BlueXP disaster recovery documentation

BlueXP disaster recovery

NetApp
April 02, 2024

Table of Contents

BlueXP disaster recovery documentation

Release notes

What's new

Learn what's new in 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:

- 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.

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 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.

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

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.

Failback uses latest Snapshot copy

In the current release, the failback process always uses the latest Snapshot copy. This occurs even if you chose a specific Snapshot copy to use.

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

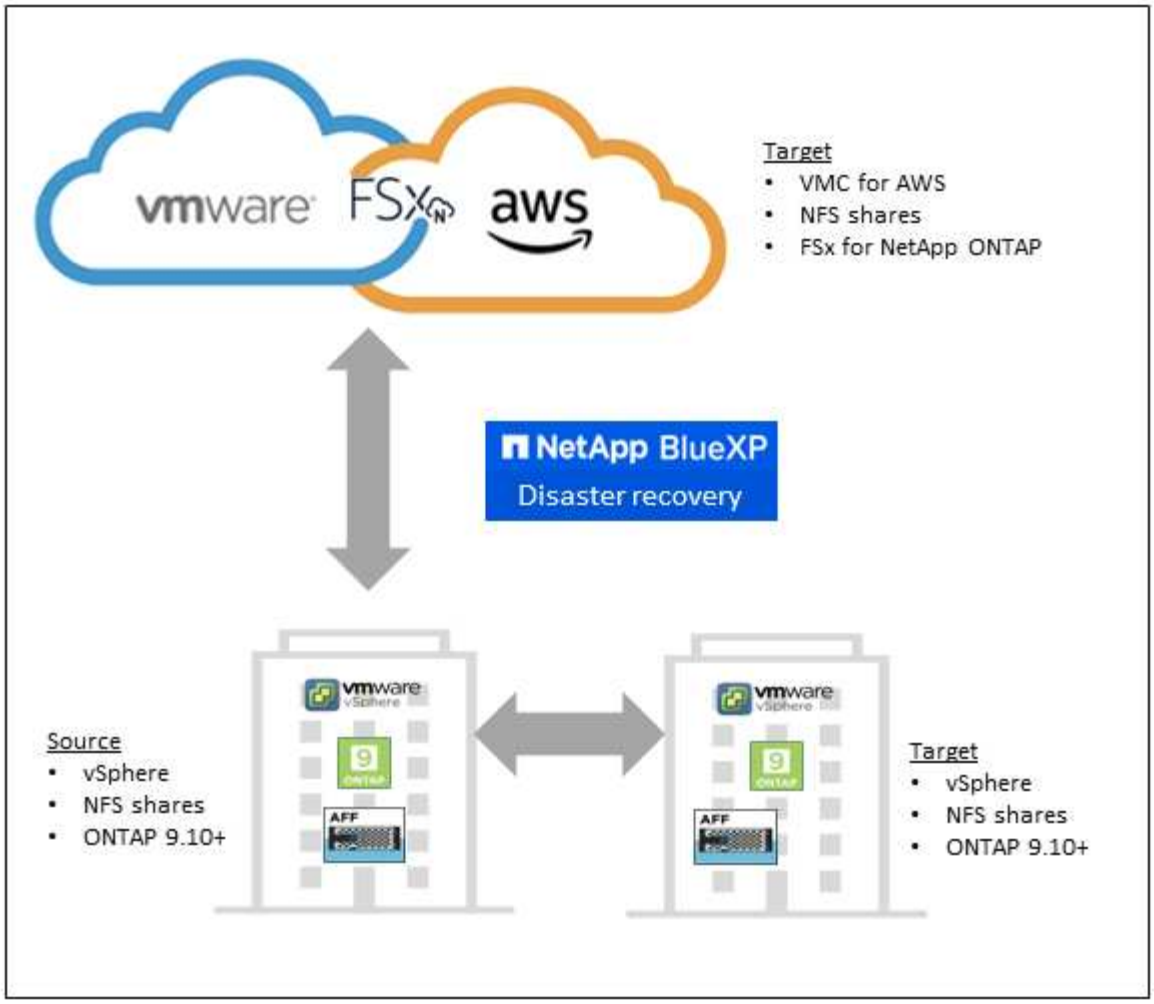
Learn about BlueXP disaster recovery for VMware

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 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. Initially, with the BlueXP disaster recovery service you can protect your on-premises, NFS-based VMware workloads 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

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.
- In case of disaster, fail over your primary site on demand to the disaster recovery site, which can be

VMware Cloud on AWS with 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.

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 full version of BlueXP disaster recovery service can be used with a NetApp license.

Licensing

You can use the following license types:

- Sign up for a 90-day free trial.
- 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 provisioned 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.

90-day free trial

You can try out BlueXP disaster recovery by using a 90-day free trial.

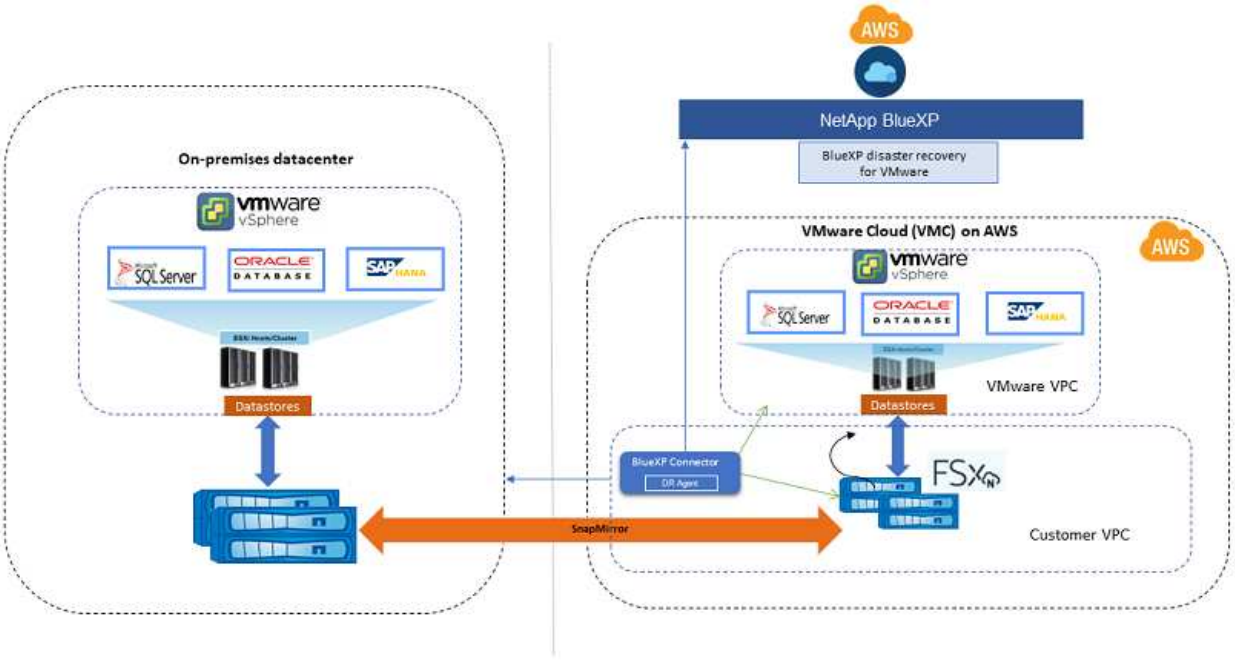
To continue after the 90-day trial, you'll need to purchase a BYOL license from NetApp.

You can purchase a license at any time and you will not be charged until the 90-day trial ends.

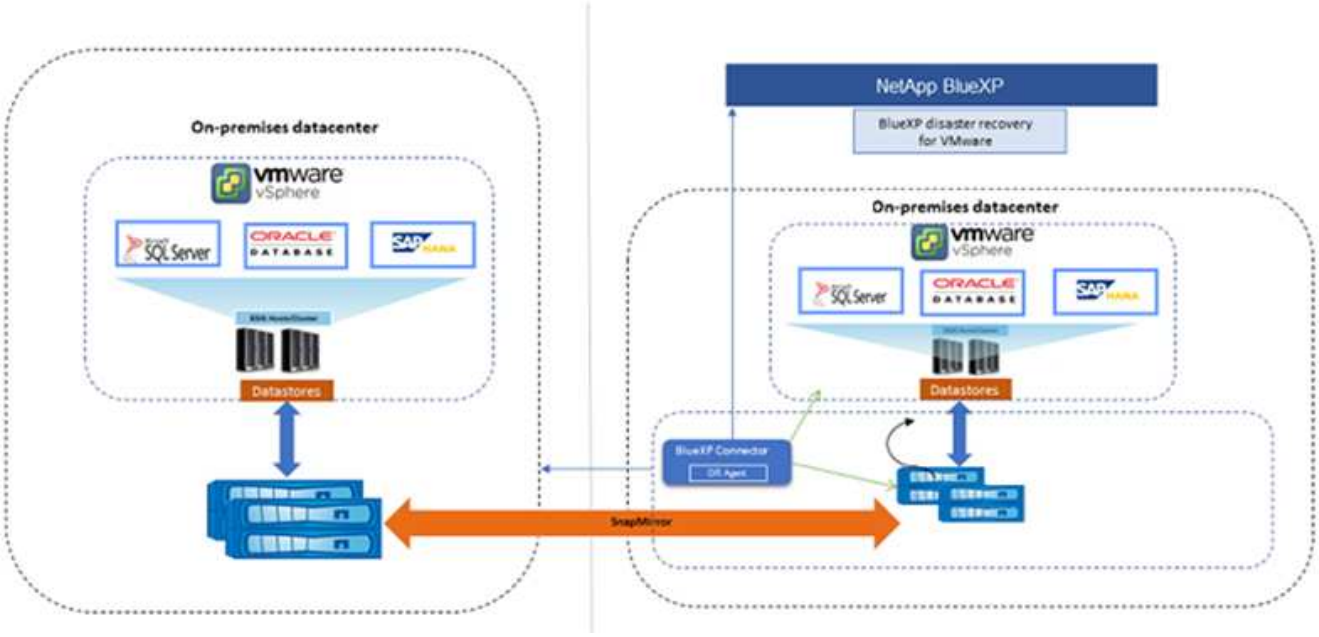
How BlueXP disaster recovery works

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.

BlueXP disaster recovery prerequisites

Get started by verifying the readiness of your operational environment, login, network access, and web browser.

To use BlueXP disaster recovery, you should ensure that your environment meets the following requirements:

- On-premises VMware working environment with NetApp storage
- On AWS:
  - An Amazon FSx for NetApp ONTAP file system. Refer to Amazon FSx for ONTAP documentation on how to get started.
  - A VMware account with a software-defined data center (SDDC) on AWS, also referred to as Virtual Machines Cloud. 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 Virtual Machines Cloud documentation.
  - Link the SDDC with Amazon FSx for NetApp ONTAP. Refer to VMware Cloud on AWS integration with Amazon FSx for NetApp ONTAP.
- In BlueXP:
  - Amazon FSx for ONTAP and AWS credentials added to the BlueXP working environment.
  - The BlueXP Connector needs to be set up in BlueXP. The on-premises and cloud Connector should have connectivity to both the on-premises and VMware Cloud (VMC) VCenter with ESXis. This enables the backup, failover, failback and migration features to work properly with the needed networking and script features.

    The BlueXP Connector requires credentials for both the source and target vCenter servers. Refer to the BlueXP Quick start and BlueXP networking information.

  - To ensure that application-consistency processes are successful, ensure the following prerequisites are met:
    - Ensure that VMware tools (or Open VM tools) are running on the VMs that will be protected.
    - For Windows VMs running SQL or Oracle or both, the databases should have their VSS Writers enabled and the databases should be in a stable state.
    - 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.

Review prerequisites

Ensure your environment meets these requirements.

2 Set up the disaster recovery service

Complete steps to set up the service.

Complete steps to set up licensing.

3 What's next?

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

- Add vCenter sites.
- Create a disaster recovery plan.
- Replicate applications to another site.
- Fail over applications to a remote site.
- Fail back applications to the original source site.
- Manage sites, plans, datastores, and virtual machines information.
- Monitor disaster recovery operations.

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.

