Reference

NetApp Disaster Recovery

NetApp
February 04, 2026

Table of Contents

Reference

Required vCenter privileges for NetApp Disaster Recovery

For NetApp Disaster Recovery to perform its services, the vCenter account must have a minimum set of vCenter privileges. These privileges include registering and deregistering datastores, starting and stopping virtual machines (VMs), and reconfiguring VMs.

The following table lists all privileges required for Disaster Recovery to interface with a vCenter cluster.

Type	Privilege name (vSphere client)	Privilege name (API)	Description
Datastore	Datastore.Config	Configure datastore	Permits configuring a datastore.
	Datastore.Delete	Remove datastore	Permits removing a datastore.
	Datastore.Rename	Rename datastore	Permits renaming a datastore.
Folder	Folder.Create	Create folder	Permits creating a new folder.
	Folder.Delete	Delete folder	Permits deleting a folder. Requires privilege on both the object and its parent.
	Folder.Rename	Rename folder	Permits modifying a folder name.
Network	Network.Assign	Assign network	Permits assigning a network to a VM.
	Network.Config	Configure	Permits configuring a network.
Virtual machine configuration	VirtualMachine.Config.AdvancedConfig	Advanced configuration	Permits adding or modifying advanced parameters in the VM's configuration file.
	VirtualMachine.Config.Settings	Change settings	Permits changing general VM settings.
	VirtualMachine.Config.CPUCount	Change CPU count	Permits changing the number of virtual CPUs.
	VirtualMachine.Config.Memory	Change memory	Permits changing the amount of memory allocated to the VM.
	VirtualMachine.Config.Resource	Change resource	Permits changing the resource configuration of VM nodes in a resource pool.
	VirtualMachine.Config.Rename	Rename	Permits renaming a VM or modifying its notes.
	VirtualMachine.Config.EditDevice	Modify device settings	Permits changing an existing device's properties.
	VirtualMachine.Config.ReloadFromPath	Reload from path	Permits changing a VM configuration path while preserving identity.
	VirtualMachine.Config.ResetGuestInfo	Reset guest information	Permits editing the guest operating system information for a VM.

Type	Privilege name (vSphere client)	Privilege name (API)	Description
Virtual machine guest	VirtualMachine.GuestOperations.ModifyAliases	Guest operation alias modification	Permits modifying the alias for the VM.
	VirtualMachine.GuestOperations.QueryAliases	Guest operation alias query	Permits querying a VM's alias.
	VirtualMachine.GuestOperations.Modify	Guest operation modifications	Permits modification operations, including transferring a file to the VM.
	VirtualMachine.GuestOperations.Execute	Guest operation program execution	Permits running an application inside the VM.
	VirtualMachine.GuestOperations.Query	Guest operation queries	Permits querying the guest OS. Operations include listing files.
Virtual machine interaction	VirtualMachine.Interact.AnswerQuestion	Answer question	Permits resolving issues during VM state transitions or runtime errors.
	VirtualMachine.Interact.PowerOff	Power off	Permits powering off a powered-on VM.
	VirtualMachine.Interact.PowerOn	Power on	Permits powering on or resuming a VM.
	VirtualMachine.Interact.ToolsInstall	VMware Tools install	Permits mounting/unmounting the VMware Tools installer.
	VirtualMachine.Inventory.CreateFromExisting	Create from existing	Permits cloning or deploying a VM from a template.
	VirtualMachine.Inventory.Create	Create new	Permits creating a VM and allocating resources.
	VirtualMachine.Inventory.Register	Register	Permits adding an existing VM to an inventory.
	VirtualMachine.Inventory.Delete	Remove	Permits deleting a VM and its files. Requires privileges on both the object and its parent.
	VirtualMachine.Inventory.Unregister	Unregister	Permits unregistering a VM. This permission requires privileges on both the object and its parent.
Virtual machine provisioning	VirtualMachine.Provisioning.Clone	Clone virtual machine	Permits cloning a VM and allocating resources.
	VirtualMachine.Provisioning.Customize	Customize guest	Permits customizing the VM's guest operating system.
	VirtualMachine.Provisioning.ModifyCustSpecs	Modify customization specification	Permits creating, modifying, or deleting customization specifications.
	VirtualMachine.Provisioning.ReadCustSpecs	Read customization specifications	Permits reading a customization specification for a VM.

Type	Privilege name (vSphere client)	Privilege name (API)	Description
Virtual machine service configuration	VirtualMachine.Namespace.Query	Query service configurations	Permits retrieving a list of VM services.
	VirtualMachine.Namespace.ReadContent	Read service configuration	Permits retrieving the existing VM service configuration.
Virtual machine snapshot	VirtualMachine.State.CreateSnapshot	Create snapshot	Permits creating a snapshot from the VM's current state.
	VirtualMachine.State.RemoveSnapshot	Remove snapshot	Permits removing a snapshot.
	VirtualMachine.State.RenameSnapshot	Rename snapshot	Permits renaming a snapshot or updating its description.
	VirtualMachine.State.RevertToSnapshot	Revert to snapshot	Permits reverting the VM to the state of a given snapshot.

Switch Console agents when using NetApp Disaster Recovery

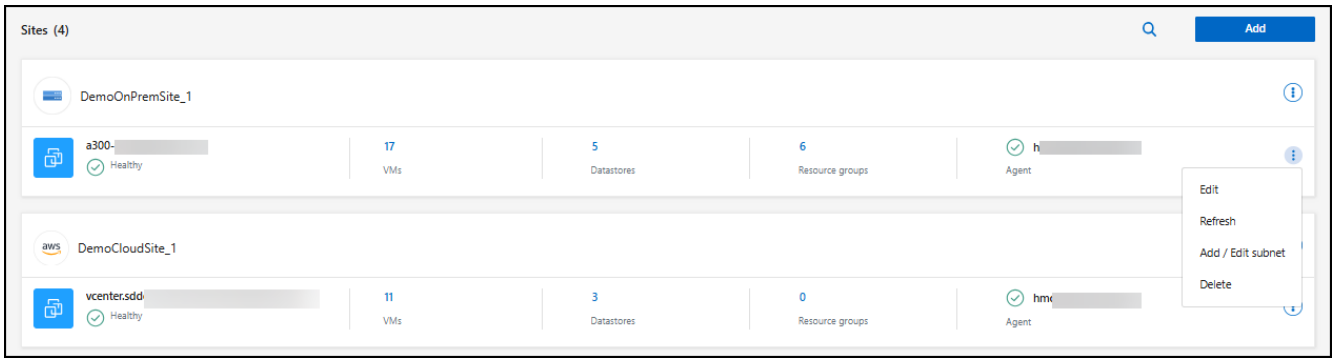
The NetApp Console supports using multiple Console agents with a single working environment. Using multiple Console agents can be helpful for maintaining access to resources while performing maitenance on another Console agent or if a Console agent fails. Because each Console agent has a unique identifier, improperly switching Console agents can compromise the availability of resources in a working environment.

Before you begin

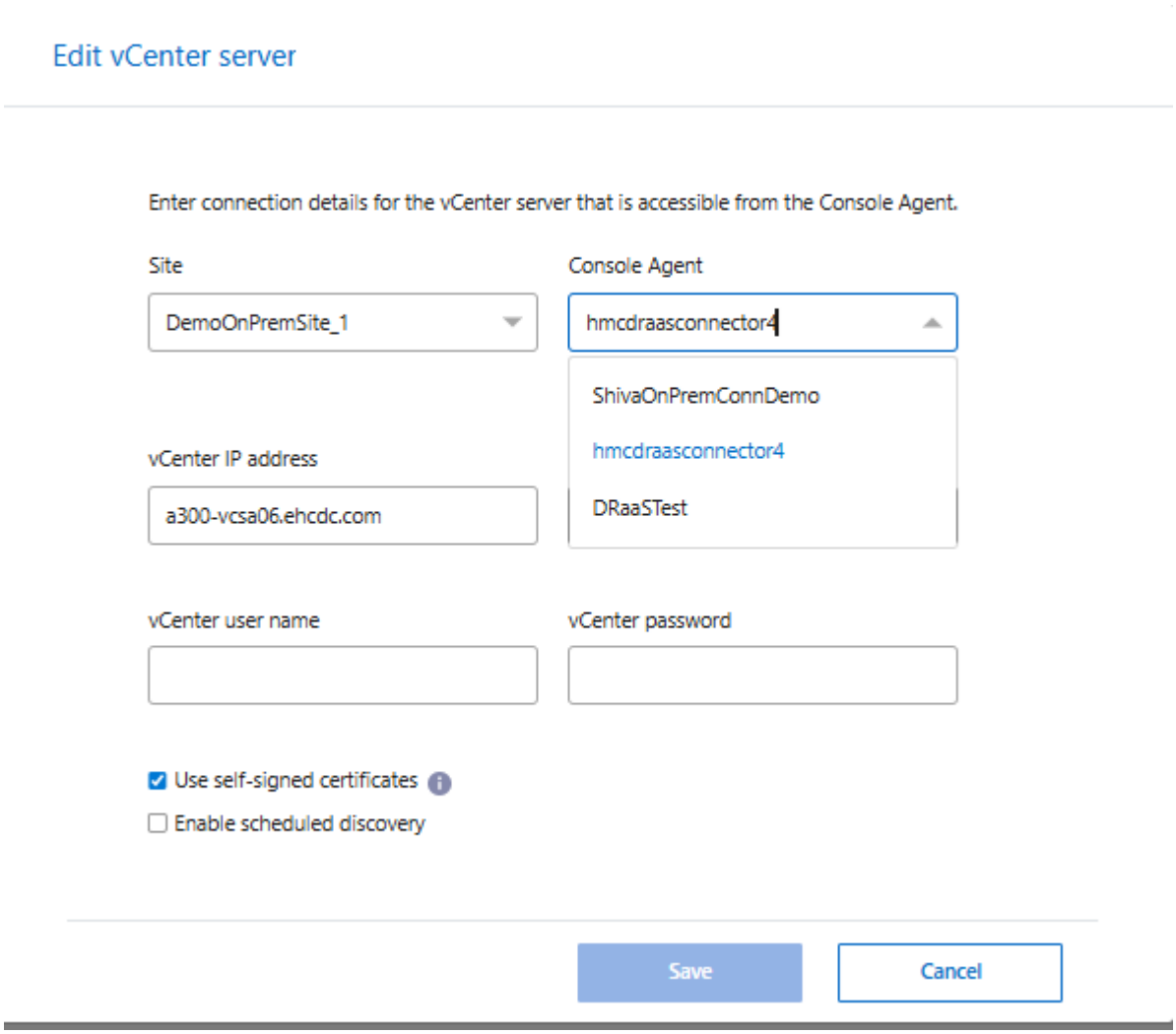
- You must have added at least two Console agents for your working environment.
- Both Console agents must contain the same ONTAP clusters.

