. If your vCenter is **NOT** configured with certificate authority (CA) certificates, you should check this box; otherwise, the connection to the vCenter will not work.

3. Select **Add**.

Next, you will add a target vCenter.

4. **Target**:
   a. Choose the target site and the location. If the target is cloud, select **AWS**.
      - (Applies only to cloud sites) **API token**: Enter the API token to authorize service access for your organization. Create the API token by providing specific organization and service roles.
      - (Applies only to cloud sites) **Long organization ID**: Enter the unique ID for the organization. You can identify this ID by clicking on the username in the Account section of the BlueXP console.
   b. Select **Add**.

The source and target vCenters appear on the list of sites.



5. To see the progress of the operation, from the top menu, select **Job monitoring**.

Add subnet mapping for a vCenter site

Manage IP addresses on failover in a new way using subnet mapping, which enables you to add subnets for each vCenter. When you do so, you define the IPv4 CIDR, the default gateway, and the DNS for each virtual network.

Upon failover, BlueXP disaster recovery determines the appropriate IP address of each vNIC by looking at the CIDR provided for the mapped virtual network and uses it to derive the new IP address.

For example:

- NetworkA = 10.1.1.0/24
- NetworkB = 192.168.1.0/24

VM1 has a vNIC (10.1.1.50) that is connected to NetworkA.
NetworkA is mapped to NetworkB in the replication plan settings.

Upon failover, BlueXP disaster recovery replaces the Network portion of the original IP address (10.1.1) and keeps the host address (.50) of the original IP address (10.1.1.50). For VM1, BlueXP disaster recovery looks at the CIDR settings for NetworkB and uses that the NetworkB network portion 192.168.1 while keeping the host portion (.50) to create the new IP address for VM1. The new IP becomes 192.168.1.50.

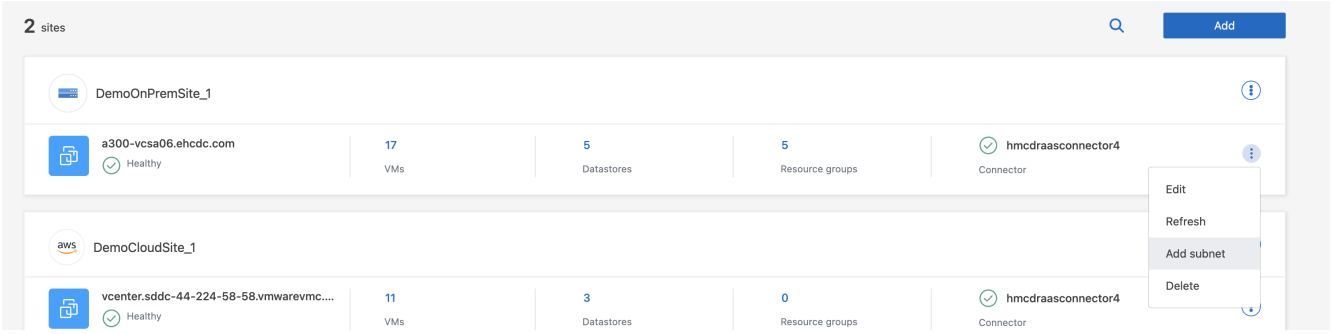
In summary, the host address stays the same, while the network address is replaced with whatever is configured in the site subnet mapping. This enables you to manage IP address reassignment upon failover more easily, especially if you have hundreds of networks and thousands of VMs to manage.

Using subnet mapping is an optional two-step process:

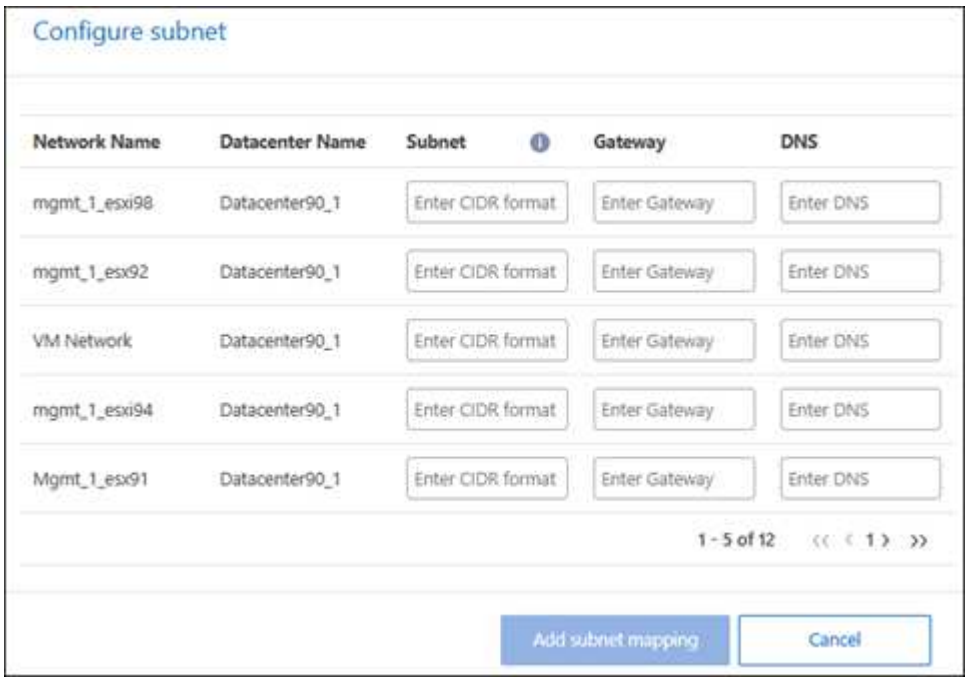
- First, add the subnet mapping for each vCenter site.
- Second, in the replication plan, indicate that you want to use subnet mapping.

Steps

1. From the top BlueXP disaster recovery menu, select **Sites**.
2. From the Actions icon on the right, select **Add subnet**.



The Configure subnet page appears:



3. In the Configure subnet page, enter the following information:
   a. Subnet: Enter the IPv4 CIDR for the subnet up to /32.

> CIDR notation is a method of specifying IP addresses and their network masks. The /24 denotes the netmask. The number consists of an IP address with the number after the "/" indicating how many bits of the IP address denote the network. For example, 192.168.0.50/24, the IP address is 192.168.0.50 and the total number of bits in the network address is 24. 192.168.0.50 255.255.255.0 becomes 192.168.0.0/24.

   b. Gateway: Enter the default gateway for the subnet.
   c. DNS: Enter the DNS for the subnet.
4. Select **Add subnet mapping**.

Select subnet mapping for a replication plan

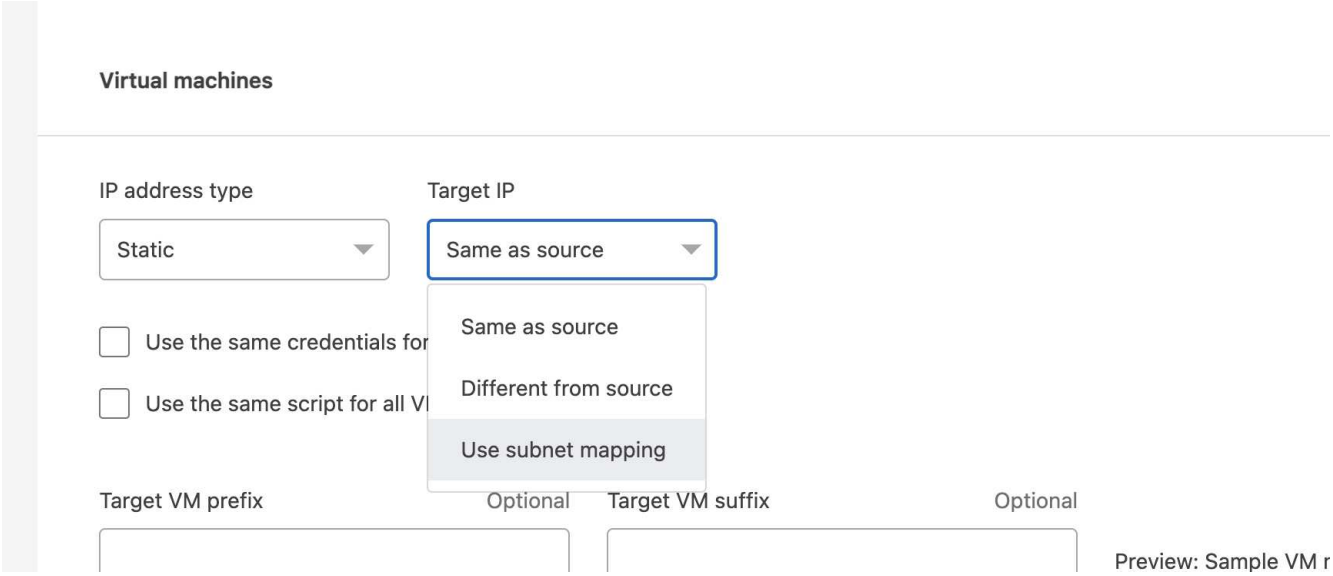
When you create a replication plan, you can select the subnet mapping for the replication plan.

Using subnet mapping is an optional two-step process:

- First, add the subnet mapping for each vCenter site.
- Second, in the replication plan, indicate that you want to use subnet mapping.

Steps

1. From the BlueXP disaster recovery top menu, select **Replication plans**.
2. Select **Add** to add a replication plan.
3. Complete the fields in the usual way by adding the vCenter servers, selecting the resource groups or applications, and completing the mappings.
4. In the Replication plan > Resource mapping page, select the **Virtual machines** section.



5. In the **Target IP** field, select **Use subnet mapping** from the drop-down list.

> If there are two VMs (for example, one is Linux and the other is Windows), credentials are needed only for Windows.

6. Continue with the creating the replication plan.

Edit the vCenter server site and customize the discovery schedule

You can edit the vCenter server site to customize the discovery schedule. For example, if you have a large number of VMs, you can set the discovery schedule to run every 23 hours and 59 minutes. If you have a small number of VMs, you can set the discovery schedule to run every 12 hours.

If you added vCenters in previous releases and want to customize the discovery schedule, you must edit the vCenter server site and set the schedule.

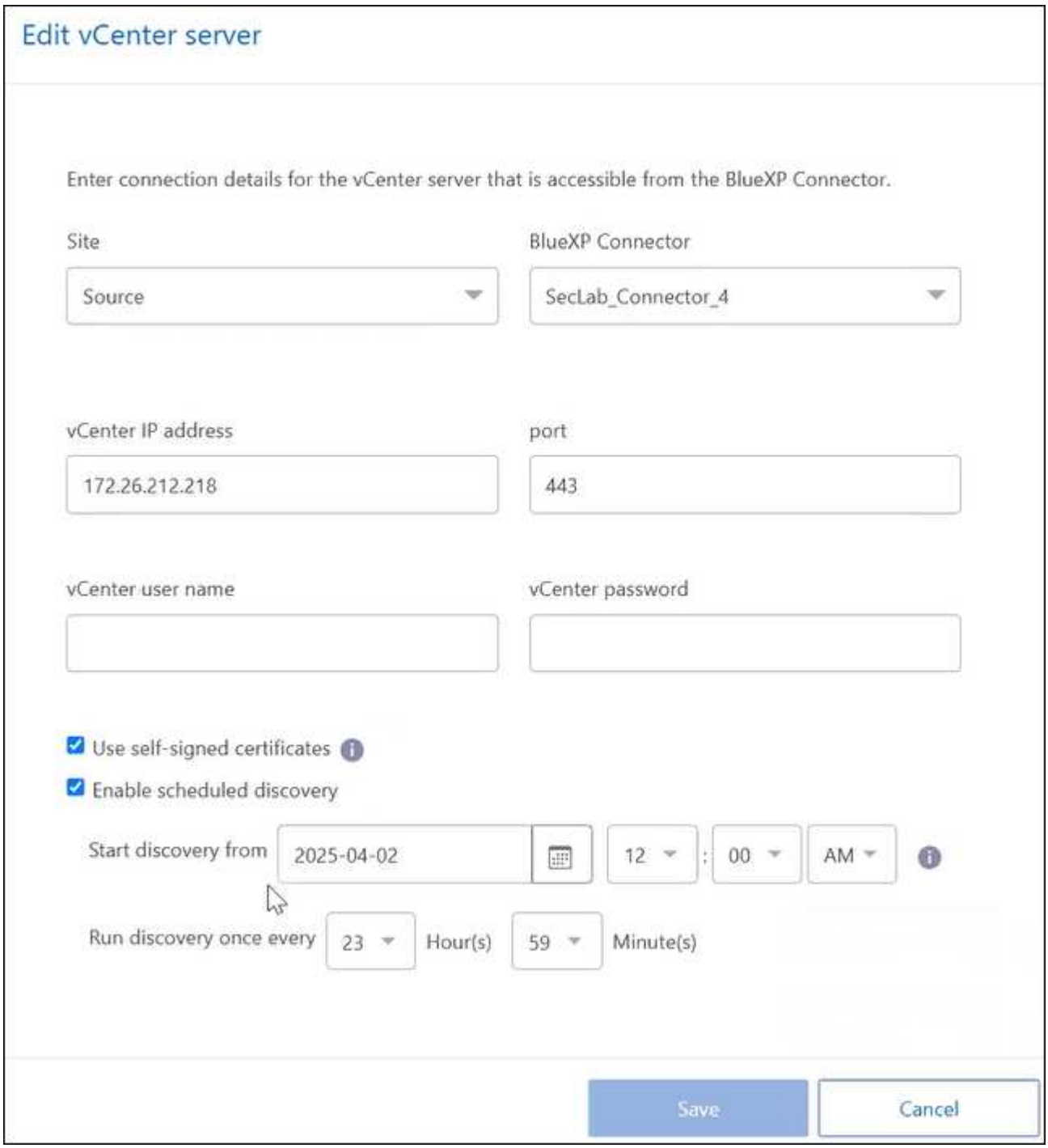
If you don’t want to schedule discovery, you can disable the scheduled discovery option and refresh the discovery manually at any time.

Steps

1. From the BlueXP disaster recovery menu, select **Sites**.
2. Select the site you want to edit.
3.

Select the Actions icon on the right and select **Edit**.

4. In the Edit vCenter server page, edit the fields as needed.
5. To customize the discovery schedule, check the **Enable scheduled discovery** box and select the date and time interval you want.



6. Select **Save**.

Refresh discovery manually

You can refresh the discovery manually at any time. This is useful if you have added or removed VMs and want

to update the information in BlueXP disaster recovery.

Steps

1. From the BlueXP disaster recovery menu, select **Sites**.
2. Select the site you want to refresh.
3. Select the Actions  icon on the right and select **Refresh**.

Create a resource group to organize VMs together in BlueXP disaster recovery

After you've added vCenter sites, you might want to create resource groups that group VMs together by VMs or by datastores. Resource groups enable you to organize a set of dependent VMs into logical groups that meet your requirements. For example, you might group VMs associated with one application or you might group applications that have similar tiers. As another example, groups could contain delayed boot orders that can be run upon recovery.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, or Disaster recovery application admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

You can group VMs themselves or VMs in datastores.

You can create resource groups using the following methods:

- From the Resource groups tab
- While you're creating a disaster recovery or *replication plan*. If you have a lot of VMs hosted by a source vCenter cluster, it might be easier for you to create the resource groups while you're creating the replication plan. For instructions on creating resource groups while you're creating a replication plan, see Create a replication plan.

Each resource group can include one or more VMs or datastores. The VMs will power on based on the sequence in which you include them in the replication plan. You can change the order by dragging the VMs or datastores up or down the resource group list.

About resource groups

Resource groups enable you to combine VMs or datastores that include VMs that are related operationally and need to be protected as a single unit.

For example, a point-of-sale application might consist of several VMs hosting databases, several VMs hosting business logic rules management, and several VMs acting as a webserver-based storefront. It might be beneficial to manage the entire application's availability with a single protection process by placing these VMs in a single resource group.

With resource groups set up, you can apply the replication plan rules for proper VM startup order, network connection, and more to ensure proper recovery of all VMs required for the application.

How does it work?

BlueXP disaster recovery protects VMs by replicating the underlying ONTAP volumes and LUNs hosting the VMs in the resource group. To do this, the system queries vCenter for the name of each data store hosting VMs in a resource group. BlueXP disaster recovery then identifies the source ONTAP volume or LUN hosting that data store. All protection is performed at the ONTAP volume level using SnapMirror replication.

If VMs in the resource group are hosted on different data stores, BlueXP disaster recovery uses one of the following methods to create a data-consistent snapshot of the ONTAP volumes or LUNs.

Relative location of FlexVol volumes	Snapshot replica process
Multiple data stores - FlexVol volumes in the **same SVM**	• ONTAP consistency group created • Snapshots of the consistency group taken • Volume-scoped SnapMirror replication performed
Multiple data stores - FlexVol volumes in **multiple SVMs**	• ONTAP API: `cg_start`. Quieces all volumes so snapshots can be taken and initiates volume-scoped snapshots of all resource group volumes. • ONTAP API: `cg_end`. Resumes I/O on all volumes and enables volume-scoped SnapMirror replication after snapshots are taken.

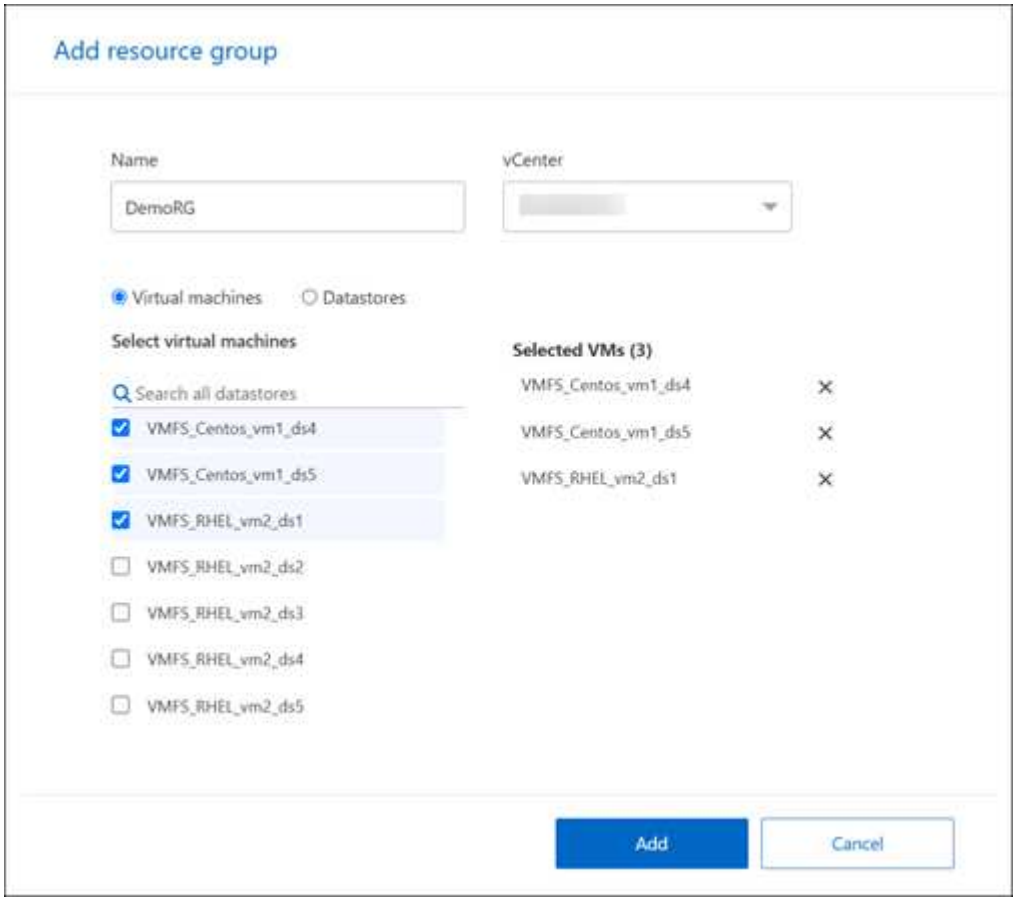
When you create resource groups, consider the following issues:

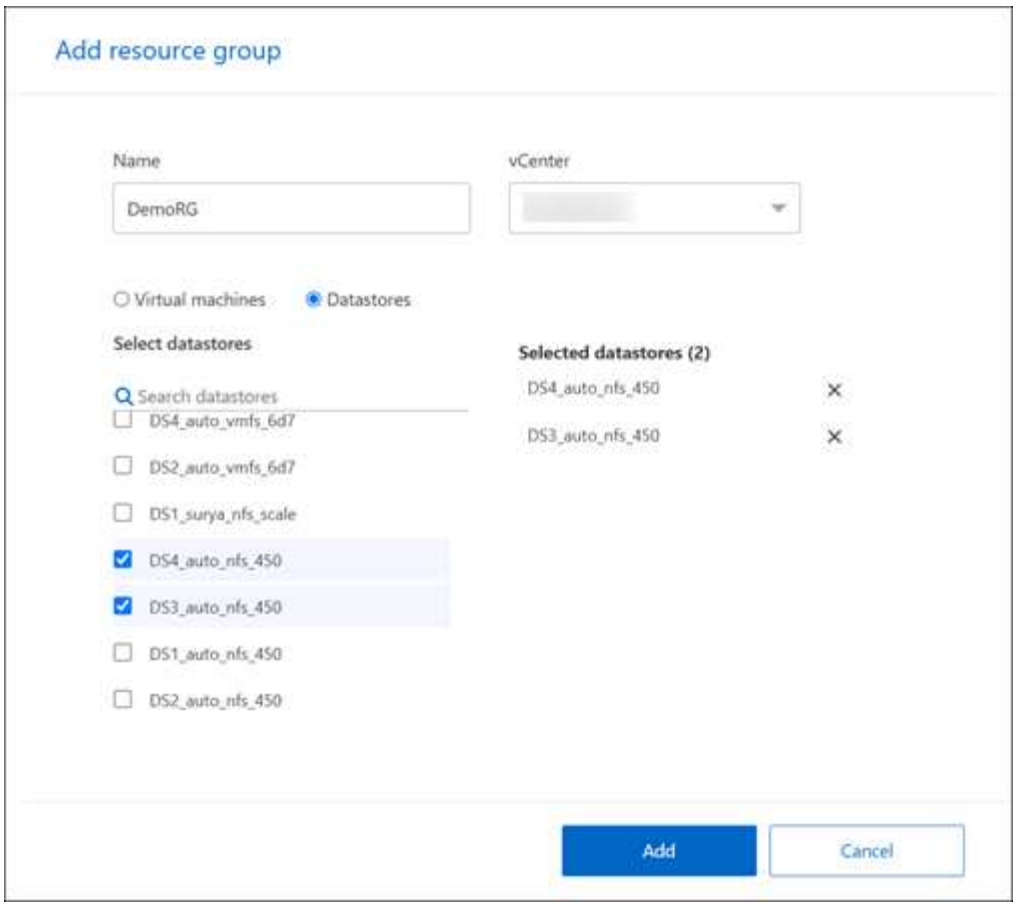
- Before you add datastores to resource groups, start a manual discovery or a scheduled discovery of the VMs first. This ensures that the VMs are discovered and listed in the resource group. If you do not trigger a manual discovery, the VMs might not be listed in the resource group.
- Ensure that there is at least one VM in the datastore. If there are no VMs in the datastore, the datastore will not be discovered.
- A single datastore should not host VMs protected by more than one replication plan.
- Do not host protected and unprotected VMs on the same datastore. If protected and unprotected VMs are hosted on the same datastore, the following issues could arise:
  - Because BlueXP disaster recovery uses SnapMirror and the system replicates entire ONTAP volumes, the used capacity of that volume is used for licensing considerations. In this case, the volume space consumed by both protected and unprotected VMs would be included in this calculation.
  - If the resource group and its associated datastores need to be failed over to the disaster recovery site, any unprotected VMs (VMs not part of the resource group, but hosted on the ONTAP volume) will no longer exist on the source site from the failover process, resulting in failure of unprotected VMs at the source site. Also, BlueXP disaster recovery will not start those unprotected VMs at the failover vCenter site.
- To have a VM protected, it must be included in a resource group.

BEST PRACTICE: Organize your VMs before deploying BlueXP disaster recovery to minimize “datastore sprawl.” Place VMs that need protection on a subset of datastores and place VMs that are not going to be protected on a different subset of datastores. Ensure that the VMs on any given datastore are not protected by different replication plans.

Steps

1. From the BlueXP disaster recovery menu, select **Resource groups**.
2. Select **Add**.
3. Enter a name for the resource group.
4. Select the source vCenter cluster where the VMs are located.
5. Select either **Virtual machines** or **Datastores** depending on how you want to search.
6. Select the **Add resource groups** tab. The system lists all datastores or VMs in the selected vCenter cluster. If you selected **Datastores**, the system lists all datastores in the selected vCenter cluster. If you selected **Virtual machines**, the system lists all VMs in the selected vCenter cluster.
7. On the left side of the Add resource groups page, select the VMs that you want to protect.





8. Optionally, change the order of the VMs on the right by dragging each VM up or down the list. The VMs will power on based on the sequence in which you include them.
9. Select **Add**.

Create a replication plan in BlueXP disaster recovery

After you've added vCenter sites, you're ready to create a disaster recovery or *replication plan*. Select the source and destination vCenters, pick the resource groups, and group how applications should be restored and powered on. For example, you might group virtual machines (VMs) associated with one application or you might group applications that have similar tiers.

Such plans are sometimes called *blueprints*.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, or Disaster recovery application admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

You can create a replication plan and also edit schedules for compliance and testing.

You can protect multiple VMs on multiple datastores. BlueXP disaster recovery creates ONTAP Consistency Groups for all ONTAP volumes hosting protected VM datastores.

VMs can be protected only if the replication plan is in one of the following states:

- Ready
- Failback committed
- Test failover committed

Create the plan

A wizard takes you through these steps:

- Select vCenter servers.
- Select the VMs or datastores that you want to replicate and assign resource groups.
- Map how resources from the source environment map to the destination.
- Identify recurrence, run a guest-hosted script, set the boot order, and select the recovery point objective.
- Review the plan.

When you create the plan, you should follow these guidelines:

- Use the same credentials for all VMs in the plan.
- Use the same script for all VMs in the plan.
- Use the same subnet, DNS, and gateway for all VMs in the plan.

Before you begin

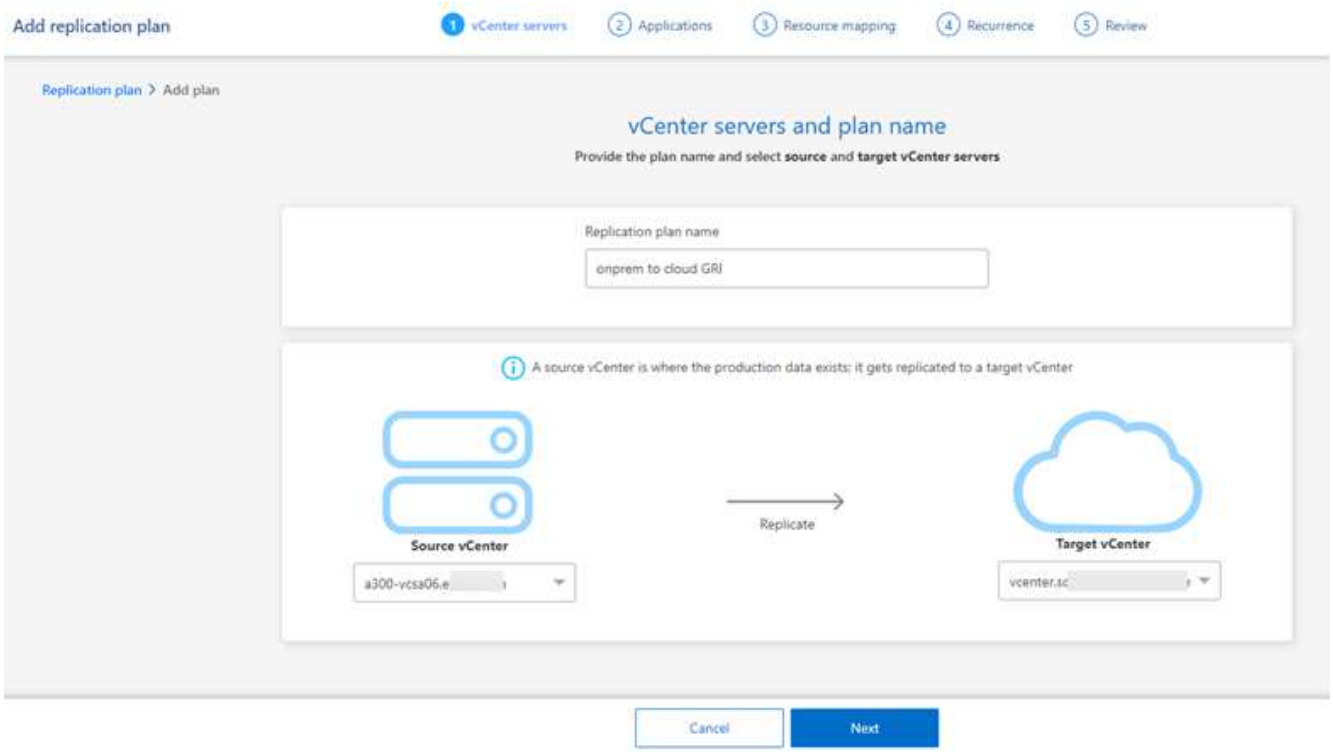
If you want to create a SnapMirror relationship in this service, the cluster and its SVM peering should have already been set up outside of BlueXP disaster recovery.

Select vCenter servers

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

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the BlueXP disaster recovery top menu, select **Replication plans** and select **Add**. Or, if you are just beginning to use the service, from the Dashboard, select **Add replication plan**.



3. Create a name for the replication plan.
4. Select the source and target vCenters from the Source and Target vCenter lists.
5. Select **Next**.

Select applications to replicate and assign resource groups

The next step is to group the required VMs or datastores into functional resource groups. Resource groups enable you to protect a set of VMs or datastores with a common snapshot.

When you select applications in the replication plan, you can see the operating system for each VM or datastore in the plan. This is helpful in deciding how to group VMs or datastores together in a resource group.

Each resource group can include one or more VMs or datastores.

When you create resource groups, consider the following issues:

- Before you add datastores to resource groups, start a manual discovery or a scheduled discovery of the VMs first. This ensures that the VMs are discovered and listed in the resource group. If you do not trigger a manual discovery, the VMs might not be listed in the resource group.
- Ensure that there is at least one VM in the datastore. If there are no VMs in the datastore, the datastore will not be discovered.
- A single datastore should not host VMs protected by more than one replication plan.
- Do not host protected and unprotected VMs on the same datastore. If protected and unprotected VMs are hosted on the same datastore, the following issues could arise:
  - Because BlueXP disaster recovery uses SnapMirror and the system replicates entire ONTAP volumes, the used capacity of that volume is used for licensing considerations. In this case, the volume space consumed by both protected and unprotected VMs would be included in this calculation.

- If the resource group and its associated datastores need to be failed over to the disaster recovery site, any unprotected VMs (VMs not part of the resource group, but hosted on the ONTAP volume) will no longer exist on the source site from the failover process, resulting in failure of unprotected VMs at the source site. Also, BlueXP disaster recovery will not start those unprotected VMs at the failover vCenter site.