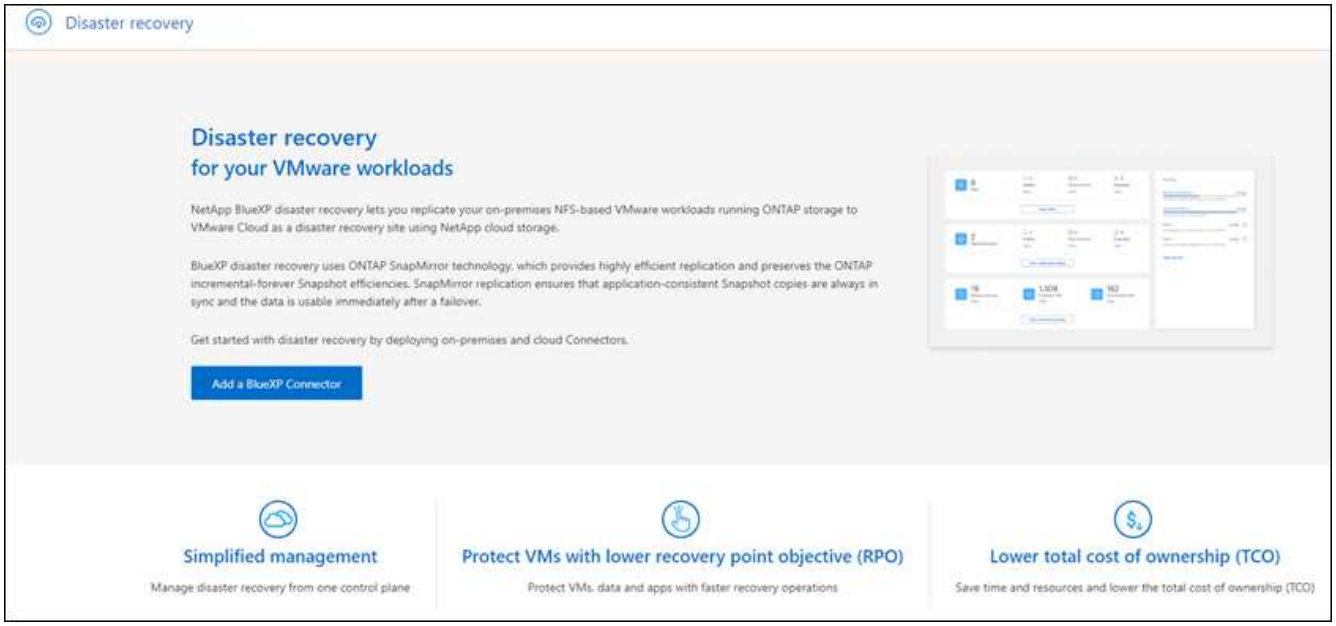
Steps

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.

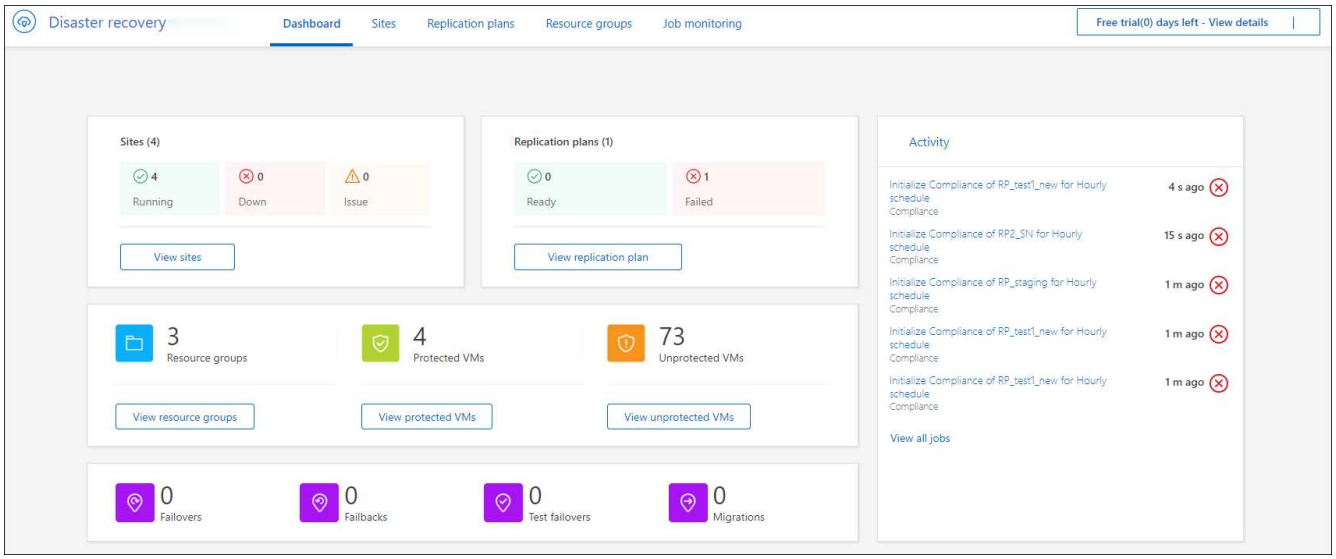


Otherwise, the BlueXP disaster recovery Dashboard appears.

- If you don’t have a BlueXP Connector or it’s not the one for this service, you might need to contact NetApp Support or follow messages to sign up for this service.

  To add a Connector, refer to Learn about Connectors.

- If you are new to BlueXP and haven’t used any Connector, when you select "Disaster recovery," a message appears about signing up. Go ahead and submit the form. NetApp will contact you about your request.
- 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," you can proceed.



Set up 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.

Set up AWS

In AWS, you'll need to do the following steps:

- Deploy and configure VMware Cloud on AWS.
- Create an Amazon FSx for ONTAP file system. Provision and configure FSx for ONTAP.
- Use a VMware account and provision the software-defined data center (SDDC). Ensure that the SDDC has connectivity with FSx for ONTAP.

Deploy VMware Cloud

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 VMC environment on AWS, follow the steps at this link. A pilot-light cluster can also be used for disaster recovery purposes.

Configure Amazon FSx for NetApp 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 popular NetApp ONTAP file system. Follow the steps at this link to provision and configure FSx for NetApp ONTAP.

Set up BlueXP disaster recovery

The next step is to set up disaster recovery in BlueXP.

- Create a Connector in BlueXP.
- Deploy and configure SnapMirror for Amazon FSx for NetApp ONTAP.
- Add the on-premises ONTAP storage working environment to BlueXP. This is the source ONTAP cluster.
- Add a BlueXP account, add FSxN to the working environment, and add AWS credentials for FSx for ONTAP.

Create a Connector in BlueXP

You need to reach out to your NetApp Sales Rep to try out this service. Then, when you use the BlueXP Connector, it will include the appropriate capabilities for the disaster recovery service.

To create a Connector in BlueXP before using the service, refer to the BlueXP documentation that describes how to create a connector.

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

Configure SnapMirror for Amazon FSx for NetApp ONTAP

The next step is to set up disaster recovery in BlueXP.

1. In BlueXP, add an account. Refer to the BlueXP documentation on how to add an account.
2. Add Amazon FSx for NetApp ONTAP to the working environment. Ensure that the SnapMirror relationship with the ONTAP cluster is in place and that it has a destination of FSx for NetApp ONTAP. Refer to how to set up an FSx for ONTAP working environment.
3. In BlueXP, deploy SnapMirror to FSx for NetApp ONTAP.
4. In BlueXP, discover the provisioned FSx for NetApp ONTAP on an AWS instance and replicate the specified datastore volumes from an on-premises environment to FSx for NetApp ONTAP with the appropriate frequency and NetApp Snapshot copy retention.

Set up licensing

With BlueXP disaster recovery, you can sign up for a 90-day free trial.

You can Bring Your Own License (BYOL), which is a NetApp License File (NLF).

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

Set up licensing for BlueXP disaster recovery

With BlueXP disaster recovery, you can use the service in a free trial or bring your own license.

You can use the following license types:

- Sign up for a 90-day free trial.
- 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 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.

After you set up your BYOL, you can see the license in the BlueXP digital wallet **Data Service Licenses** tab.

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 90-day free trial

You can try BlueXP disaster recovery out by using a 90-day free trial.

No capacity limits are enforced during the trial.

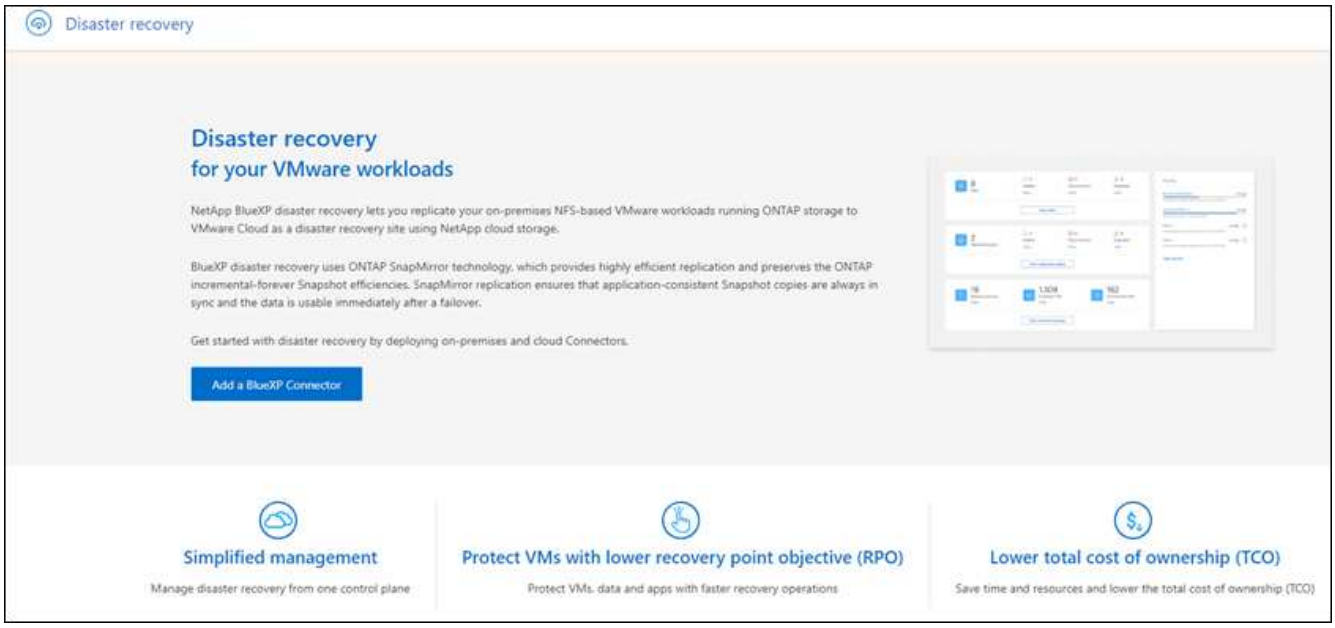
You can get a license at any time and you will not be charged until the 90-day trial ends. To continue after the 90-day trial, you'll need to purchase a BYOL license.

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. Review the free trial information and select **Let's go**.

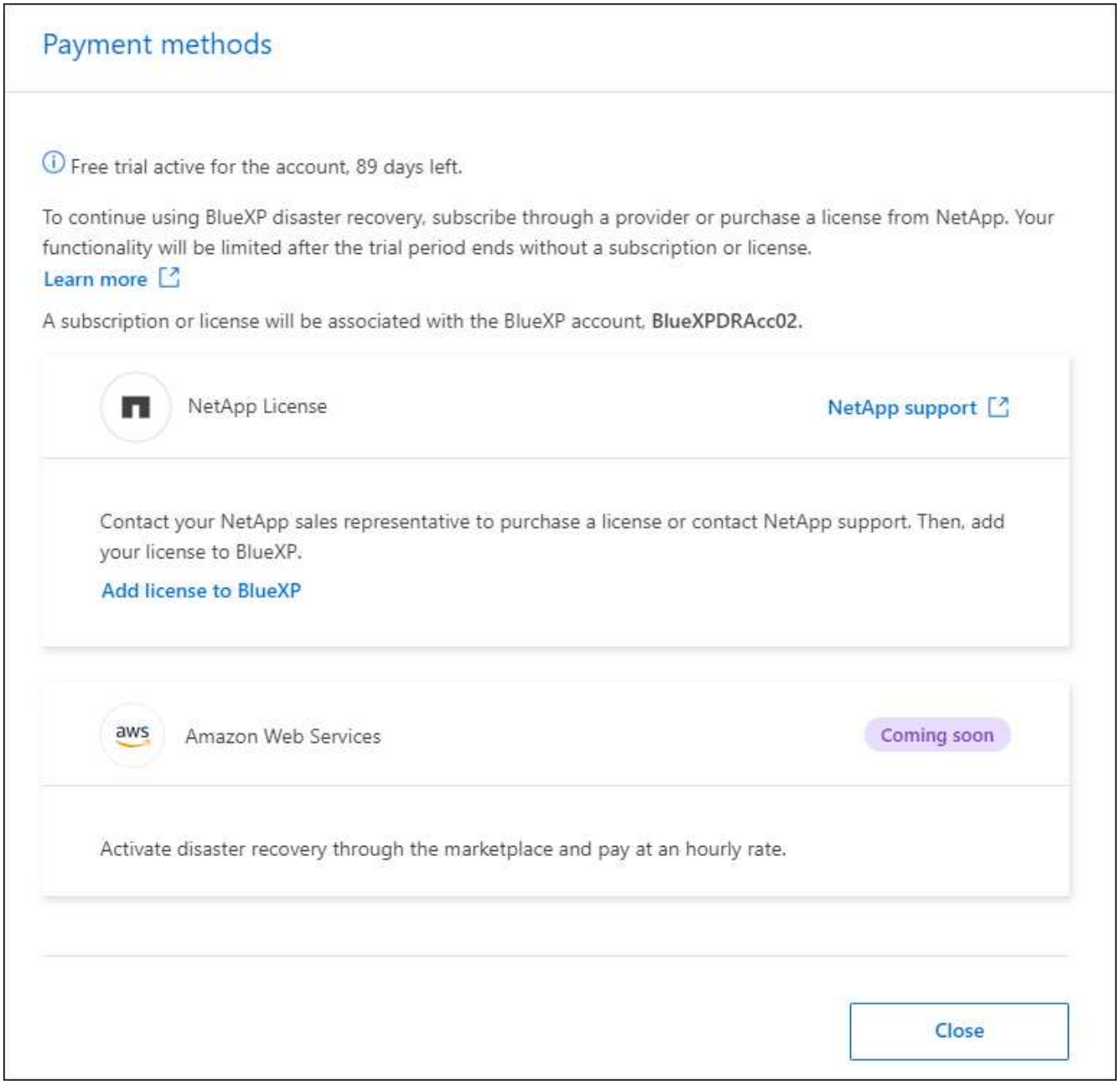
After the trial ends, purchase a BYOL license through NetApp