Steps

1. In Disaster Recovery, select **Sites**.
2. You must change the Console agent for both the source and destination vCenters. Identify the vCenters you want to modify. Select the action menu for the vCenter then **Edit**.



3. Select the Console agent you want to use from the dropdown menu and reenter your vCenter username and password. Select **Save**.



4. Repeat steps 2 and 3 for each additional vCenter you want to modify.
5. In the vCenter that you modified, refresh the vCenter to discover the new Console agent. Repeat this step for every vCenter you've modified.
6. In Disaster Recovery, navigate to **Replication plans**.
7. Identify the replication plans that you want to use to resume workflows. Select the action menu … then **Refresh resources**. You can monitor the status of the jobs in **Job monitoring**.

More information

- Learn about Console agents

Use NetApp Disaster Recovery with Amazon EVS

Introduction of NetApp 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 NetApp Disaster Recovery service.

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 NetApp Disaster Recovery using Amazon EVS and Amazon FSs for NetApp ONTAP

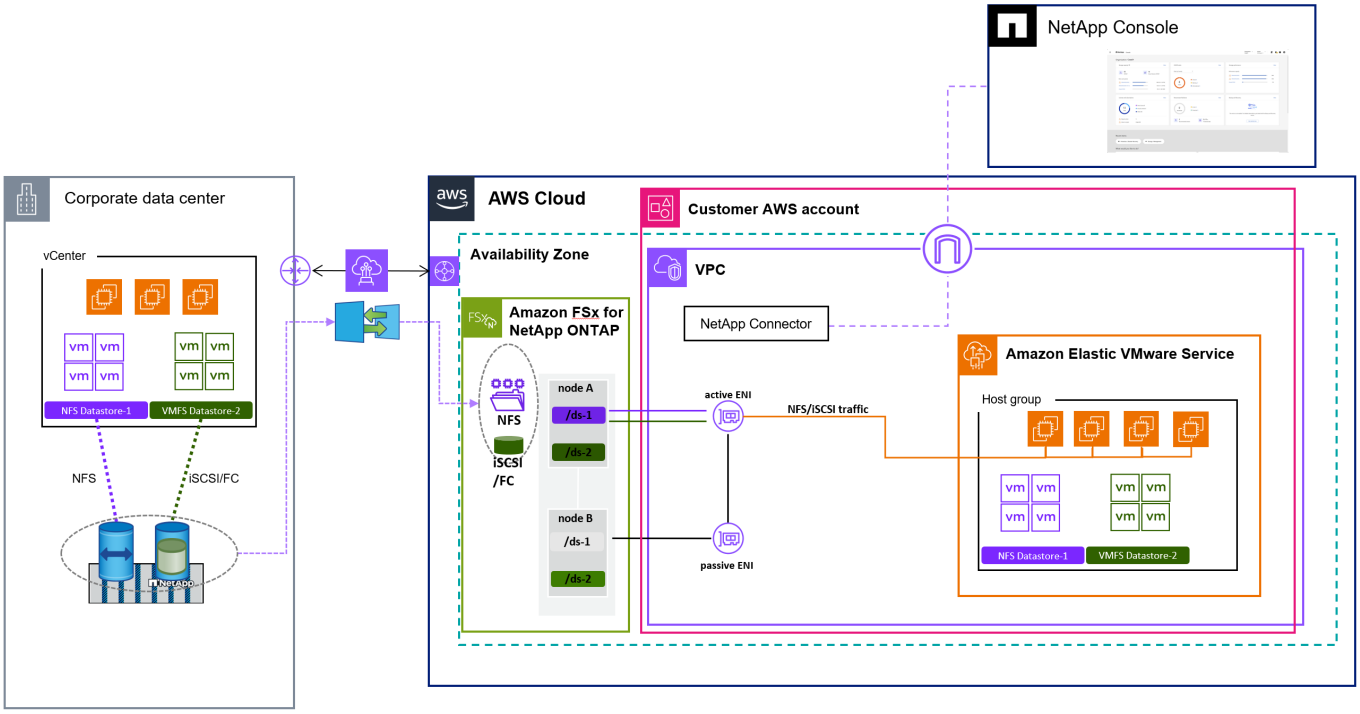
NetApp Disaster Recovery is a value-added service hosted within the NetApp Console software-as-a-service environment, which depends on the core NetApp Console architecture. Several main components comprise the DR service for VMware protection within the Console.

For a complete overview of the NetApp Disaster Recovery solution, see Learn about NetApp 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 NetApp 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 Console agent is installed in your VPC. The NetApp Console agent hosts multiple data management services (called agents), including the NetApp Disaster Recovery agent that manages DR of the VMware infrastructure on both your local physical datacenters and your Amazon AWS hosted resources.
4. The NetApp Disaster Recovery agent securely communicates with the NetApp Console 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 NetApp Console 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, NetApp 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 NetApp Console and selects a backup to use as the restore point.
9. The NetApp 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 NetApp Console agent for NetApp Disaster Recovery

A NetApp Console agent enables you to connect your NetApp Console deployments to your infrastructure in order to securely orchestrate solutions across AWS, Azure, Google Cloud, or on-premises environments. The Console agent executes the actions that the NetApp Console needs to perform to manage your data infrastructure. The Console agent constantly polls the NetApp Disaster Recovery software as a service layer for any actions that it needs to take.

For NetApp Disaster Recovery, 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. Although the Console agent can be installed in any of your network locations, it's recommended you install the Console agent in the disaster recovery site for NetApp Disaster Recovery. Installing in the DR site ensures that in the event of a failure of the primary site, the NetApp console UI maintains its connection to the Console agent and can orchestrate the recovery process within that DR site.

Installation

- To use Disaster Recovery, install the Console agent in standard mode. To learn more about the types of Console agent installations, visit Learn about NetApp Console deployment modes.

The specific installation steps for the Console agent depend on your deployment type. See Learn about Console agents for more information.

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

Configure NetApp Disaster Recovery for Amazon EVS

Configure NetApp Disaster Recovery for Amazon EVS overview

After you install the NetApp Console agent, you need to integrate all the ONTAP storage and VMware vCenter resources that will participate in the disaster recovery process with NetApp Disaster Recovery.

- Prerequisites for Amazon EVS with NetApp Disaster Recovery
- Add ONTAP storage arrays to NetApp Disaster Recovery
- Enable NetApp Disaster Recovery for Amazon EVS
- Add vCenter sites to NetApp Disaster Recovery
- Add vCenter clusters to NetApp Disaster Recovery

Prerequisites for Amazon EVS with NetApp Disaster Recovery

Ensure you review and meet the requirements to configure Amazon EVS with NetApp Disaster Recovery.

Prerequisites

- Review the general prerequisites for Disaster Recovery.

- Create a vCenter user account with the specific VMware privileges required for NetApp Disaster Recovery to perform the necessary operations.

> It's recommended you do **not** use the default "administrator@vsphere.com" administrator account. Instead, you should create a NetApp Disaster Recovery specific user account on all vCenter clusters that will participate in the disaster recovery process. For a list of specific privileges required, see vCenter privileges needed for NetApp Disaster Recovery.

- Ensure that all vCenter datastores that will host VMs protected by Disaster Recovery are located on NetApp ONTAP storage resources.

  Disaster Recovery supports NFS and VMFS on iSCSI (and not FC) when using Amazon FSx on NetApp ONTAP. Although Disaster Recovery supports FC, Amazon FSx for NetApp ONTAP does not.

- Ensure your Amazon EVS vCenter is connected to an Amazon FSx for NetApp ONTAP storage cluster.
- Ensure VMware tools are installed on all protected VMs.
- Ensure your on-premises network is connected to your AWS VPC network using an Amazon-approved connection method. It's recommended you use AWS Direct Connect, AWS Private Link, or an AWS Site-to-Site VPN.
- Review and ensure compliance with the connection and port requirements for EVS with Disaster Recovery:

Source	Destination	Port	Details
Amazon FSxN	On-premises ONTAP	TCP 11104, 11105, ICMP	SnapMirror
On-premises ONTAP	Amazon FSxN	TCP 11104, 11105, ICMP	SnapMirror
NetApp Console agent	On-premises ONTAP	TCP 443, ICMP only	API calls
NetApp Console agent	Amazon FSxN	TCP 441, ICMP only	API calls
NetApp Console agent	vCenter (on-premises, EVS), ESXi host (on-premises, EVS)	443	API calls, script execution

Add on-premises arrays to the NetApp Console system for Amazon EVS with NetApp Disaster Recovery

Before using NetApp Disaster Recovery, you must add on-premises and cloud-hosted storage instances to the NetApp Console system.

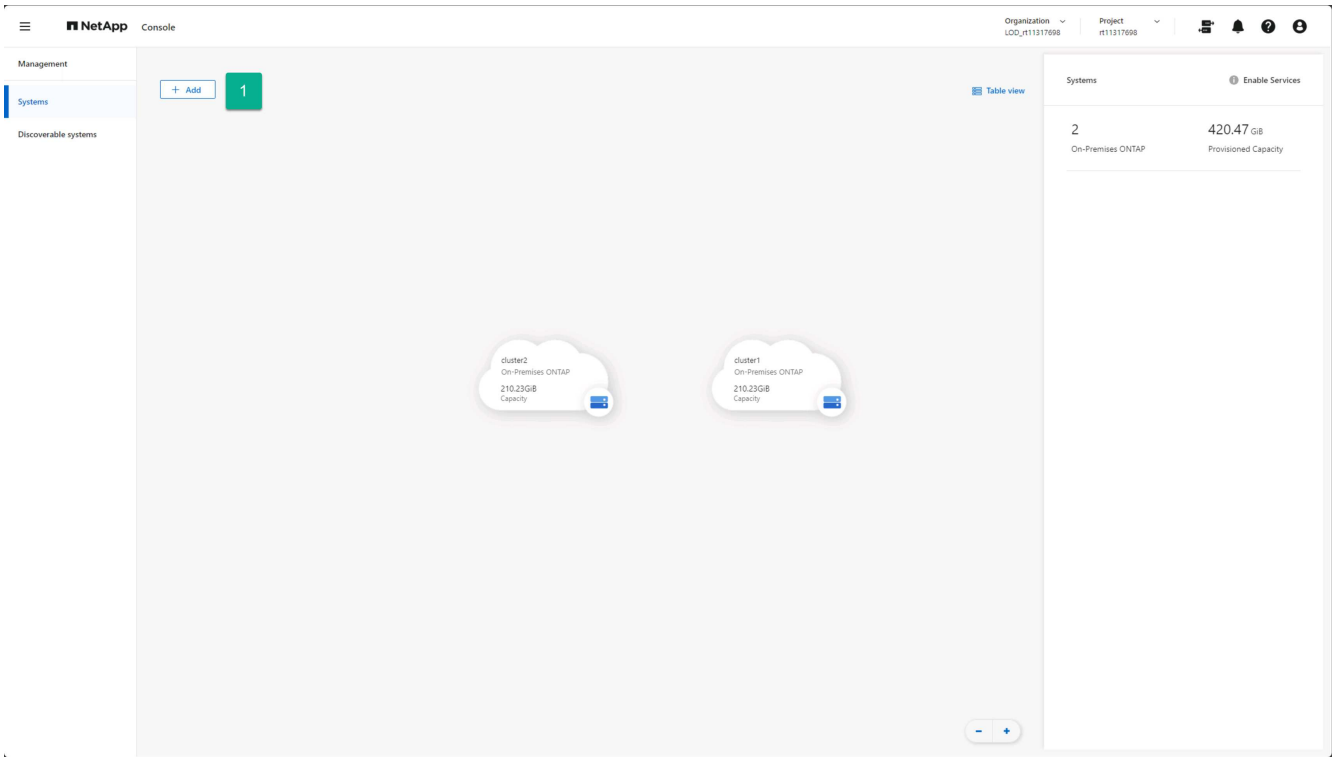
You need to do the following:

- Add on-premises arrays to your NetApp Console system.
- Add Amazon FSx for NetApp ONTAP (FSx for ONTAP) instances to your NetApp Console system.