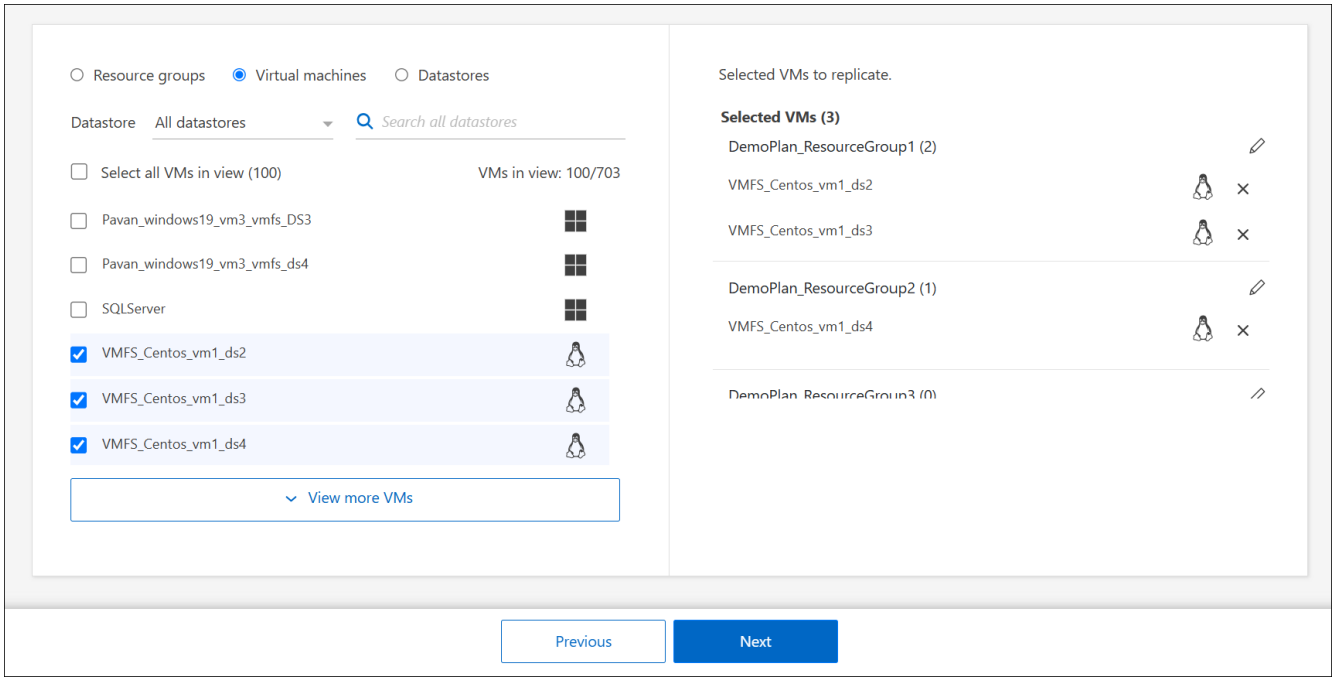
- To have a VM protected, it must be included in a resource group.

BEST PRACTICE: Organize your VMs before deploying BlueXP disaster recovery to minimize “datastore sprawl.” Place VMs that need protection on a subset of datastores and place VMs that are not going to be protected on a different subset of datastores. Use datastore-based protection to ensure that the VMs on any given datastore are protected.

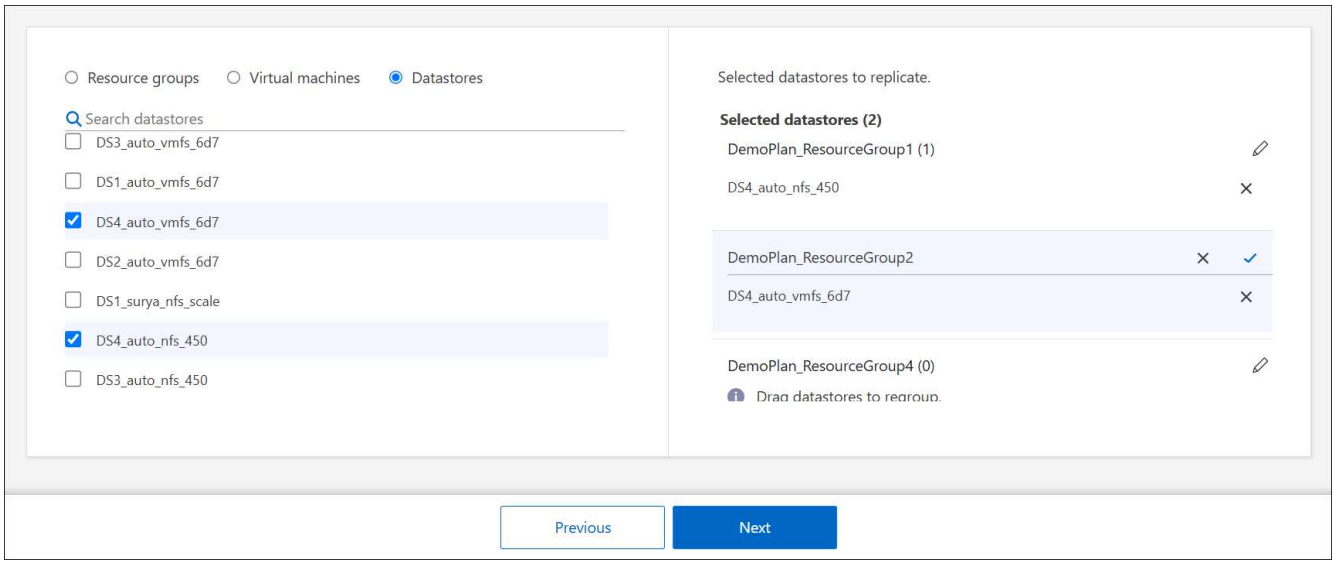
Steps

1. Select **Virtual machines** or **Datastores**.
2. Optionally search for specific VM or datastore by name.
3. On the left side of the Applications page, select the VMs or datastores that you want to protect and assign to the selected group.

   The selected resource is automatically added to group 1 and a new group 2 is started. Each time you add a resource to the last group, another group is added.



   Or, for datastores:



4. Optionally, do any of the following:
   - To change the group's name, click the group **Edit** icon.
   - To remove a resource from a group, select **X** next to the resource.
   - To move a resource to a different group, drag and drop it into the new group.

   To move a datastore to a different resource group, unselect the unwanted datastore and submit the replication plan. Then, create or edit the other replication plan and reselect the dataastore.

5. Select **Next**.

Map source resources to the target

In the Resource mapping step, specify how the resources from the source environment should map to the target. When you create a replication plan, you can set a boot delay and order for each VM in the plan. This enables you to set a sequence for the VMs to start.

Before you begin

If you want to create a SnapMirror relationship in this service, the cluster and its SVM peering should have already been set up outside of BlueXP disaster recovery.

Steps

1. In the Resource mapping page, to use the same mappings for both failover and test operations, check the box.

2. In the Failover mappings tab, select the down arrow to the right of each resource and map the resources in each.

Map resources > Compute resources section

Select the down arrow next to **Compute resources**.

- **Source and target datacenters**
- **Target cluster**
- **Target host** (optional): After you select the cluster, you can then set this information.

If a vCenter has a Distributed Resource Scheduler (DRS) configured to manage multiple hosts in a cluster, you don't need to select a host. If you select a host, BlueXP disaster recovery will place all the VMs on the selected host.
* **Target VM folder** (optional): Create a new root folder to store the selected VMs.

Map resources > Virtual networks section

In the Failover mappings tab, select the down arrow next to **Virtual networks**. Select the source virtual LAN and target virtual LAN.

Select the network mapping to the appropriate virtual LAN. The virtual LANs should already be provisioned, so select the appropriate virtual LAN to map the VM.

Map resources > Virtual machines section

In the Failover mappings tab, select the down arrow next to **Virtual machines**.

The default for the VMs is mapped. Default mapping uses the same settings that the VMs use in the production environment (same IP address, subnet mask, and gateway).

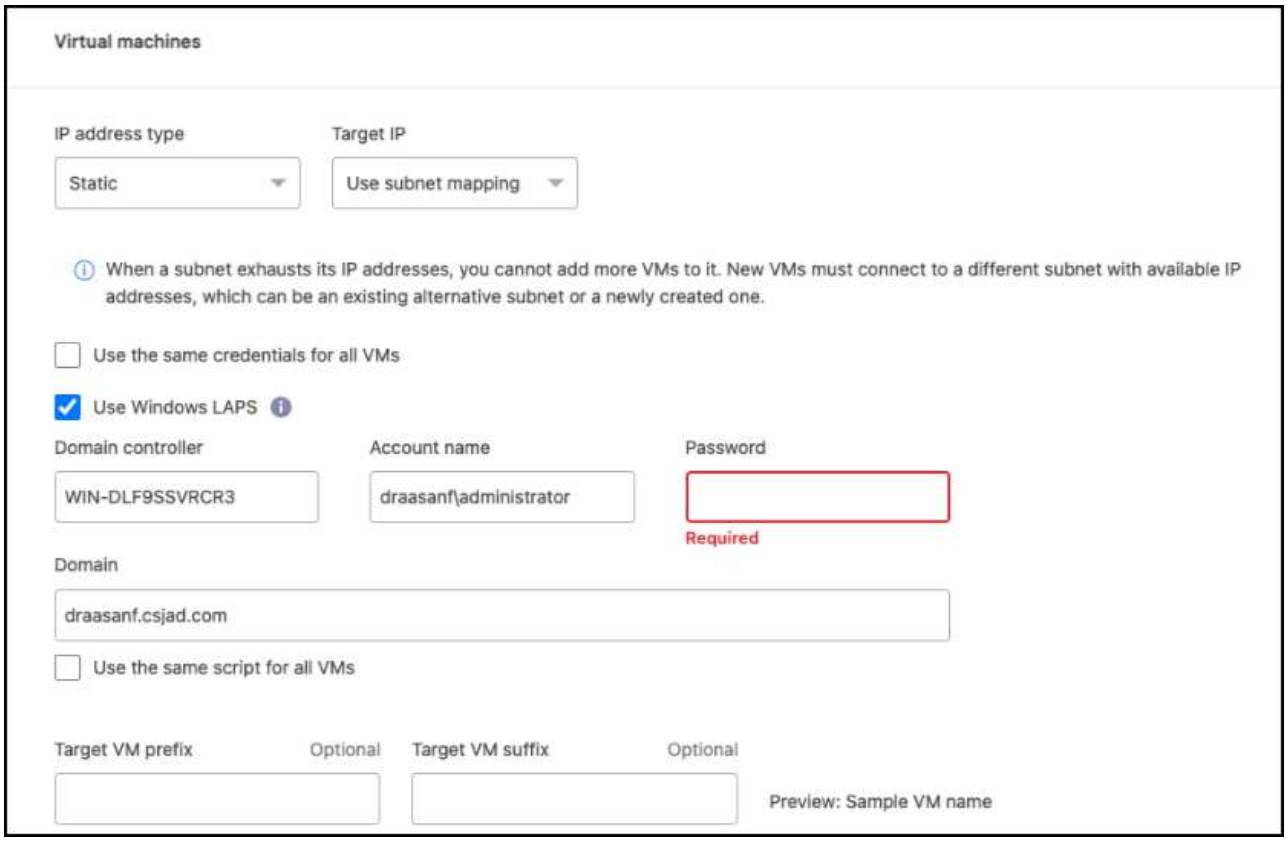
If you make any changes from the default settings, you must change the Target IP field to "Different from source."

If you change settings to "Different from source," you need to provide VM guest OS credentials.

This section might display different fields depending on your selection.

- **IP address type**: Reconfigure the VMs configuration to match the target virtual network requirements. BlueXP disaster recovery offers two options: DHCP or static IP. For static IPs, configure the subnet mask, gateway, and DNS servers. Additionally, enter credentials for VMs.
  - **DHCP**: Select this setting if you want your VMs to obtain network configuration information from a DHCP server. If you choose this option, you provide just the credentials for the VM.
  - **Static IP**: Select this setting if you want to specify IP configuration information manually. You can select one of the following: same as source, different from source, or subnet mapping. If you choose the same as the source, you do not need to enter credentials. On the other hand, if you choose to use different information from the source, you can provide the credentials, IP address of the VM, subnet mask, DNS, and gateway information. VM guest OS credentials should be supplied to either the global level or at each VM level.

    This can be very helpful when recovering large environments to smaller target clusters or for conducting disaster recovery tests without having to provision a one-to-one physical VMware infrastructure.



- **Target IP** field, select one of the following:
  - **Same as source**
  - **Different from source**
  - **Subnet mapping**: Select this option if you want to map the source subnet to a different target subnet. You can select the source subnet and then select the target subnet. This is useful when you want to change the IP address of the VM in the target environment.

> Using subnet mapping is an optional two-step process: First, add the subnet mapping for each vCenter site in the Sites tab. Second, in the replication plan, indicate that you want to use subnet mapping.

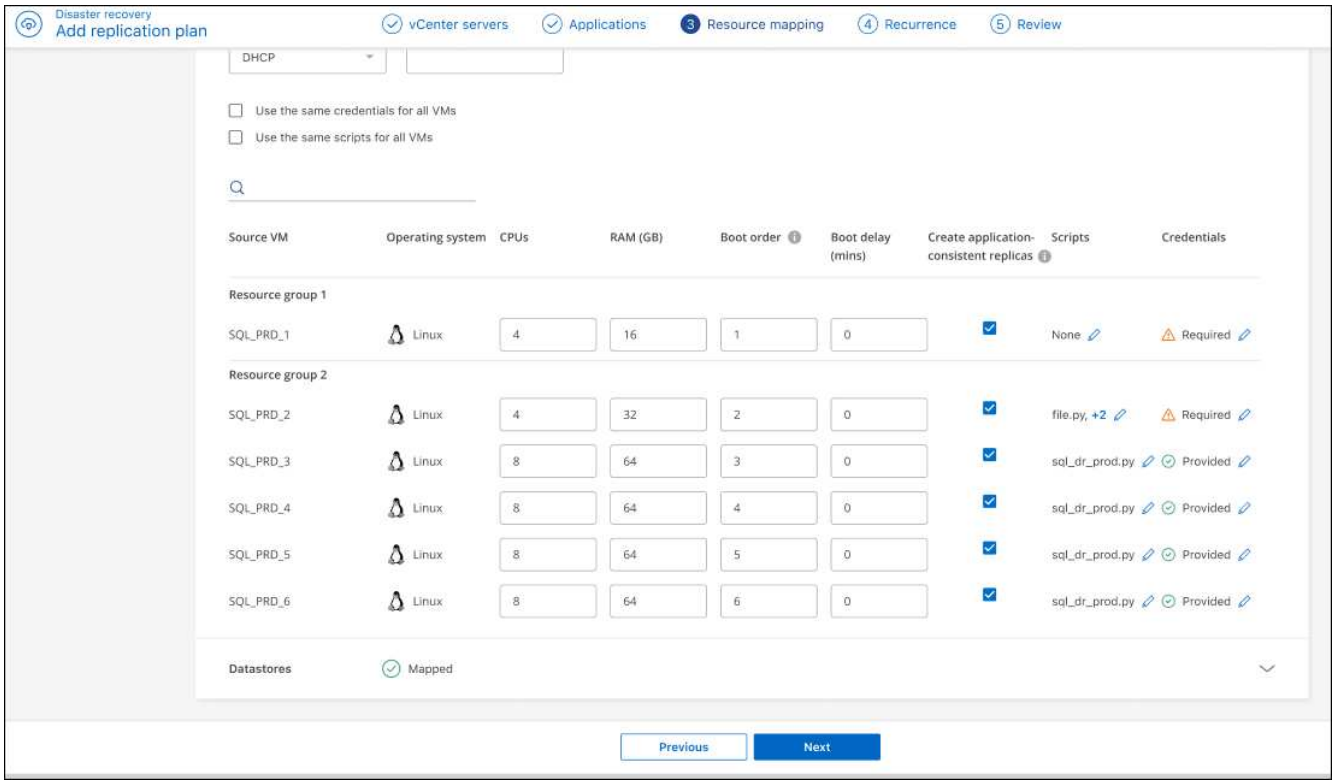
> If there are two VMs (for example, one is Linux and the other is Windows), credentials are needed only for Windows.

- **Use Windows LAPS**: If you are using Windows Local Administrator Password Solution (Windows LAPS), check this box. This option is available only if you have selected the **Static IP** option. When you check this box, you do not need to provide a password for each of your virtual machines. Instead, you provide the domain controller details.

  If you do not use Windows LAPS, then the VM is a Windows VM and the credentials option on the VM row is enabled. You can provide the credentials for the VM.

- **Scripts**: You can include custom scripts in .sh, .bat, or .ps1 format as post failover processes. With custom scripts, you can have BlueXP disaster recovery run your script after a failover process. For example, you can use a custom script to resume all database transactions after the failover is complete.
- **Target VM prefix and suffix**: Under the virtual machines details, you can optionally add a prefix and suffix to the VM name.

- **Source VM CPU and RAM**: Under the virtual machines details, you can optionally resize the VM CPU and RAM parameters.



- **Boot order**: You can modify the boot order after a failover for all the selected virtual machines across the resource groups. By default, all VMs boot together in parallel; however, you can make changes at this stage. This is helpful to ensure that all your priority one VMs are running before subsequent priority VMs are started.

  Any VMs with the same boot order number will be booted in parallel.

  - Sequential boot: Assign each VM a unique number to boot the in the assigned order, for example, 1,2,3,4,5.
  - Simultaneous boot: Assign the same number to any VMs to boot them at the same time, for example, 1,1,1,1,2,2,3,4,4.
- **Boot delay**: Adjust the delay in minutes of the boot up action.

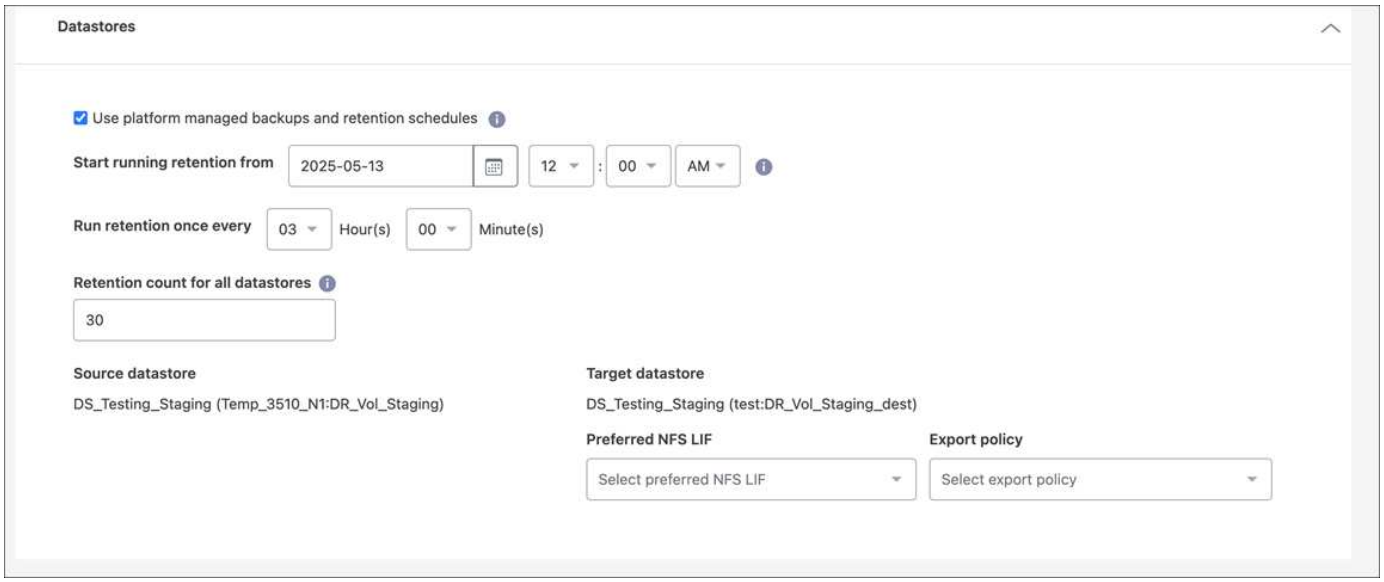
  To reset the boot order to the default, select **Reset VM settings to default** and then choose which settings you want to change back to the default.

- **Create application-consistent replicas**: Indicate whether to create application-consistent snapshot copies. The service will quiesce the application and then take a snapshot to obtain a consistent state of the application. This feature is supported with Oracle running on Windows and Linux and SQL Server running on Windows.

Map resources > Datastores section

Select the down arrow next to **Datastores**. Based on the selection of VMs, datastore mappings are automatically selected.

This section might be enabled or disabled depending on your selection.



- **Use platform managed backups and retention schedules**: If you are using an external snapshot management solution, check this box. BlueXP disaster recovery supports the use of external snapshot management solutions such as the native ONTAP SnapMirror policy scheduler or third-party integrations. If every datastore (volume) in the replication plan already has a SnapMirror relationship that is being managed elsewhere, you can use those snapshots as recovery points in BlueXP disaster recovery.

  When selected, BlueXP disaster recovery does not configure a backup schedule. However, you still need to configure a retention schedule because snapshots might still be taken for testing, failover, and failback operations.

  After this is configured, the service doesn't take any regularly scheduled snapshots, but instead relies on the external entity to take and update those snapshots.

- **Start time**: Enter the date and time when you want backups and retention to start running.
- **Run interval**: Enter the time interval in hours and minutes. For example, if you enter 1 hour, the service will take a snapshot every hour.
- **Retention count**: Enter the number of snapshots you want to retain.
- **Source and Target datastores**: If multiple (fan-out) SnapMirror relationships exist, you can select the destination to use. If a volume has a SnapMirror relationship already established, the corresponding source and target datastores appear. If a volume that does not have a SnapMirror relationship, you can create one now by selecting a target cluster, selecting a target SVM, and providing a volume name. The service will create the volume and SnapMirror relationship.

  If you want to create a SnapMirror relationship in this service, the cluster and its SVM peering should have already been set up outside of BlueXP disaster recovery.

  - If the VMs are from same volume and same SVM, then the service performs a standard ONTAP snapshot and updates the secondary destinations.
  - If the VMs are from different volume and same SVM, the service creates a consistency group snapshot by including all the volumes and updates the secondary destinations.
  - If the VMs are from different volume and different SVM, the service performs a consistency group start phase and commit phase snapshot by including all the volumes in the same or different cluster and updates the secondary destinations.

- During the failover, you can select any snapshot. If you select the latest snapshot, the service creates on on-demand backup, updates the destination, and uses that snapshot for the failover.

Add test failover mappings

Steps

1. To set different mappings for the test environment, uncheck the box and select the **Test mappings** tab.
2. Go through each tab as before, but this time for the test environment.

   On the Test mappings tab, the Virtual machines and Datastores mappings are disabled.

   You can later test the entire plan. Right now, you are setting up the mappings for the test environment.

Review the replication plan

Finally, take a few moments to review the replication plan.

You can later disable or delete the replication plan.

Steps

1. Review information in each tab: Plan Details, Failover Mapping, and VMs.
2. Select **Add plan**.

   The plan is added to the list of plans.

Edit schedules to test compliance and ensure failover tests work

You might want to set up schedules to test compliance and failover tests so that you ensure that they will work correctly should you need them.

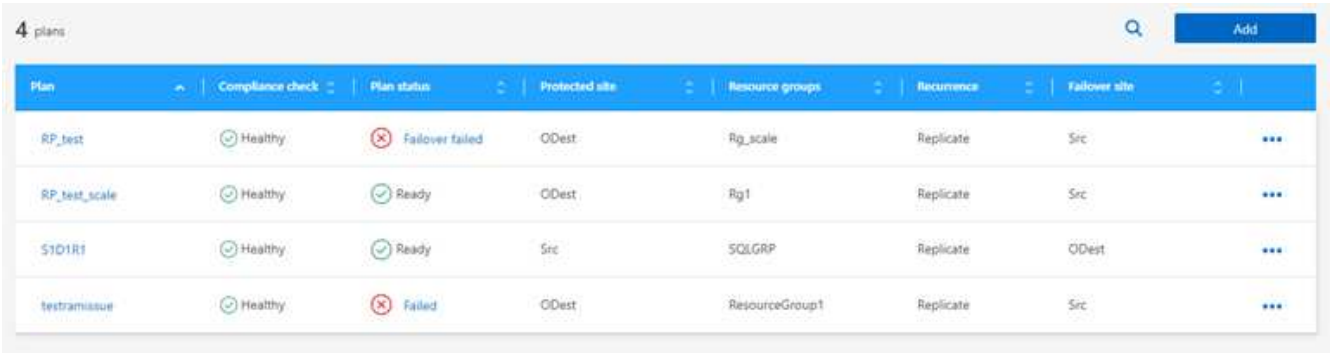
- **Compliance time impact**: When a replication plan is created, the service creates a compliance schedule by default. The default compliance time is 30 minutes. To change this time, you can use edit the schedule in the replication plan.
- **Test failover impact**: You can test a failover process on demand or by a schedule. This lets you test the failover of virtual machines to a destination that is specified in a replication plan.

  A test failover creates a FlexClone volume, mounts the datastore, and moves the workload on that datastore. A test failover operation does *not* impact production workloads, the SnapMirror relationship used on the test site, and protected workloads that must continue to operate normally.

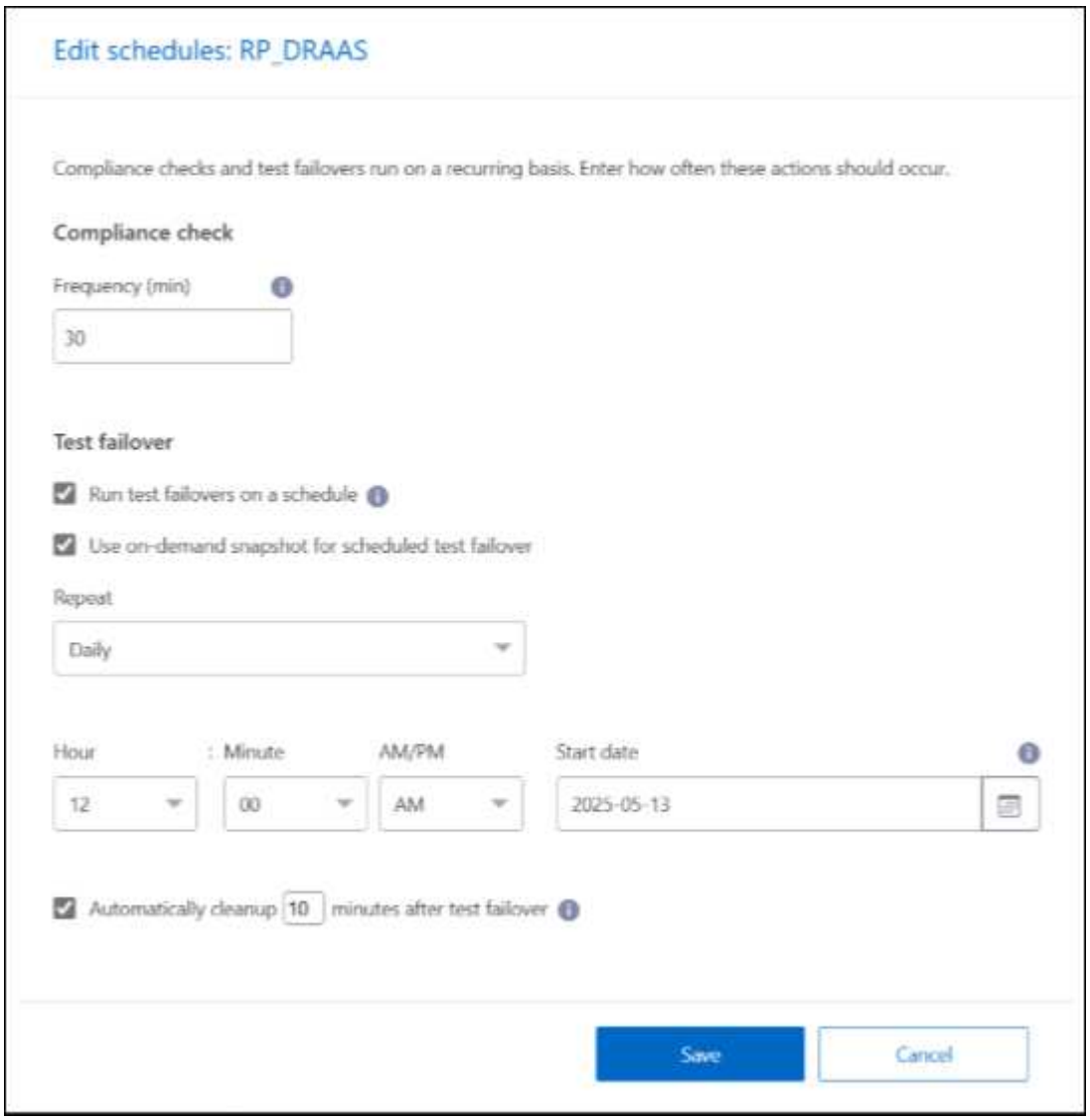
Based on the schedule, the failover test runs and ensures that workloads are moving to the destination specified by the replication plan.

Steps

1. From the BlueXP disaster recovery top menu, select **Replication plans**.



2. Select the **Actions** ••• icon and select **Edit schedules**.
3. Enter how frequently in minutes that you want BlueXP disaster recovery to check test compliance.
4. To check that your failover tests are healthy, check **Run failovers on a monthly schedule**.
   a. Select the day of the month and time you want these tests to run.
   b. Enter the date in yyyy-mm-dd format when you want the test to start.



5. **Use ondemand snapshot for scheduled test failover**: To take a new snapshot before initiating the automated test failover, check this box.

6. To clean up the test environment after the failover test finishes, check **Automatically clean up after test failover** and enter the number of minutes you want to wait before the cleanup starts.

   This process unregisters the temporary VMs from the test location, deletes the FlexClone volume that was created, and unmounts the temporary datastores.

7. Select **Save**.

Replicate applications to another site with BlueXP disaster recovery

Using BlueXP disaster recovery, you can replicate VMware apps on your source site to a disaster recovery remote site in the cloud using SnapMirror replication.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, or Disaster recovery failover admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

After you create the disaster recovery plan, identify the recurrence in the wizard, and initiate a replication to a disaster recovery site, every 30 minutes BlueXP disaster recovery verifies that the replication is actually occurring according to the plan. You can monitor the progress in the Job Monitor page.

Before you begin

Before you initiate the replication, you should have created a replication plan and selected to replicate the apps. Then, the **Replicate** option appears in the Actions menu.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the top menu, select **Replication plans**.
3. Select the replication plan.
4. On the right, select the **Actions** option ••• and select **Replicate**.

Migrate applications to another site with BlueXP disaster recovery

Using BlueXP disaster recovery, you can migrate VMware apps on your source site to another site.

After you create the replication plan, identify the recurrence in the wizard, and initiate the migration, every 30 minutes BlueXP disaster recovery verifies that the migration is actually occurring according to the plan. You can monitor the progress in the Job Monitor page.

Before you begin

Before you initiate the migration, you should have created a replication plan and selected to migrate the apps.

Then, the **Migrate** option appears in the Actions menu.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the top menu, select **Replication plans**.
3. Select the replication plan.
4. On the right, select the **Actions** option ••• and select **Migrate**.