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

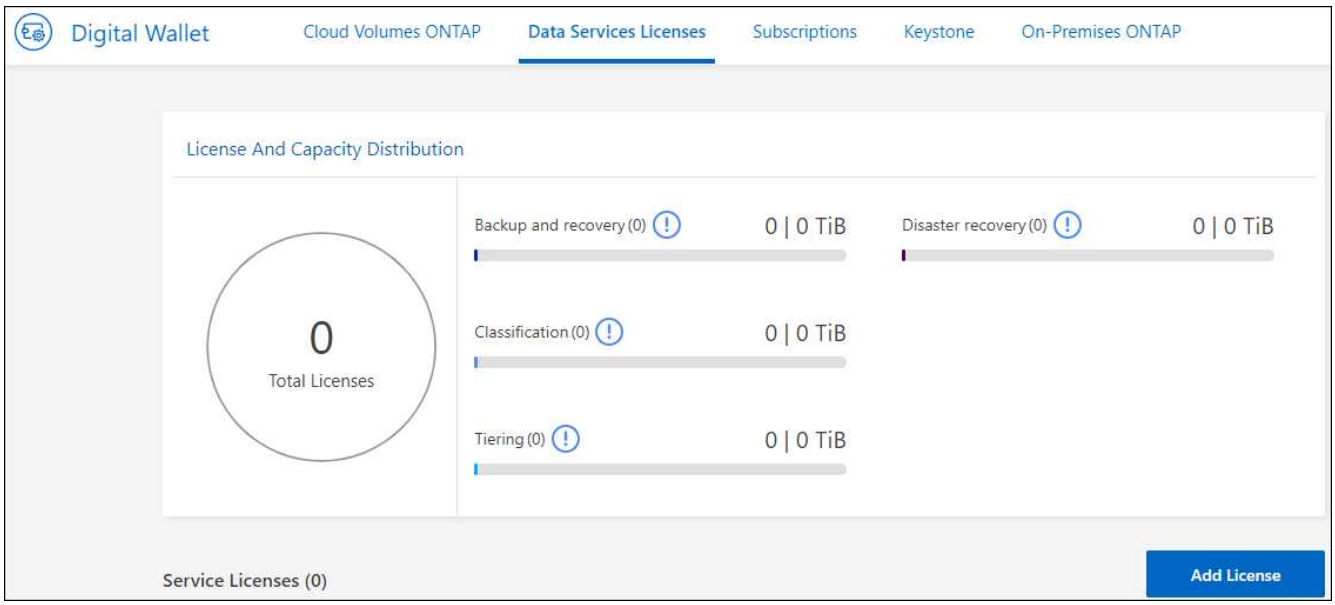
Steps

1. Contact your NetApp Sales Rep to purchase a license.
2. After you obtain the license, return to BlueXP disaster recovery. Select the **View payment methods** option

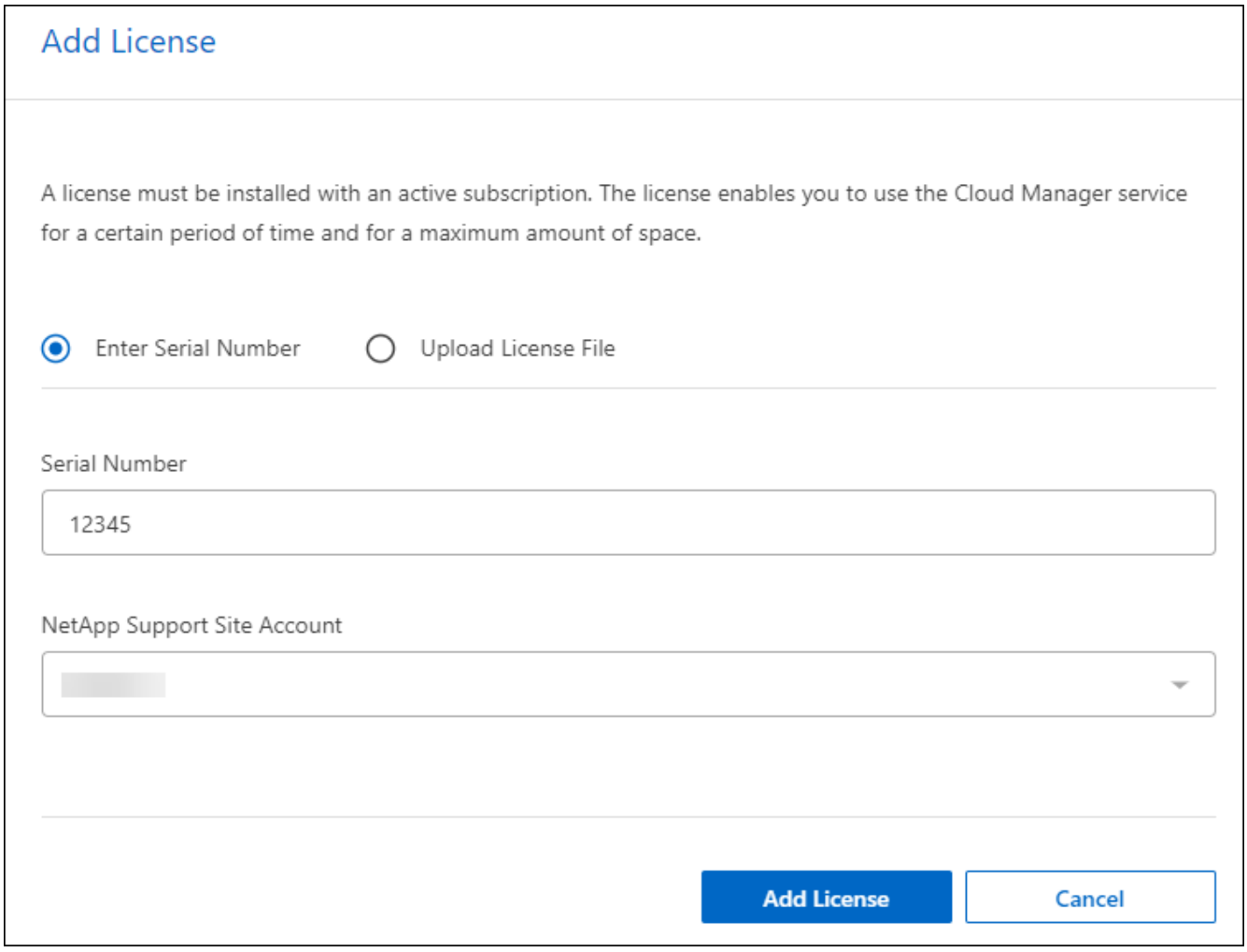
in the upper right. Or, in the message that the free trial is expiring, select **Subscribe or purchase a license**.



3. Select **Add license to BlueXP**. You will be directed to BlueXP digital wallet.



4. In BlueXP digital wallet, from the **Data Services Licenses** tab, select **Add license**.
5. In the Add License page, enter the serial number and NetApp Support Site account information.



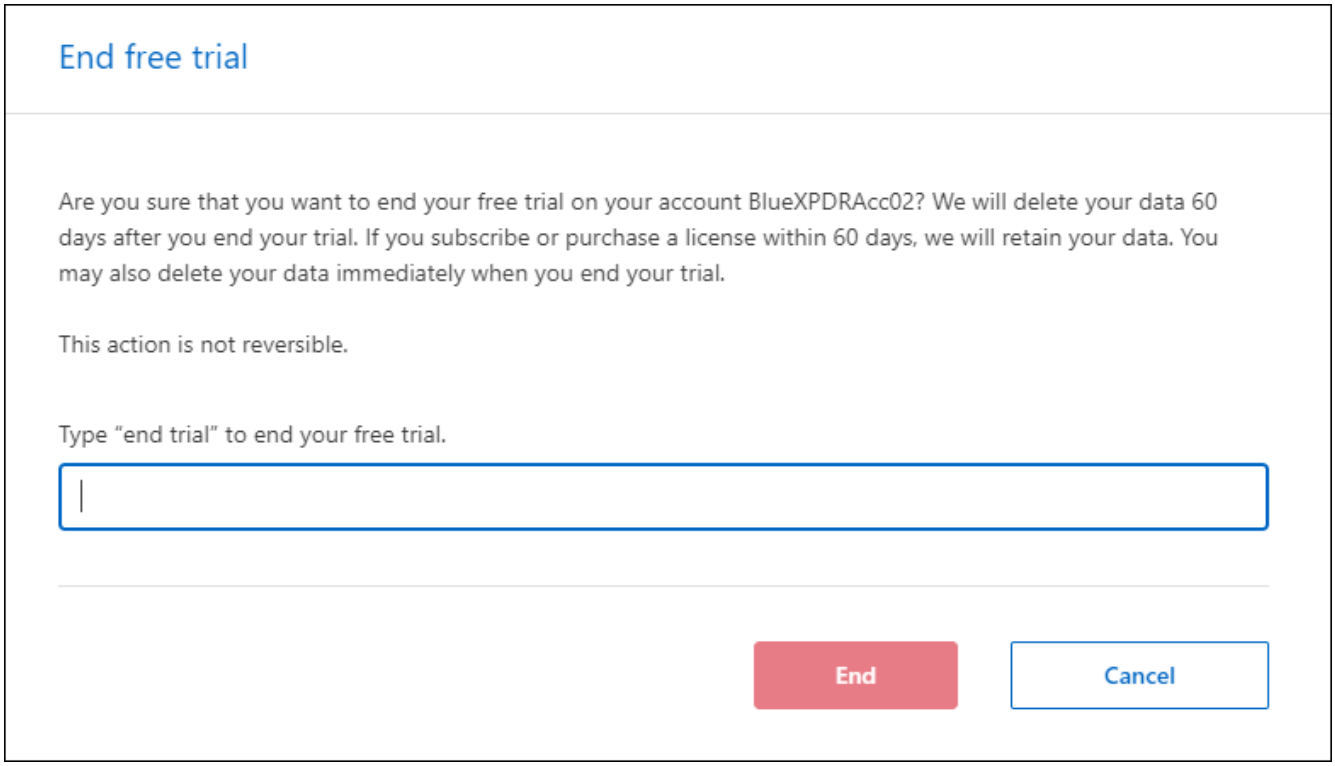
6. Select **Add License**.

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 all data when my trial ends**.

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

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

Bring your own license (BYOL)

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.

Purchase a BlueXP disaster recovery license

If you don’t have a BlueXP disaster recovery license, contact us to purchase one.

1. Do one of the following:

- Contact NetApp Sales to purchase a license.
- Click the chat icon in the lower-right of BlueXP to request a license.

Obtain your BlueXP disaster recovery license file

After you've purchased your BlueXP disaster recovery license from your NetApp Sales Rep, you activate the license by entering the BlueXP disaster recovery serial number and NetApp Support Site (NSS) account information.

Before you begin

You'll need to have the following information before you start:

- BlueXP disaster recovery serial number

  Locate this number from your Sales Order, or contact the account team for this information.