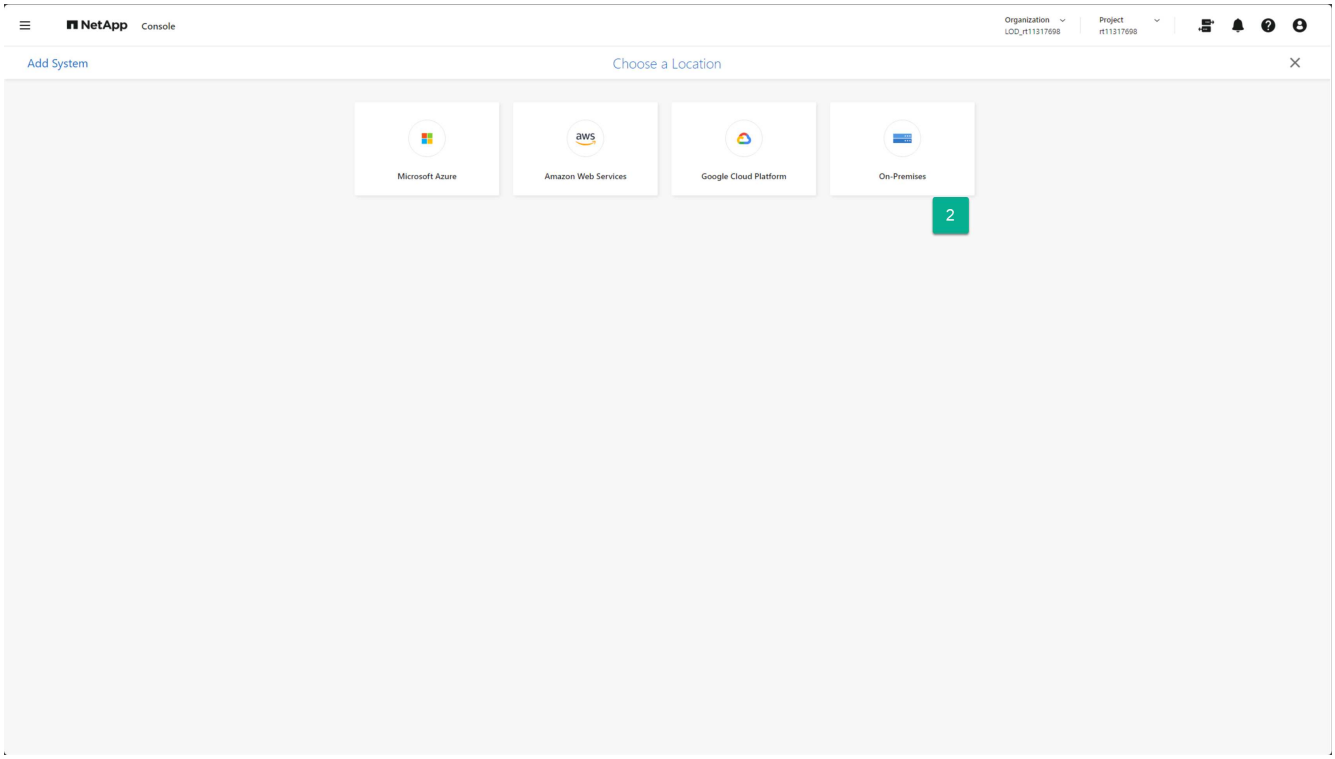
Add on-premises storage arrays to NetApp Console system

Add on-premises ONTAP storage resources to your NetApp Console system.

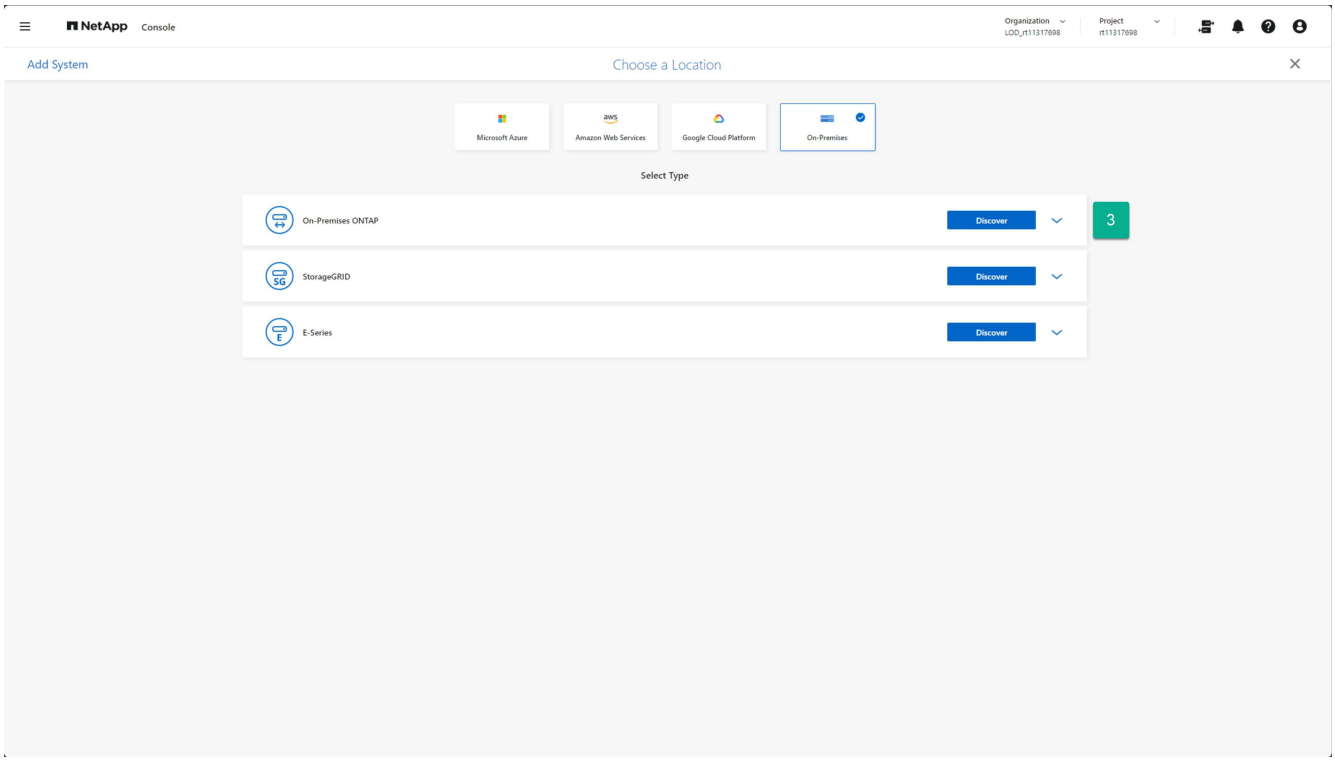
1. From the NetApp Console Systems page, select **Add System**.



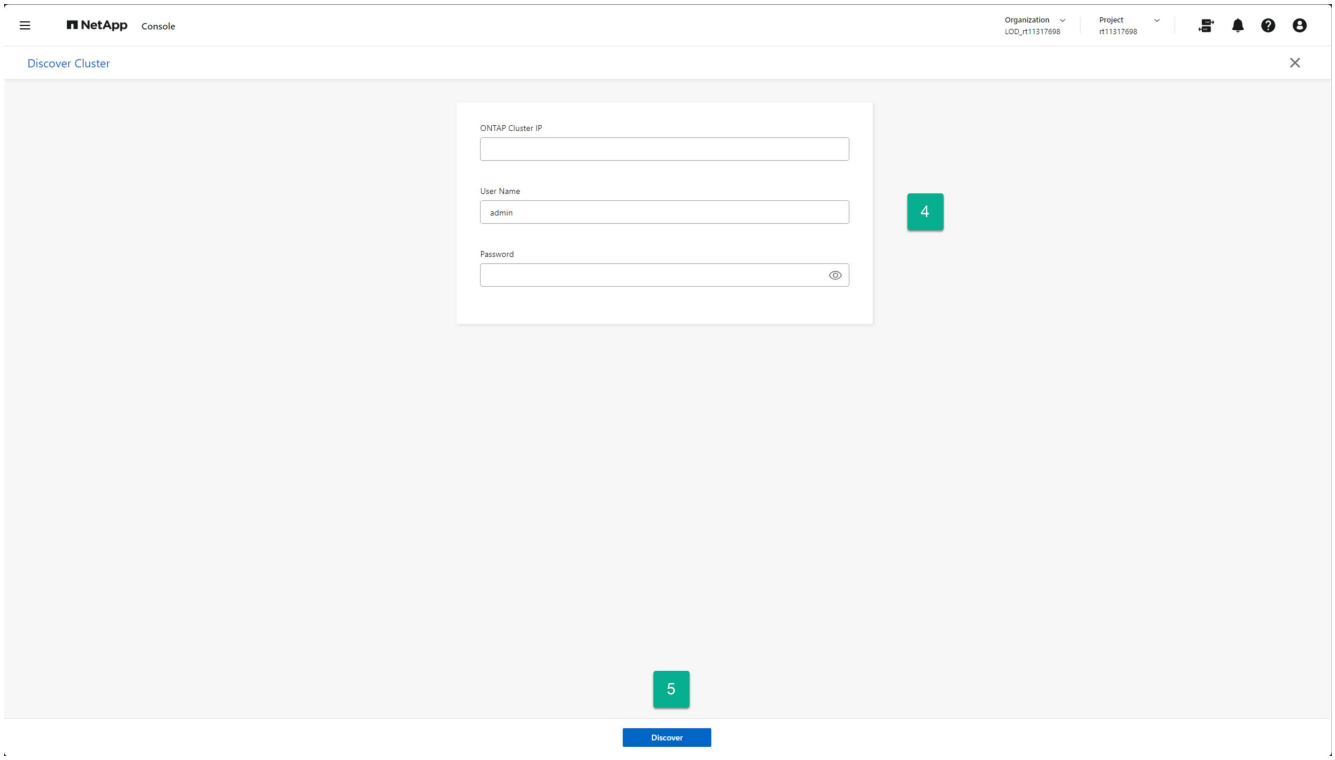
2. From the Add System page, select the **On-Premises** card.