Fail over applications to a remote site with BlueXP disaster recovery

In case of a disaster, fail over your primary on-premises VMware site to another on-premises VMware site or VMware Cloud on AWS. You can test the failover process to ensure success when you need it.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, or Disaster recovery failover admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

During a failover, the most recent SnapMirror snapshot copy is used. Or, you can select a specific snapshot from a point-in-time snapshot (per the retention policy of SnapMirror). The point-in-time option can be helpful if you are facing a corruption event such as ransomware, where the most recent replicas are already compromised or encrypted. BlueXP disaster recovery shows all available points in time.

This process differs depending on whether the production site is healthy and you are performing a failover to the disaster recovery site for reasons other than a critical infrastructure failure:

- Critical production site failure where the source vCenter or ONTAP cluster is not accessible: BlueXP disaster recovery lets you select any available snapshot from which to restore.
- Production environment is healthy: You can either "Take a snapshot now" or select a previously created snapshot.

This procedure breaks the replication relationship, places the vCenter source VMs offline, registers the volumes as datastores in the disaster recovery vCenter, restarts the protected VMs using the failover rules in the plan, and enables read/write on the target site.

Test the failover process

Before you start the failover, you can test the process. The test does not place the virtual machines offline.

During a failover test, virtual machines are temporarily created. BlueXP disaster recovery does not map the 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.

This process doesn’t consume additional physical capacity on on-premises ONTAP storage or FSx for NetApp ONTAP storage in AWS. The original source volume is not modified and replica jobs can continue even during disaster recovery.

When you finish the test, you should reset the virtual machines with the **Clean up test** option. While this is

recommended, it is not required.

A test failover operation does *not* impact production workloads, the SnapMirror relationship used on the test site, and protected workloads that must continue to operate normally.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the BlueXP disaster recovery top menu, select **Replication plans**.
3. Select the replication plan.
4. On the right, select the **Actions** option ••• and select **Test failover**.
5. In the Test failover page, enter “Test failover” and select **Test fail over**.
6. After the test is complete, clean up the test environment.

Clean up the test environment after a failover test

After the failover test finishes, you should clean up the test environment. This process removes the temporary VMs from the test location, the FlexClones, and the temporary datastores.

Steps

1. From the BlueXP disaster recovery top menu, select **Replication plans**.
2. Select the replication plan.
3. On the right, select the **Actions** option ••• and select **Clean up failover test**.
4. In the Test failover page, enter “Clean up failover” and select **Clean up failover test**.

Fail over the source site to a disaster recovery site

In case of a disaster, fail over your primary on-premises VMware site on demand to another on-premises VMware site or VMware Cloud on AWS with FSx for NetApp ONTAP.

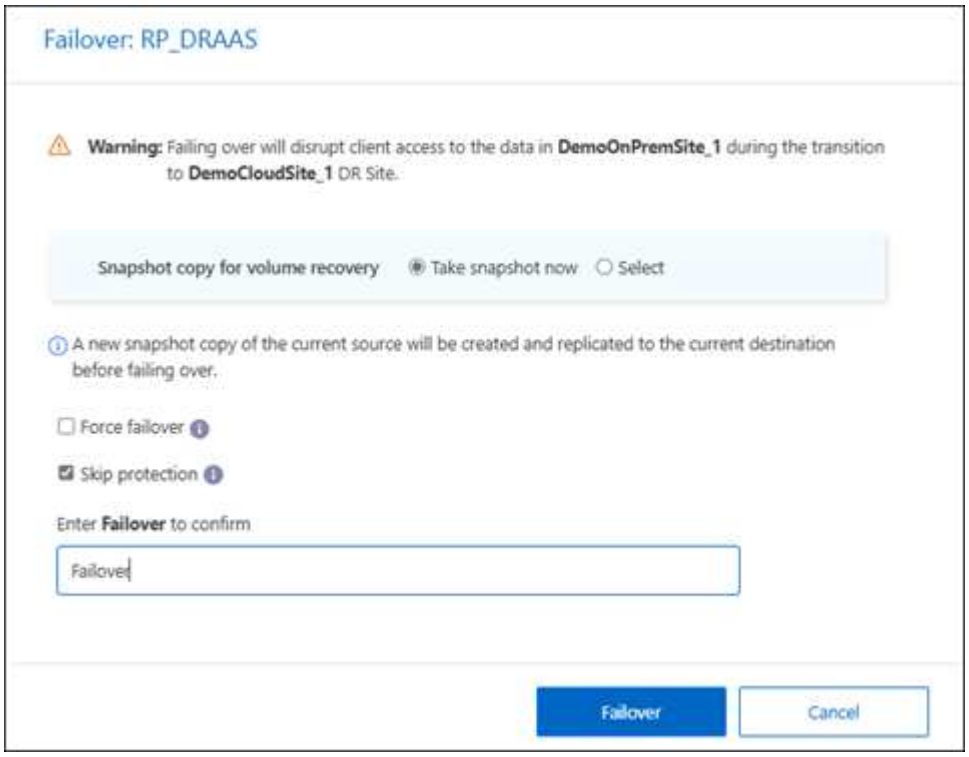
The failover process involves in the following operations:

- If you selected the latest snapshot, the SnapMirror update is performed to replicate the latest changes.
- The source virtual machines are powered down.
- The SnapMirror relationship is broken and the target volume is made read/write.
- Based on the selection of the snapshot, the active file system is restored to the specified snapshot (latest or selected)
- Datastores are created and mounted to the VMware or VMC cluster or host based on the information captured in the replication plan.
- The target virtual machines are registered and powered on based on the order captured in the Resource groups page.
- The SnapMirror relationship is reversed from target to source virtual machine.

After the failover starts, the recovered VMs can be seen in the vCenter of the disaster recovery site (virtual machines, networks, and datastores). By default, the virtual machines are recovered to the Workload folder.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the BlueXP disaster recovery top menu, select **Replication plans**.
3. Select the replication plan.
4. On the right, select the **Actions** option ••• and select **Fail over**.



5. In the Fail over page, either initiate a snapshot now or choose the snapshot for the datastore from which to recover. The default is the latest.

   A snapshot of the current source will be taken and replicated to the current destination before the fail over occurs.

6. Optionally, select **Force failover** if you want the failover to occur even if an error is detected that would normally prevent the failover from occurring.
7. Optionally, select **Skip protection** if you want the service to not automatically create a reverse SnapMirror protection relationship after a replication plan failover. This is useful if you want to perform additional operations on the restored site before you bring it back online within BlueXP disaster recovery.

   You can establish reverse protection by selecting **Protect resources** from the Replication plan Actions menu. This attempts to create a reverse replication relationship for each volume in the plan. You can run this job repeatedly until protection is restored. When protection is restored, you can initiate a failback in the usual way.

8. Type "failover" in the box.
9. Select **Fail over**.
10. To check the progress, in the top menu, select **Job monitoring**.

Fail back applications to the original source with BlueXP disaster recovery

After a disaster has been resolved, fail back from the disaster recovery site to the source site to return to normal operations. You can select the snapshot from which to recover.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, or Disaster recovery failover admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

In this workflow, BlueXP disaster recovery 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:

- On the target site, the virtual machines are powered off and unregistered, and volumes are unmounted.
- The SnapMirror relationship on the original source is broken to make it read/write.
- The SnapMirror relationship is resynchronized to reverse the replication.
- The source virtual machines are powered on and registered, and volumes are mounted on the source.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the BlueXP disaster recovery top menu, select **Replication plans**.
3. Select the replication plan.
4. On the right, select the **Actions** option ••• and select **Fail back**.
5. Enter the replication plan name to confirm and start the failback.
6. Choose the snapshot for the datastore from which to recover. The default is the latest.
7. To check the progress, in the top menu, select **Job monitoring**.

Manage sites, resource groups, replication plans, datastores and virtual machines information with BlueXP disaster recovery

You can get a quick glance of all your BlueXP disaster recovery resources or look at each in detail:

- Sites
- Resource groups
- Replication plans
- Datastores
- Virtual machines

Tasks require different BlueXP roles. For details, see the **Required BlueXP role** section in each task.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

Manage vCenter sites

You can edit the vCenter site name and the site type (on-premises or AWS).

Required BlueXP role
Organization admin, Folder or project admin, or Disaster recovery admin role.

Steps

1. From the top menu, select **Sites**.
2. Select the **Actions** option  on the right of the vCenter name and select **Edit**.
3. Edit the vCenter site name and location.

Manage resource groups

While you can add a resource group as part of creating a replication plan, you might find it more convenient to add the groups separately and later use those groups in the plan. You create resource groups by VMs or by datastores.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, or Disaster recovery application admin role.

You can create a resource group by datastores in the following ways:

- When you're adding a resource group using datastores, you can see a list of datastores. You can select one or more datastores to create a resource group.
- When you're creating a replication plan and creating a resource group within the plan, you can see the VMs in the datastores.

You can also edit and delete resource groups.

Steps

1. From the top menu, select **Resource groups**.
2. To add a resource group, select **Add group**.
3. To perform actions with the resource group, select the **Actions** option ••• at the right and select any of the options, such as **Edit resource group** or **Delete resource group**.

Manage replication plans

You can disable, enable and delete replication plans. You can change schedules.

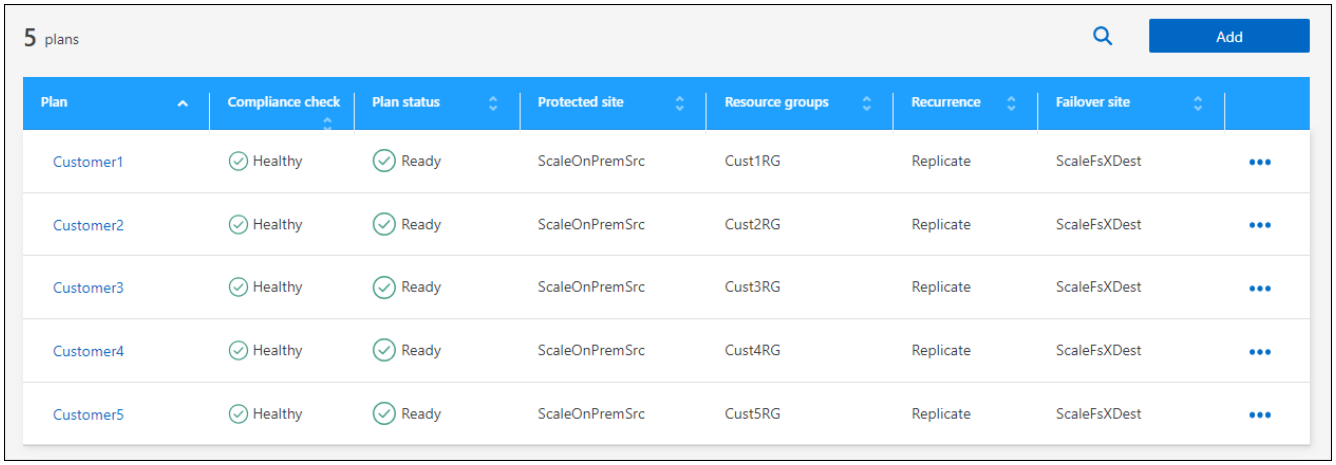
Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, or Disaster recovery application admin role.

- If you want to pause a replication plan temporarily, you can disable it and later enable it.

- If you no longer need the plan, you can delete it.

Steps

1. From the top menu, select **Replication plans**.



2. To view the plan details, select the **Actions** option ••• and select **View plan details**.
3. Do any of the following:
   - To edit the plan details (change the recurrence), select the **Plan details** tab and select the **Edit** icon to the right.
   - To edit the resource mappings, select the **Failover mapping** tab and select the **Edit** icon.
   - To add or edit the virtual machines, select the **Virtual machines** tab and select the **Add VMs** option or **Edit** icon.
4. Return to the list of plans by selecting "Replication plans" in the breadcrumbs at the top left.
5. To perform actions with the plan, from the list of replication plans, select the **Actions** option ••• to the right of the plan and select any of the options, such as **Edit schedules**, **Test failover**, **Fail over**, **Fail back**, **Migrate**, **Take snapshot now**, **Clean up old snapshots**, **Disable**, **Enable**, or **Delete**.
6. To set or change a test failover schedule or set the compliance frequency check, select the **Actions** option ••• to the right of the plan and select **Edit schedules**.
   a. In the Edit schedules page, enter how often in minutes you want the failover compliance check to occur.
   b. Check **Run test failovers on a schedule**.
   c. In the Repeat option, select the daily, weekly, or monthly schedule.
   d. Select **Save**.

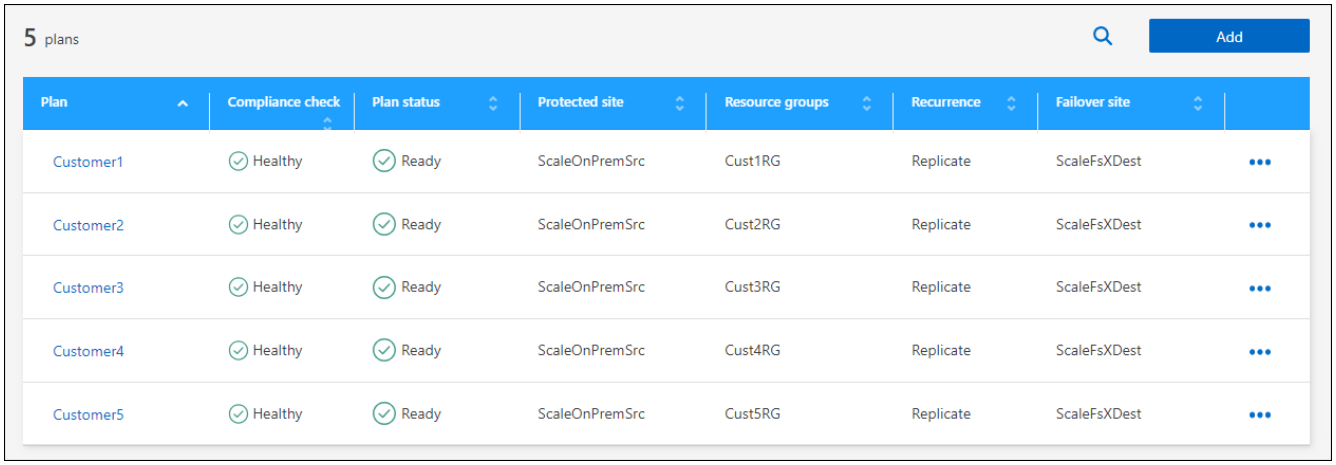
Reconcile snapshots on demand

You can reconcile snapshots that are out of sync between the source and target. This might occur if snapshots are deleted on a target outside of BlueXP disaster recovery. The service automatically deletes the snapshot on the source automatically every 24 hours. However, you can perform this on demand. This feature enables you to ensure that the snapshots are consistent across all sites.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, or Disaster recovery application admin role.

Steps

1. From the top menu, select **Replication plans**.



2. From the list of replication plans, select the **Actions** option ••• to the right of the plan and select **Reconcile snapshots**.
3. Review the reconciliation information.
4. Select **Reconcile**.

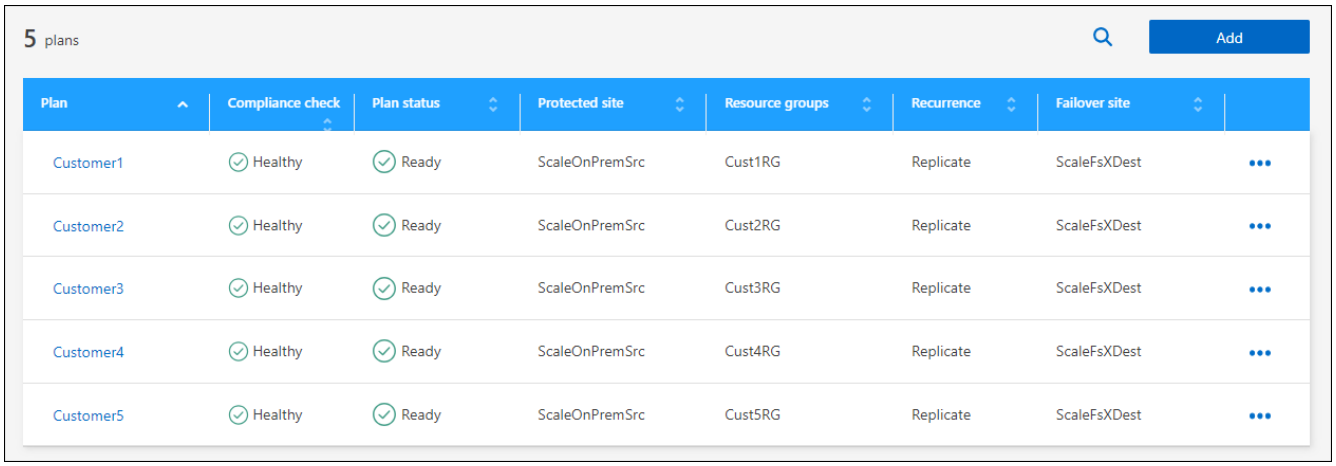
Delete a replication plan

You can delete a replication plan if you no longer need it. If you delete a replication plan, you can also delete the primary and secondary snapshots created by the plan.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, or Disaster recovery application admin role.

Steps

1. From the top menu, select **Replication plans**.



2. Select the **Actions** option ••• to the right of the plan and select **Delete**.
3. Select whether you want to delete the primary snapshots, secondary snapshots, or just the metadata created by the plan.

4. Type "delete" to confirm the deletion.
5. Select **Delete**.

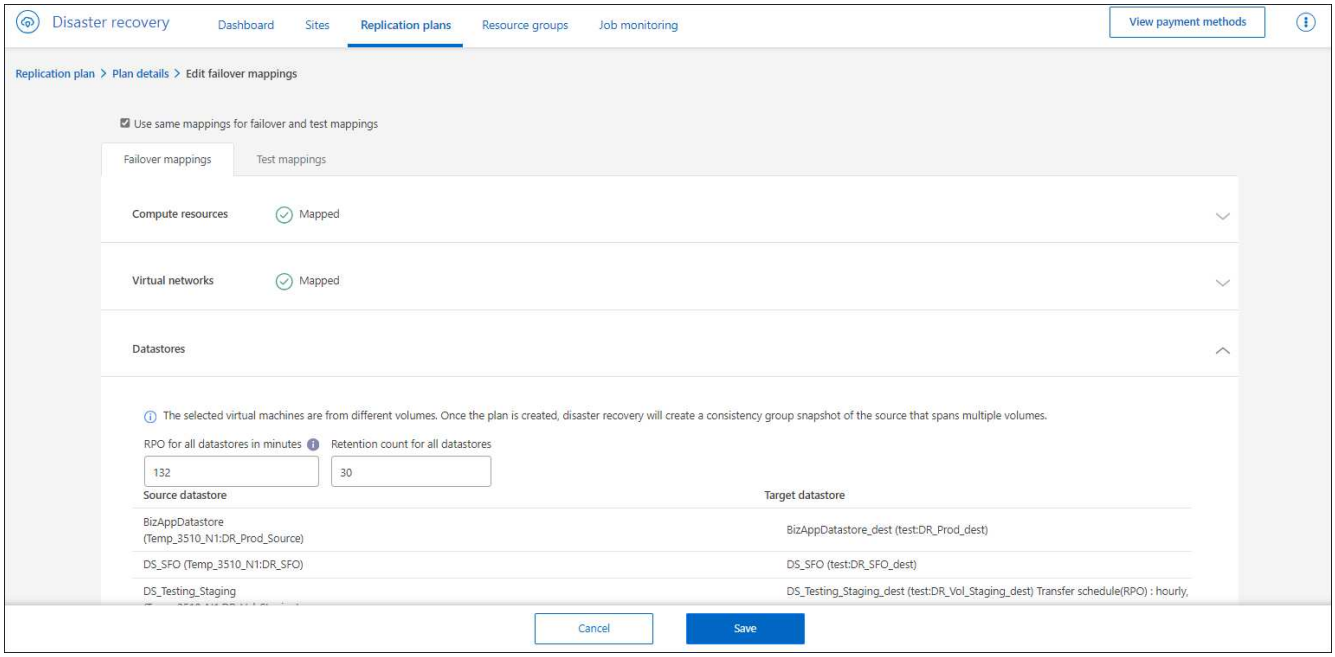
Change retention count for failover schedules

You can change how many datastores are retained.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, or Disaster recovery application admin role.

Steps

1. From the top menu, select **Replication plans**.
2. Select the replication plan, click the **Failover mapping** tab, and click the **Edit** pencil icon.
3. Click the **Datastores** arrow to expand it.



4. Change the value of the retention count in the replication plan.
5. With the replication plan selected, select the Actions menu, select *Clean up old snapshots" to remove old snapshots on the target to match the new retention count.

View datastores information

You can view information about how many datastores exist on the source and on the target.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, Disaster recovery application admin, or Disaster recovery viewer role.

Steps

1. From the top menu, select **Dashboard**.
2. Select the vCenter in the site row.

3. Select **Datastores**.
4. View the datastores information.

View virtual machines information

You can view information about how many virtual machines exist on the source and on the target along with CPU, memory, and available capacity.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, Disaster recovery application admin, or Disaster recovery viewer role.

Steps

1. From the top menu, select **Dashboard**.
2. Select the vCenter in the site row.
3. Select **Virtual machines**.
4. View the virtual machines information.

Monitor BlueXP disaster recovery jobs

You can monitor all BlueXP disaster recovery jobs and determine their progress.

View jobs

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery application admin, or Disaster recovery viewer role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the top menu, select **Job monitoring**.
3. Explore all jobs related to operations and review their timestamps and status.
4. To view details of a particular job, select that row.
5. To refresh information, select **Refresh**.

Cancel a job

If a job is in progress or in a queued state and you don’t want it to continue, you can cancel it. You might want to cancel a job if it is stuck in the same state and you want to free up the next operation in the queue. You might want cancel a job before it times out.

Required BlueXP role
Organization admin, Folder or project admin, Disaster recovery admin, Disaster recovery failover admin, or Disaster recovery application admin role.

Learn about user roles and permissions in BlueXP disaster recovery.
Learn about BlueXP access roles for all services.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery**.
2. From the top menu, select **Job monitoring**.
3. In the Job monitor page, note the ID of the job you want to cancel.

   The job must be in an "In progress" or "Queued" state.

4. In the Actions column, select **Cancel job**.

Create BlueXP disaster recovery reports

Reviewing BlueXP disaster recovery reports can help you analyze your disaster recovery preparedness. Predesigned reports include a summary of test failovers, replication plan details, and job details on all sites within an account for the past seven days.

You can download reports in PDF, HTML, or JSON format.

The Download link is valid for six hours.

Steps

1. From the BlueXP left nav, select **Protection** > **Disaster recovery** > **Replication plans**.
2. From the top of the page, select **Create report**.
3. Select the type of file format and the time period within the last 7 days.
4. Select **Create**.

   The report might take a few minutes to display.

5. To download a report, select **Download report** and select it in the administrator's Download folder.

Reference

vCenter privileges needed for BlueXP disaster recovery

The vCenter account must have a minimum set of vCenter privileges to allow BlueXP disaster recovery to perform its services, such as registering and deregistering datastores, starting and stopping VMs, and reconfiguring virtual machines (VMs). The following table lists all privileges required for BlueXP disaster recovery to interface with a vCenter cluster.

Type	Privilege name	Description
Datastore	Datastore.Configure datastore	Use to configure a datastore.
	Datastore.Remove datastore	Use to remove a datastore.
Virtual Machine	Virtual machine.Configuration.Change Settings	Use to change general VM settings.
	Virtual machine.Configuration.Modify device settings	Use to change the properties of an existing device.
	Virtual machine.Configuration.Reload from path	Use to change a VM configuration patch while preserving the identity of the VM. Solutions such as VMware vCenter Site Recovery Manager use this operation to maintain VM identify during failover and failback.
	Virtual machine.Configuration.Rename	Use to rename a VM or modify the associated nodes of a VM.
	Virtual machine.Configuration.Reset guest information	Use to edit the guest operating system information for a VM.
	Virtual machine.Configuration.Change Memory	Use to change the amount of memory allocated to the VM.
	Virtual machine.Configuration.Change CPU count	Use to change the number of virtual CPUs.
Virtual Machine Guest	Virtual machine.Guest Operations.Guest Operation Modifications	Enables VM guest operations that involve changes to a guest operating system in a VM, such as transferring a file to the VM.

Type	Privilege name	Description
Virtual Machine Interaction	Virtual machine.Interaction.Power Off	Use to power off a powered-on VM. This operation powers down the guest operating system.
	Virtual machine.Interaction.Power on	Use to power on a powered-off VM and resume a suspended VM.
	Virtual machine.Interaction.VMware Tools install	Use to mount and unmount the VMware Tools CD installer as a CD-ROM for the guest operating system.
Virtual Machine Inventory	Virtual machine.Inventory.Create new	Use to create a VM and allocate resources for its execution.
	Virtual machine.Inventory.Register	Use to add an existing VM to a vCenter Server or host inventory.
	Virtual machine.Inventory.Unregister	Use to unregister a VM from a vCenter Server or host inventory.
Virtual Machine State	Virtual machine.Snapshot management.Create snapshot	Use to create a snapshot from the VM's current state.
	Virtual machine.Snapshot management.Remove Snapshot	Use to remove a snapshot from the snapshot history.
	Virtual machine.Snapshot management.Revert to snapshot	Use to set the VM to the state it was in at a given snapshot.

BlueXP disaster recovery role-based access to features

BlueXP disaster recovery employs roles to govern the access that each user has to specific features and actions.

The service uses the following roles that are specific to BlueXP disaster recovery.

- **Disaster recovery admin**: Perform any actions in BlueXP disaster recovery.
- **Disaster recovery failover admin**: Perform failover and migrate actions in BlueXP disaster recovery.
- **Disaster recovery application admin**: Create and modify replication plans and start test failovers.
- **Disaster recovery viewer**: View information in BlueXP disaster recovery, but cannot perform any actions.

These roles are specific to BlueXP disaster recovery and are not the same as the platform roles that are used in BlueXP. For details about all BlueXP platform roles, see the BlueXP setup and administration documentation.

The following table indicates the actions that each BlueXP disaster recovery role can perform.

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View dashboard and all tabs	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No
Initiate discovery of workloads	Yes	No	No	No
View license information	Yes	Yes	Yes	Yes
Activate license	Yes	No	Yes	No
On the Sites tab:				
View sites	Yes	Yes	Yes	Yes
Add, modify, or delete sites	Yes	No	No	No
On the Replication plans tab:				
View replication plans	Yes	Yes	Yes	Yes
View replication plan details	Yes	Yes	Yes	Yes
Create or modify replication plans	Yes	Yes	Yes	No
Create reports	Yes	No	No	No
View snapshots	Yes	Yes	Yes	Yes
Perform failover tests	Yes	Yes	Yes	No
Perform failovers	Yes	Yes	No	No
Perform failbacks	Yes	Yes	No	No
Perform migations	Yes	Yes	No	No
On the Resource groups tab:				
View resource groups	Yes	Yes	Yes	Yes
Create, modify, or delete resource groups	Yes	No	Yes	No
On the Job Monitoring tab:				

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View jobs	Yes	No	Yes	Yes
Cancel jobs	Yes	Yes	Yes	No

Use BlueXP disaster recovery with Amazon EVS

Introduction of BlueXP disaster recovery using Amazon Elastic VMware Service and Amazon FSx for NetApp ONTAP

Increasingly, customers have become more dependent on virtualized infrastructures for production compute workloads such as those based on VMware vSphere. As these virtual machines (VMs) have become more critical to their businesses, customers need to protect these VMs from the same types of disasters as their physical compute resources. Disaster recovery (DR) solutions currently offered are complex, expensive, and resource intensive. NetApp, the largest storage provider used for virtualized infrastructures, has a vested interest in ensuring its customers' VMs are protected in the same way that we protect ONTAP storage-hosted data of any type. To meet this goal, NetApp created the BlueXP disaster recovery service.

THIS DOCUMENTATION REGARDING AMAZON EVS IS PROVIDED AS A TECHNOLOGY PREVIEW. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

One of the primary challenges with any DR solution is managing the incremental cost of purchasing, configuring, and maintaining additional compute, network, and storage resources just to provide a DR replication and recovery infrastructure. One popular option for protecting critical on-premises virtual resources is to use cloud-hosted virtual resources as the DR replication and recovery infrastructure. Amazon is one example of such a solution that can provide cost-effective resources that are compatible with NetApp ONTAP hosted VM infrastructures.

Amazon introduced its Amazon Elastic VMware Service (Amazon EVS) that enables VMware Cloud Foundation within your virtual private cloud (VPC). Amazon EVS provides the resilience and performance of AWS alongd with the familiar VMware software and tools enabling Amazon EVS vCenters to be integrated as an extension of your on-premises virtualized infrastructure.

While Amazon EVS comes with included storage resources, using native storage can reduce its effectiveness for organizations with storage-heavy workloads. In these cases, teaming Amazon EVS with Amazon FSx for NetApp ONTAP storage (Amazon FSxN) can provide a more flexible storage solution. In addition, when you are using NetApp ONTAP storage solutions on-premises to host your VMware infrastructure, using Amazon EVS with FSx for ONTAP means you get best-in-class data interoperability and protection features between your on-premises and cloud-hosted infrastructures.

For information about Amazon FSx for NetApp ONTAP, see Getting started with Amazon FSx for NetApp ONTAP.

Solution overview of BlueXP disaster recovery using Amazon EVS and Amazon FSs for NetApp ONTAP

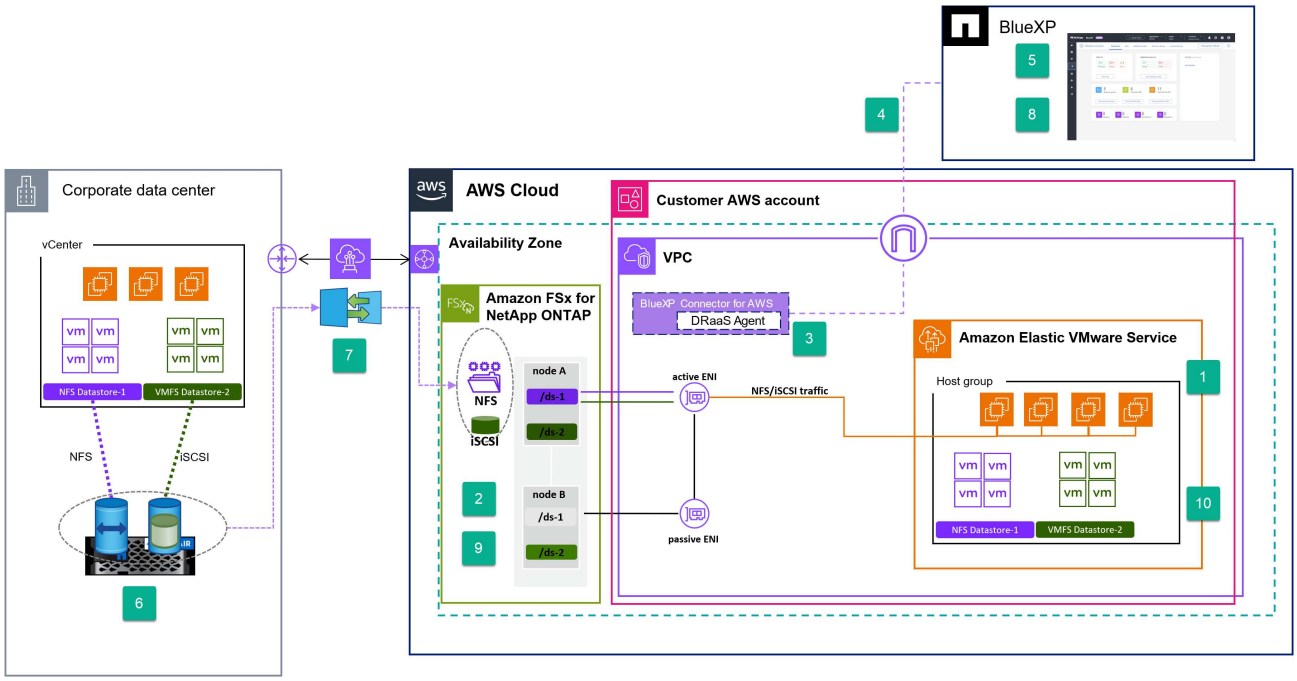
BlueXP disaster recovery is a value-added service hosted within the BlueXP software-as-a-service environment, which depends on the core BlueXP architecture. Several main components comprise the DR service for VMware protection within BlueXP.