- BlueXP Account ID

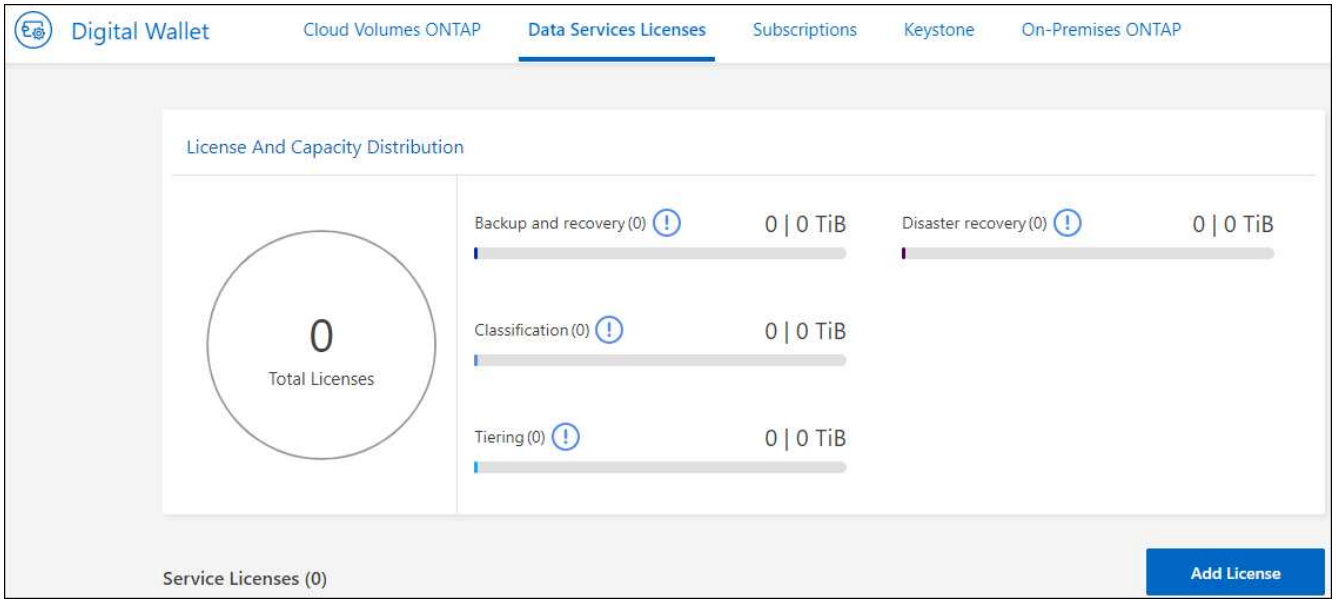
  You can find your BlueXP Account ID by selecting the **Account** drop-down from the top of BlueXP, and then selecting **Manage Account** next to your account. Your Account ID is in the Overview tab. For private mode site without internet access, use **account-DARKSITE1**.

Add BlueXP disaster recovery license to BlueXP digital wallet

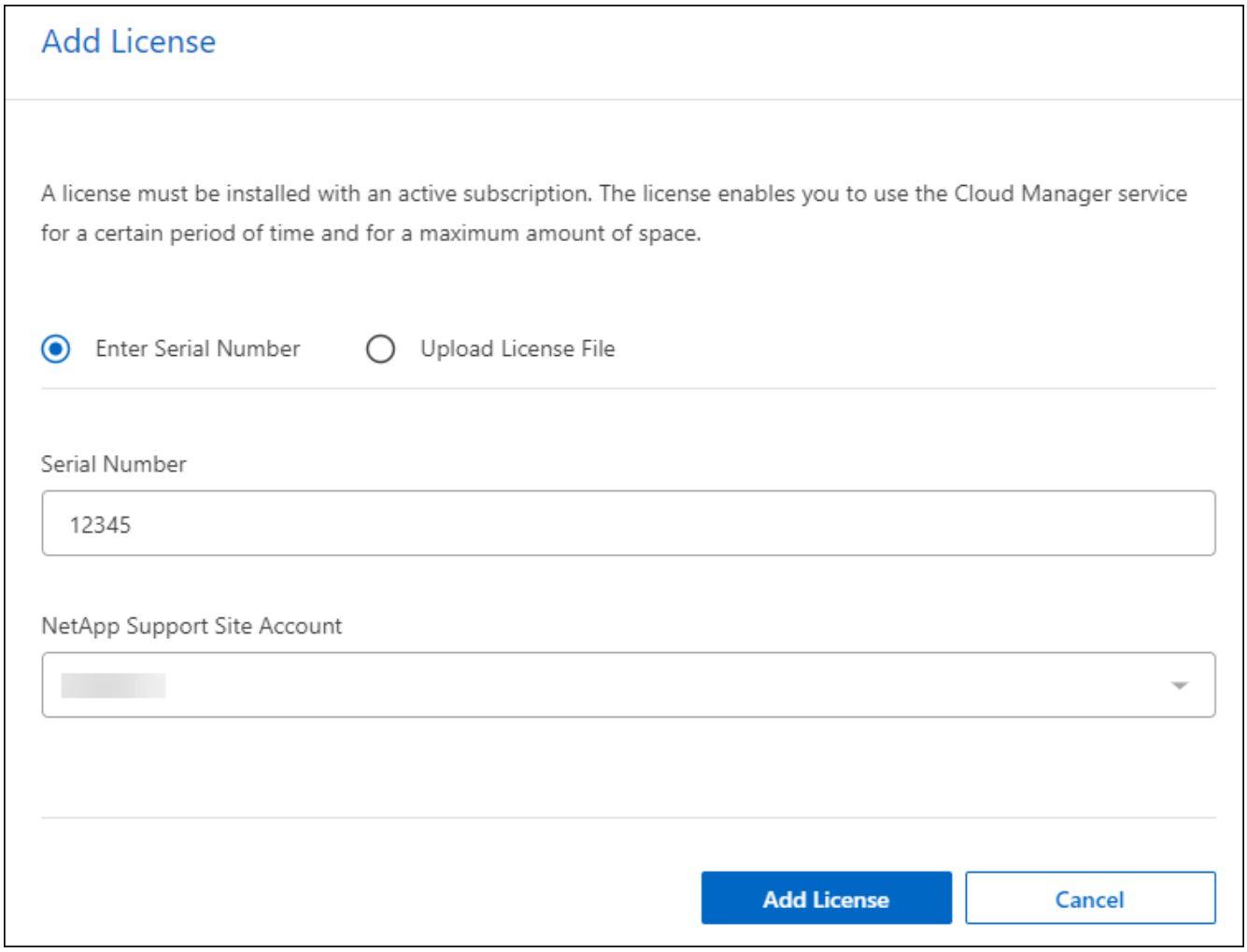
After you purchase a BlueXP disaster recovery license for your BlueXP account, you need to add the license to the BlueXP digital wallet.

Steps

1. From the BlueXP menu, select **Governance** > **Digital wallet** > **Data Services Licenses**.



2. Select **Add License**.



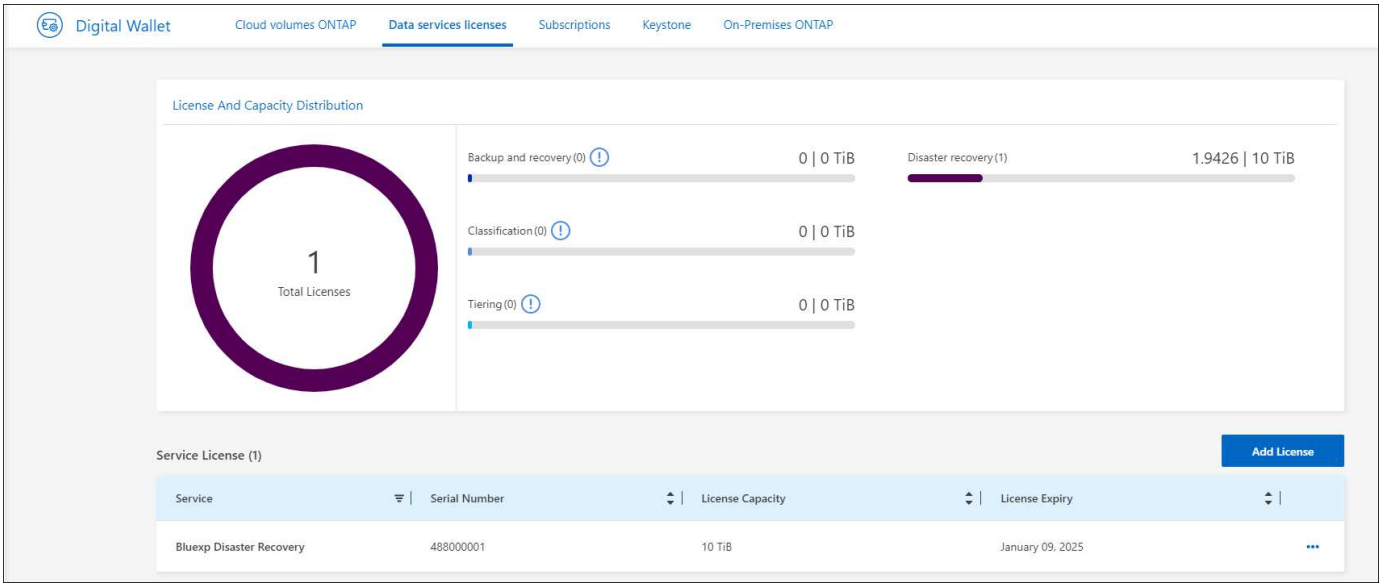
3. In the Add License page, enter the license information and select **Add License**:
   - If you have the BlueXP license serial number and know your NSS account, select the **Enter Serial Number** option and enter that information.

     If your NetApp Support Site account isn't available from the drop-down list, add the NSS account to BlueXP.

   - If you have the BlueXP license file (required when installed in a dark site), select the **Upload License File** option and follow the prompts to attach the file.

Result

BlueXP digital wallet now shows Disaster recovery with a license.



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.

Steps

1. Select the chat icon in the lower-right of BlueXP to request an extension to your term or additional capacity to your license for the particular serial number. You can also send an email to request an update to your license.

   After you pay for the license and it is registered with the NetApp Support Site, BlueXP automatically updates the license in the BlueXP digital wallet and the Data Services Licenses page will reflect the change in 5 to 10 minutes.

2. If BlueXP can't automatically update the license (for example, when installed in a dark site), then you'll need to manually upload the license file.
   a. You can obtain the license file from the NetApp Support Site.
   b. Access the BlueXP digital wallet.
   c. Select the **Data Services Licenses** tab, select the **Actions …** icon for the service serial number you are updating, and select **Update License**.

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:

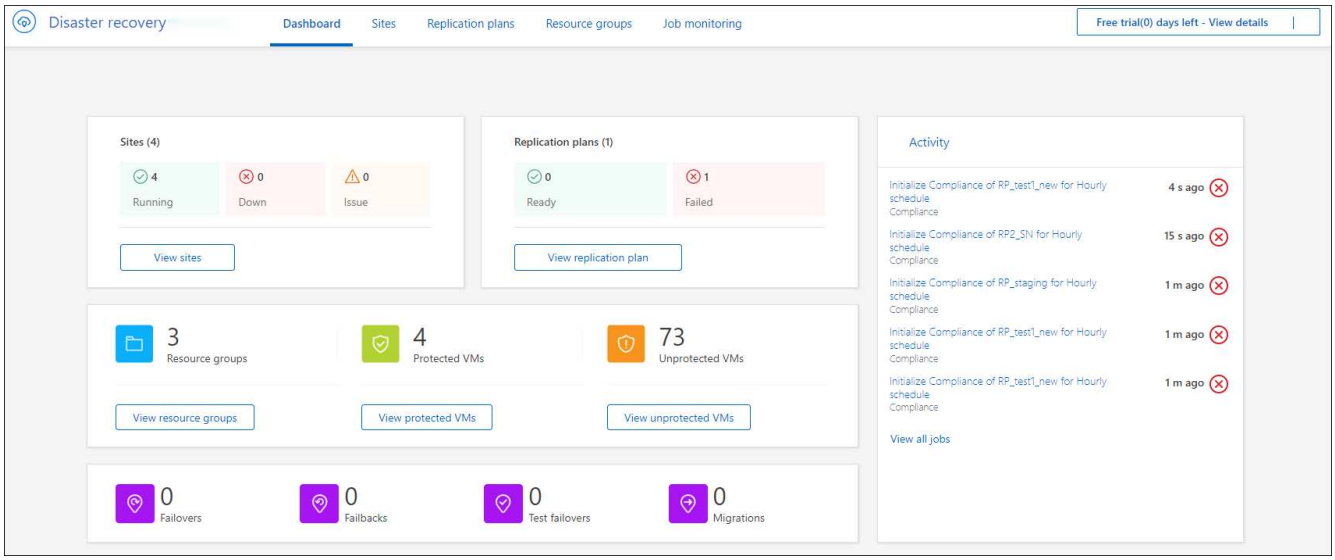
- View the health of your disaster recovery plans
- Add vCenter sites.
- Create a disaster recovery plan.
- Replicate VMware apps on your primary site to a disaster recovery remote site in the cloud using SnapMirror replication.
- Migrate VMware apps on your primary site to another site.
- Test the fail 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 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.