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.

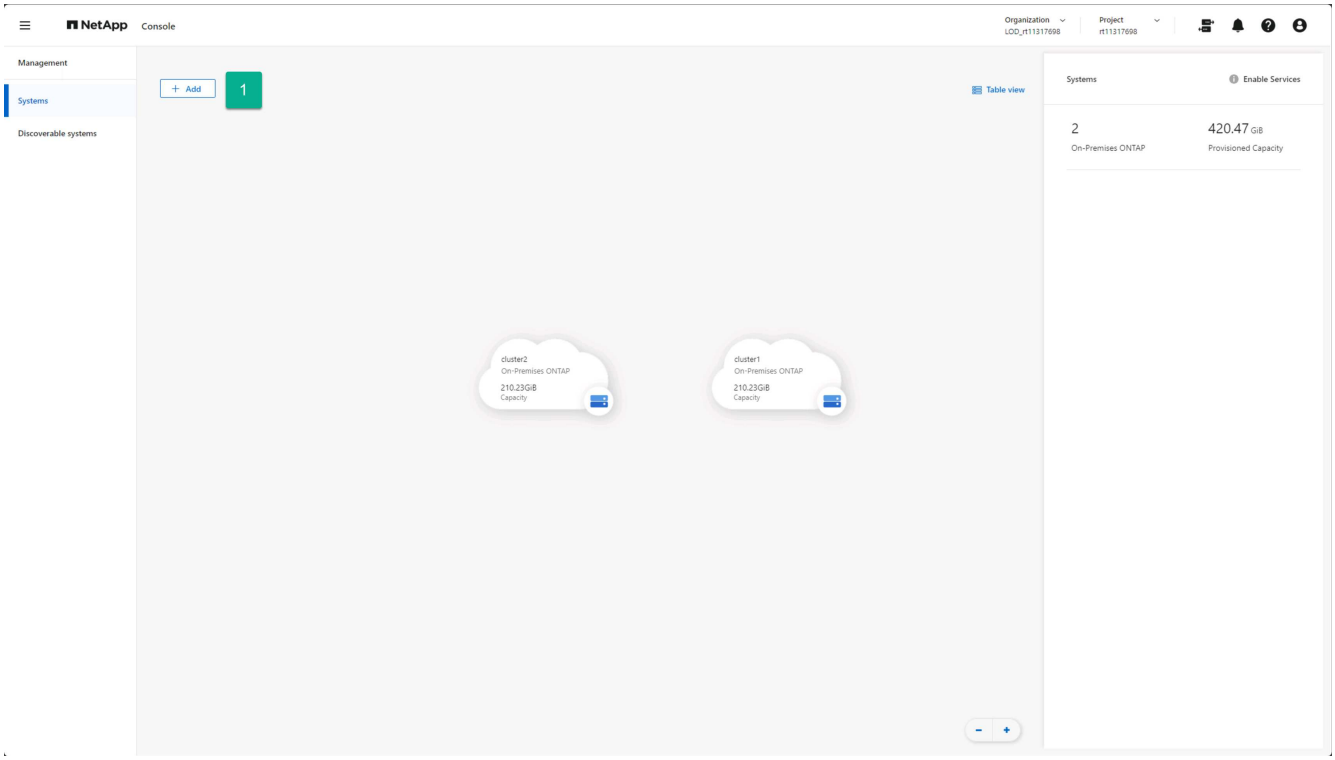


6. Repeat steps 1-5 for each ONTAP array that will host vCenter datastores.

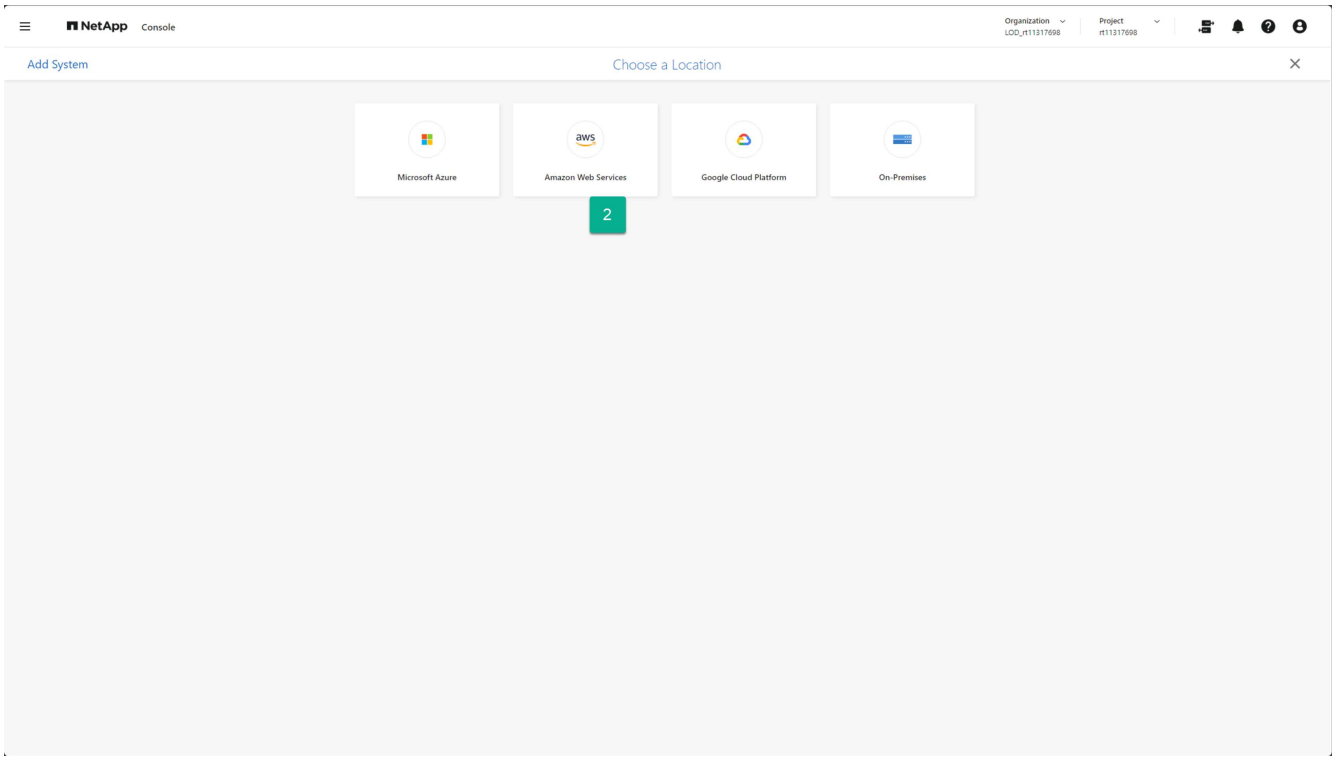
Add Amazon FSx for NetApp ONTAP storage instances to NetApp Console system

Next, add an Amazon FSx for NetApp ONTAP storage resources to your NetApp Console system.

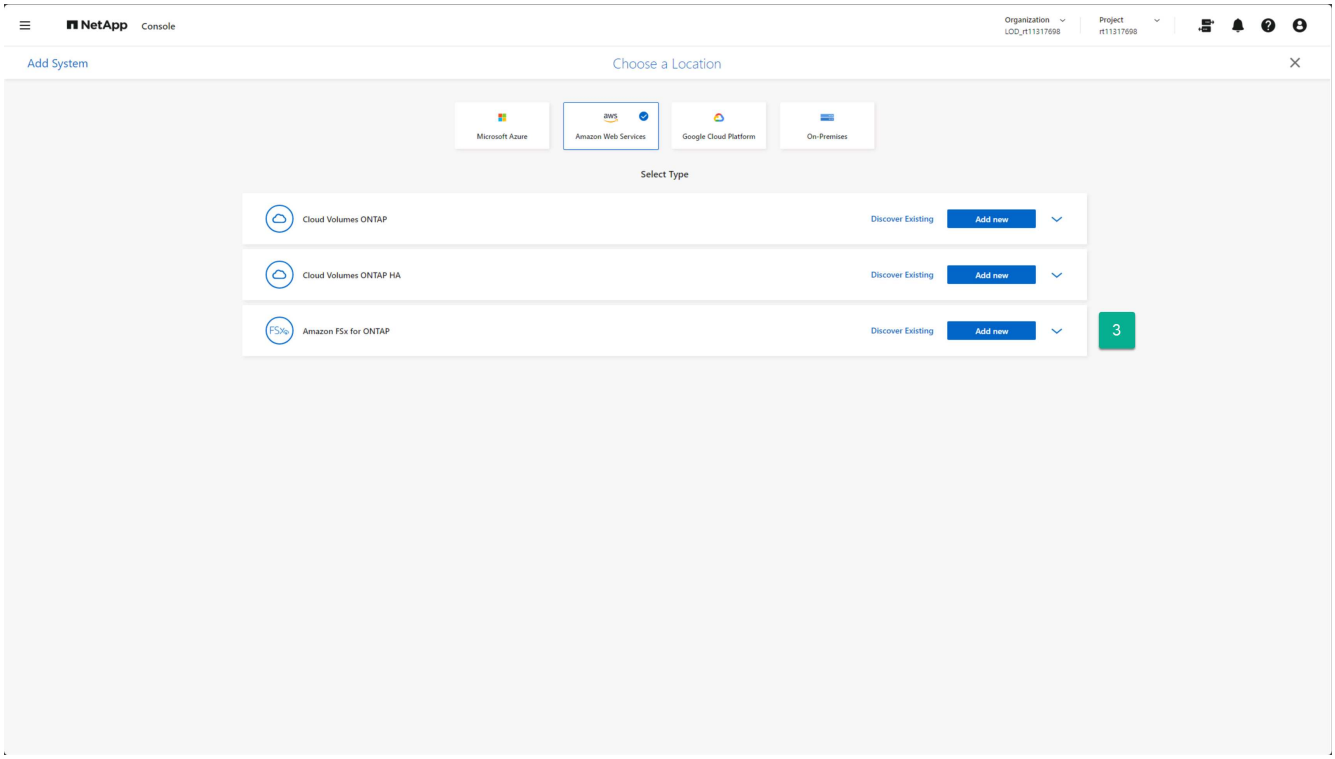
1. From the NetApp Console Systems page, select **Add System**.