For a complete overview of the BlueXP disaster recovery solution, see Learn about BlueXP disaster recovery for VMware.

If you want to protect your on-premises VMware hosted virtual machines to Amazon AWS, use the service to back up to Amazon EVS with Amazon FSx for NetApp ONTAP storage hosted datastores.

The following figure shows how the service works to protect your VMs with Amazon EVS.

Overview of BlueXP disaster recovery using Amazon EVS and FSx for ONTAP



1. Amazon EVS is deployed in your account in a single Availability Zone (AZ) configuration and within the your Virtual Private Cloud (VPC).
2. An FSx for ONTAP file system is deployed in the same AZ as the Amazon EVS deployment. The file system connects to Amazon EVS either directly through an Elastic Network Interface (ENI), a VPC peer connection, or an AmazonTransit Gateway.
3. The NetApp BlueXP Connector is installed in your VPC. The BlueXP Connector hosts multiple data management services (called agents), including the BlueXP disaster recovery agent that manages DR of the VMware infrastructure on both your local physical datacenters and your Amazon AWS hosted resources.
4. The BlueXP disaster recovery agent securely communicates with the BlueXP cloud-hosted service to receive tasks and distributes those tasks to the appropriate on-premises and AWS hosted vCenter and ONTAP storage instances.
5. You create a replication plan by using the BlueXP cloud-hosted UI console indicating the VMs that should be protected, the frequency those VMs should be protected, and the procedures that need to be performed

to restart those VMs in the event of a failover from the on-premises site.

6. The replication plan determines which vCenter datastores are hosting the protected VMs and the ONTAP volumes that are hosting those datastores. If volumes do not yet exist on the FSx for ONTAP cluster, BlueXP disaster recovery automatically creates them.
7. A SnapMirror relationship is created for each identified source ONTAP volume to each destination FSx for ONTAP hosted ONTAP volume and a replication schedule is created based on the user-provided RPO in the replication plan.
8. In the event of the primary site failure, an administrator initiates a manual failover process within the BlueXP console and selects a backup to use as the restore point.
9. The BlueXP disaster recovery agent activates the FSx for ONTAP hosted data protection volumes.
10. The agent registers each activated FSx for ONTAP volume with the Amazon EVS vCenter, registers each protected VM with the Amazon EVS vCenter, and starts each according to the predefined rules contained in the replication plan.

Install the BlueXP Connector for BlueXP disaster recovery

A BlueXP Connector is NetApp software running in your cloud or on-premises network. It executes the actions that BlueXP needs to perform to manage your data infrastructure. The Connector constantly polls the BlueXP disaster recovery software as a service layer for any actions that it needs to take.

For the BlueXP disaster recovery service, the actions that are performed orchestrate VMware vCenter clusters and ONTAP storage instances using native APIs for each respective service to provide protection for production VMs running in an on-premises location. While the Connector can be installed in any of your network locations, for BlueXP disaster recovery we recommend that you install the Connector in the DR site. This ensures that in the event of a failure of the primary site, the BlueXP cloud-based console UI continues to have contact with the Connector and can orchestrate the recovery process within that DR site.

To use the service, install the Connector in standard mode. To learn more about the types of Connector installations, visit Learn about BlueXP deployment modes | NetApp Documentation.

While the Connector is critical to using the service, the installation steps to install the Connector depend on your needs and network configuration. It is beyond the scope of this information to provide specific instructions for installation.

The simplest method for installing a Connector with Amazon AWS is to use the AWS Marketplace. For details about Connector installation using the AWS Marketplace, see Create a Connector from the AWS Marketplace | NetApp Documentation.

Configure BlueXP disaster recovery for Amazon EVS

Configure BlueXP disaster recovery for Amazon EVS overview

After you install the BlueXP Connector, you need to integrate all the ONTAP storage and VMware vCenter resources that will participate in the disaster recovery process with BlueXP disaster recovery.

- Prerequisites for Amazon EVS with BlueXP disaster recovery
- Add ONTAP storage arrays to BlueXP disaster recovery

- Enable BlueXP disaster recovery for Amazon EVS
- Add vCenter sites to BlueXP disaster recovery
- Add vCenter clusters to BlueXP disaster recovery

Prerequisites for Amazon EVS with BlueXP disaster recovery

You should ensure that several prerequisites are met before you continue to configure Amazon EVS with BlueXP disaster recovery.

Specifically, do the following:

- Create a vCenter user account with the specific VMware privileges required for BlueXP disaster recovery to perform the necessary operations.

  > We do not recommend using the default "administrator@vsphere.com" administrator account. Instead, you should create a BlueXP disaster recovery specific user account on all vCenter clusters that will participate in the DR process. For a list of specific privileges required, see vCenter privileges needed for BlueXP disaster recovery.

- Ensure that all vCenter datastores that will host VMs protected by BlueXP disaster recovery are located on NetApp ONTAP storage resources.

  The service supports NFS and VMFS on iSCSI (and not FC) when using Amazon FSx on NetApp ONTAP. While the service supports FC, Amazon FSx for NetApp ONTAP does not.

- Ensure that your Amazon EVS vCenter is connected to an Amazon FSx for NetApp ONTAP storage cluster.
- Ensure that VMware tools are installed on all protected VMs.
- Ensure that your on-premises network is connected to your AWS VPC network using an Amazon approved connection method. We recommend that you use AWS Direct Connect, AWS Private Link, or an AWS Site-to-Site VPN.

Add on-premises arrays to the BlueXP working environment for Amazon EVS with BlueXP disaster recovery

Before using BlueXP disaster recovery, you must add on-premises and cloud-hosted storage instances to the BlueXP working environment.

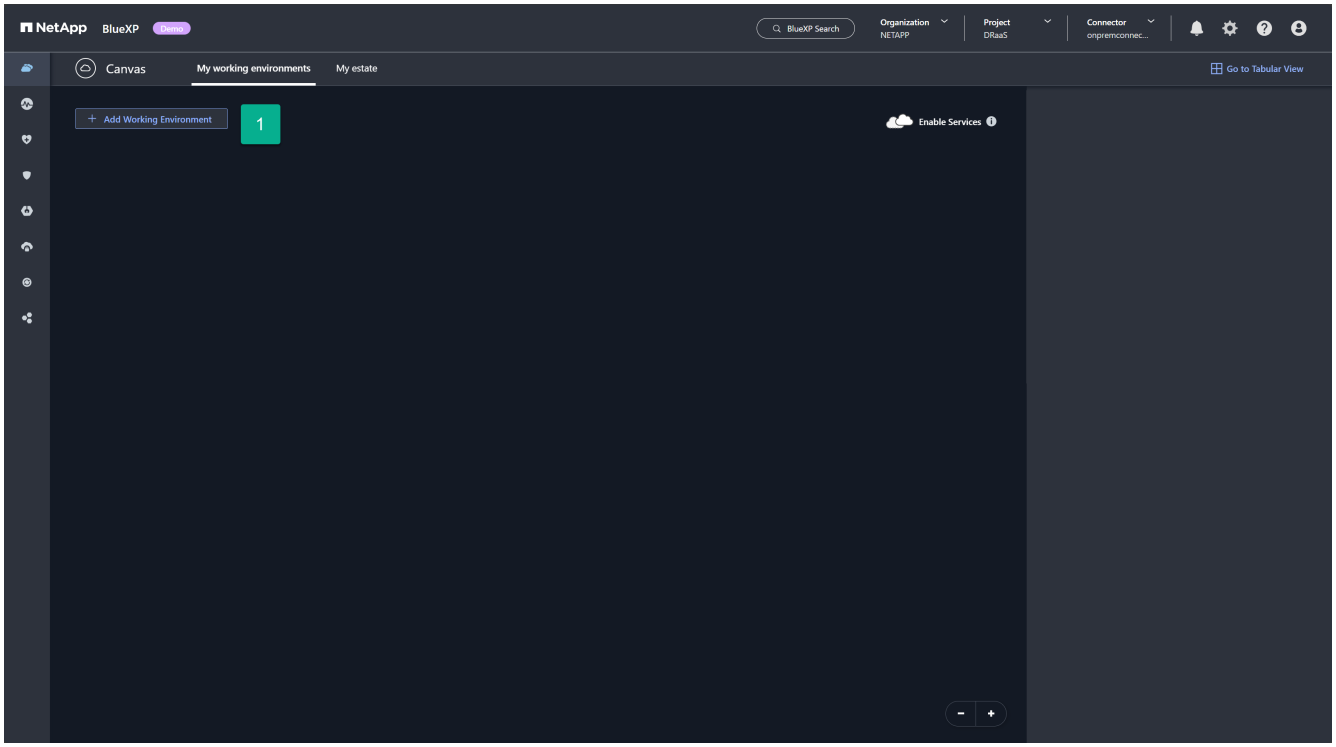
You need to do the following:

- Add on-premises arrays to your BlueXP working environment.
- Add Amazon FSx for NetApp ONTAP (FSx for ONTAP) instances to your BlueXP working environment.

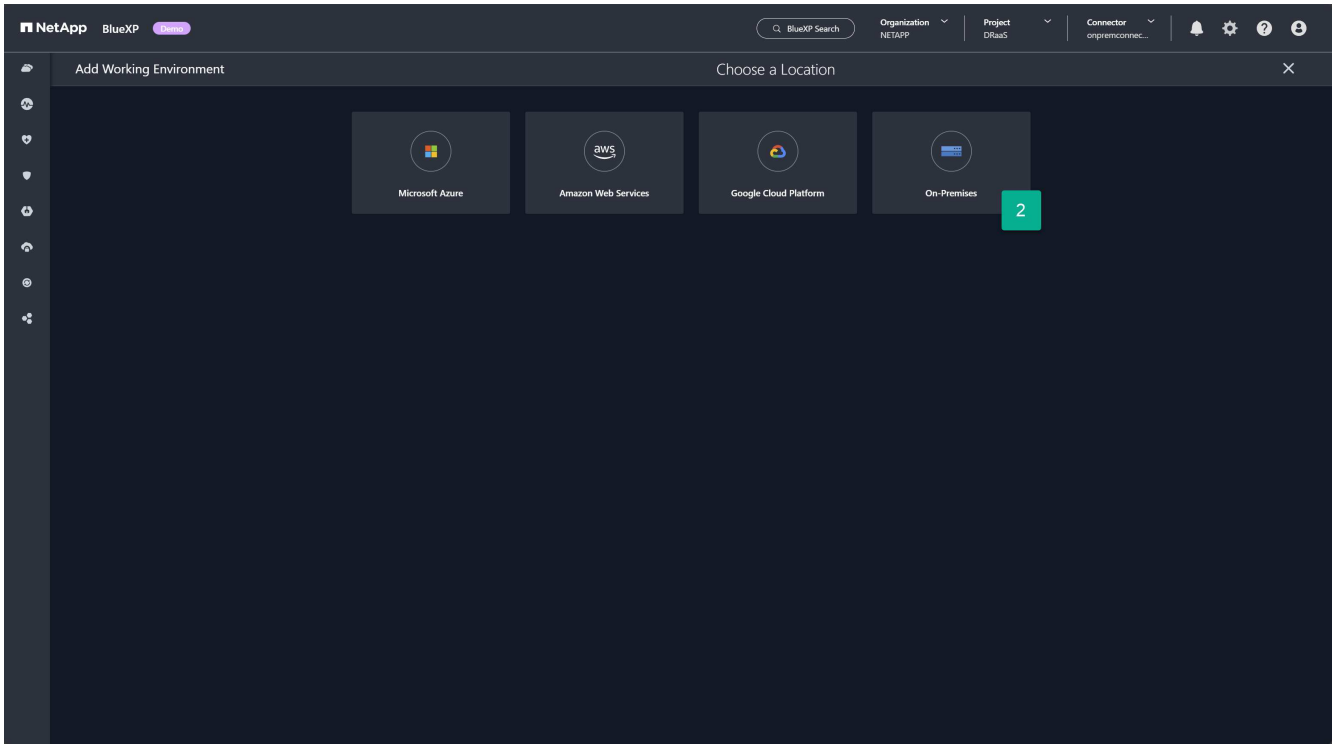
Add on-premises storage arrays to BlueXP working environment

Add on-premises ONTAP storage resources to your BlueXP working environment.

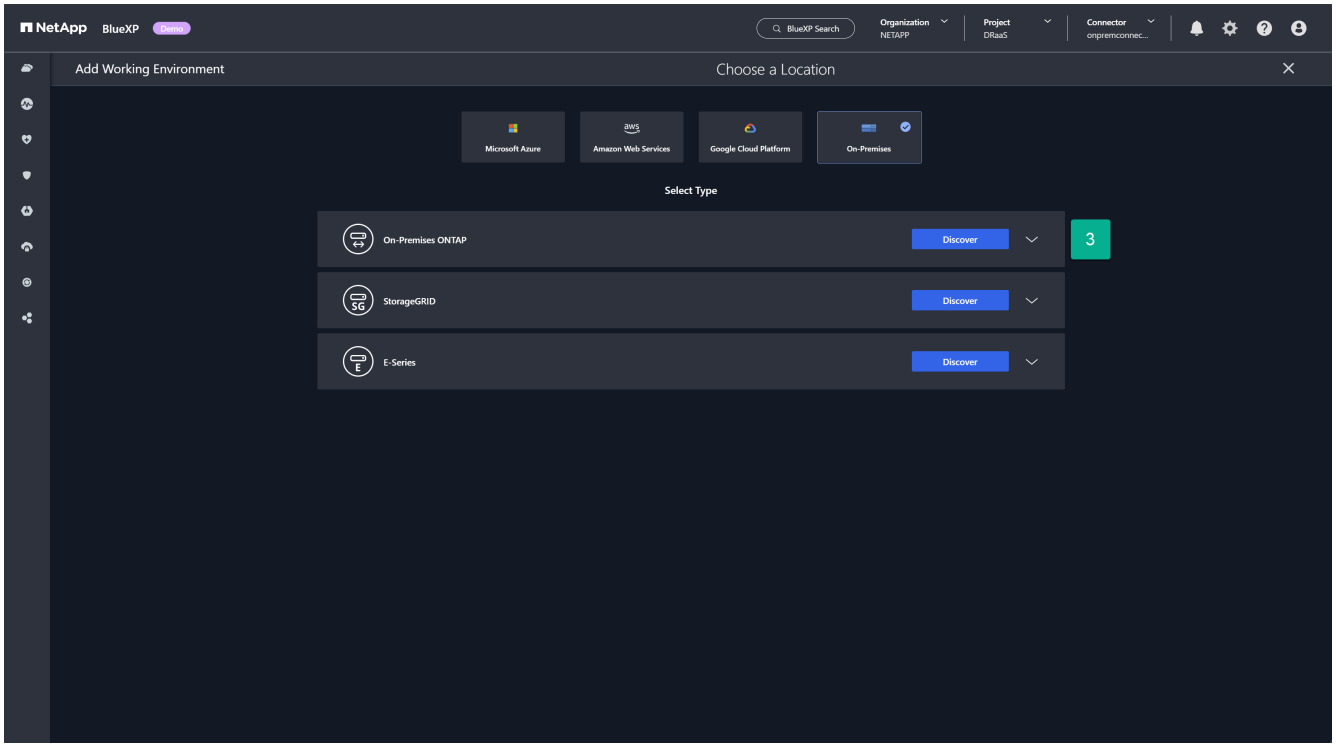
1. From the BlueXP Canvas, select **Add Working Environment**.



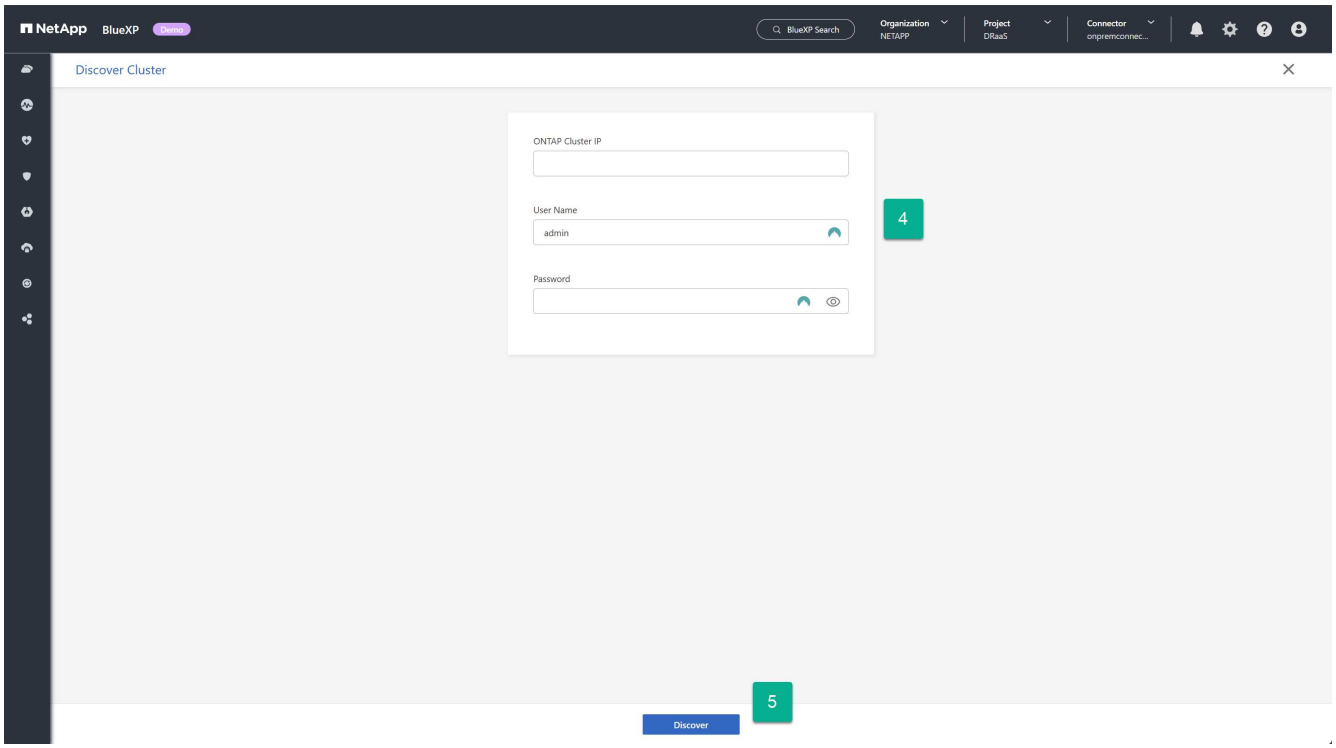
2. From the Add Working Environment page, select the **On-Premises** card.



3. Select **Discover** on the On-Premises ONTAP card.



4. On the Discover Cluster page, enter the following information:
   a. The IP address of the ONTAP array cluster management port
   b. The administrator username
   c. The administrator password
5. Select **Discover** at the bottom of the page.

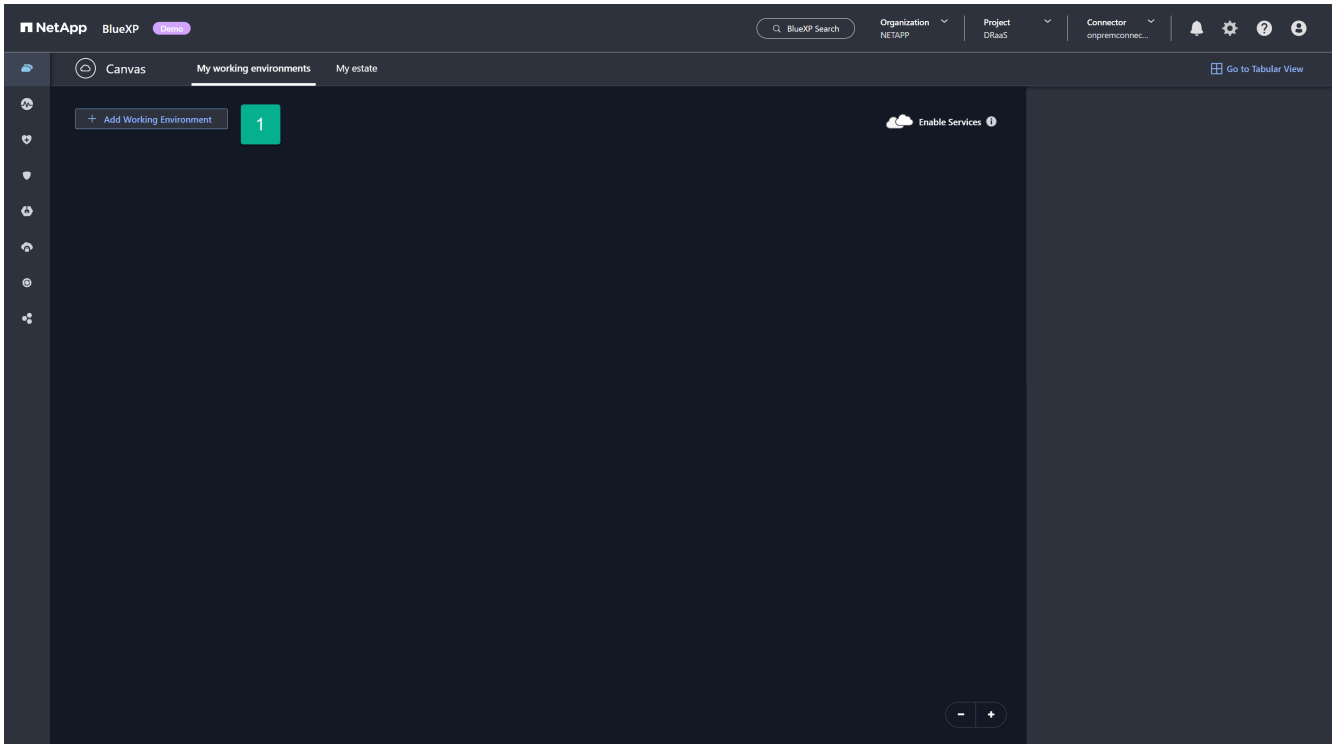


6. Repeat steps 1-5 for each ONTAP array that will host vCenter datastores.

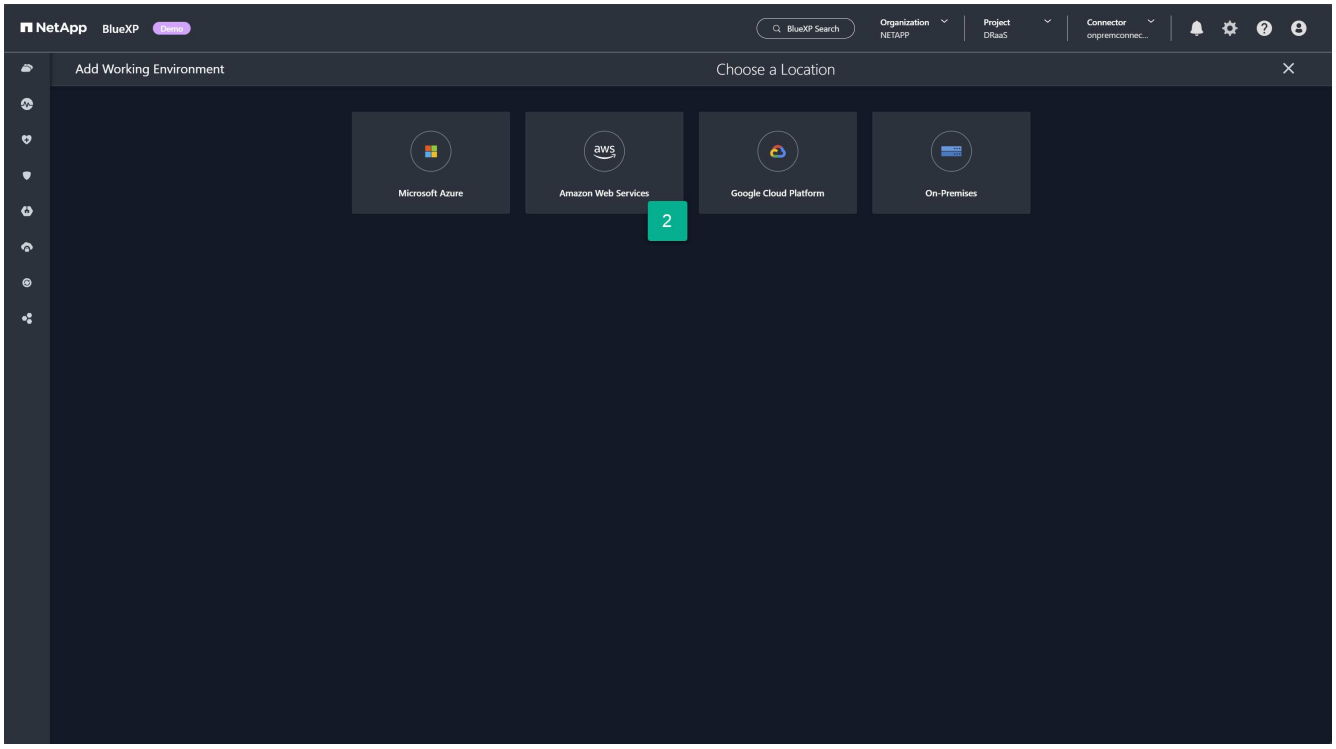
Add Amazon FSx for NetApp ONTAP storage instances to BlueXP working environment

Next, add an Amazon FSx for NetApp ONTAP storage resources to your BlueXP working environment.

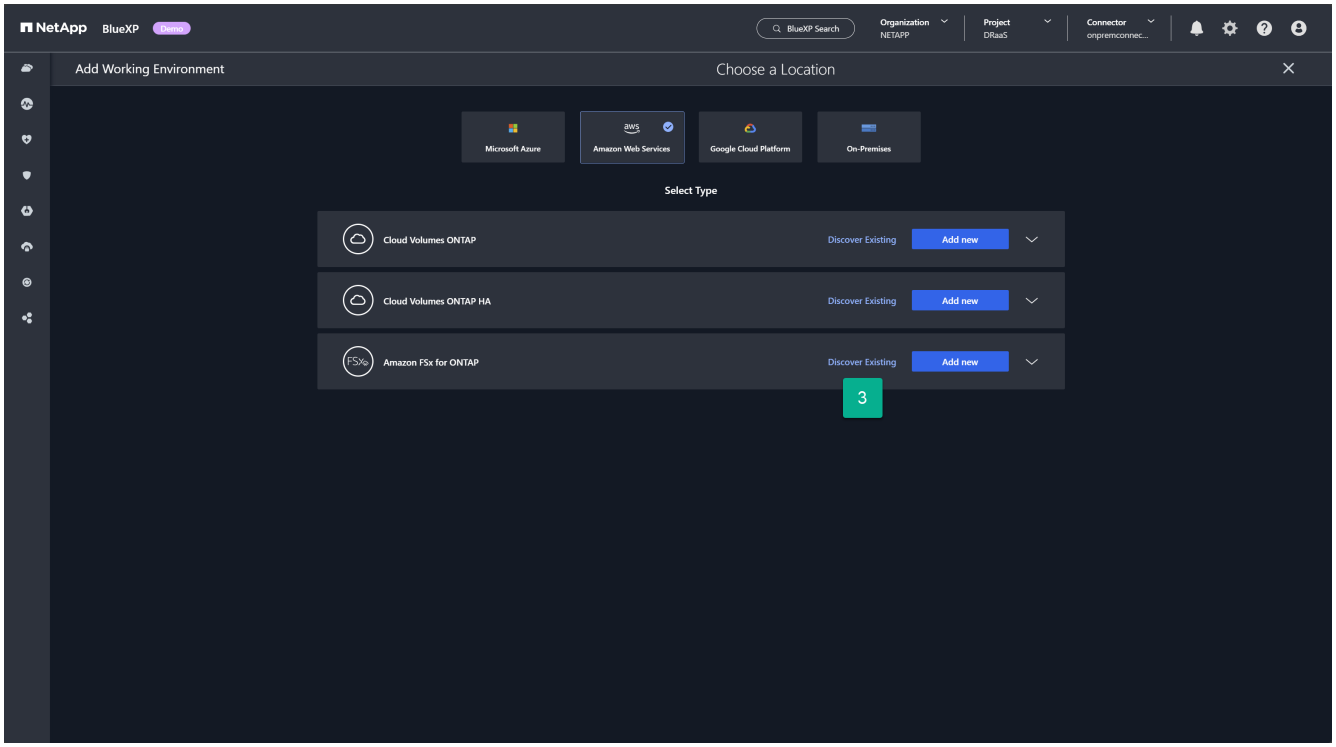
1. From the BlueXP Canvas, select **Add Working Environment**.



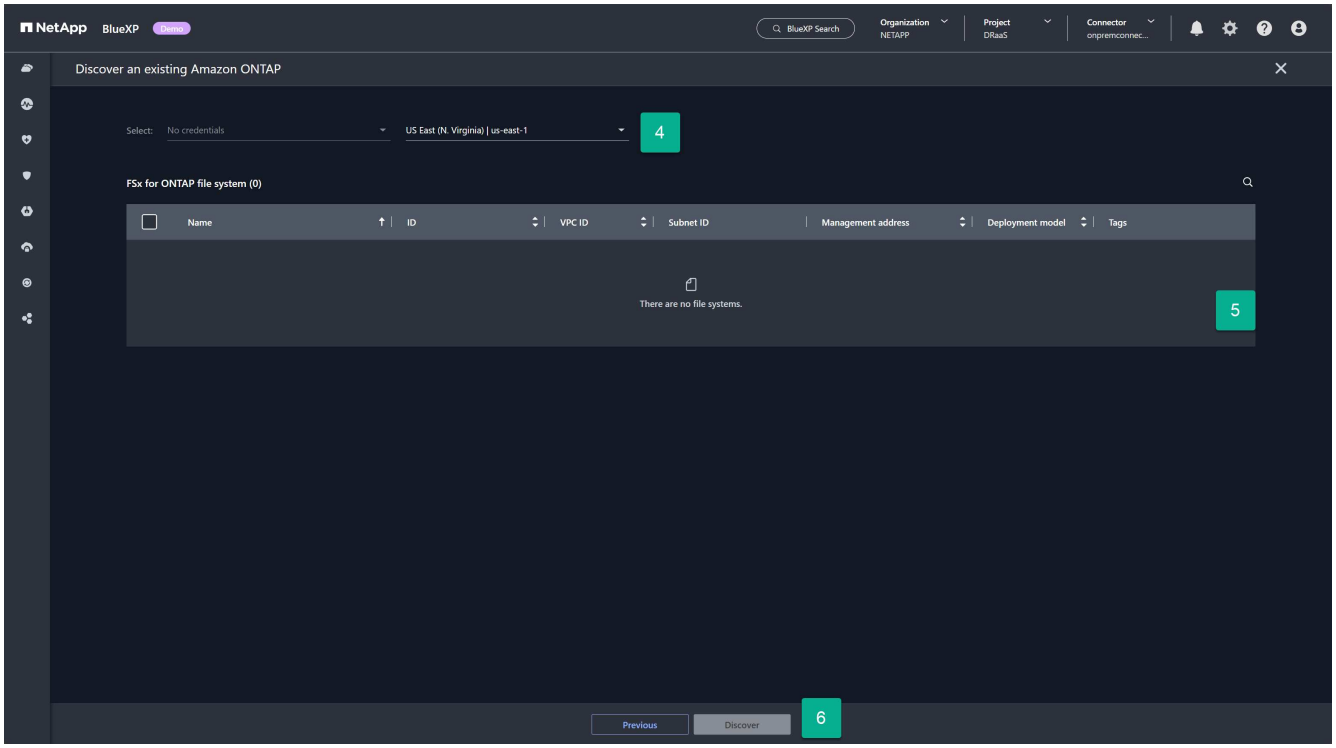
2. From the Add Working Environment page, select the **Amazon Web Services** card.