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 resource group details, select **View all** for a status or **View resource groups** to see them all.
- 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 vCenter sites

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

After they 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.

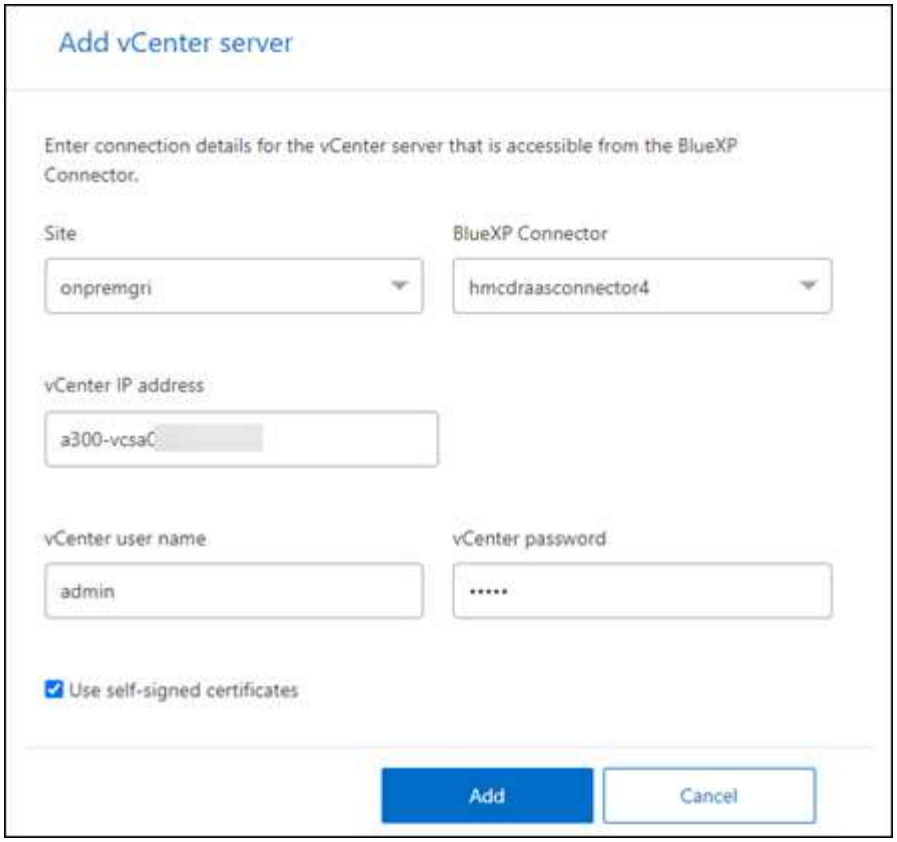
Steps

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

   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.

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**.



a. Add a site, select the BlueXP Connector, and provide vCenter credentials.

b. 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.

c. Select **Add**.

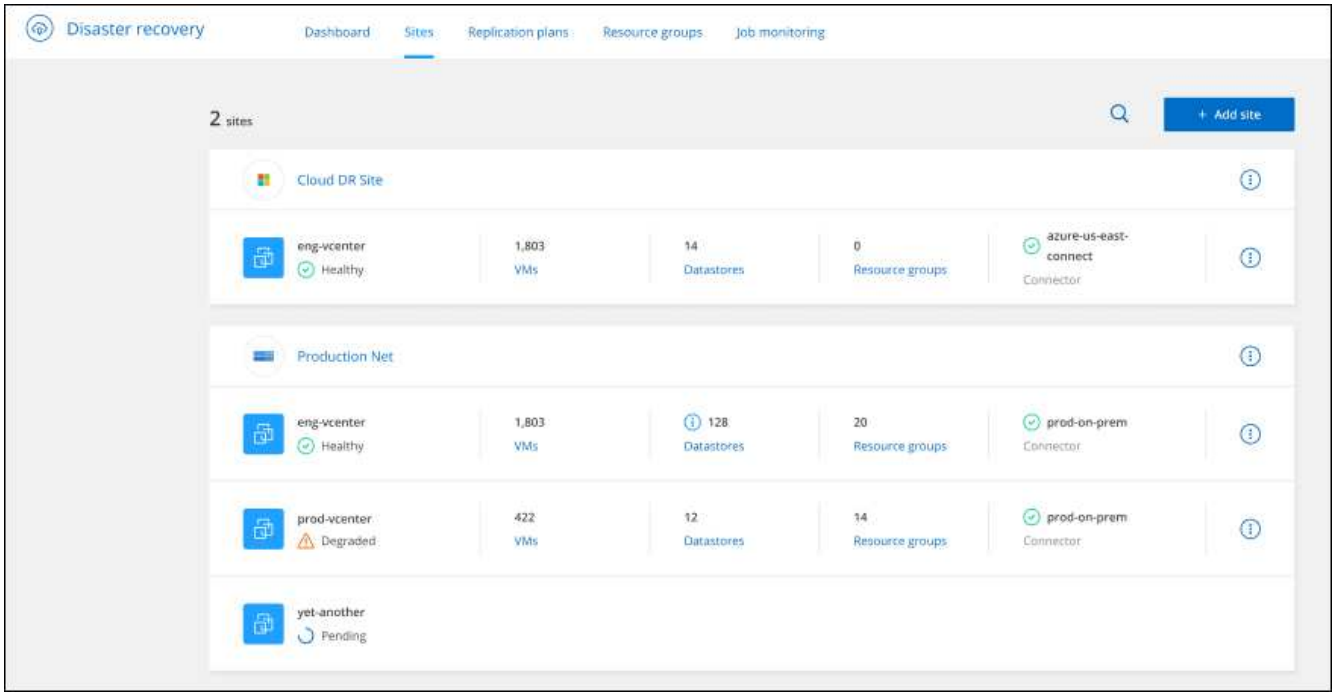
Next, you will add a target vCenter.

3. **Target**:

a. Choose the target site and the location. If the target is cloud, select **AWS**.

b. Select **Add**.

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



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

Create a replication plan

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 associated with one application or you might group applications that have similar tiers.

Such plans are sometimes called *blueprints*.

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

Create the plan

A wizard takes you through these steps:

- Select vCenter servers
- Select the VMs you want to replicate and assign groups
- Map how resources from the source environment map to the destination.
- Identify recurrence
- Review the plan

While you are creating the replication plan, 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 in a Consistency Group
- Many to many

Before you begin

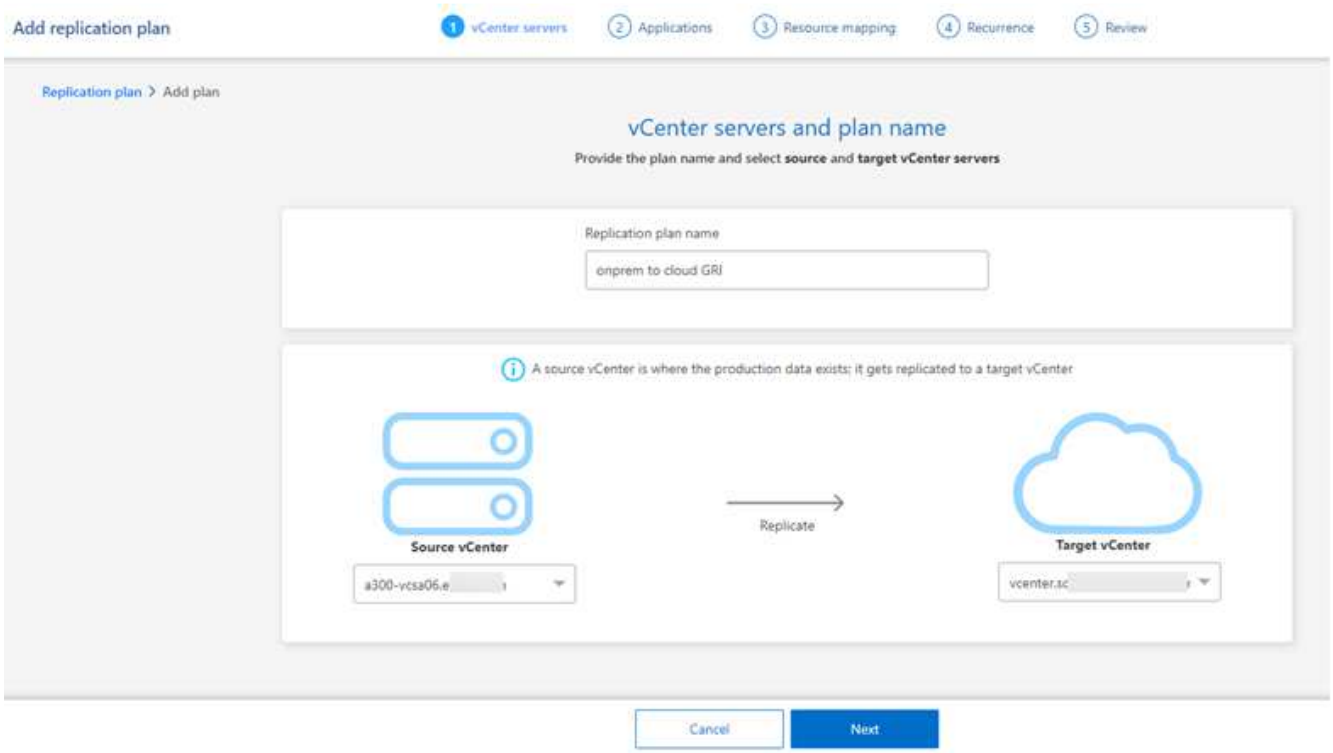
If you want to create a SnapMirror relationship in this service, the cluster and its SVM peering should have already been set up outside of BlueXP disaster recovery.

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**. 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

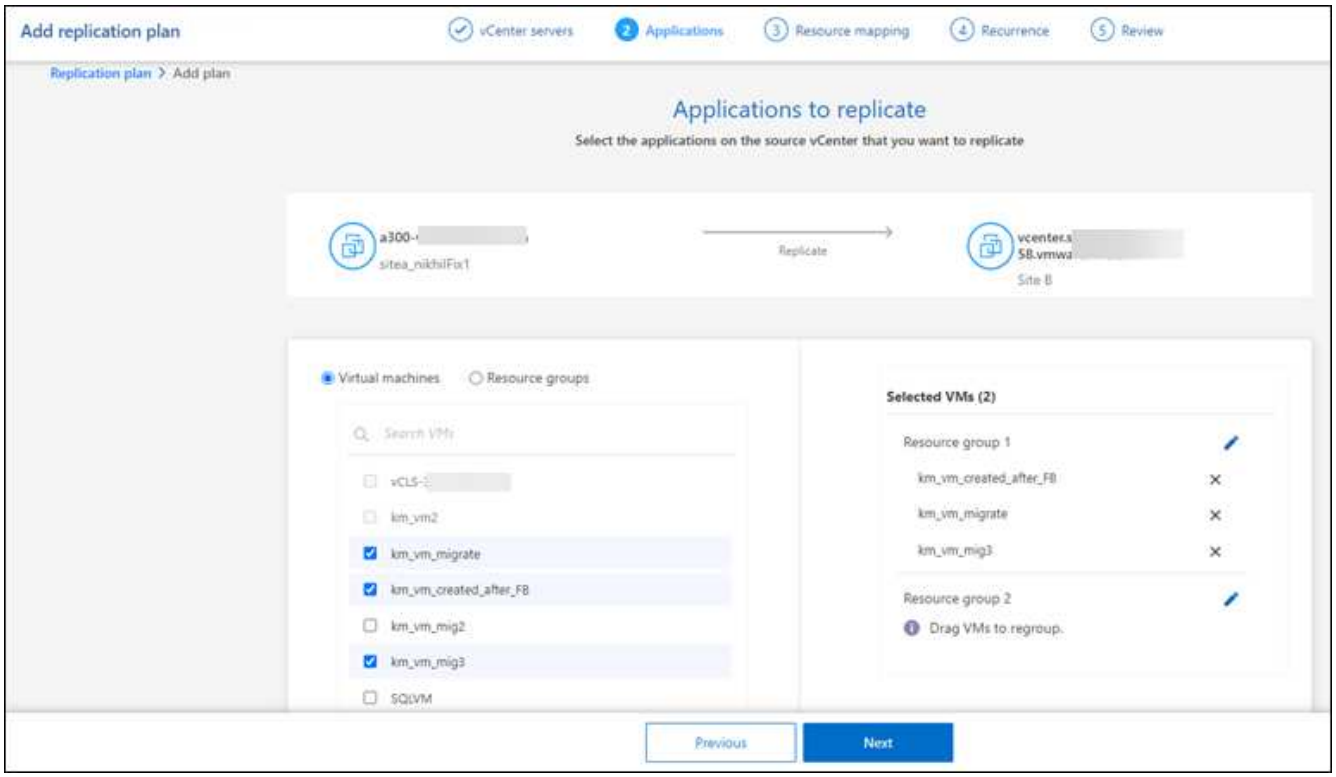
The next step is to group the required virtual machines into functional resource groups. Resource groups enable you to group a set of dependent virtual machines into logical groups that meet your requirements. For example, groups could contain delayed boot orders that can be run upon recovery.