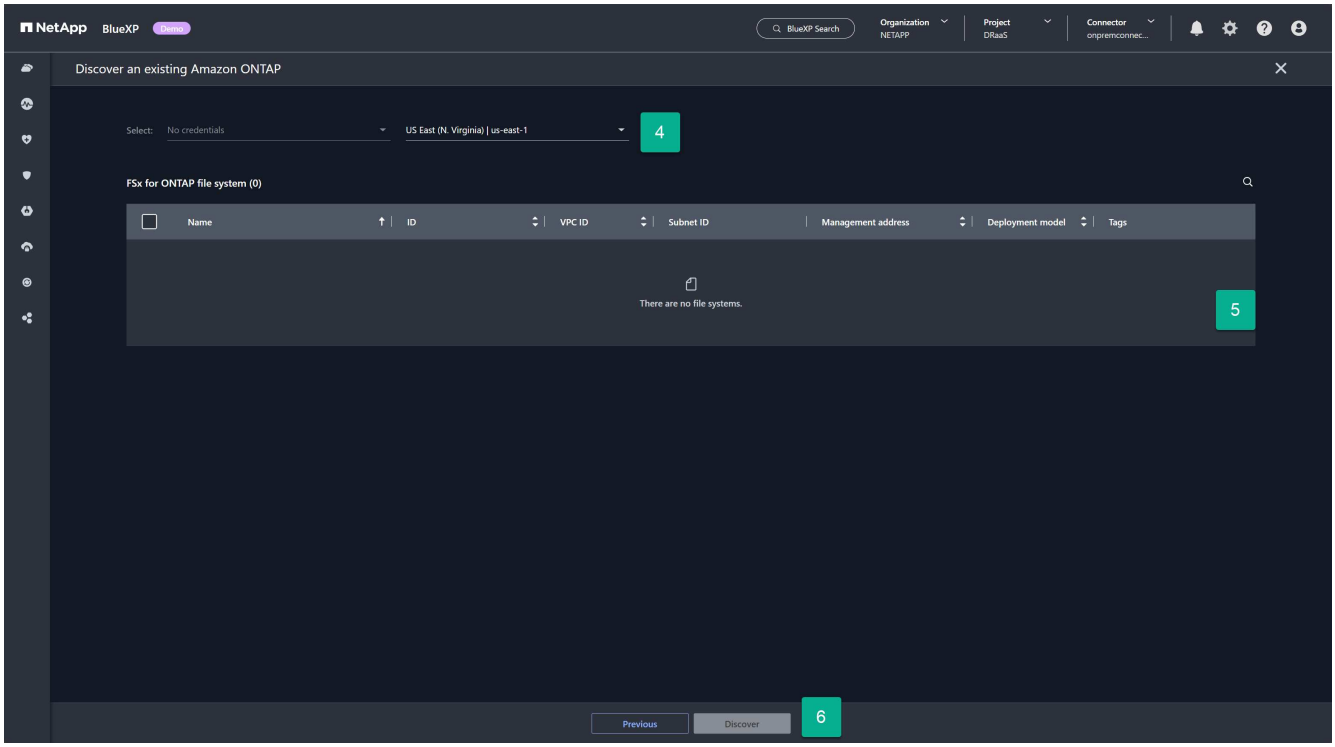
2. From the Add System page, select the **Amazon Web Services** card.



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 NetApp Disaster Recovery service to your NetApp Console account for Amazon EVS

NetApp 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 NetApp Disaster Recovery licenses, see Set up licensing for NetApp Disaster Recovery.

License types

There are two primary license types:

- NetApp offers a 30-day trial license that you can use to evaluate NetApp 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 marketplace license for NetApp 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 NetApp 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). NetApp 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 NetApp 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 NetApp 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:

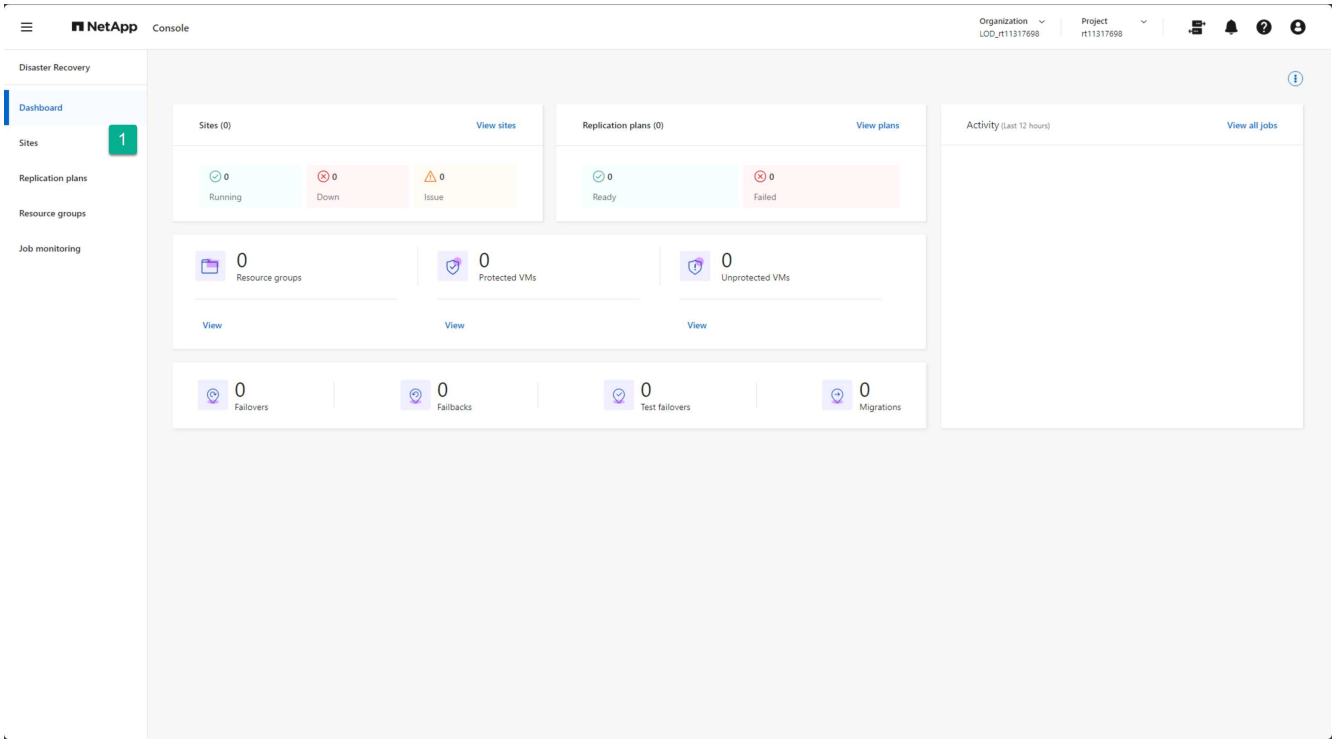
- A site to represent each production datacenter where your production vCenter clusters reside
- A site for your Amazon EVS/Amazon FSx for NetApp ONTAP cloud datacenter

Create on-premises sites

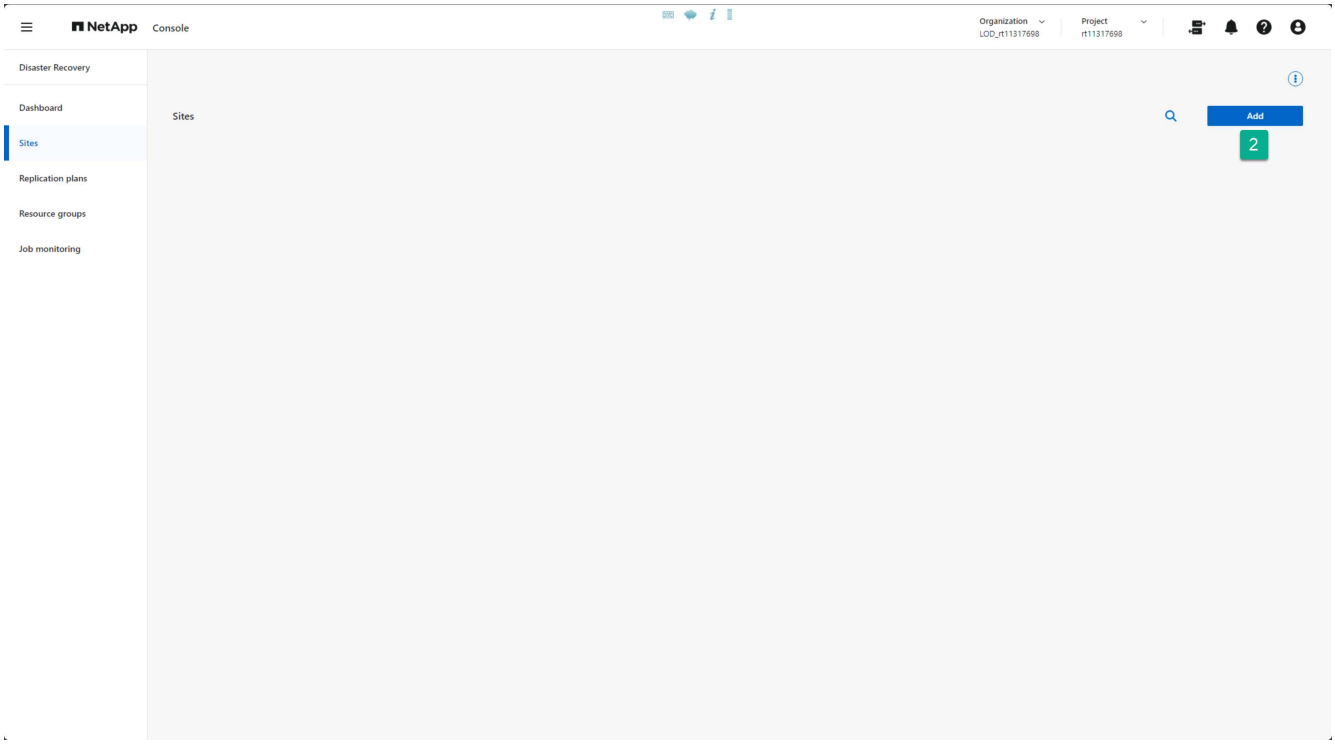
Create a production vCenter site.