3. Select the **Discover Existing** link on the Amazon FSx for ONTAP card.



4. Select the credentials and AWS region hosting the FSx for ONTAP instance.
5. Select one or more FSx for ONTAP file systems to be added.
6. Select **Discover** at the bottom of the page.



7. Repeat steps 1-6 for each FSx for ONTAP instance that will host vCenter datastores.

Add BlueXP disaster recovery service to your BlueXP account for Amazon EVS

BlueXP disaster recovery is a licensed product offering that must be purchased before it can be used. There are several types of licenses and several ways that you can purchase licenses. A license entitles you to protect a specific amount data for a specific span of time.

For more information about BlueXP disaster recovery licenses, see Set up licensing for BlueXP disaster recovery.

License types

There are two primary license types:

- NetApp offers a 30-day trial license that you can use to evaluate BlueXP disaster recovery using your ONTAP and VMware resources. This license provides 30 days of use for an unlimited amount of protected capacity.
- Purchase a production license if you want DR protection beyond the 30-day trial period. This license can be purchased through the marketplaces of any of NetApp's cloud partners, but for this guide, we recommend that you purchase your **NetApp Intelligent Services** license for BlueXP disaster recovery using the Amazon AWS Marketplace. To learn more about purchasing a license through the Amazon Marketplace, see Subscribe through AWS Marketplace.

Size your disaster recovery capacity needs

Before you purchase your license, you should understand how much ONTAP storage capacity you need to protect. One of the advantages of using NetApp ONTAP storage is the high efficiency with which NetApp stores your data. All data stored in an ONTAP volume — such as VMware datastore hosting VMs — is that the data is stored in a highly efficient manner. ONTAP defaults to three types of storage efficiency when writing data to physical storage: compaction, deduplication, and compression. The net result is storage efficiencies of between 1.5:1 and 4:1 depending on the types of data being stored. In fact, NetApp offers a storage efficiency guarantee for certain workloads.

This can benefit you because BlueXP disaster recovery computes capacity for the purposes of licensing after all ONTAP storage efficiencies are applied. For example, let's say you have provisioned a 100 terabyte (TiB) NFS datastore within vCenter to host 100 VMs that you want to protect using the service. Additionally, let's assume when the data is written to the ONTAP volume, automatically applied storage efficiency techniques result in those VMs consuming only 33TiB (3:1 storage efficiency). BlueXP disaster recovery needs to be licensed only for 33TiB, not 100TiB. This can be a very large benefit to the total cost of ownership for your DR solution when compared to other DR solutions.

Steps

1. To determine how much data is being consumed on each volume hosting a VMware datastore to be protected, determine the on-disk capacity consumption by running the ONTAP CLI command for each volume: `volume show-space -volume < volume name > -vserver < SVM name >`.

   For example:

```
cluster1::> volume show-space
Vserver : vm-nfs-ds1
Volume  : vol0
Feature                                  Used      Used%
--------------------------------      --------     ------
User Data                              163.4MB         3%
Filesystem Metadata                      172KB         0%
Inodes                                  2.93MB         0%
Snapshot Reserve                       292.9MB         5%
Total Metadata                           185KB         0%
Total Used                             459.4MB         8%
Total Physical Used                    166.4MB         3%
```

2. Note the **Total Physical Used** value for each volume. This is the amount of data that BlueXP disaster recovery needs to protect, and it is the value that you will use to determine how much capacity you need to license.

Add sites in BlueXP disaster recovery for Amazon EVS

Before you can protect your VM infrastructure, identify which VMware vCenter clusters are hosting the VMs to be protected and where those vCenters are located. The first step is to create a site to represent the source and destination datacenters. A site is a failure domain or a recovery domain.

You need to create the following:

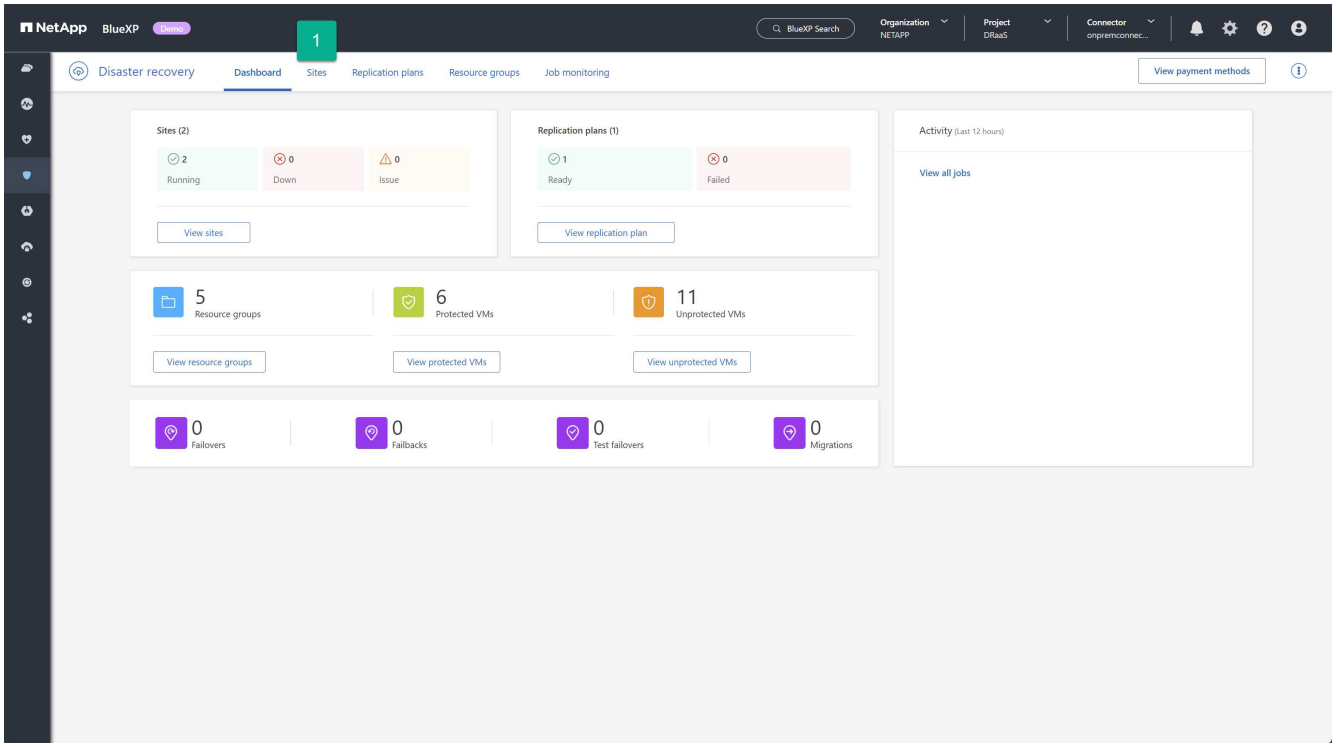
- A site to represent each production datacenter where your production vCenter clusters reside
- A site for your Amazon EVS/Amazon FSx for NetApp ONTAP cloud datacenter

Create on-premises sites

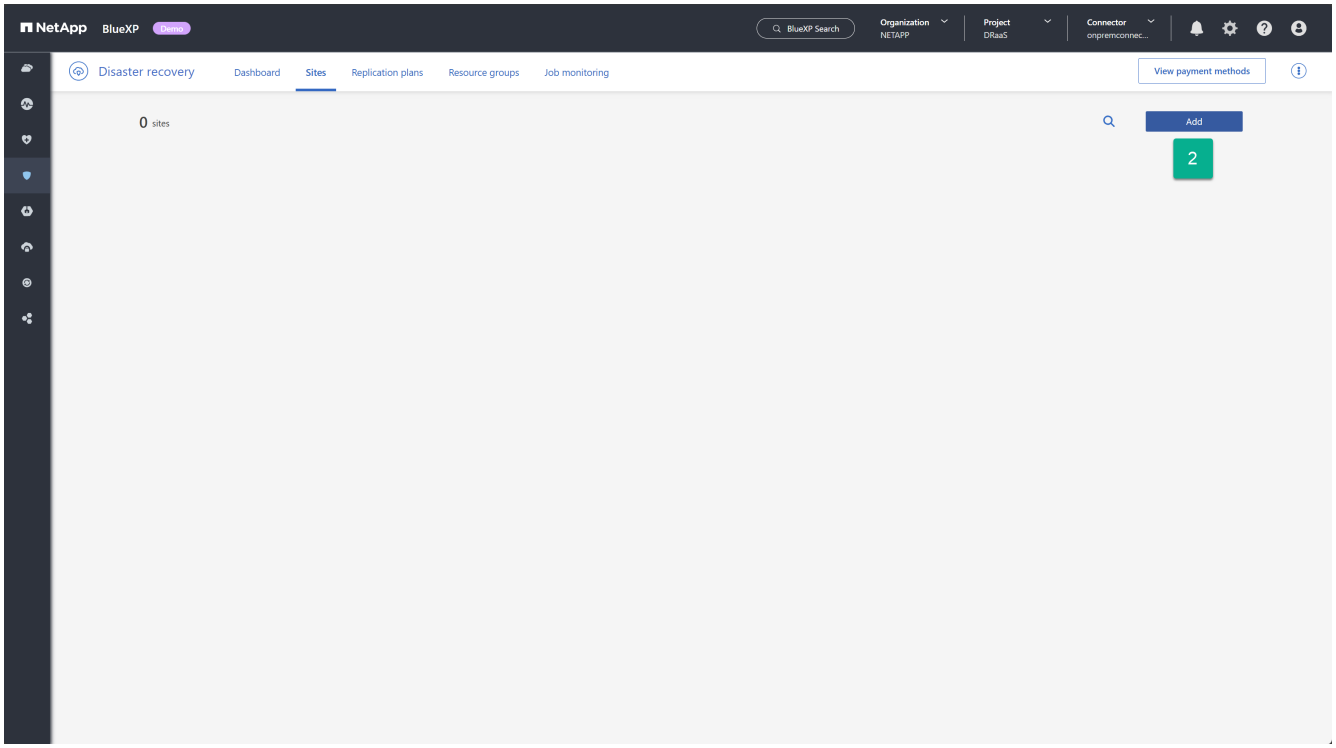
Create a production vCenter site.

Steps

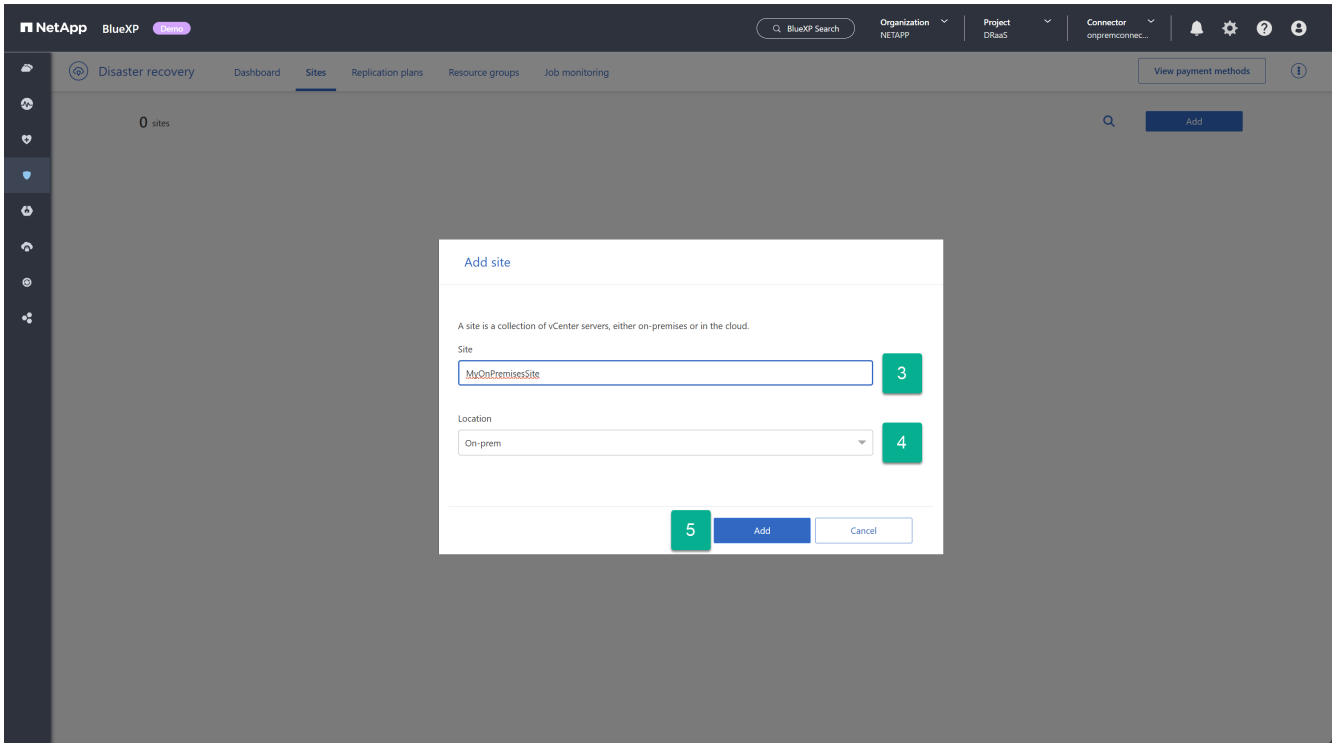
1. From the BlueXP left navigation, select **Protection** > **Disaster Recovery**.
2. From any page in BlueXP disaster recovery, select the **Sites** tab.



3. From the Sites tab, select **Add**.



4. In the Add site dialog box, provide a site name.
5. Select “On-prem” as the Location.
6. Select **Add**.

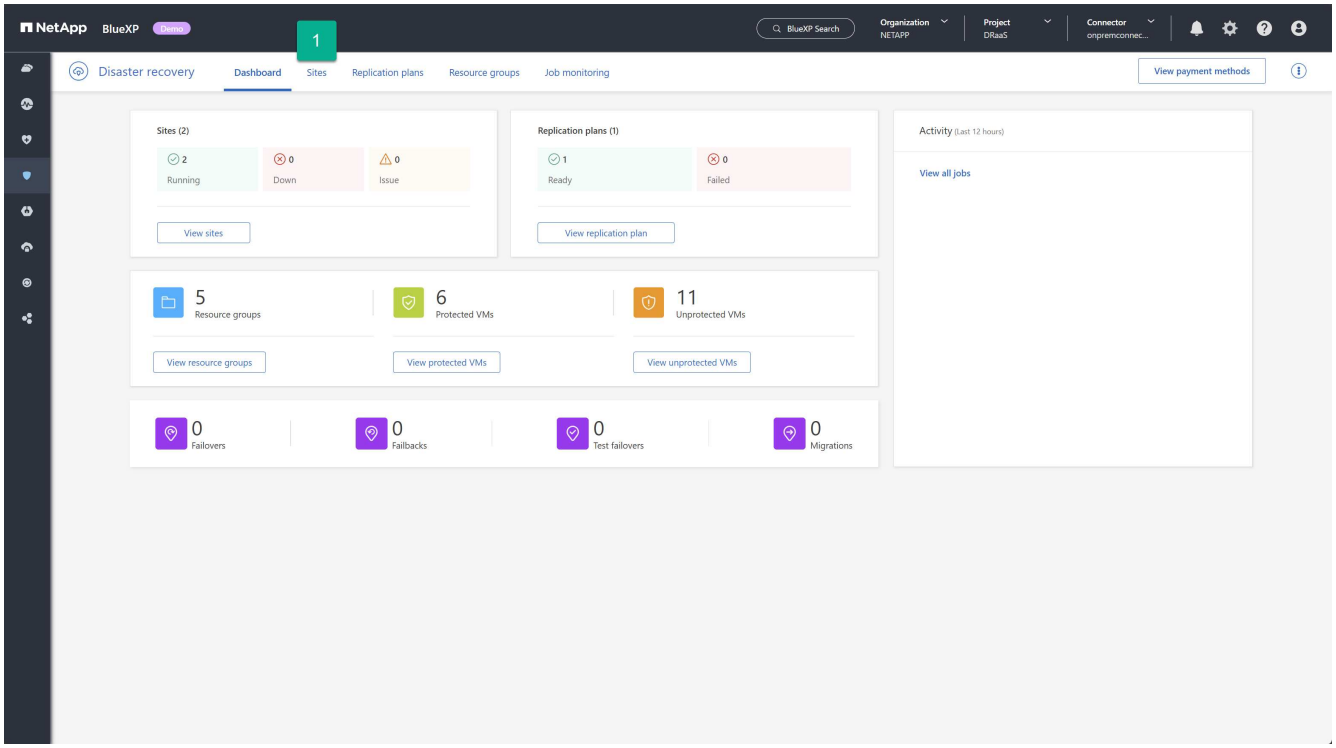


If you have other production vCenter sites, you can add them using the same steps.

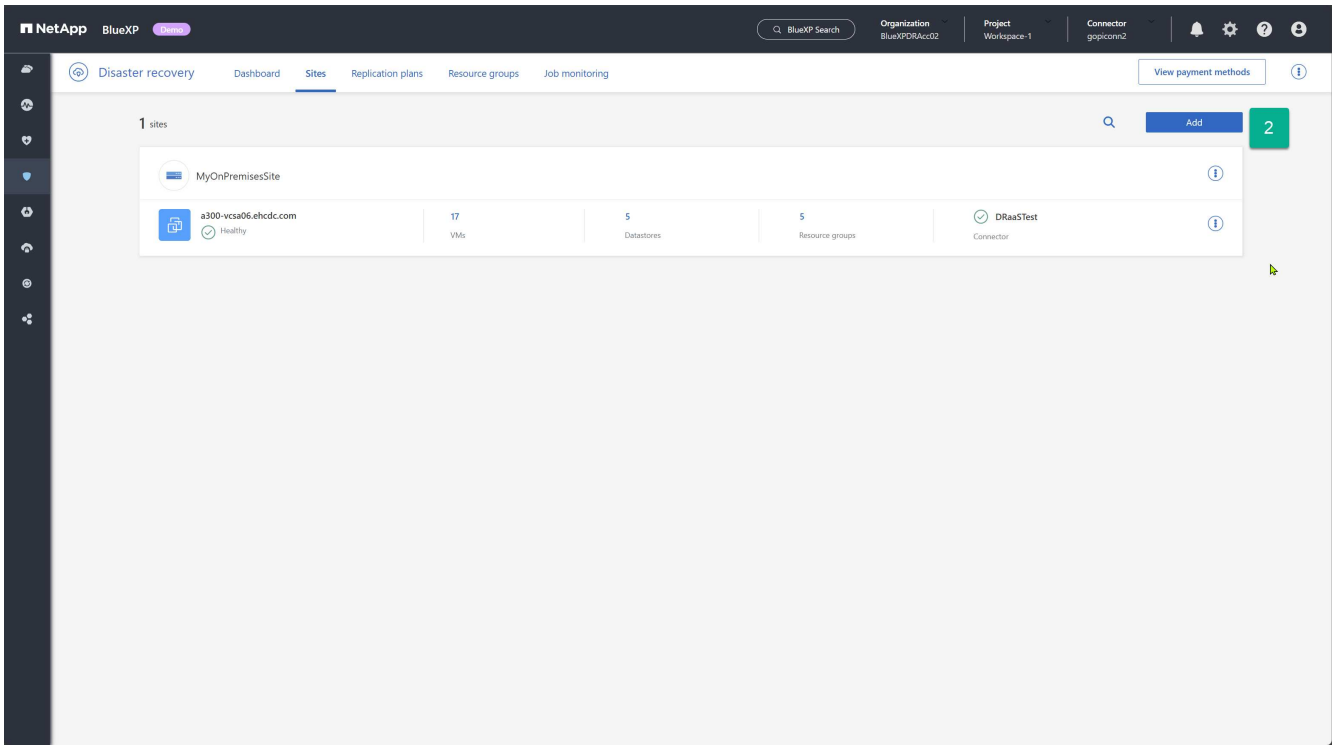
Create Amazon cloud sites

Create a DR site for Amazon EVS using Amazon FSx for NetApp ONTAP storage.

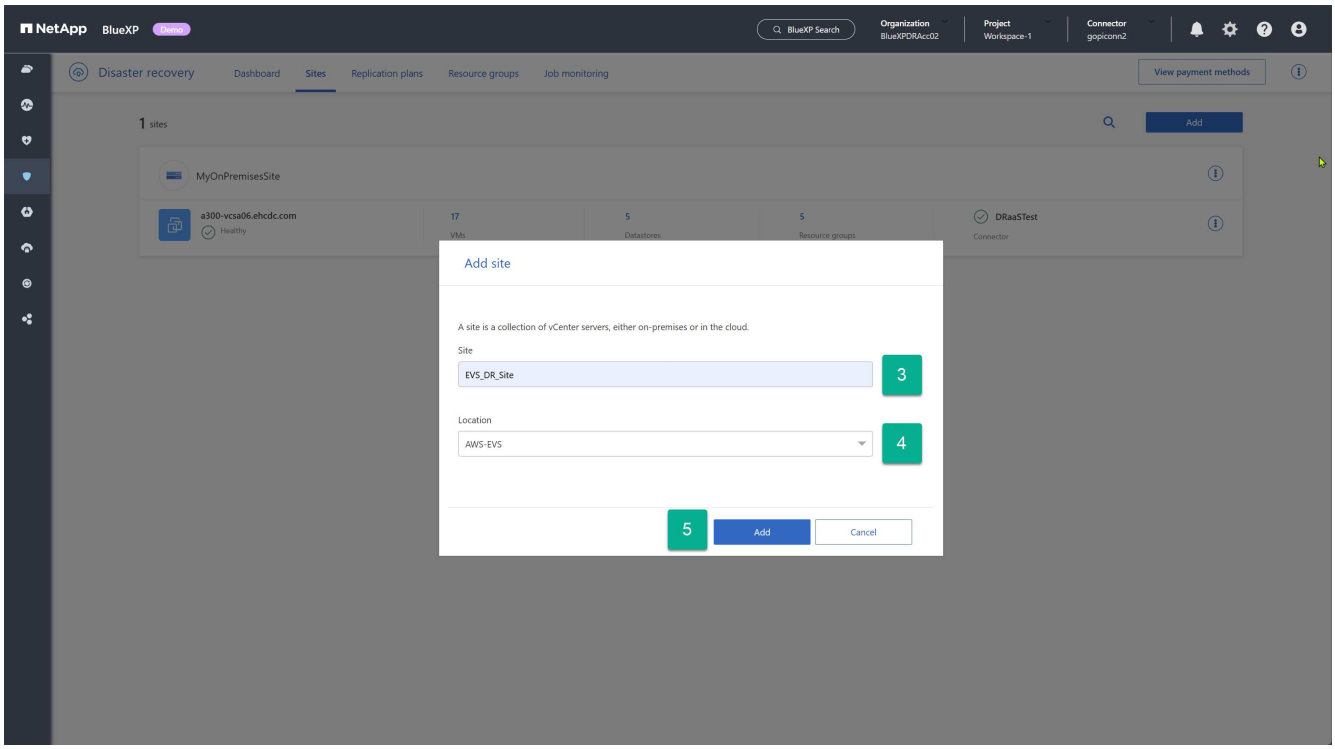
1. From any page in BlueXP disaster recovery, select the **Sites** tab.



2. From the Sites tab, select **Add**.



3. In the Add site dialog box, provide a site name.
4. Select "AWS-EVS" as the Location.
5. Select **Add**.



Result

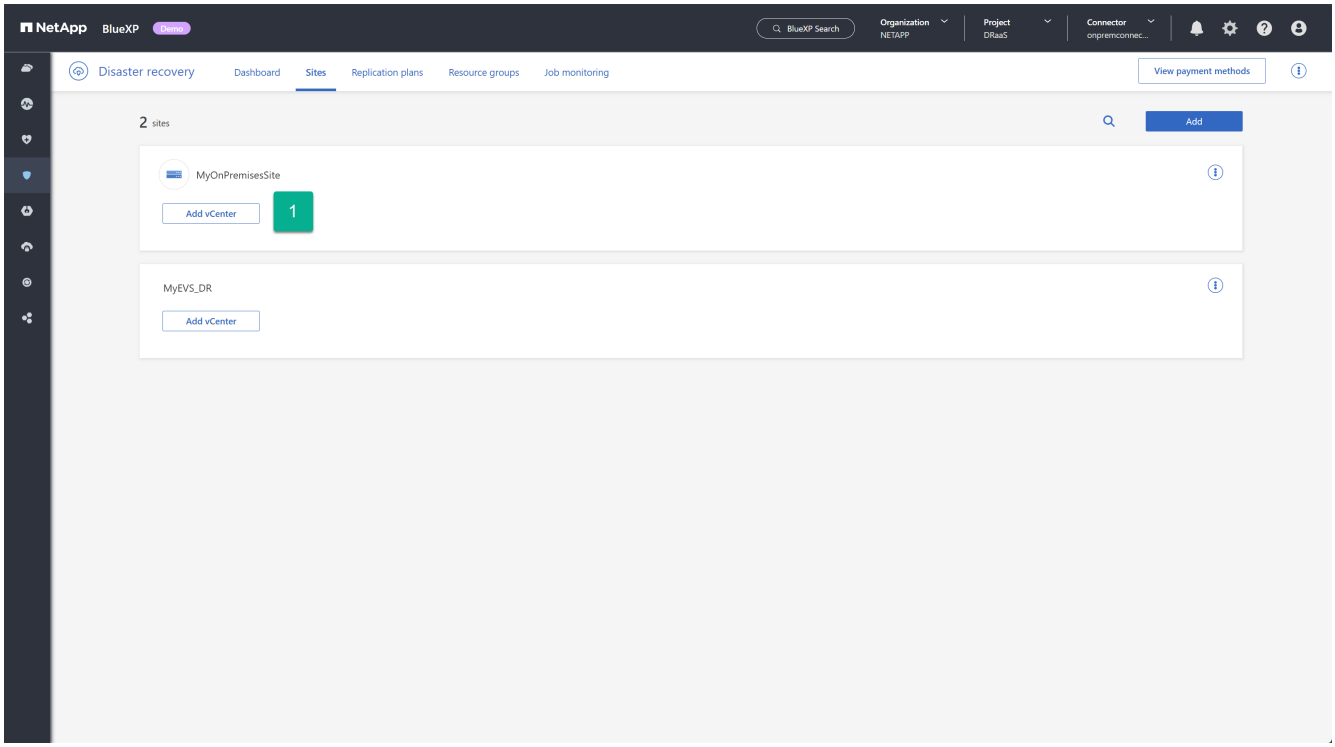
You now have a production (source) site and a DR (destination) site created.

Add on-premises and Amazon EVS vCenter clusters in BlueXP disaster recovery

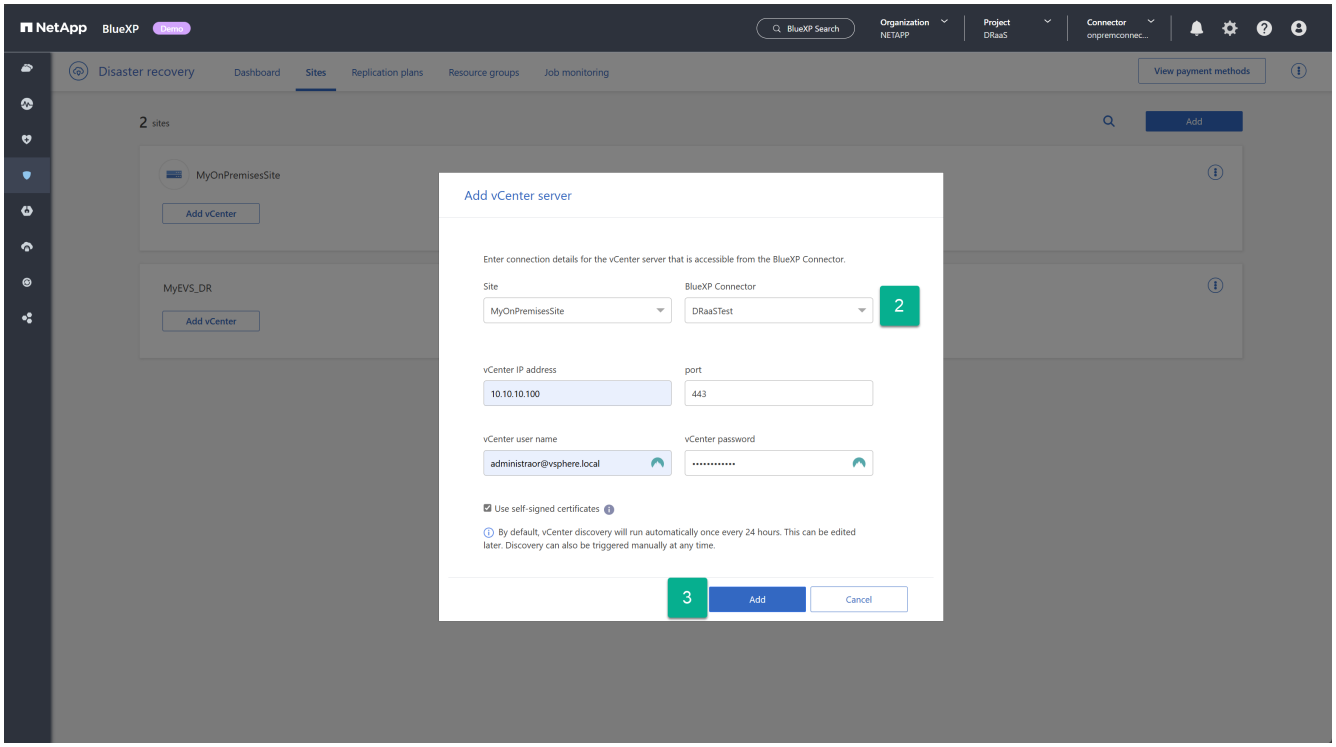
With sites created, you now add your vCenter clusters to each site in BlueXP disaster recovery. When we created each site, we indicated each type of site. This tells BlueXP disaster recovery what type of access is required for the vCenters hosted in each site type. One of the advantages of Amazon EVS is that there is no real differentiation between an Amazon EVS vCenter and an on-premises vCenter. Both require the same connection and authentication information.