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 here.

Steps

1. On the left side of the Applications page, select the virtual machines that you want to replicate and assign to the selected group.

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



2. Optionally, do any of the following:
   - To change groups, click the group **Edit** icon.
   - To remove a virtual machine from a group, select **X**.
   - To move a virtual machine to a different group, drag and drop it in the new group.
3. When you have multiple resource groups, ensure that the sequence of the groups matches the operational sequence that should occur.

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

4. Optionally, rename the group by clicking the **Edit** icon.
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.

Before you begin

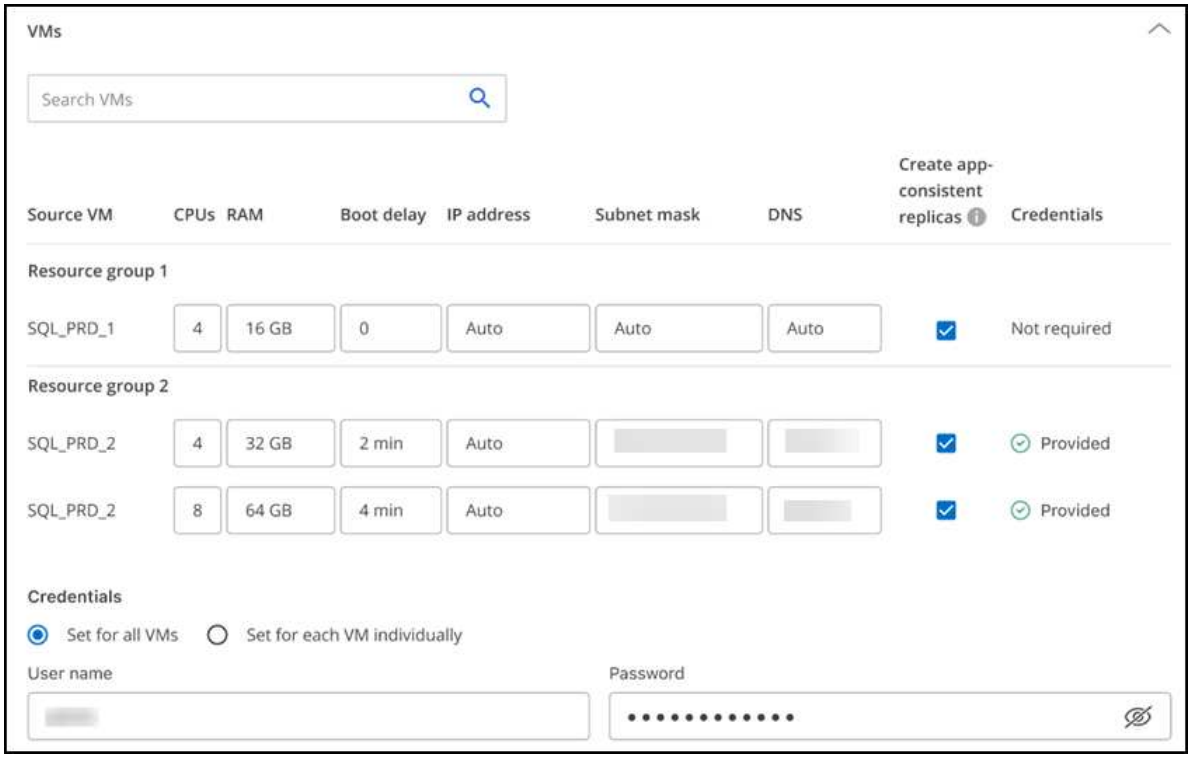
If you want to create a SnapMirror relationship in this service, the cluster and its SVM peering should have already been set up outside of BlueXP disaster recovery.

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:
    - **Compute resources**
    - **Virtual networks**
3. In the Failover mappings tab, select the down arrow to the right of each resource:
    - **Virtual machines**: Select the network mapping to the appropriate segment. The segments should already be provisioned, so select the appropriate segment to map the virtual machine.

      SnapMirror is at the volume level. So, all virtual machines are replicated to the replication target. Make sure to select all virtual machines that are part of the datastore. If they are not selected, only the virtual machines that are part of the replication plan are processed.

        - **VM CPU and RAM**: Under the Virtual machines details, you can optionally resize the VM CPU and RAM parameters.
        - **Boot order delay**: Also, you can modify the boot order for all the selected virtual machines across the resource groups. By default, the boot order selected during resource-group selection is used; however, you can make changes at this stage.
        - **DHCP or static IP**: When you are mapping networking between source and target locations in the virtual machines section of the replication plan, BlueXP disaster recovery offers two options: DHCP or static IP. For static IPs, configure the subnet, gateway, and DNS servers. Additionally, enter credentials for virtual machines.
            - **DHCP**: If you choose this option, you provide just the 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 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.

- **App-consistent replicas**: Indicate whether to create app-consistent Snapshot copies. The service will quiesce the application and then take a Snapshot to obtain a consistent state of the application.
- **Datastores**: Based on the selection of virtual machines, datastore mappings are automatically selected.
  - **RPO**: Enter the Recovery Point Objective (RPO) to indicate the amount of data to recover (measured in time). For example, if you enter an RPO of 60 minutes, the recovery must have data that is not older than 60 minutes at all times. If there is a disaster, you are allowing the loss of up to 60 minutes of data. Also enter the number of Snapshot copies to retain for all datastores.
  - **SnapMirror relationships**: If a volume has a SnapMirror relationship already established, you can select the corresponding source and target datastores. If you select a volume that does not have a SnapMirror relationship, you can create one now by selecting the working environment and its peer SVM.

    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.

- **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.
  - If you specify the Recovery Point Objective (RPO), the service schedules a primary backup based on the RPO and updates the secondary destinations.
  - 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.

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

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

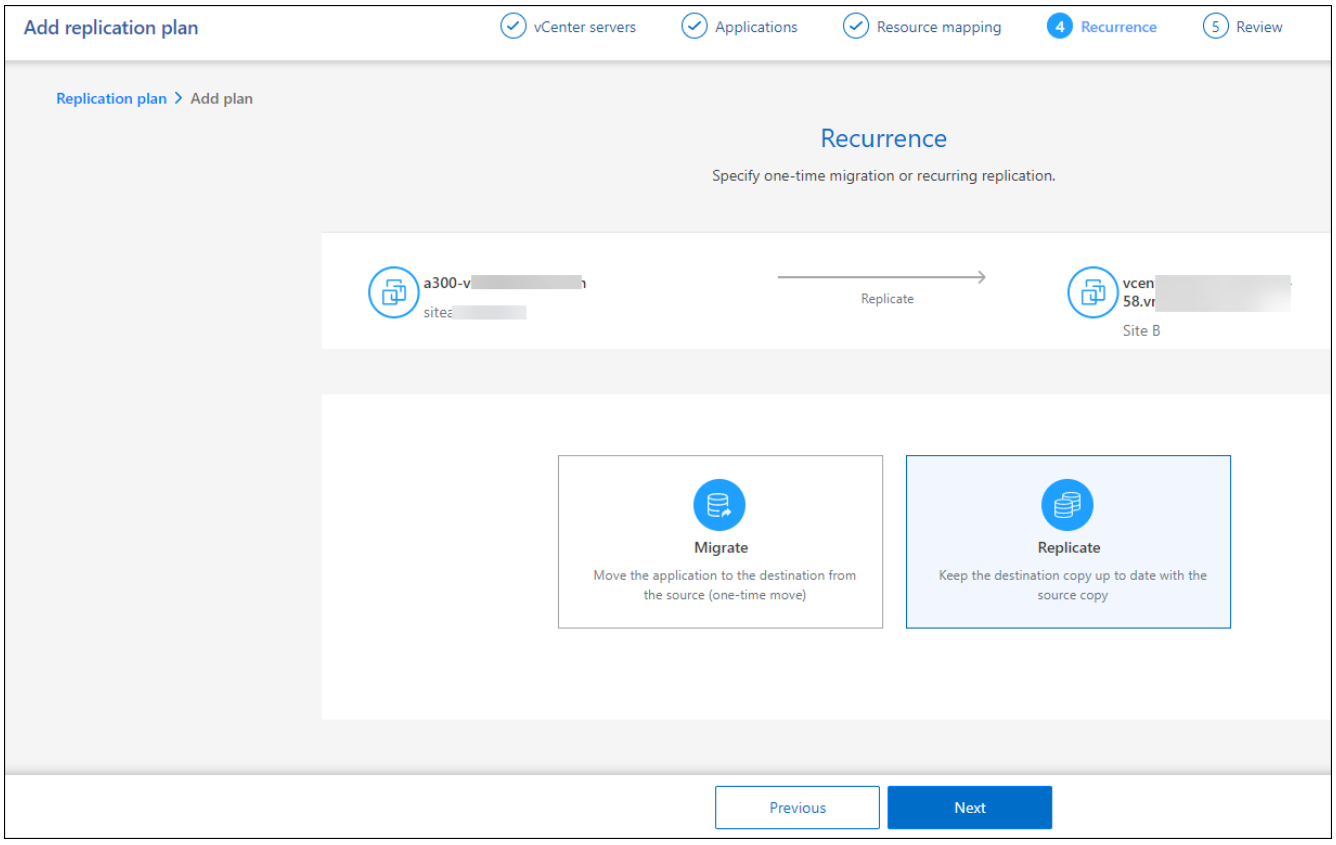
Identify the recurrence

Select whether you want to migrate data (a one-time move) to another target or replicate it at the SnapMirror frequency.

If you want to replicate it, identify how often data should be mirrored.

Steps

1. In the Recurrence page, select **Migrate** or **Replicate**.
   - **Migrate**: Select to move the application to the target location.
   - **Replicate**: Keep the target copy up to date with changes from the source copy in a recurring replication.



2. Select **Next**.

Confirm the replication plan

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

You can later disable or delete the replication plan.

Steps

1. Review information in each tab: Plan Details, Failover Mapping, Virtual Machines.
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.

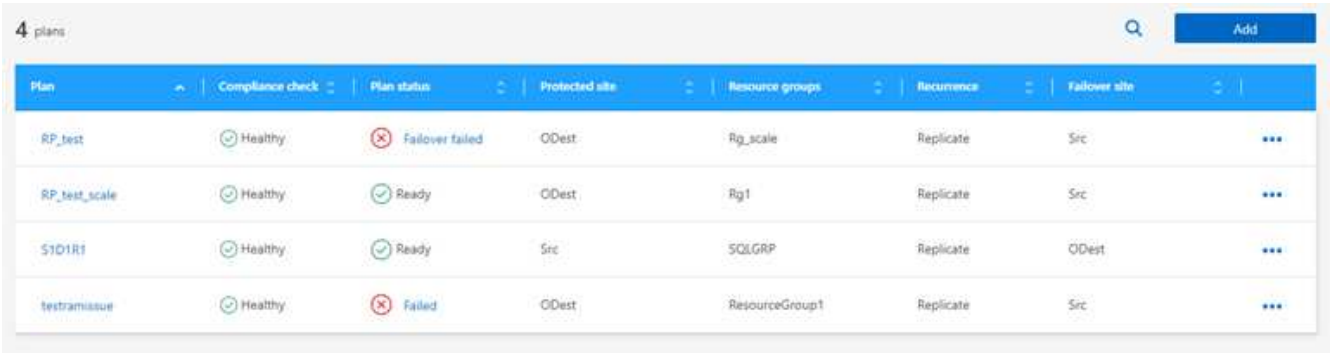
- **Compliance time impact**: When a replication plan is created, the service creates a compliance schedule by default. The default compliance time is 30 minutes. To change this time, you can use edit the schedule in the replication plan.
- **Test failover impact**: You can test a failover process on 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.