Steps

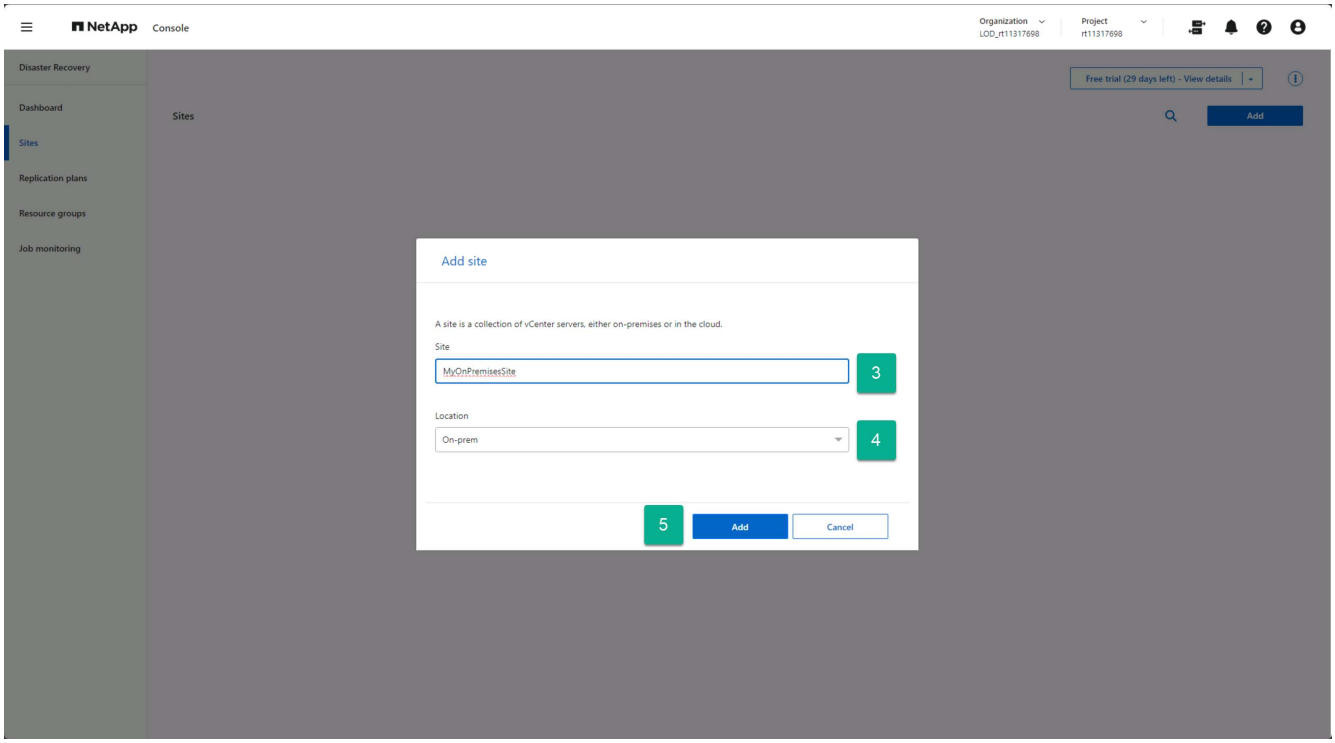
1. From the NetApp Console left navigation bar, select **Protection** > **Disaster Recovery**.
2. From any page in NetApp Disaster Recovery, select the **Sites** option.



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



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

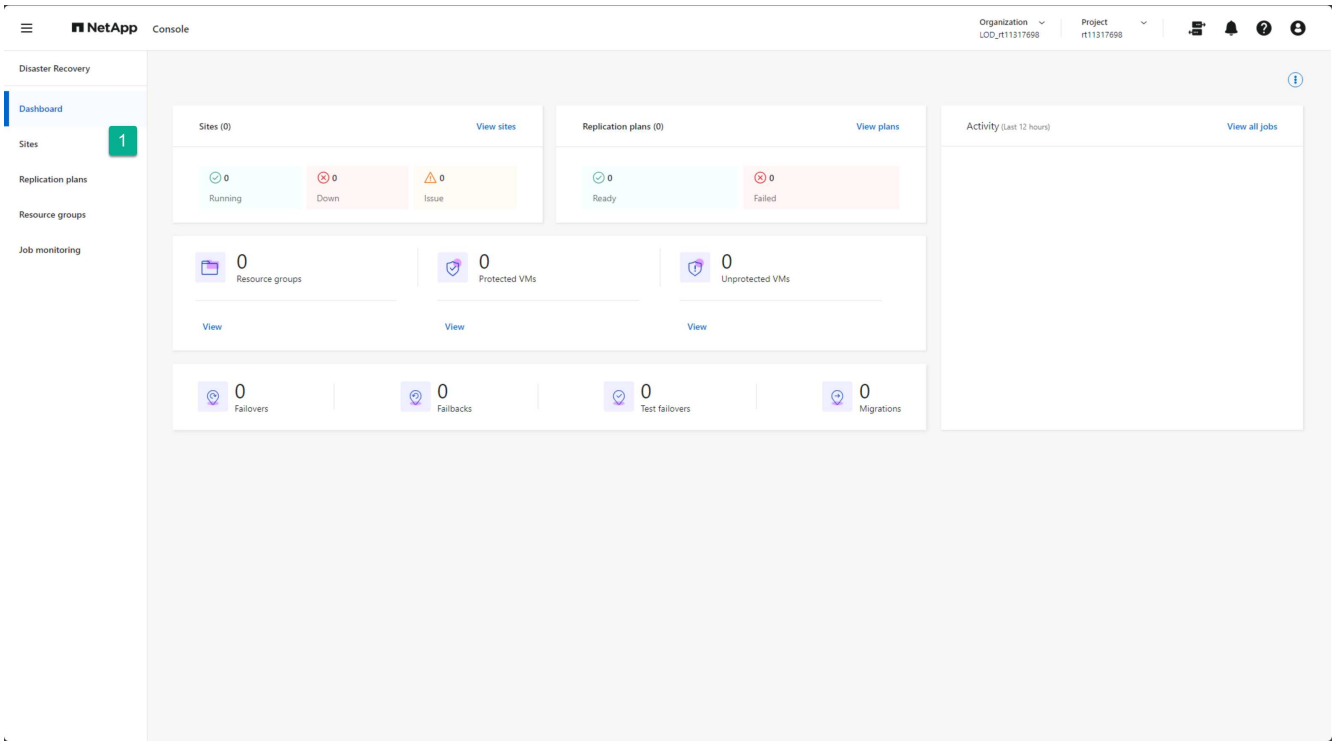


If you have other production vCenter sites, you can add them using the same steps.