Steps to add a vCenter to each site

1. From the **Sites** tab, select **Add vCenter** for the site you want.



2. In the Add vCenter server dialog box, select or provide the following information:
   a. The BlueXP connector hosted within your AWS VPC.
   b. The IP address or FQDN for the vCenter to be added.
   c. If different, change the port value to the TCP port used by your vCenter cluster manager.
   d. The vCenter username for the account created earlier that will be used by BlueXP disaster recovery to manage the vCenter.
   e. The vCenter password for the provided username.
   f. If your company uses an external Certificate Authority (CA) or the vCenter Endpoint Certificate Store to gain access to your vCenters, uncheck the **Use self-signed certificates** checkbox. Otherwise, leave the box checked.
3. Select **Add**.



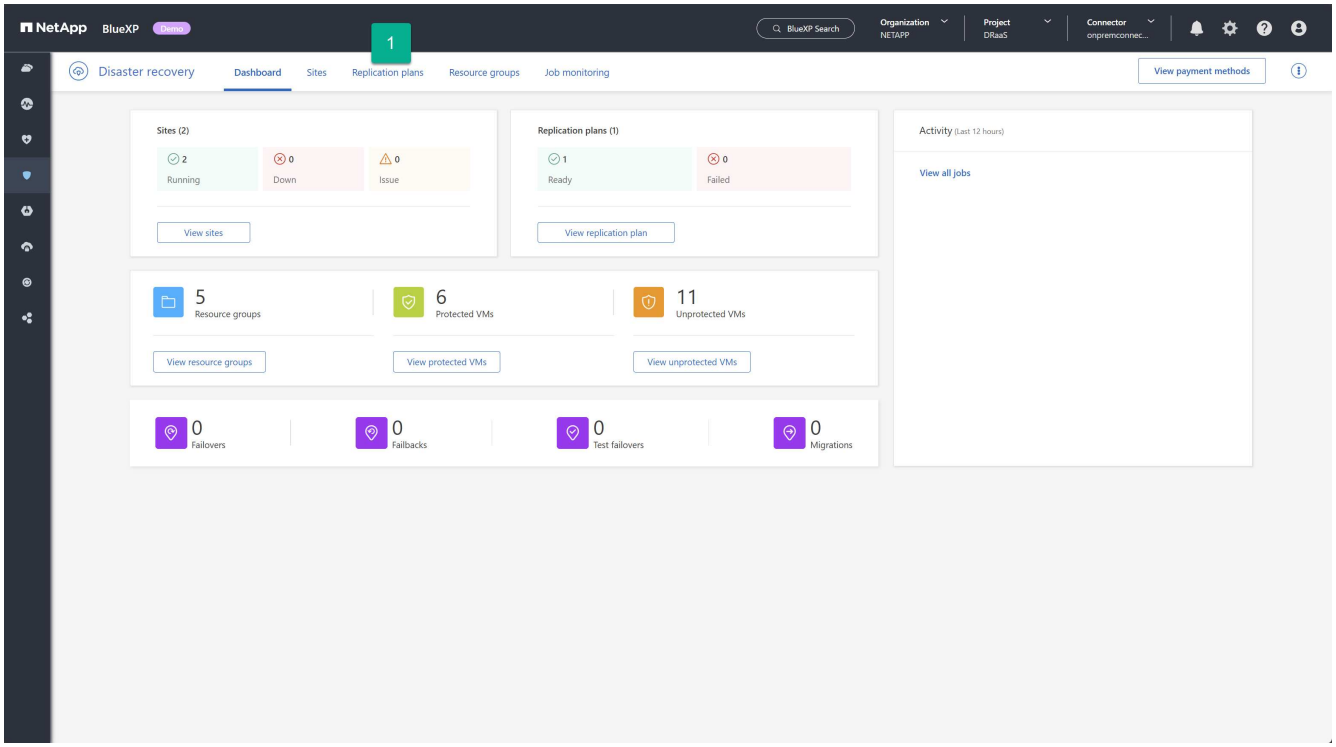
Create replication plans for Amazon EVS

Create replication plans in BlueXP disaster recovery overview

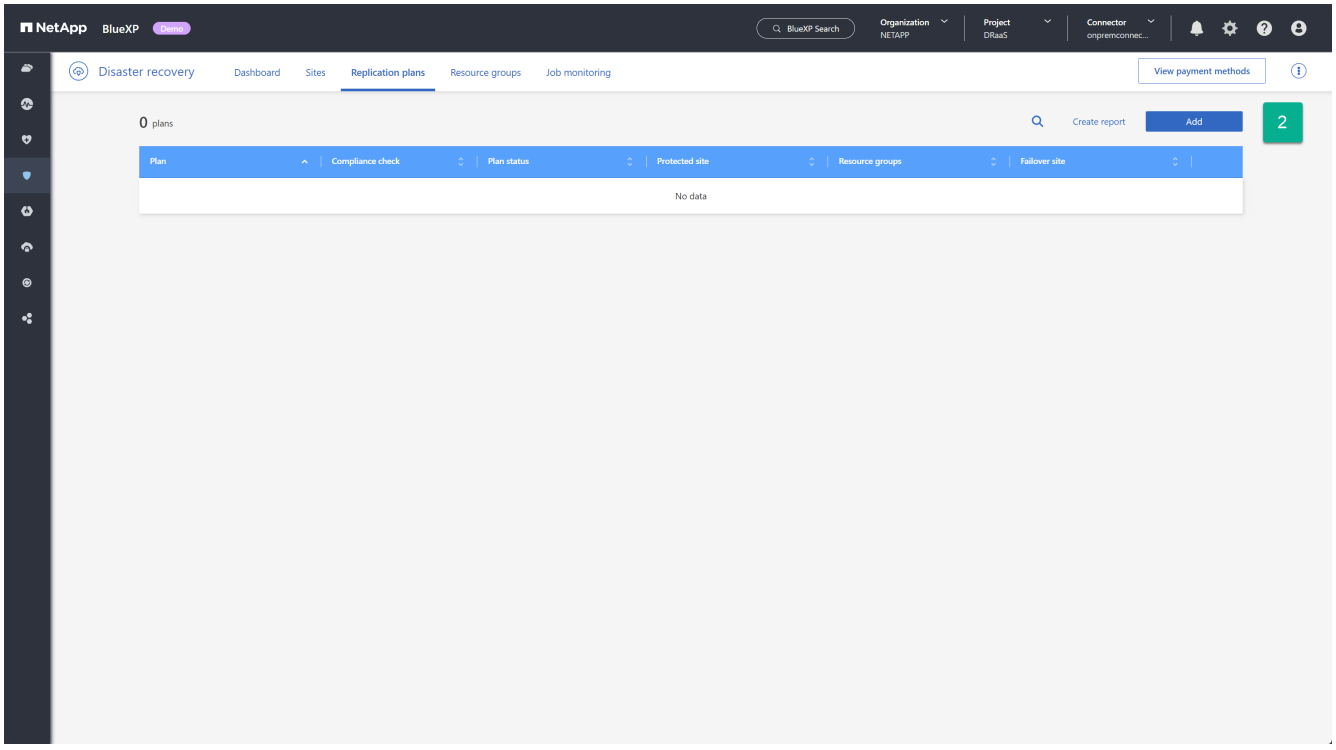
After you have vCenters to protect on the on-premises site and you have an Amazon EVS site configured to use Amazon FSx for NetApp ONTAP that you can use as a DR destination, you can create a replication plan (RP) to protect any set of VMs hosted on the vCenter cluster within your on-premises site.

To start the replication plan creation process:

1. From any BlueXP disaster recovery screen, select the **Replication plans** tab.



2. From the Replication plans screen, select **Add**.



This opens the Create replication plan wizard.

Continue with Create replication plan wizard Step 1.

Create a replication plan: Step 1 - Select vCenters in BlueXP disaster recovery

First, using BlueXP disaster recovery, provide a replication plan name and select the

source and destination vCenters for the replication.

1. Enter a unique name for the replication plan.

   Only alpha-numeric characters and underscores (_) are allowed for replication plan names.

2. Select a source vCenter cluster.
3. Select a destination vCenter cluster.
4. Select **Next**.

Continue with Create replication plan wizard Step 2.

Create a replication plan: Step 2 - Select VM resources in BlueXP disaster recovery

Select the virtual machines to be protected using BlueXP disaster recovery.

There are several ways to select VMs for protection:

- **Select individual VMs**: Clicking on the **Virtual machines** button enables you to select individual VMs to protect. As you select each VM, the service adds it to a default resource group located on the right-hand side of the screen.
- **Select previously created resource groups**: You can create custom resource groups beforehand using the Resource group tab at the top of the BlueXP disaster recovery UI. This is not a requirement as you can use the other two methods to create a resource group as part of the replication plan process. For details, see Create a replication plan.
- **Select entire vCenter datastores**: If you have a lot of VMs to protect with this replication plan, it may not be as efficient to select individual VMs. Because BlueXP disaster recovery uses volume-based SnapMirror replication to protect the VMs, all VMs residing on a datastore will be replicated as part of the volume. In most cases, you should have BlueXP disaster recovery protect and restart any VMs located on the datastore. Use this option to tell the service to add any VMs hosted on a selected datastore to the list of protected VMs.

For this guided instruction, we select the entire vCenter datastore.

Steps to access this page

1. From the **Replication plan** page, continue to the **Applications** section.
2. Review the information in the **Applications** page that opens.

Steps to select the datastore or datastores:

1. Select **Datastores**.
2. Check the checkboxes beside each datastore you want to protect.
3. (Optionally) Rename the resource group to a suitable name by selecting the pencil icon next to the resource group name.
4. Select **Next**.

Continue with Create replication plan wizard Step 3.

Create a replication plan: Step 3 - Map resources in BlueXP disaster recovery

After you have a list of VMs that you want to protect using BlueXP disaster recovery, provide failover mapping and VM configuration information to use during a failover.

You need to map four primary types of information:

- Compute resources
- Virtual networks
- VM reconfiguration
- Datastore mapping

Each VM requires the first three types of information. Datastore mapping is required for each datastore that hosts VMs to be protected.

- The sections with the caution icon () require that you provide mapping information.
- The section marked with the check icon () have been mapped or have default mappings. Review them to make sure that the current configuration meets your requirements.

Steps to access this page

1. From the **Replication plan** page, continue to the **Resource mapping** section.
2. Review the information on the **Resource mapping** page that opens.
3. To open each category of mappings required, select the down arrow (**v**) beside the section.

Compute resource mapping

Because a site could host multiple virtual datacenters and multiple vCenter clusters, you need to identify which vCenter cluster to recover VMs on in the event of a failover.

Steps to map compute resources

1. Select the virtual datacenter from the list of datacenters located at the DR site.
2. Select the cluster to host the datastores and VMs from the list of clusters within the selected virtual datacenter.
3. (Optional) Select a target host in the target cluster.

   This step is not required because BlueXP disaster recovery selects the first host added to the cluster in vCenter. At that point, the VMs either continue to run on that ESXi host or VMware DRS moves the VM to a different ESXi host as needed based on DRS rules configured.

4. (Optional) Provide the name of a top-level vCenter folder to place the VM registrations into.

   This is for your organizational needs and is not required.

Map virtual network resources

Each VM can have one or more virtual NICs connected to virtual networks within the vCenter network infrastructure. To ensure that each VM is properly connected to the desired networks upon restarting in the DR site, identify which DR site virtual networks to connect these VMs. Do this by mapping each virtual network in the on-premises site to an associated network on the DR site.

Select which destination virtual network to map each source virtual network

1. Select the Target segment from the drop-down list.
2. Repeat the previous step for each source virtual network listed.

Define options for VM reconfiguration during failover

Each VM might require modifications to work correctly in the DR vCenter site. The Virtual machines section enables you to provide the necessary changes.

By default, BlueXP disaster recovery uses the same settings for each VM as used on the source on-premises site. This assumes that VMs will use the same IP address, virtual CPU, and virtual DRAM configuration.

Network reconfiguration

Supported IP address types are static and DHCP. For static IP addresses, you have the following Target IP settings:

- **Same as source**: As the name suggests, the service uses the same IP address on the destination VM that was used on the VM at the source site. This requires that you configure the virtual networks that were mapped in the previous step for the same subnet settings.
- **Different from source**: The service provides a set of IP address fields for each VM that must be configured for the appropriate subnet used on the destination virtual network, which you mapped in the previous section. For each VM you must provide an IP address, subnet mask, DNS, and default gateway values. Optionally, use the same subnet mask, DNS, and gateway settings for all VMs to simplify the process when all VMs attach to the same subnet.
- **Subnet mapping**: This option reconfigures each VM's IP address based on the destination virtual network's CIDR configuration. To use this feature, ensure that each vCenter's virtual networks have a defined CIDR setting within the service, as changed in the vCenter information in the Sites tab.

After you configure subnets, Subnet mapping uses the same unit component of the IP address for both source and destination VM configuration, but replaces the subnet component of the IP address based on the provided CIDR information. This feature also requires that both the source and destination virtual networks have the same IP address class (the `/xx` component of the CIDR). This ensures that there are enough IP addresses available at the destination site to host all of the protected VMs.

For this EVS setup, we assume that the source and destination IP configurations are the same and do not require any additional reconfiguration.

Make changes to network settings reconfiguration

1. Select the type of IP addressing to use for failed over VMs.
2. (Optional) Provide a VM renaming scheme for restarted VMs by providing an optional prefix and suffix value.

VM compute resource reconfiguration

There are several options for reconfiguring VM compute resources. BlueXP disaster recovery supports changing the number of virtual CPUs, the amount of virtual DRAM, and the VM name.

Specify any VM configuration changes

1. (Optional) Modify the number of virtual CPUs each VM should use. This might be needed if your DR vCenter cluster hosts do not have as many CPU cores as the source vCenter cluster.
2. (Optional) Modify the amount of virtual DRAM each VM should use. This might be needed if your DR vCenter cluster hosts do not have as much physical DRAM as the source vCenter cluster hosts.

Boot order

BlueXP disaster recovery supports an ordered restart of VMs based on a boot order field. The Boot order field indicates how the VMs in each resource group start. Those VMs with the same value in the Boot order field boot in parallel.

Modify the boot order settings

1. (Optionally) Modify the order you would like your VMs to be restarted. This field takes any numeric value. BlueXP disaster recovery tries to restart VMs that have the same numeric value in parallel.
2. (Optionally) Provide a delay to be used between each VM restart. The time is injected after this VM's restart has completed and before the VM(s) with the next higher boot order number. This number is in minutes.

Custom guest OS operations

BlueXP disaster recovery supports performing some guest OS operations for each VM:

- BlueXP disaster recovery can take application-consistent backups of VMs for VMs running Oracle databases and Microsoft SQL Server databases.
- BlueXP disaster recovery can execute custom defined scripts suitable for the guest OS for each VM. Executing such scripts requires user credentials acceptable to the guest OS with ample privileges to execute the operations listed in the script.

Modify each VM's custom guest OS operations

1. (Optional) Check the **Create application consistent replicas** checkbox if the VM is hosting an Oracle or SQL Server database.
2. (Optional) To take custom actions within the guest OS as part of the startup process, upload a script for any VMs. To run a single script in all VMs, use the checkbox highlighted and complete the fields.
3. Certain configuration changes require user credentials with adequate permissions to perform the operations. Provide credentials in the following cases:
    - A script will be executed within the VM by the guest OS.
    - An application-consistent snapshot needs to be performed.

Map datastores

The final step in creating a replication plan is identifying how ONTAP should protect the datastores. These settings define the replication plans recovery point objective (RPO), how many backups should be maintained, and where to replicate each vCenter datastore's hosting ONTAP volumes.

By default, BlueXP disaster recovery manages its own snapshot replication schedule; however, optionally, you can specify that you would like to use the existing SnapMirror replication policy schedule for datastore protection.

In addition, you can optionally customize which data LIFs (logical interfaces) and export policy to use. If you don't provide these settings, BlueXP disaster recovery uses all data LIFs associated with the appropriate protocol (NFS, iSCSI, or FC) and uses the default export policy for NFS volumes.

To configure datastore (volume) mapping

1. (Optional) Decide whether you want to use an existing ONTAP SnapMirror replication schedule or have BlueXP disaster recovery manage protection of your VMs (default).
2. Provide a starting point for when the service should start taking backups.
3. Specify how often the service should take a backup and replicate it to the DR destination Amazon FSx for NetApp ONTAP cluster.
4. Specify how many historical backups should be retained. The service maintains the same number of backups on the source and destination storage cluster.
5. (Optional) Select a default logical interface (data LIFs) for each volume. If none is selected, all the data LIFs in the destination SVM that support the volume access protocol are configured.
6. (Optional) Select an export policy for any NFS volumes. If not selected, the default export policy is used

Continue with Create replication plan wizard Step 4.

Create a replication plan: Step 4 - Verify settings in BlueXP disaster recovery

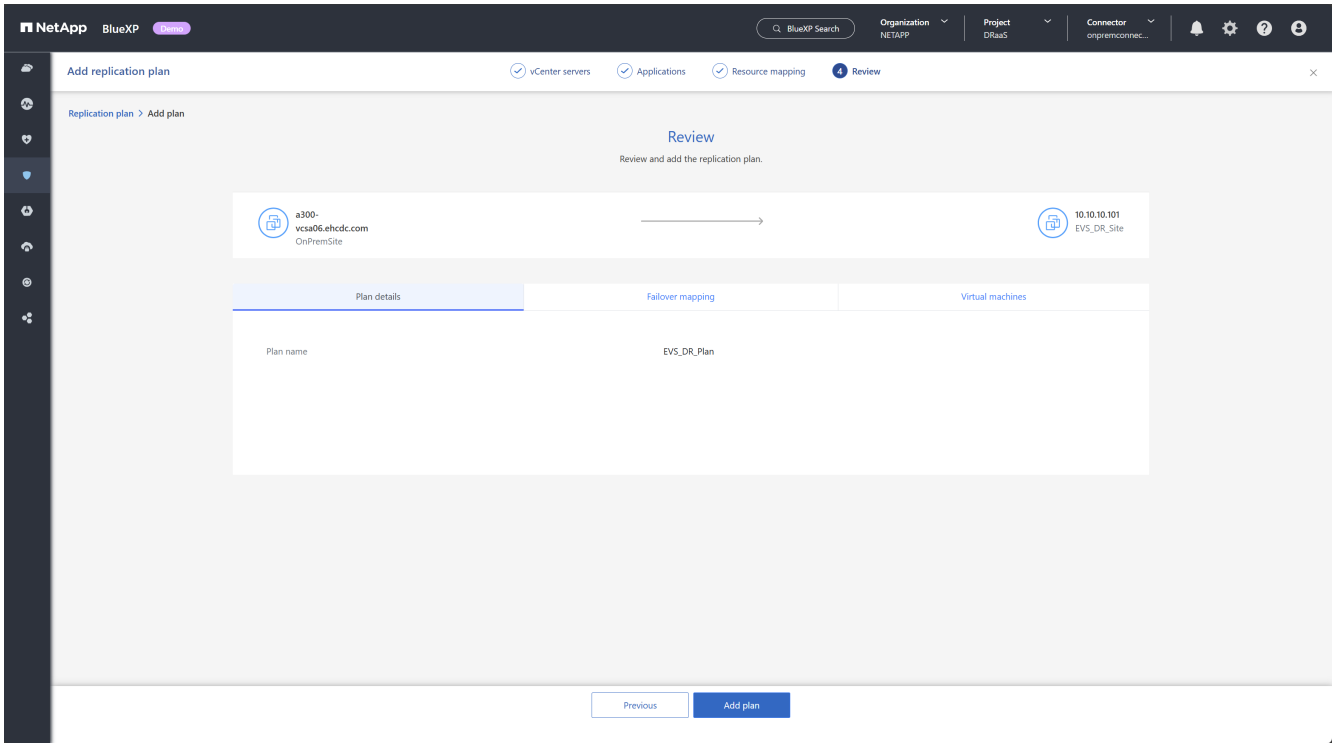
After you add the replication plan information in BlueXP disaster recovery, verify that the information you entered is correct.

Steps

1. Select **Save** to review your settings before activating the replication plan.

   You can select each tab to review the settings and make changes on any tab by selecting the pencil icon.

   Replication plan settings review



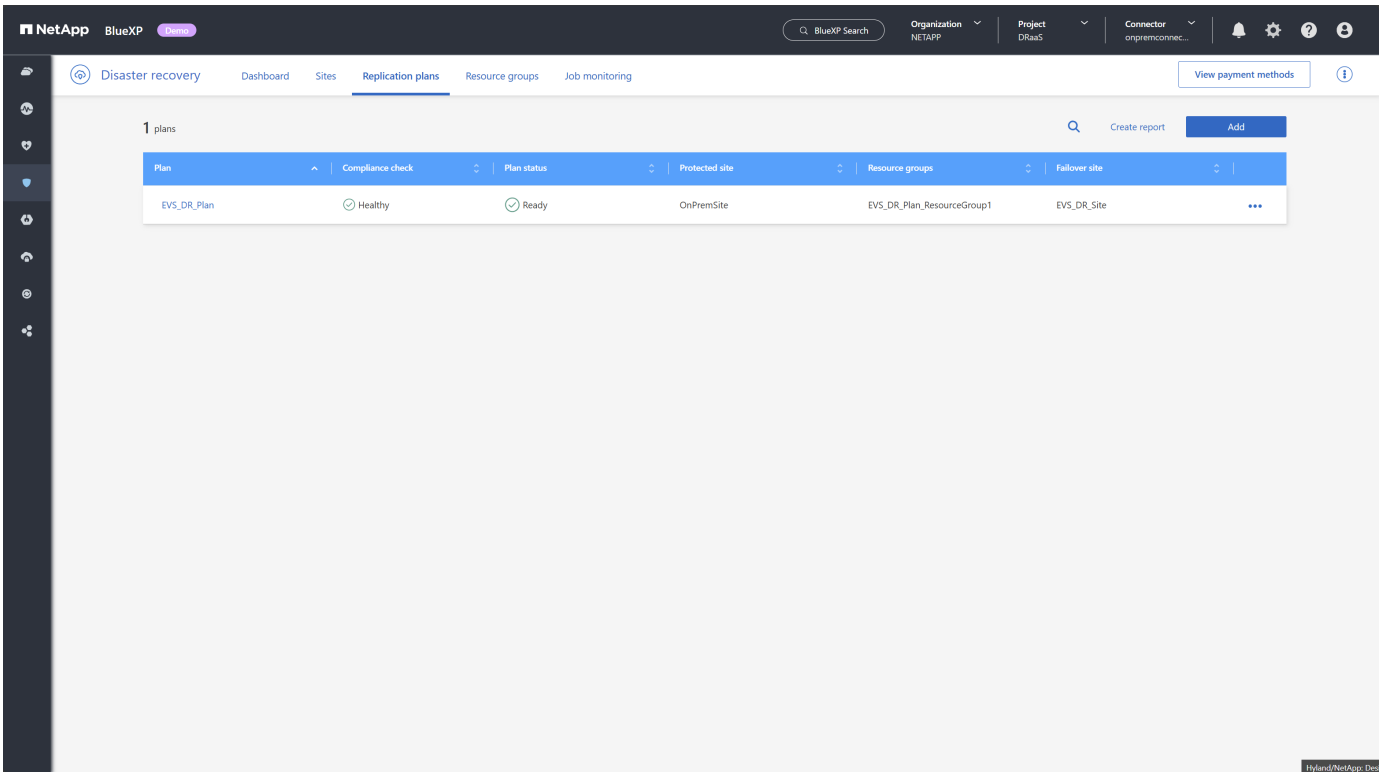
2. When you are satisfied that all settings are correct, select **Add plan** at the bottom of the screen.

Continue with Verify the replication plan.

Verify that everything is working in BlueXP disaster recovery

After you add the replication plan in BlueXP disaster recovery, you return to the Replication plans page where you can view your replication plans and their status. You should verify that the replication plan is in the **Healthy** state. If it is not, you should check the status of the replication plan and correct any issues before proceeding.

Figure: Replication plans page



BlueXP disaster recovery performs a series of tests to verify that all the components (ONTAP cluster, vCenter clusters, and VMs) are accessible and in the proper state for the service to protect the VMs. This is called a compliance check, and it is run on a regular basis.

From the Replication plans page, you can see the following information:

- Status of the last compliance check
- The replication plan's replication state
- The name of the protected (source) site
- The list of resource groups protected by the replication plan
- The name of the failover (destination) site

Perform replication plan operations with BlueXP disaster recovery

Use BlueXP disaster recovery with Amazon EVS and Amazon FSx for NetApp ONTAP to perform the following operations: failover, test failover, refresh resources, migrate, take a snapshot now, disable/enable replication plan, clean up old snapshots, reconcile snapshots, delete replication plan, and edit schedules.

Fail over

The primary operation that you might need to perform is the one you hope never happens: failing over to the DR (destination) datacenter in the event of a catastrophic failure at the production on-premises site.

Failover is a manually initiated process.

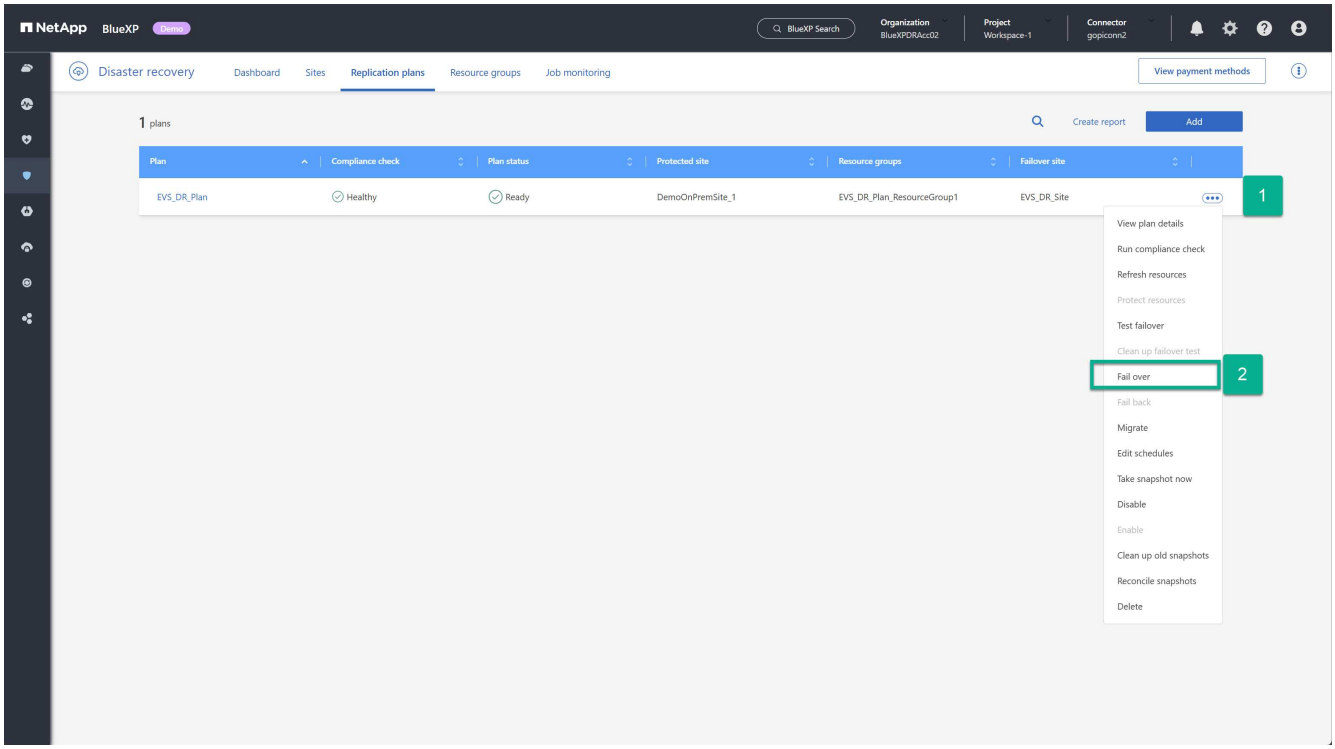
Steps to access the failover operation

1. From the BlueXP left navigation, select **Protection** > **Disaster Recovery**.

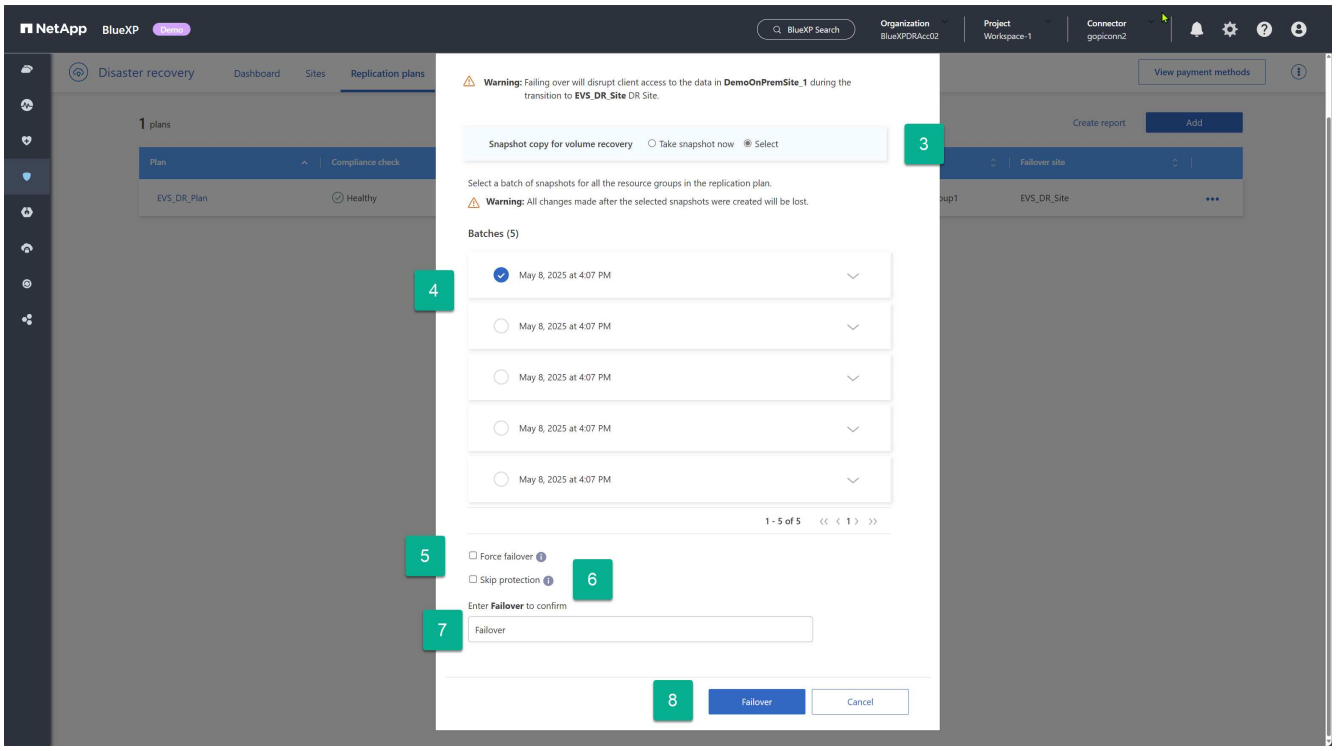
2. From the BlueXP disaster recovery menu, select **Replication plans**.