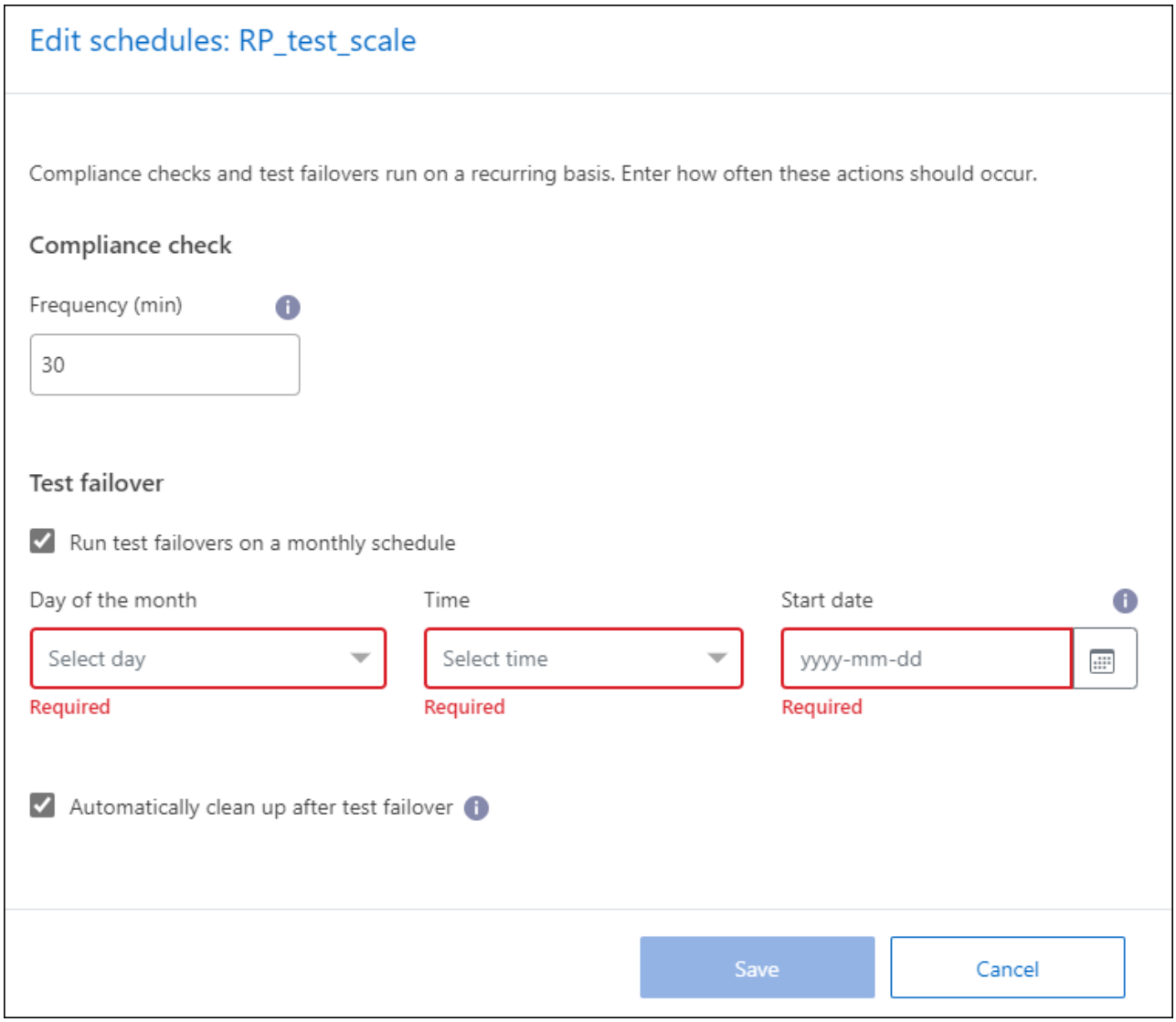
Based on the schedule, the failover test runs and ensures that workloads are moving to the destination specified by the replication plan.

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. To clean up the test environment after the failover test finishes, check **Automatically clean up after test failover**.

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

6. Select **Save**.

Replicate applications to another site

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.

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

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

In case of a disaster, fail over your primary on-premises VMware site to another on-premises VMware site or VMware Cloud on AWS.

During the failover, the most recent SnapMirror Snapshot copy is used. Or, you can select a specific Snapshot copy from a point-in-time Snapshot copy (per the retention policy of SnapMirror). The point-in-time option can be 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 procedure breaks the replication relationship, places the vCenter source VMs offline, and enables read/write on the target site.

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.

Before you start the failover, you can test the process, ensuring success when you need it. The test does not place the virtual machines offline.

Test the failover process

Before you start an actual failover, you should test the failover process.

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 Test failover page, enter the replication plan name to confirm and select **Fail over**.
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**.

Fail back applications to the original source

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.

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, plans, datastores and virtual machines information

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

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

Manage vCenter sites

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

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.

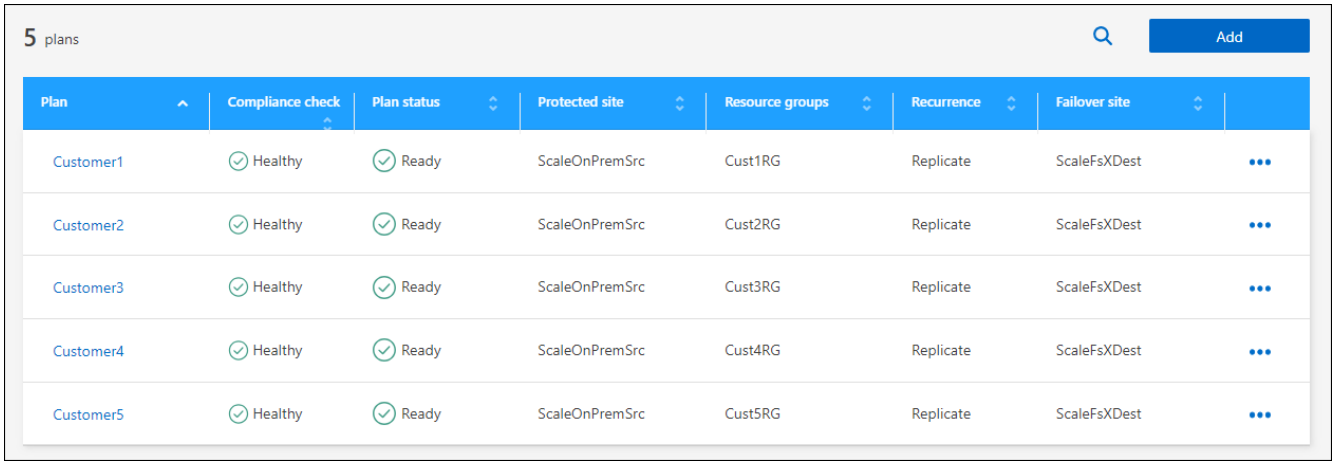
Manage replication plans

You can disable, enable and delete replication plans.

- 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 machine** tab and select the **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**, **Disable**, **Enable**, or **Delete**.

View datastores information

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

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.

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.

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 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**.

Monitor disaster recovery jobs

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

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 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.

To cancel a job, you use Swagger.

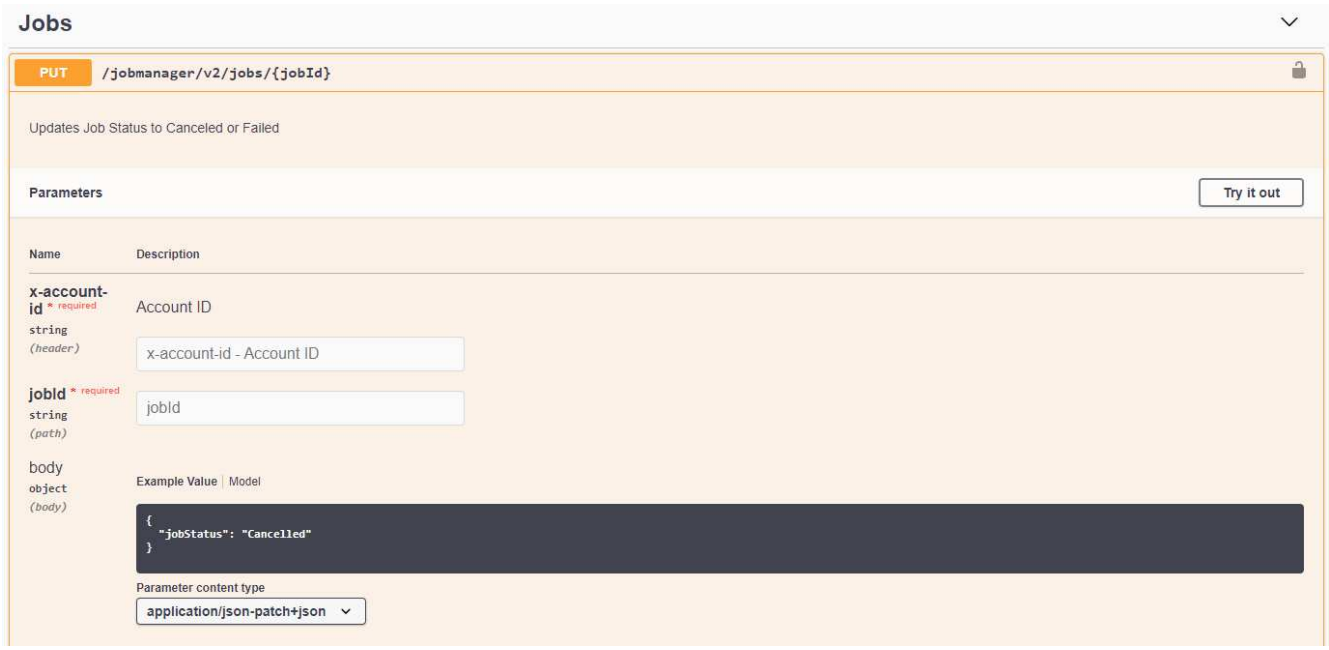
Before you begin

To cancel a job, you must have the Account ID.

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.
4. Access the BlueXP disaster recovery Swagger URL: Swagger.

   "https://snapcenter.cloudmanager.cloud.netapp.com/api-doc/#/Jobs/put_jobmanager_v2_jobs__jobId_"



   For details about Swagger, see Swagger docs.

5. From Swagger, obtain the security token, also called the *bearer token*, from the Authorize option.
6. Enter the Account ID and Job ID.
7. Select **Try it out**.

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
- Cloud Volumes Service for Google Cloud

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account ID support subscription (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 your BlueXP account for NetApp support

To register for support and activate support entitlement, one user in your BlueXP 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

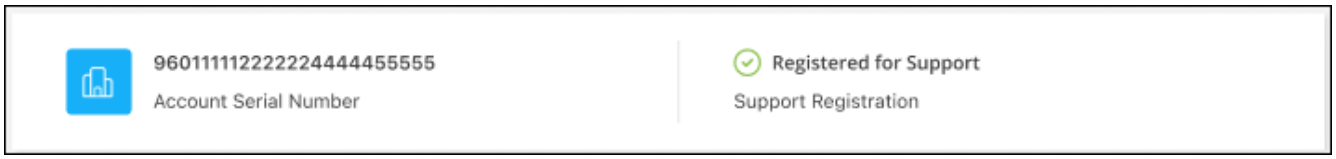
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

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 account 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 account is not registered for support. As long as one user in the account has followed these steps, then your account 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

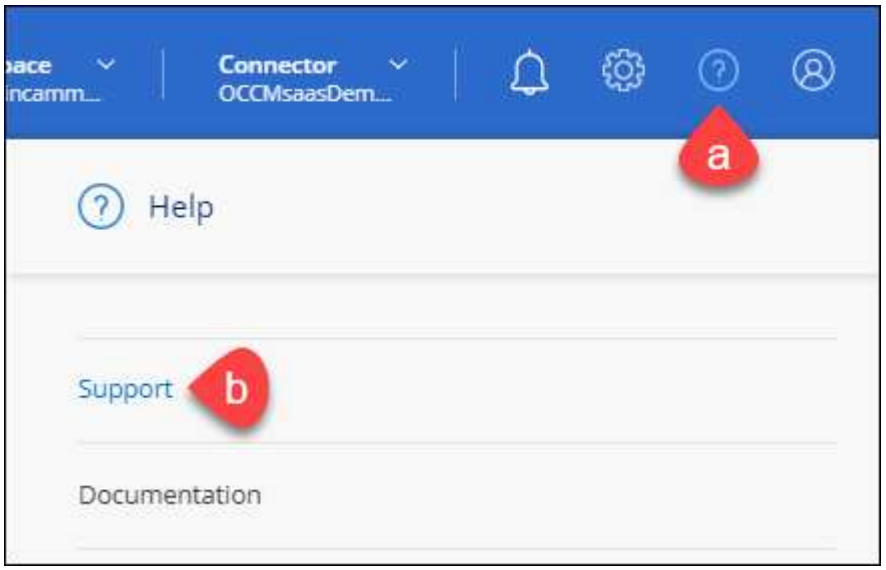
1. Create a NetApp Support Site account by completing the NetApp Support Site User Registration form
   a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
   b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field.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

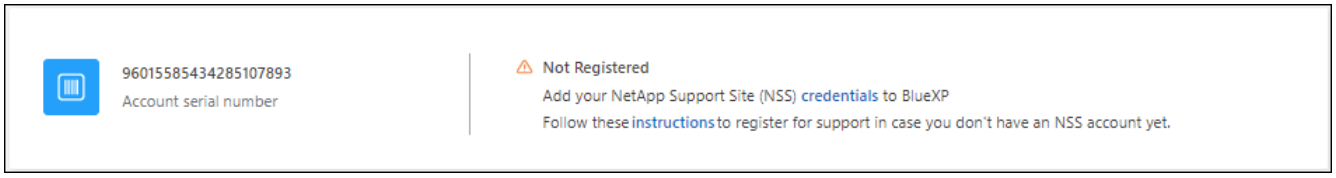
If you are brand new to NetApp and you don't have an NSS account, follow each step below.