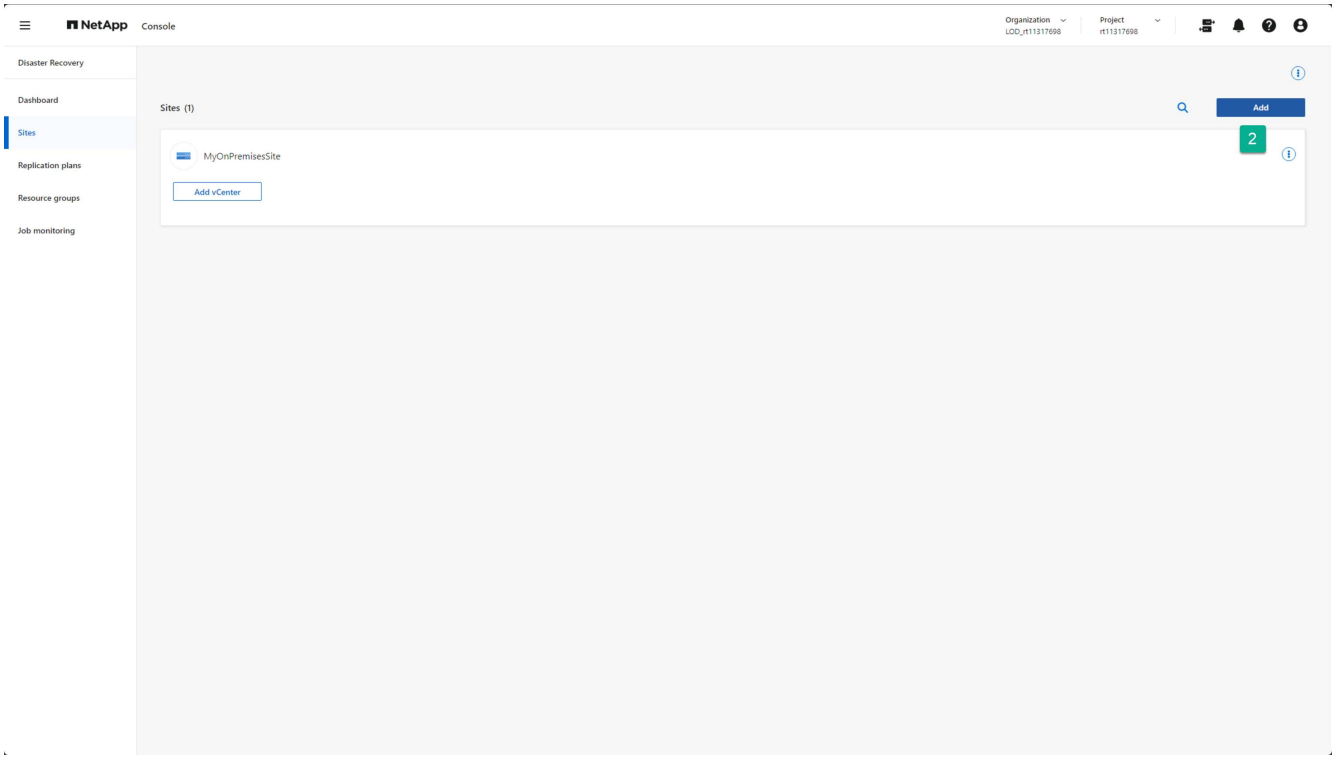
Create Amazon cloud sites

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

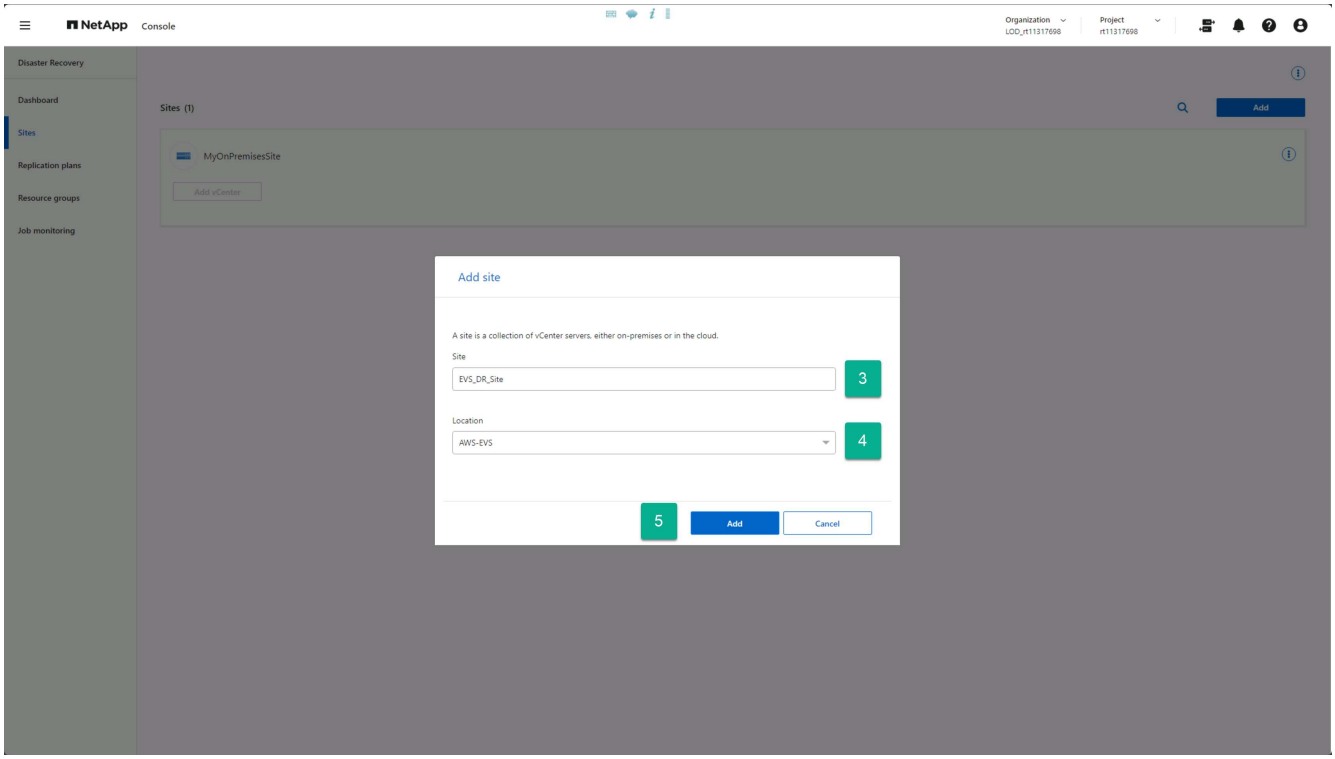
1. From any page in NetApp Disaster Recovery, select the **Sites** option.



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



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



Result

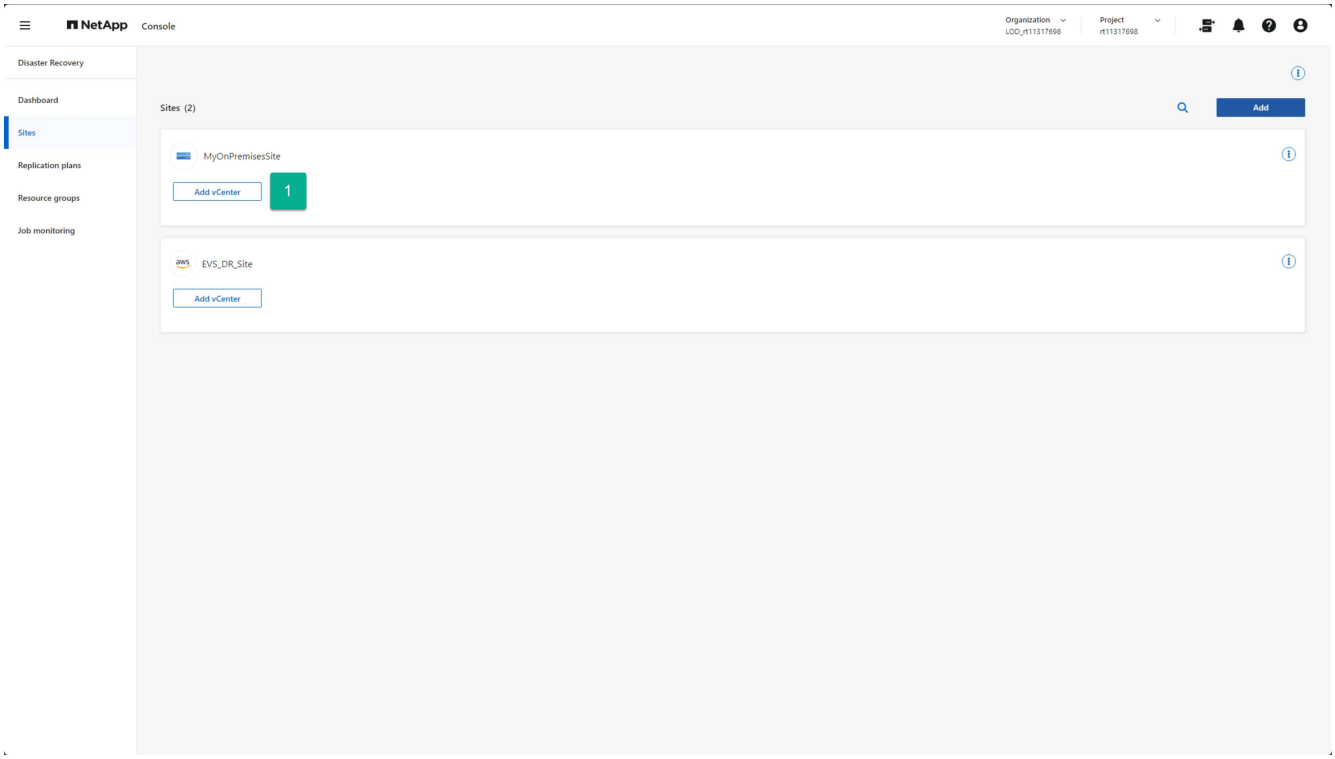
You now have a production (source) site and a DR (destination) site created.

Add on-premises and Amazon EVS vCenter clusters in NetApp Disaster Recovery

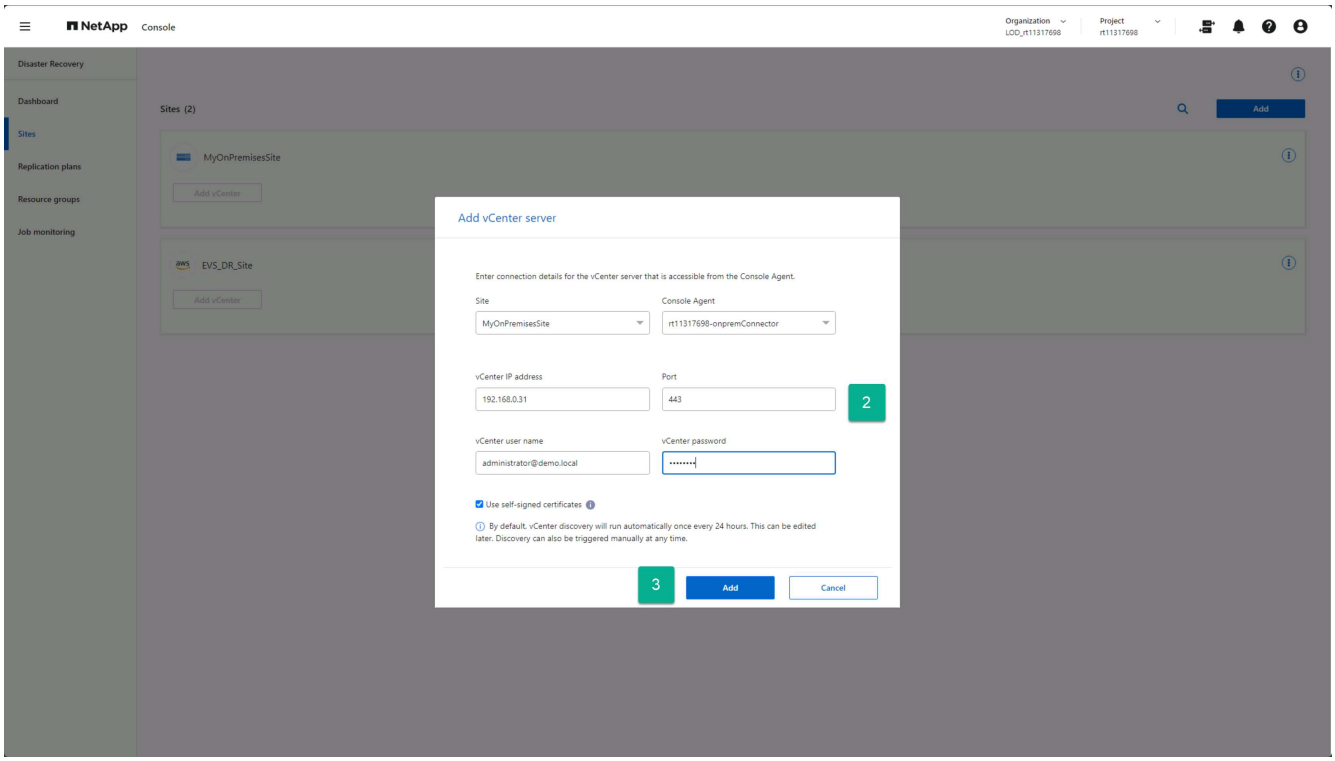
With sites created, you now add your vCenter clusters to each site in NetApp Disaster Recovery. When we created each site, we indicated each type of site. This tells NetApp Disaster Recovery what type of access is required for the vCenters hosted in each site type. One of the advantages of Amazon EVS 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** option, select **Add vCenter** for the site you want.



2. In the Add vCenter server dialog box, select or provide the following information:
   a. The NetApp Console agent 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 NetApp 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**.