Steps to perform a failover

1. From the Replication plans page, select the replication plan's Actions option ⋯.
2. Select **Fail over**.



3. If the production (protected) site is not accessible, select a previously created snapshot as your recovery image. To do this, select **Select**.
4. Select the backup to be used for the recovery.
5. (Optional) Select whether you want BlueXP disaster recovery to force the failover process regardless of the state of the replication plan. This should only be done as a last resort.
6. (Optional) Select whether you want BlueXP disaster recovery to automatically create a reverse protection relationship after the production site has been recovered.
7. Type the word "Failover" to verify that you would like to proceed.
8. Select **Failover**.



Test failover

A test failover is similar to a failover except for two differences.

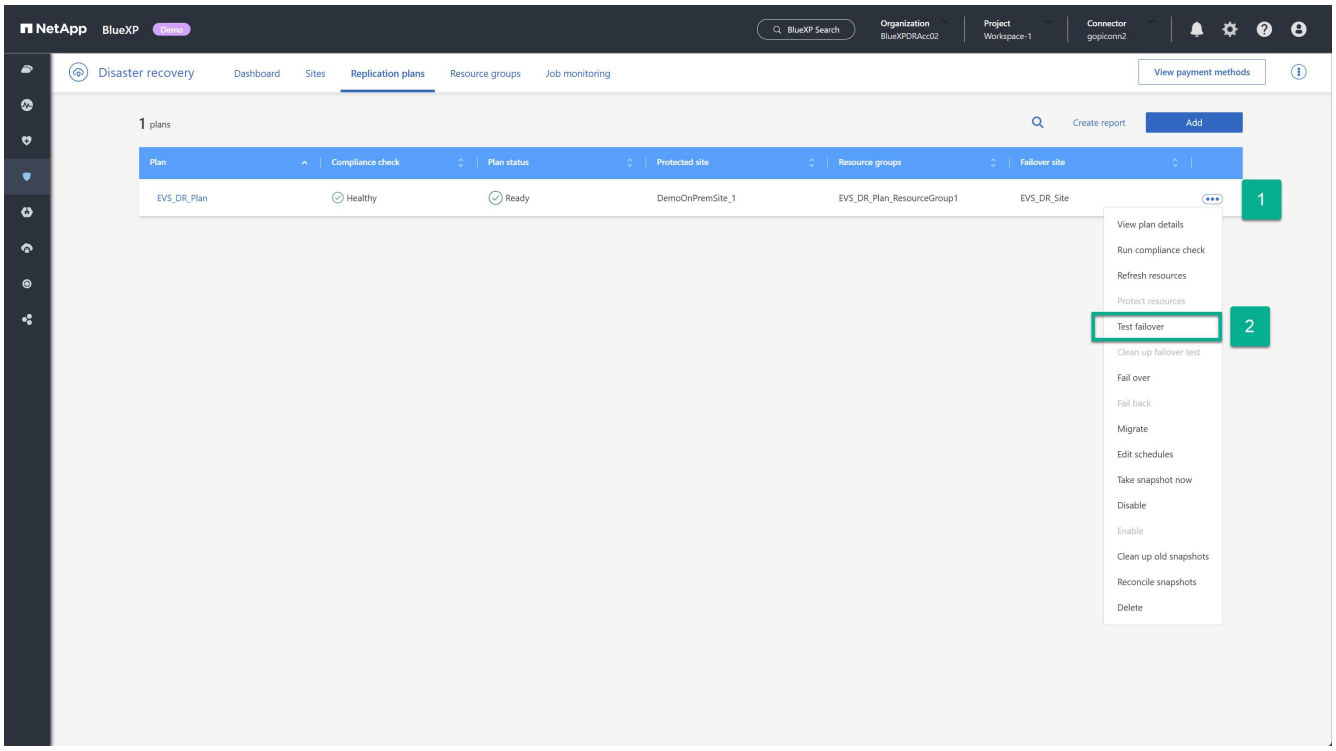
- The production site is still active and all VMs are still operating as expected.
- BlueXP disaster recovery protection of the production VMs continues.

This is accomplished by using native ONTAP FlexClone volumes at the destination site. To learn more about test failover, see Fail over applications to a remote site | NetApp Documentation.

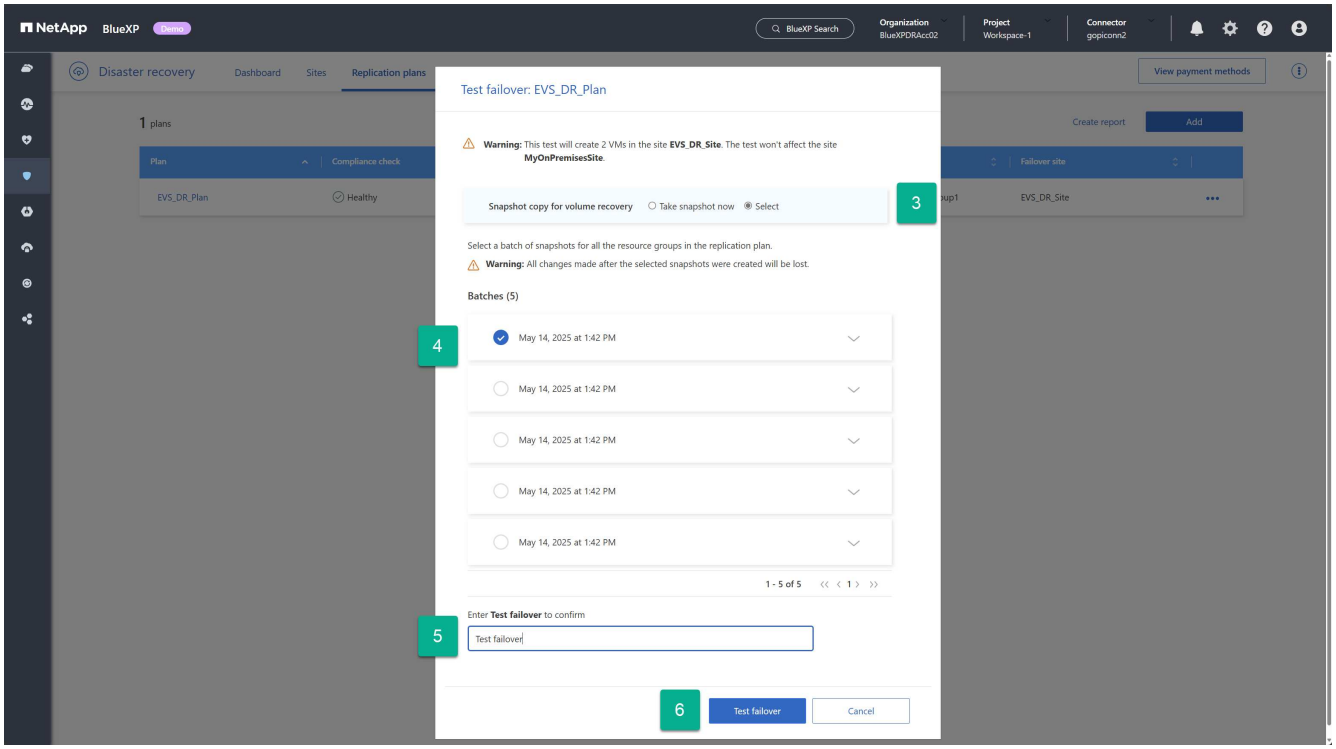
The steps for executing a test failover are identical to those used to execute a real failover except that you use the Test failover operation on the replication plan's context menu.

Steps

1. Select the replication plan's Actions option •••.
2. Select **Test failover** from the menu.



3. Decide if you want get the latest state of the production environment (Take snapshot now) or use a previously created replication plan backup (Select)
4. If you chose a previously created backup, then select the backup to be used for the recovery.
5. Type the word “Test failover” to verify that you would like to proceed.
6. Select **Test failover**.

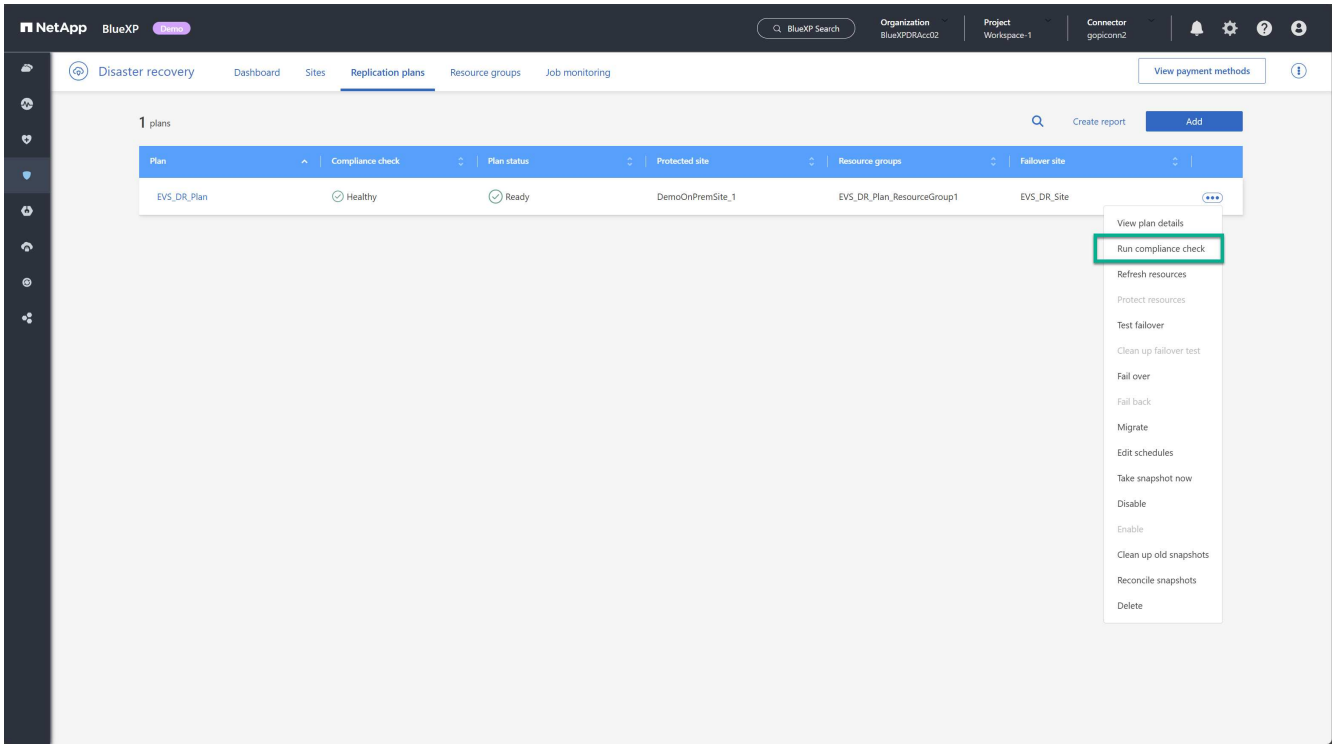


Run a compliance check

Compliance checks are run every three hours, by default. At any time, you might want to manually run a compliance check.

Steps

1. Select the **Actions** option ••• next to the replication plan.
2. Select the **Run compliance check** option from the replication plan's Actions menu:



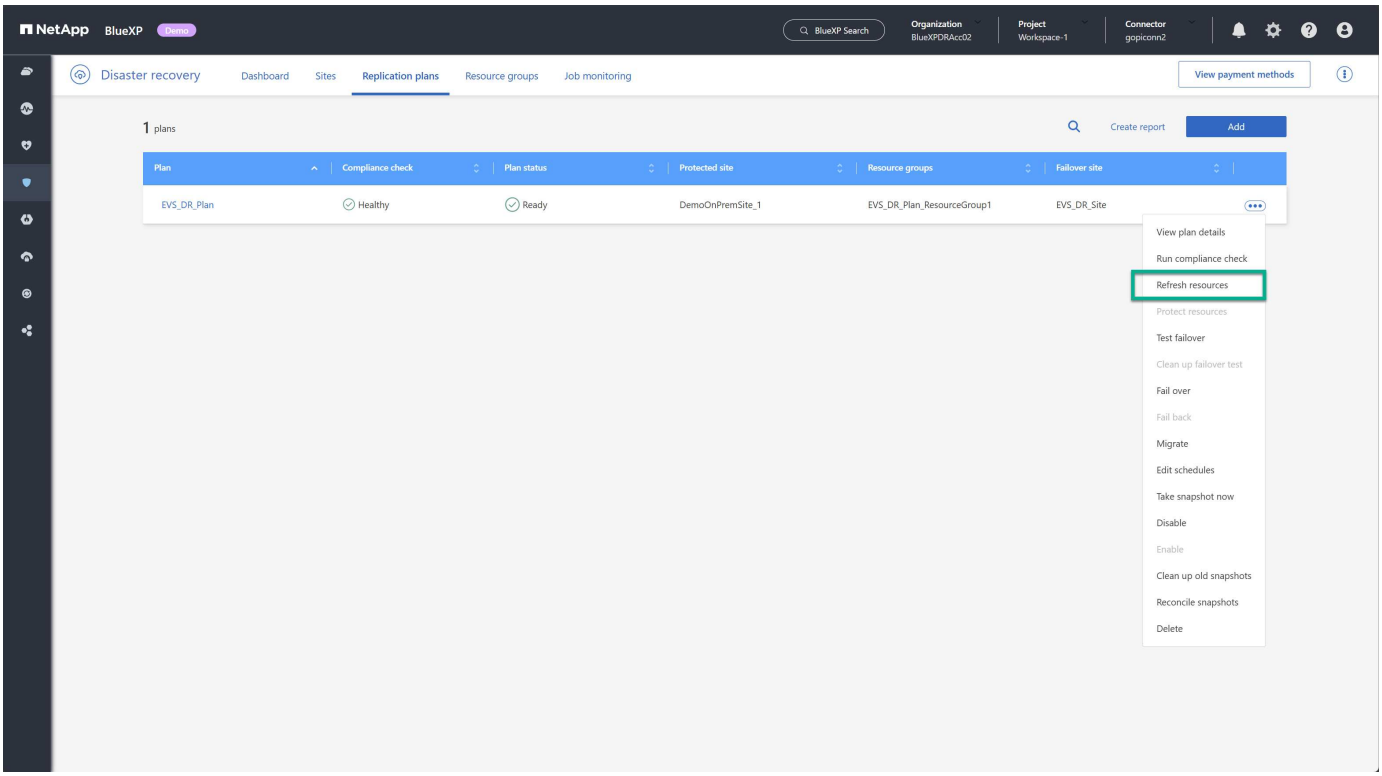
3. To change how often BlueXP disaster recovery automatically runs compliance checks, select **Edit schedules** option from the replication plan's Actions menu.

Refresh resources

Any time you make changes to your virtual infrastructure — such as adding or deleting VMs, adding or deleting datastores, or moving VMs between datastores — you need to perform a refresh of the impacted vCenter clusters in BlueXP disaster recovery service. The service does this automatically once every 24 hours by default, but a manual refresh ensures that the latest virtual infrastructure information is available and taken into account for DR protection.

There are two instances where a refresh is necessary:

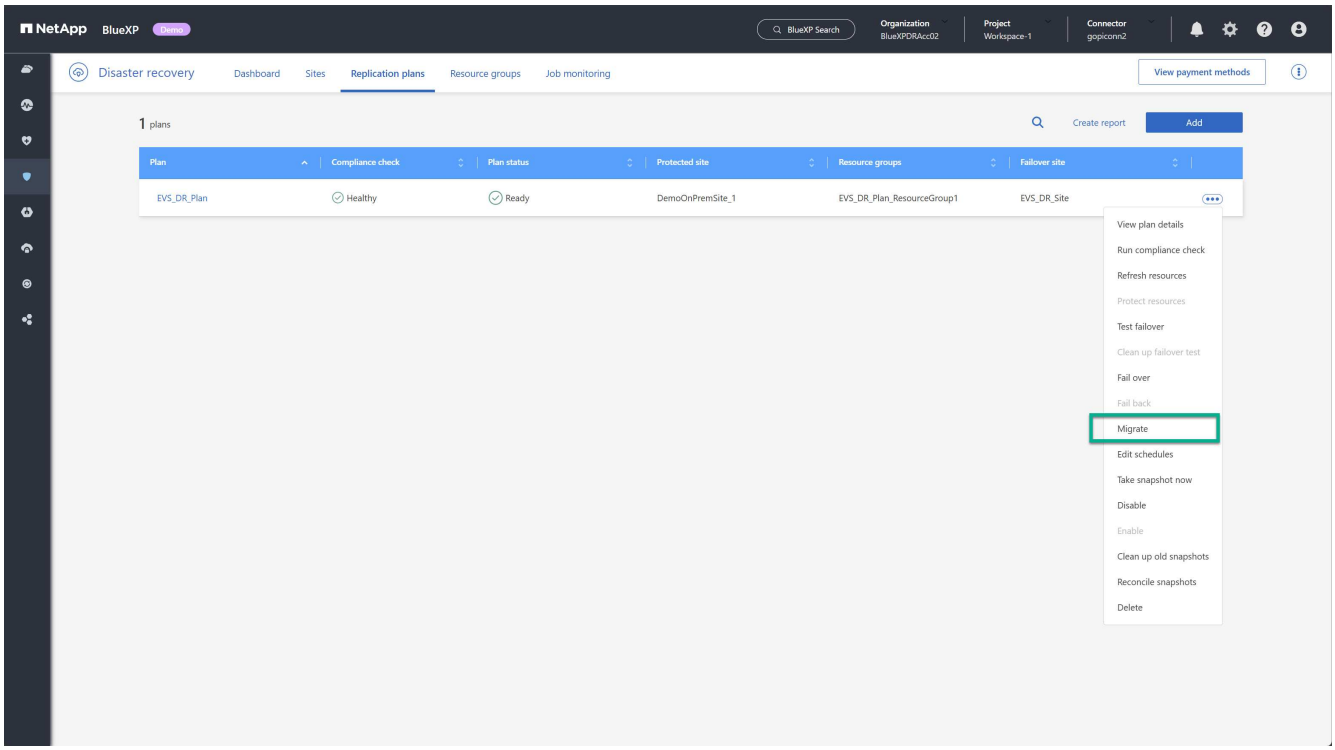
- vCenter refresh: Perform a vCenter refresh anytime VMs are added or deleted from or moved out of a vCenter cluster:
- Replication plan refresh: Perform a replication plan refresh anytime a VM is moved between datastores in the same source vCenter cluster.



Migrate

While BlueXP disaster recovery is primarily used for disaster recovery use cases, it can also enable one-time moves of a set of VMs from the source site to the destination site. This could be for a concerted migration to cloud project or it could be used for disaster avoidance — such as bad weather, political strife, or other potential temporary catastrophic events.

1. Select the **Actions** option ••• next to the replication plan.
2. To move the VMs in a replication plan to the destination Amazon EVS cluster, select **Migrate** from the replication plan's Actions menu:

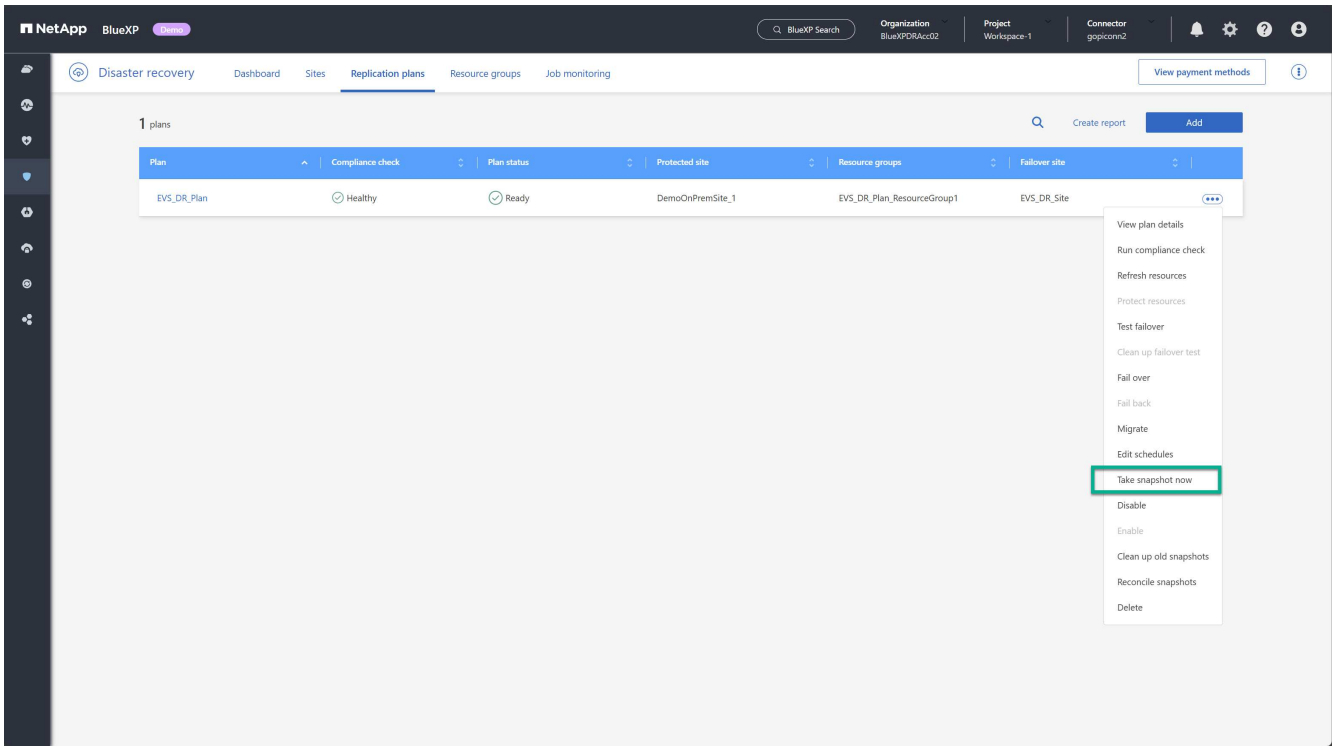


3. Enter information in the Migrate dialog box.

Take a snapshot now

At any time, you can take an immediate snapshot of the replication plan. This snapshot is included in the BlueXP disaster recovery considerations set by the replication plan's snapshot retention count.

1. Select the **Actions** option ••• next to the replication plan.
2. To take an immediate snapshot of the replication plan's resources, select **Take snapshot now** on the replication plan's Actions menu:

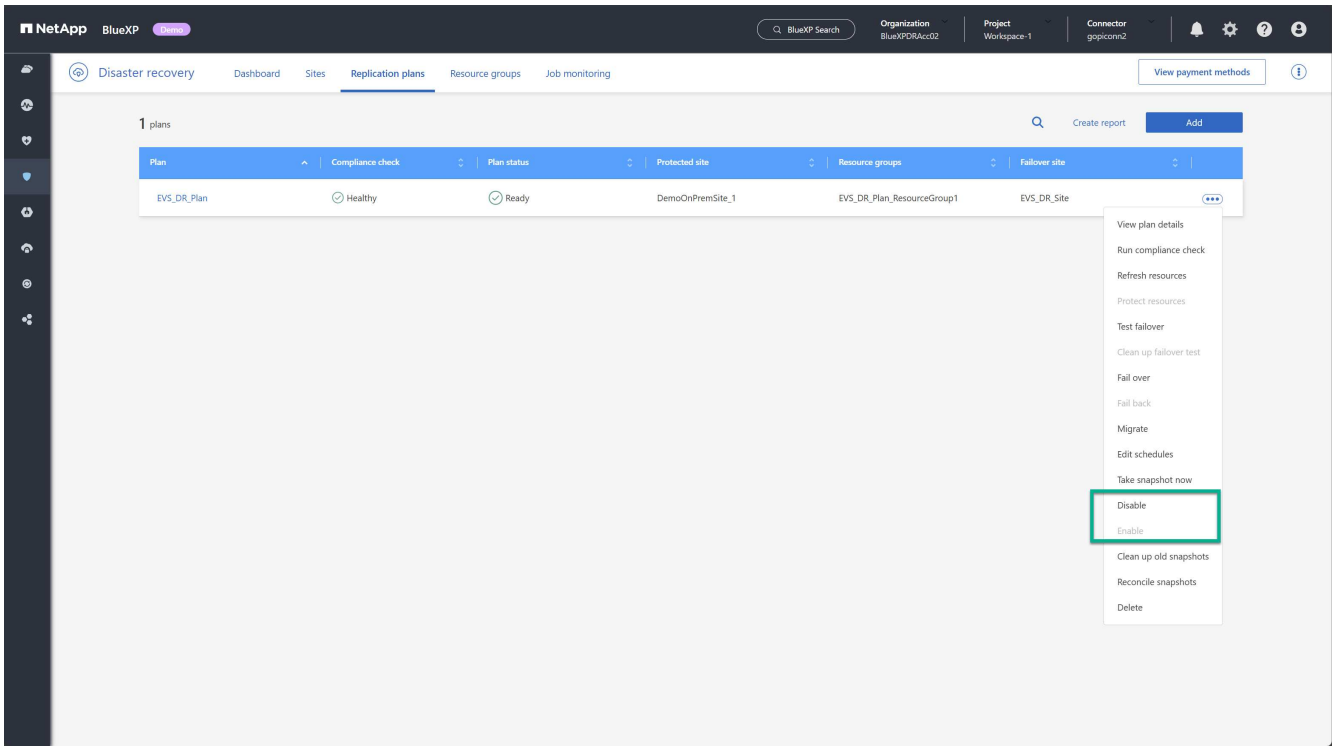


Disable or enable replication plan

You might need to temporarily stop the replication plan to perform some operation or maintenance that could impact the replication process. The service provides a method to stop and start replication.

1. To temporarily stop replication, select **Disable** on the replication plan's Actions menu.
2. To restart replication, select **Enable** on the replication plan's Actions menu.

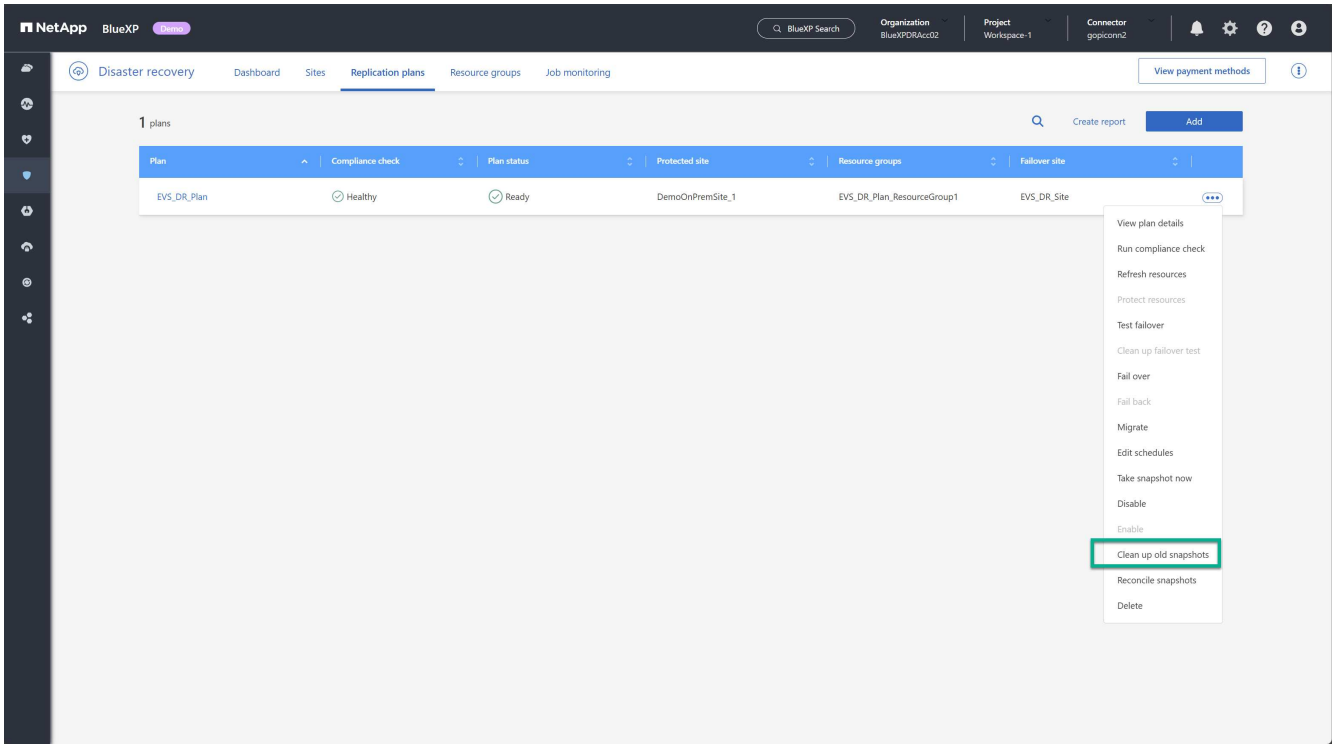
   When the replication plan is active, the **Enable** command is grayed out. When the replication plan is disabled, the **Disable** command is grayed out.



Clean up old snapshots

You might want to clean up older snapshots that have been retained on the source and destination sites. This can happen if the replication plan's snapshot retention count is altered.

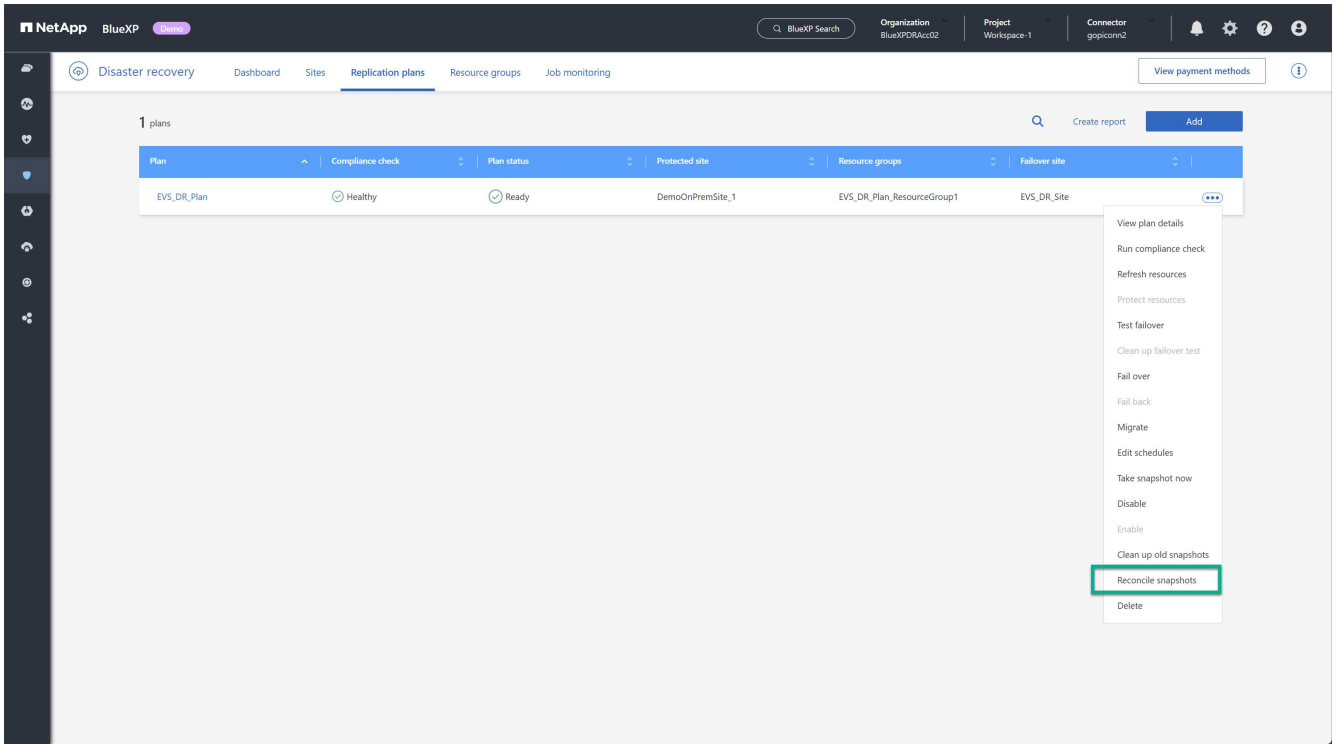
1. Select the **Actions** option ••• next to the replication plan.
2. To remove these older snapshots manually, select **Clean up old snapshots** from the replication plan's Actions menu.