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 the account 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 account 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

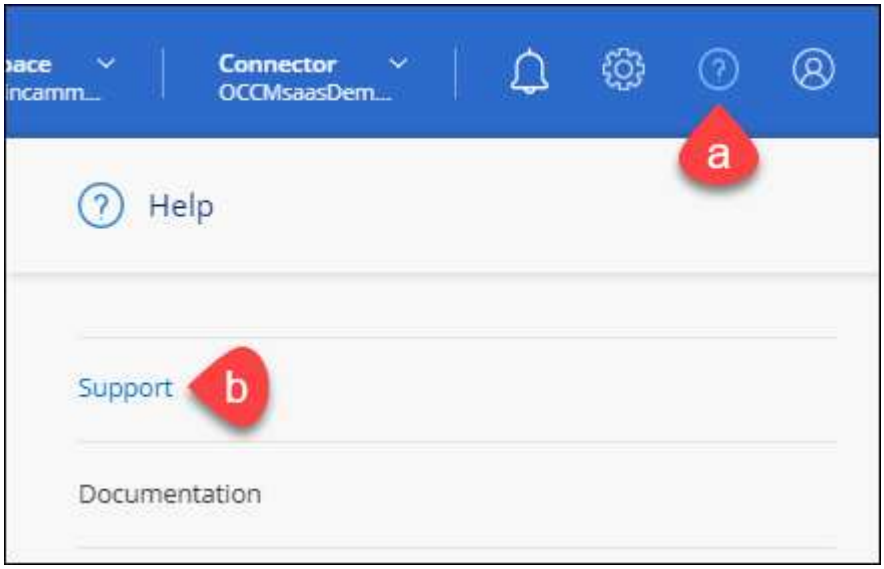
Associating NSS credentials with your BlueXP account is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP account ID. Users who belong to the BlueXP account 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 24x7, 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
- Cloud Volumes Service for Google Cloud

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.

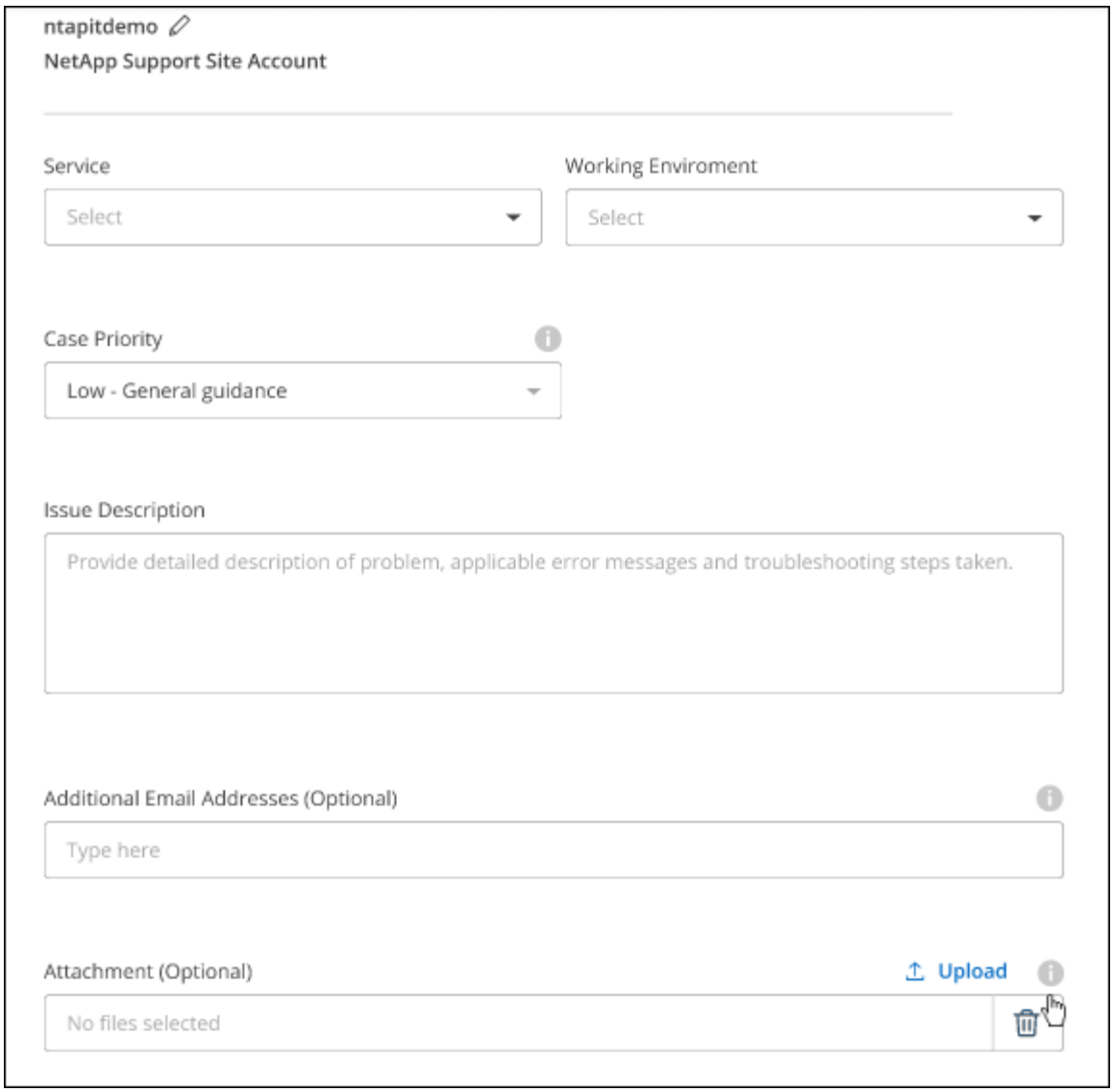
          The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.

        - **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.

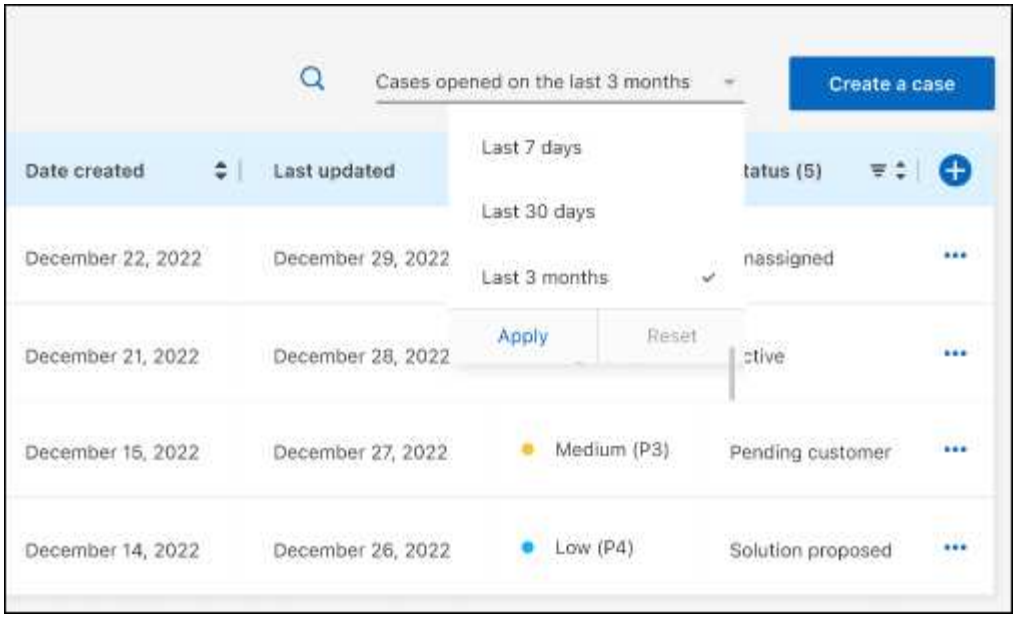
  The results in the table reflect the cases related to the view that you selected.
- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

  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.

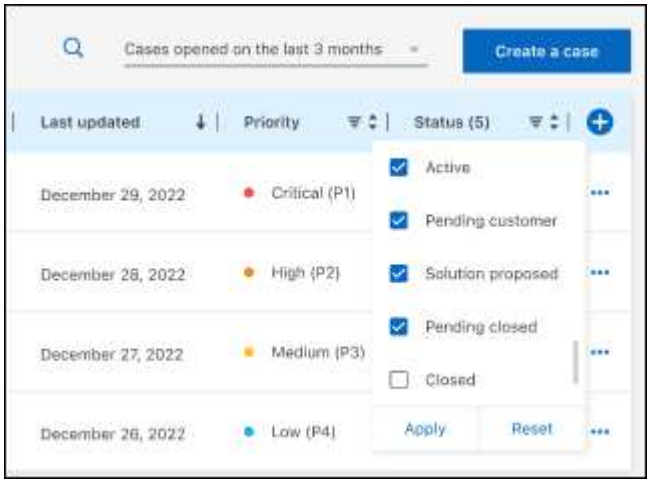
Steps

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

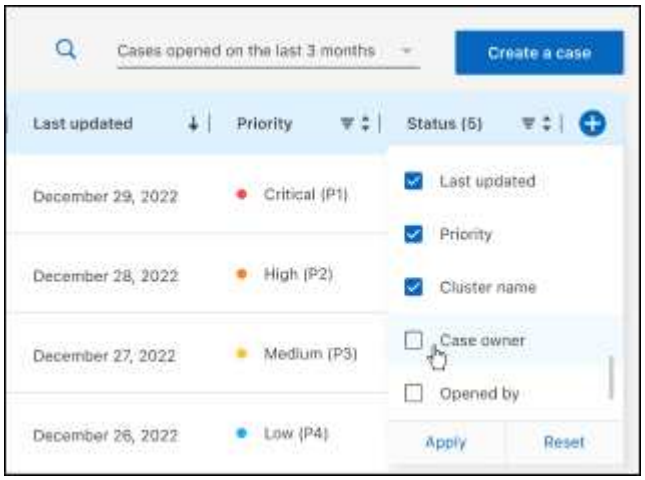
   The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.
3. Optionally modify the information that displays in the table:
   - Under **Organization's 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.

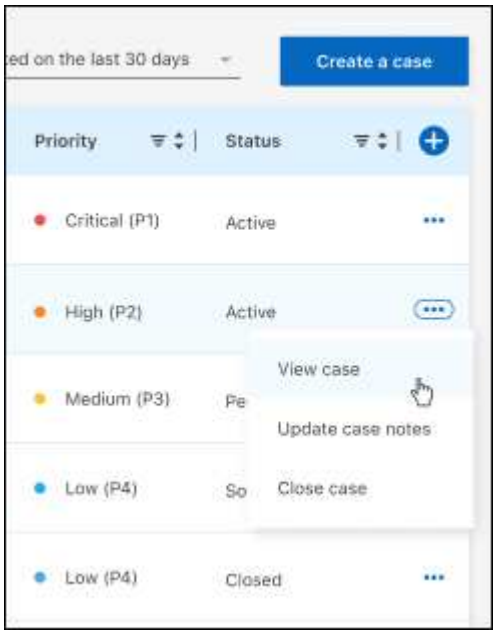


4. Manage an existing case by selecting ••• and selecting one of the available options:

   - **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.

Copyright information

Trademark information