Reconcile snapshots

Because the service orchestrates ONTAP volume snapshots, it is possible for an ONTAP storage administrator to directly delete snapshots using either ONTAP System Manager, the ONTAP CLI, or the ONTAP REST APIs without the service's knowledge. The service automatically deletes any snapshots on the source that are not on the destination cluster automatically every 24 hours. However, you can perform this on demand. This feature enables you to ensure that the snapshots are consistent across all sites.

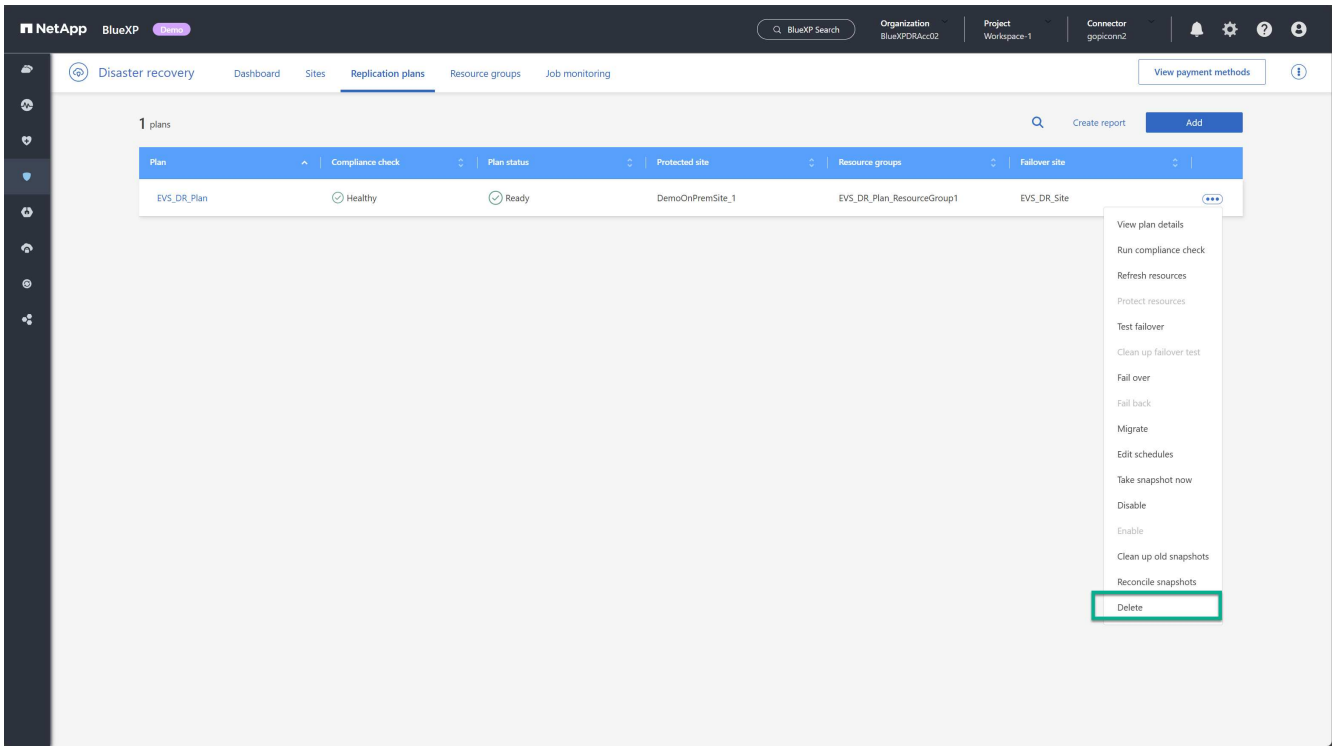
1. Select the **Actions** option ••• next to the replication plan.
2. To delete snapshots from the source cluster that do not exist on the destination cluster, select **Reconcile snapshots** from the replication plan's Actions menu.



Delete replication plan

If the replication plan is no longer needed, you can delete it.

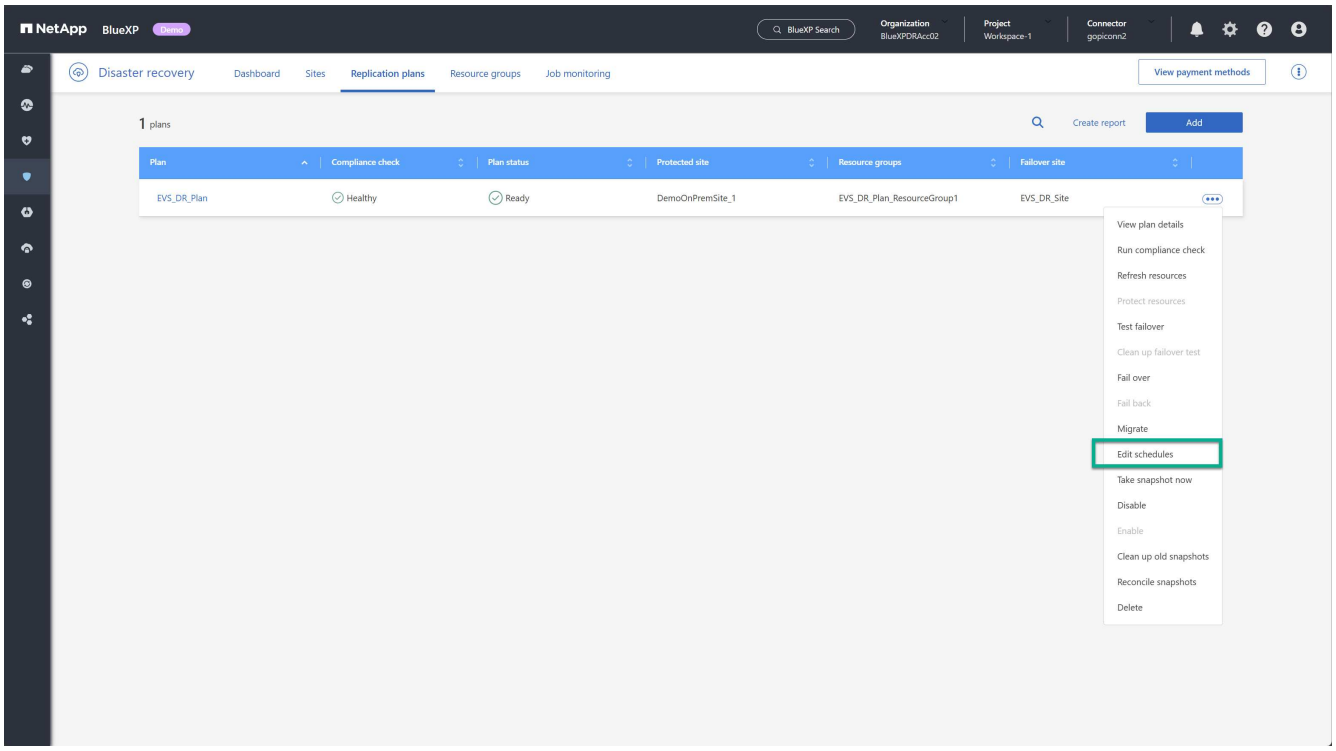
1. Select the **Actions** option ••• next to the replication plan.
2. To delete the replication plan, select **Delete** from the replication plan's context menu.



Edit schedules

Two operations are performed automatically on a regular schedule: test failovers and compliance checks.

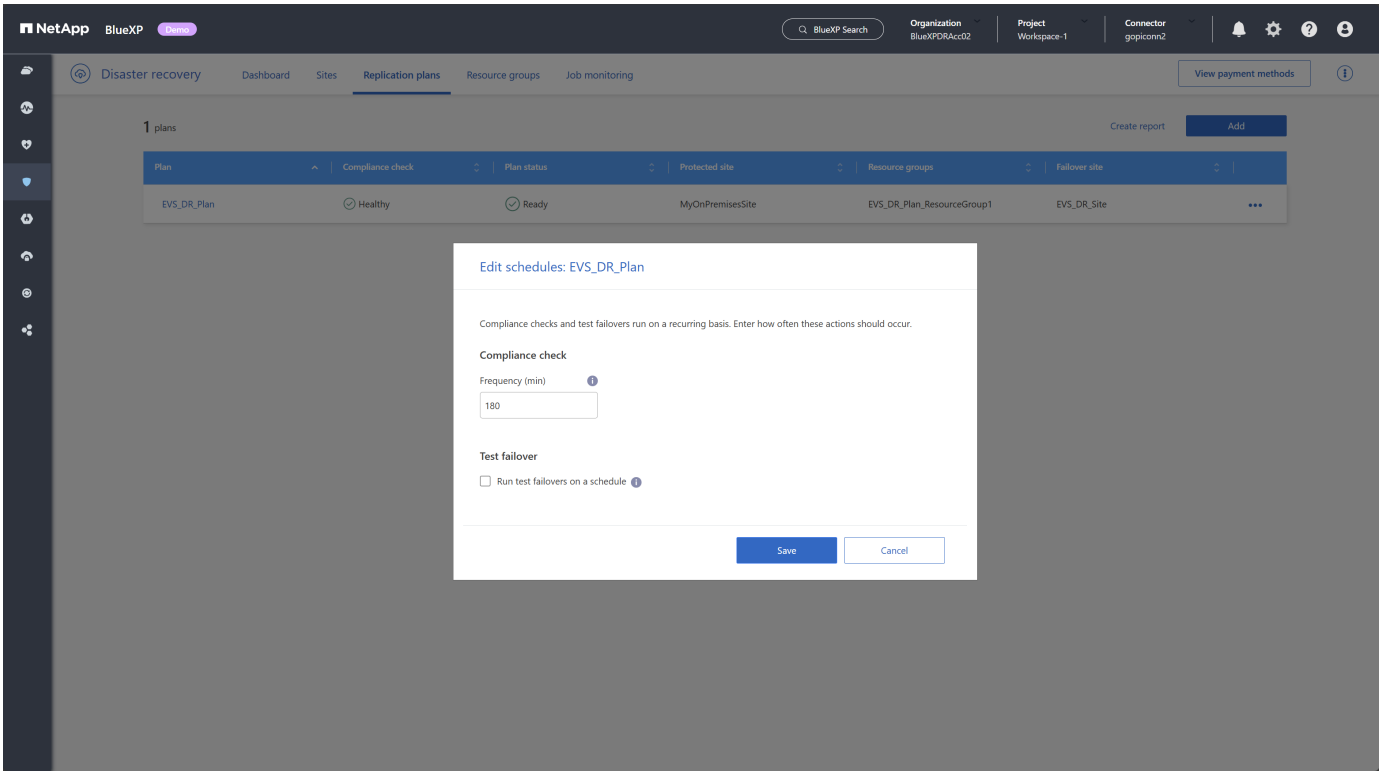
1. Select the **Actions** option ••• next to the replication plan.
2. To change these schedules for either of these two operations, select **Edit schedules** for the replication plan.



Change compliance check interval

By default, compliance checks are performed every three hours. You can change this to any interval between 30 minutes and 24 hours.

To change this interval, change the Frequency field in the Edit schedules dialog box:



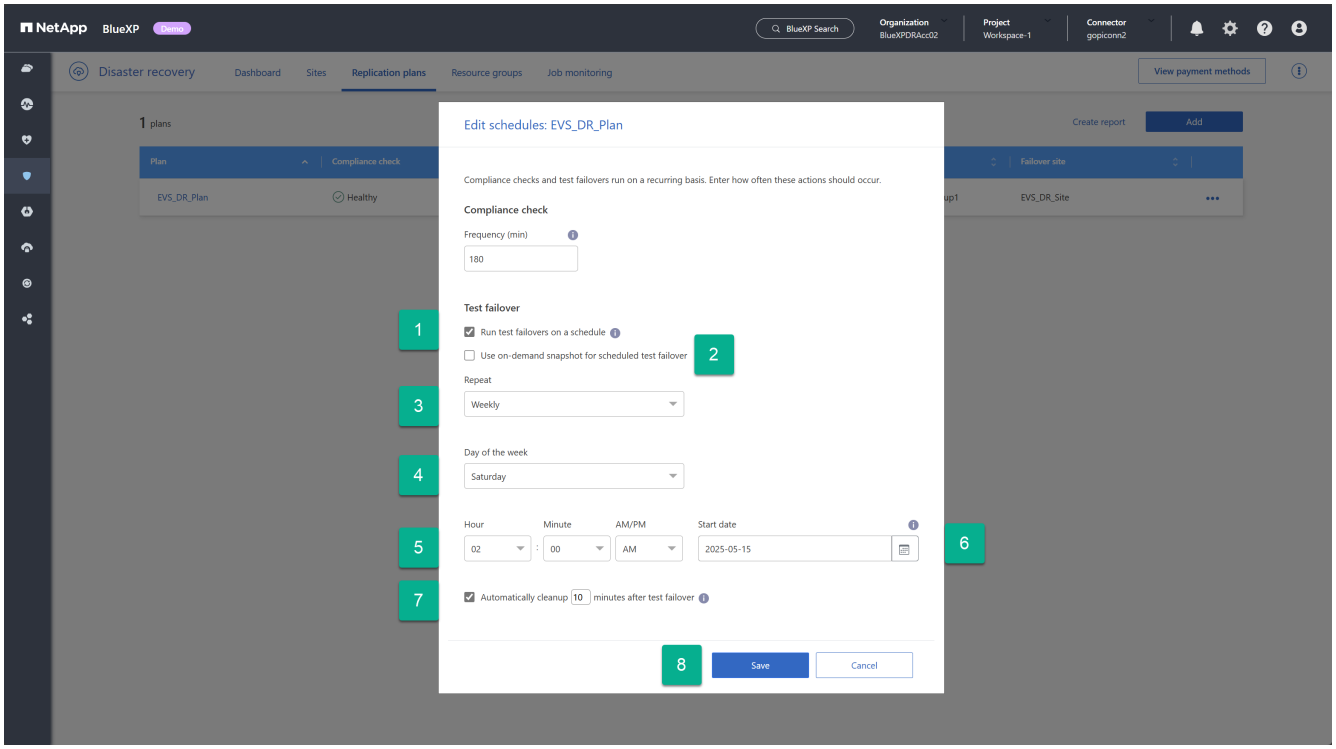
Schedule automated test failovers

Test failovers are manually executed by default. You can schedule automatic test failovers, which helps ensure that your replication plans perform as expected. To learn more about the test failover process, see Test the failover process.

Steps to schedule test failovers

1. Select the **Actions** option ••• next to the replication plan.
2. Select **Run failover**.
3. Check the **Run test failovers on a schedule** checkbox.
4. (Optional) Check the **Use on-demand-snapshot for scheduled test failover**.
5. Select an interval type in the Repeat drop-down.
6. Select when to perform the test failover
    a. Weekly: select the Day of the Week
    b. Monthly: select the Day of the month
7. Choose the time of day to run the test failover
8. Chose the start date.
9. Decide if you want the service to automatically clean up the test environment and how long you would like the test environment to run before the clean up process starts.

10. Select **Save**.



Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account serial number (your 20 digit 960xxxxxxxxx serial number located on the Support Resources page in BlueXP).

  This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxxx serial numbers).

  These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

Register BlueXP for NetApp support

To register for support and activate support entitlement, one user in your BlueXP organization (or account) must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

   The **Resources** page should show that your BlueXP organization is registered for support.

   Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP organization is not registered for support. As long as one user in the organization has followed these steps, then your organization has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

Steps

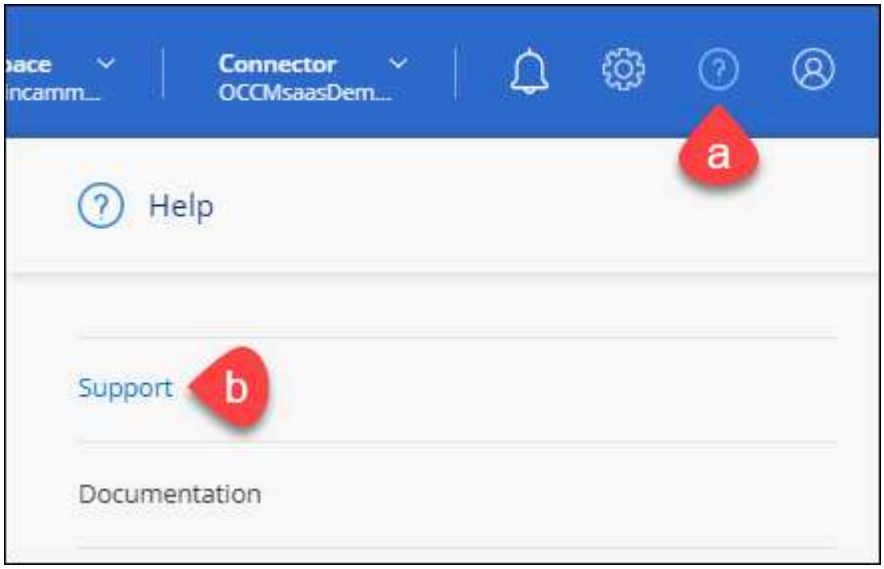
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Brand new to NetApp

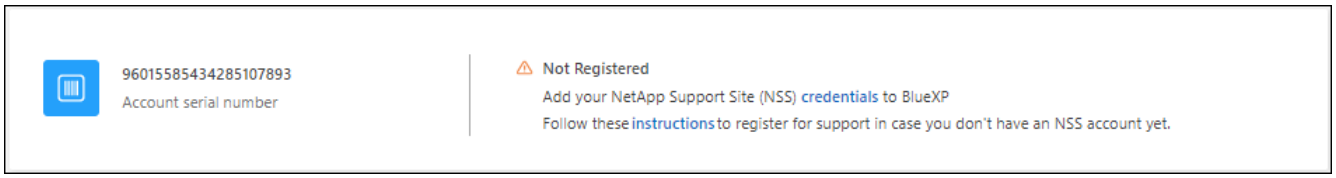
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



3. Navigate to NetApp's support registration site and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

   An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

   Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under Existing customer with an NSS account.

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP organization is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- Upgrading Cloud Volumes ONTAP software to the latest release

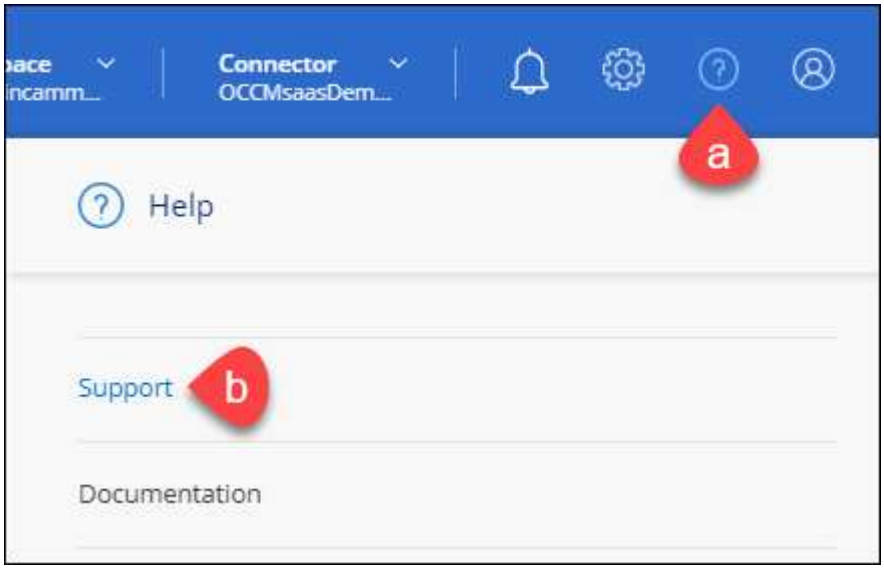
Associating NSS credentials with your BlueXP organization is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP organization ID. Users who belong to the BlueXP organization can access these credentials from **Support > NSS Management**.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   - The NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
   - There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

     "The NSS customer type is not allowed for this account as there are already NSS Users of different type."

     The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level account.

   - Upon successful login, NetApp will store the NSS user name.

     This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu.

  Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24/7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- Amazon FSx for ONTAP
- Azure NetApp Files
- Google Cloud NetApp Volumes

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- Documentation

  The BlueXP documentation that you're currently viewing.

- Knowledge base

  Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- Communities

  Join the BlueXP community to follow ongoing discussions or create new ones.

Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. Learn how to manage credentials associated with your BlueXP login.
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be

associated with the serial number for that system.

Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:

   a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.

   b. Select **Create a Case** to open a ticket with a NetApp Support specialist:

      - **Service**: Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
      - **Working Environment**: If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

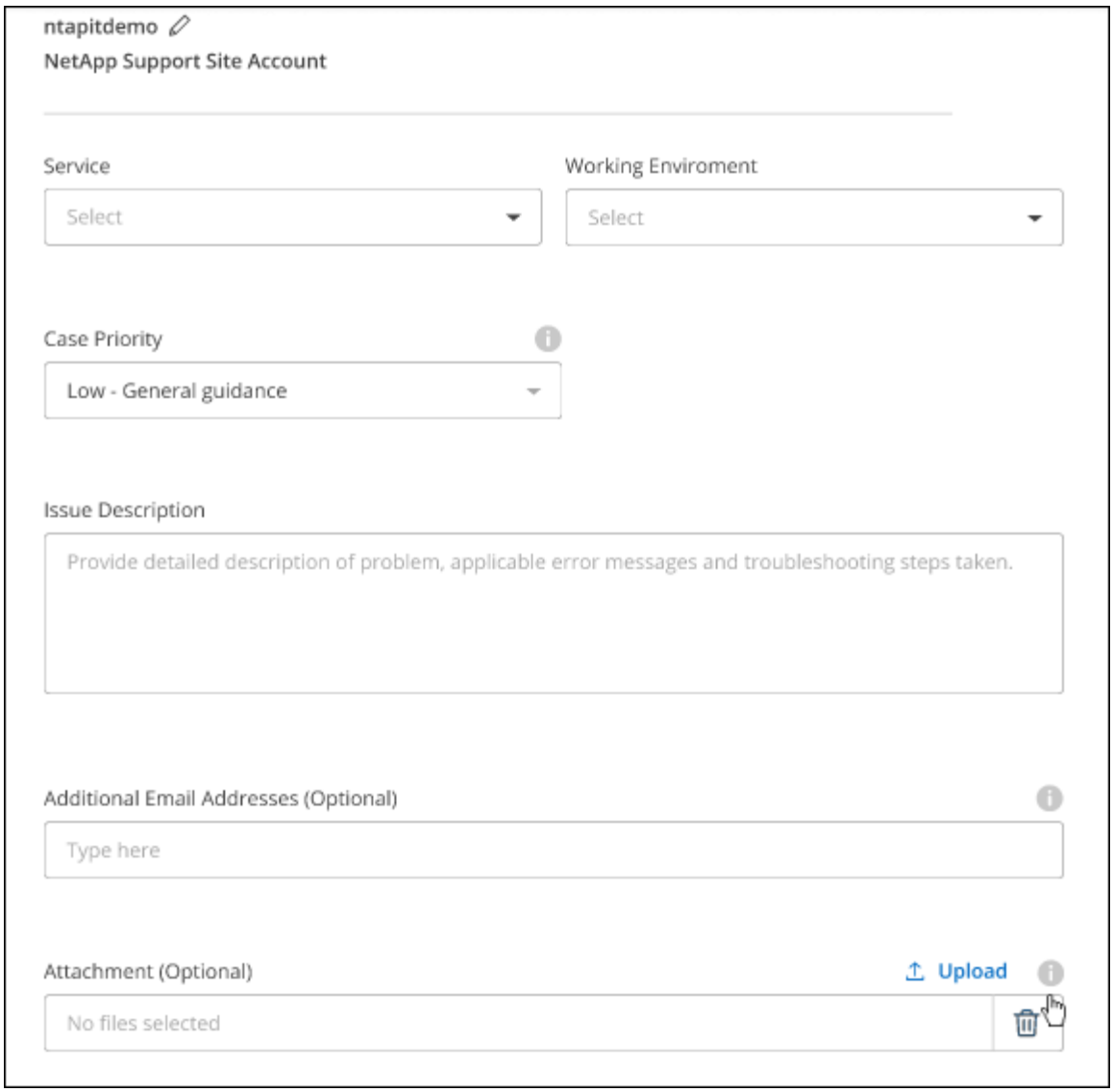
        The list of working environments are within scope of the BlueXP organization (or account), project (or workspace), and Connector you have selected in the top banner of the service.

      - **Case Priority**: Choose the priority for the case, which can be Low, Medium, High, or Critical.

        To learn more details about these priorities, hover your mouse over the information icon next to the field name.

      - **Issue Description**: Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
      - **Additional Email Addresses**: Enter additional email addresses if you'd like to make someone else aware of this issue.
      - **Attachment (Optional)**: Upload up to five attachments, one at a time.

        Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.



After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at https://mysupport.netapp.com/site/help

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
  - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
  - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

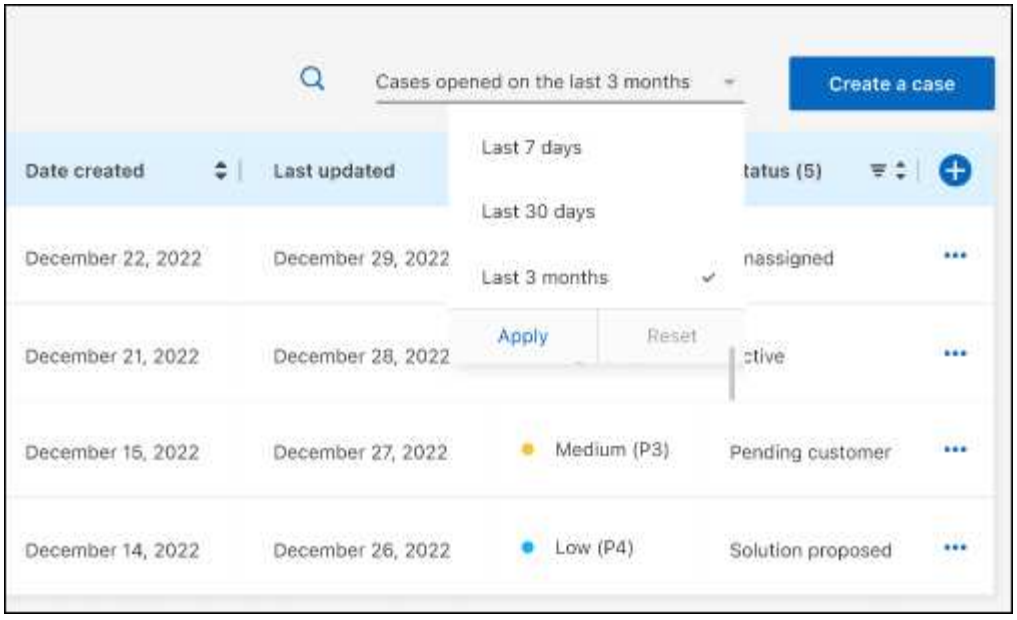
  The results in the table reflect the cases related to the view that you selected.
- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

  View the steps below for more details.
- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

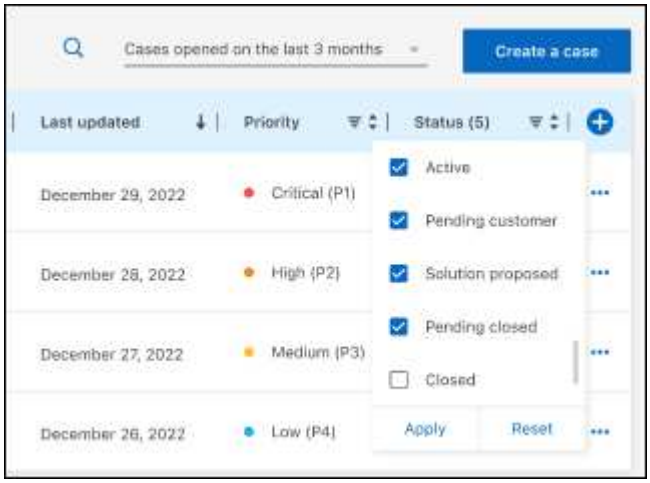
Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

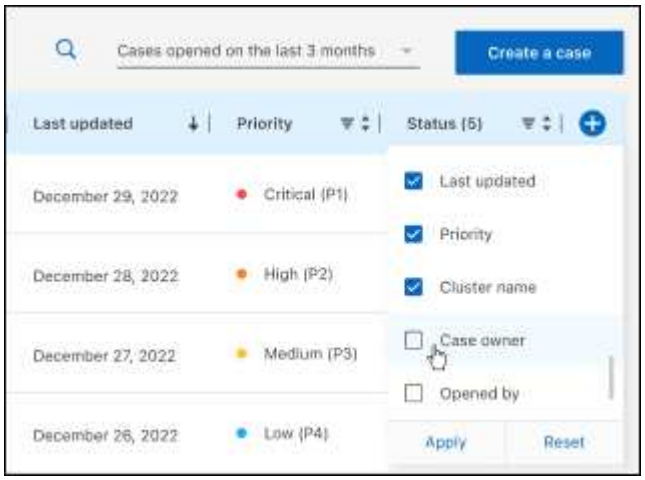
   The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.
3. Optionally modify the information that displays in the table:
   - Under **Organization's cases**, select **View** to view all cases associated with your company.
   - Modify the date range by choosing an exact date range or by choosing a different time frame.



- Filter the contents of the columns.



- Change the columns that appear in the table by selecting ⊕ and then choosing the columns that you'd like to display.

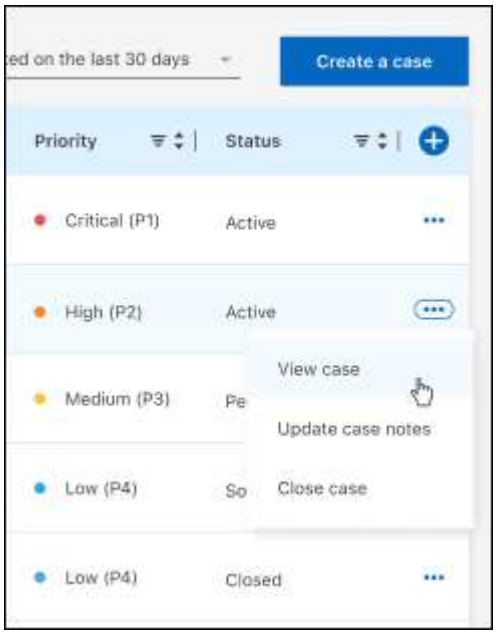


4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **View case**: View full details about a specific case.
   - **Update case notes**: Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

     Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

   - **Close case**: Provide details about why you're closing the case and select **Close case**.



Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Notice for BlueXP disaster recovery

Copyright information

Trademark information