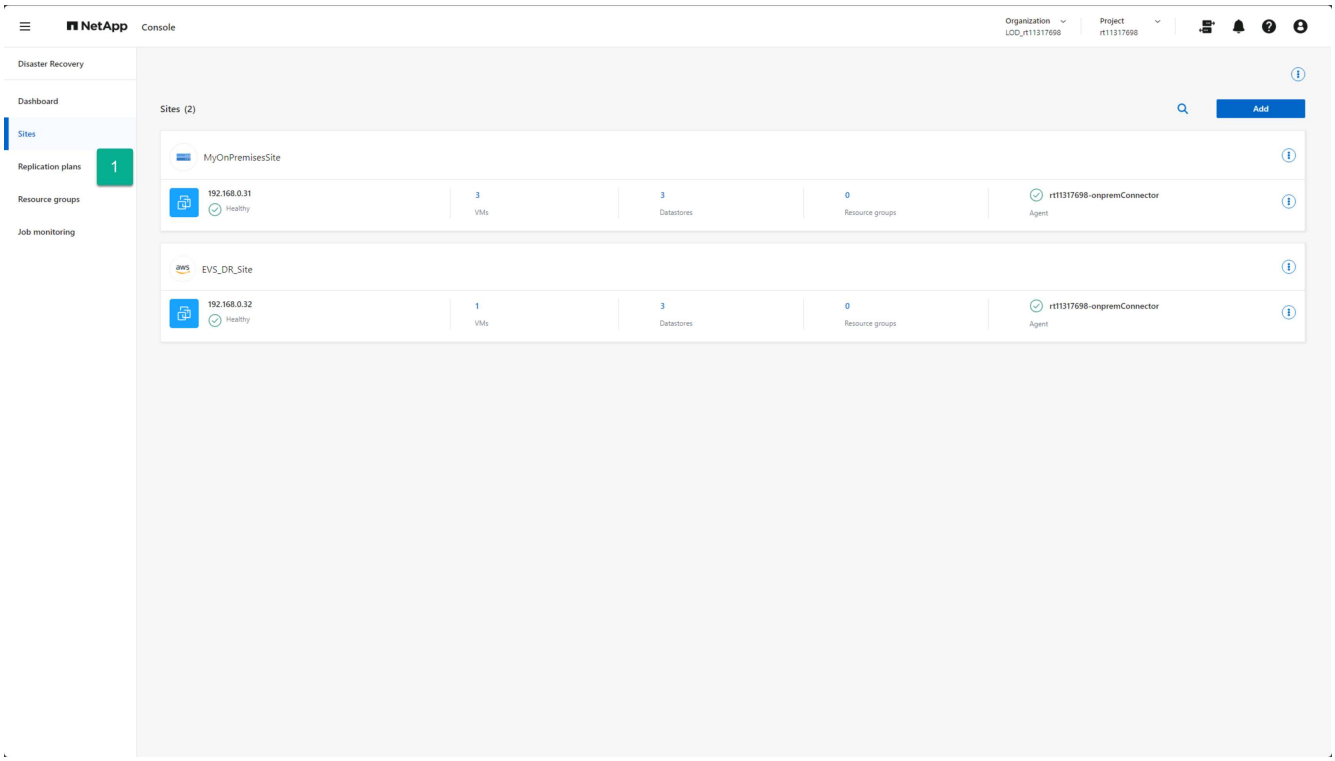
Create replication plans for Amazon EVS

Create replication plans in NetApp Disaster Recovery overview

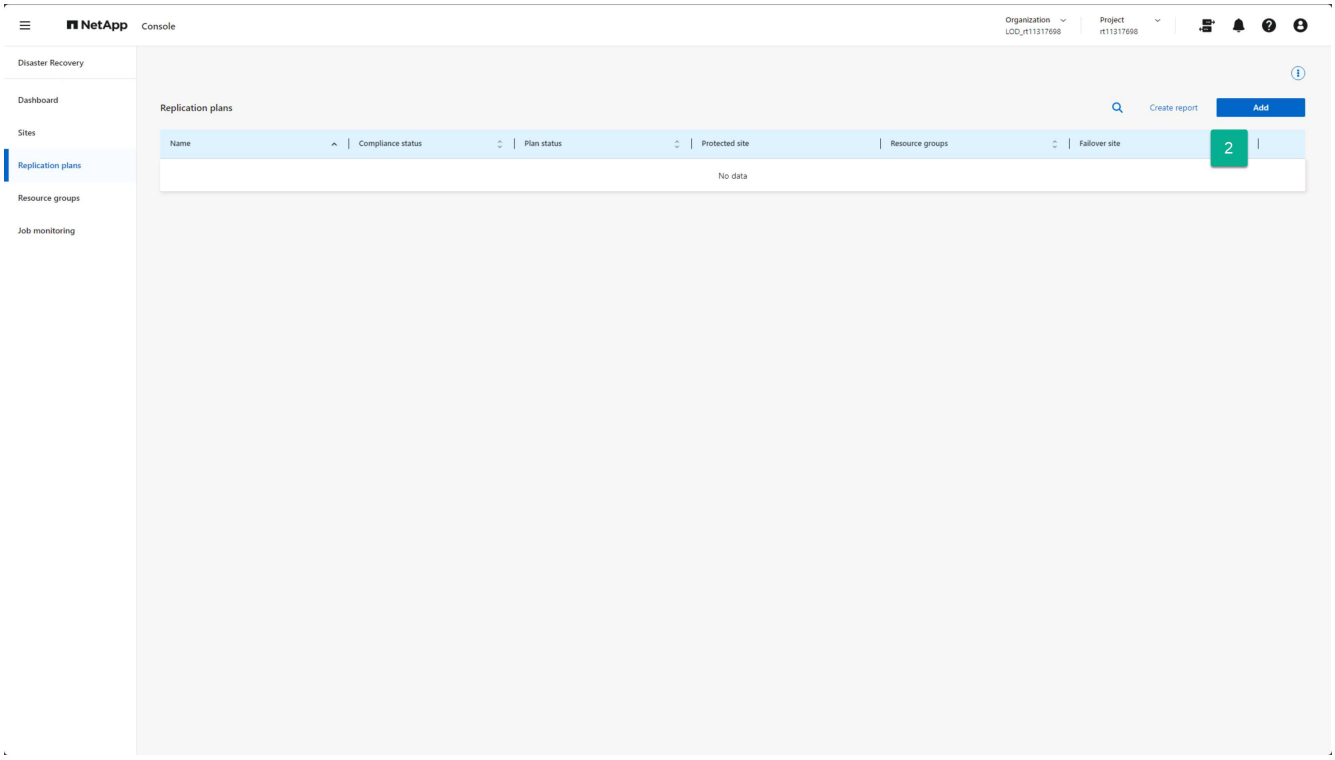
After you have vCenters to protect on the on-premises site and you have an Amazon EVS site configured to use Amazon FSx for NetApp ONTAP that you can use as a DR destination, you can create a replication plan (RP) to protect any set of VMs hosted on the vCenter cluster within your on-premises site.

To start the replication plan creation process:

1. From any NetApp Disaster Recovery screen, select the **Replication plans** option.



2. From the Replication plans page, 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 NetApp Disaster Recovery

First, using NetApp 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 NetApp Disaster Recovery

Select the virtual machines to be protected using NetApp 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 option from the NetApp Disaster Recovery menu. 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 NetApp 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 NetApp 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 NetApp Disaster Recovery

After you have a list of VMs that you want to protect using NetApp 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 NetApp 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, NetApp 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 page.

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. NetApp 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

NetApp 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. NetApp 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

NetApp Disaster Recovery supports performing some guest OS operations for each VM:

- NetApp Disaster Recovery can take application-consistent backups of VMs for VMs running Oracle databases and Microsoft SQL Server databases.
- NetApp 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, NetApp 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, NetApp 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 NetApp 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 NetApp Disaster Recovery

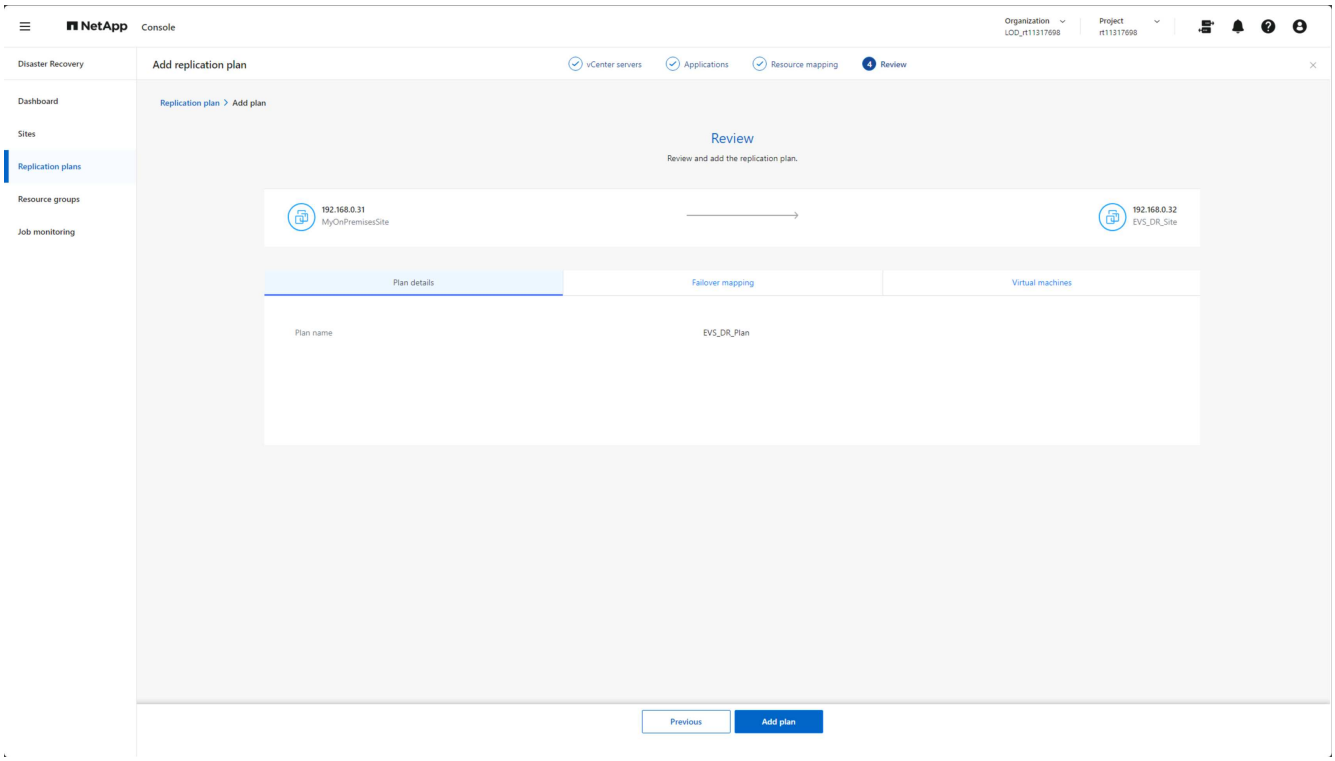
After you add the replication plan information in NetApp Disaster Recovery, verify that the information you entered is correct.

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



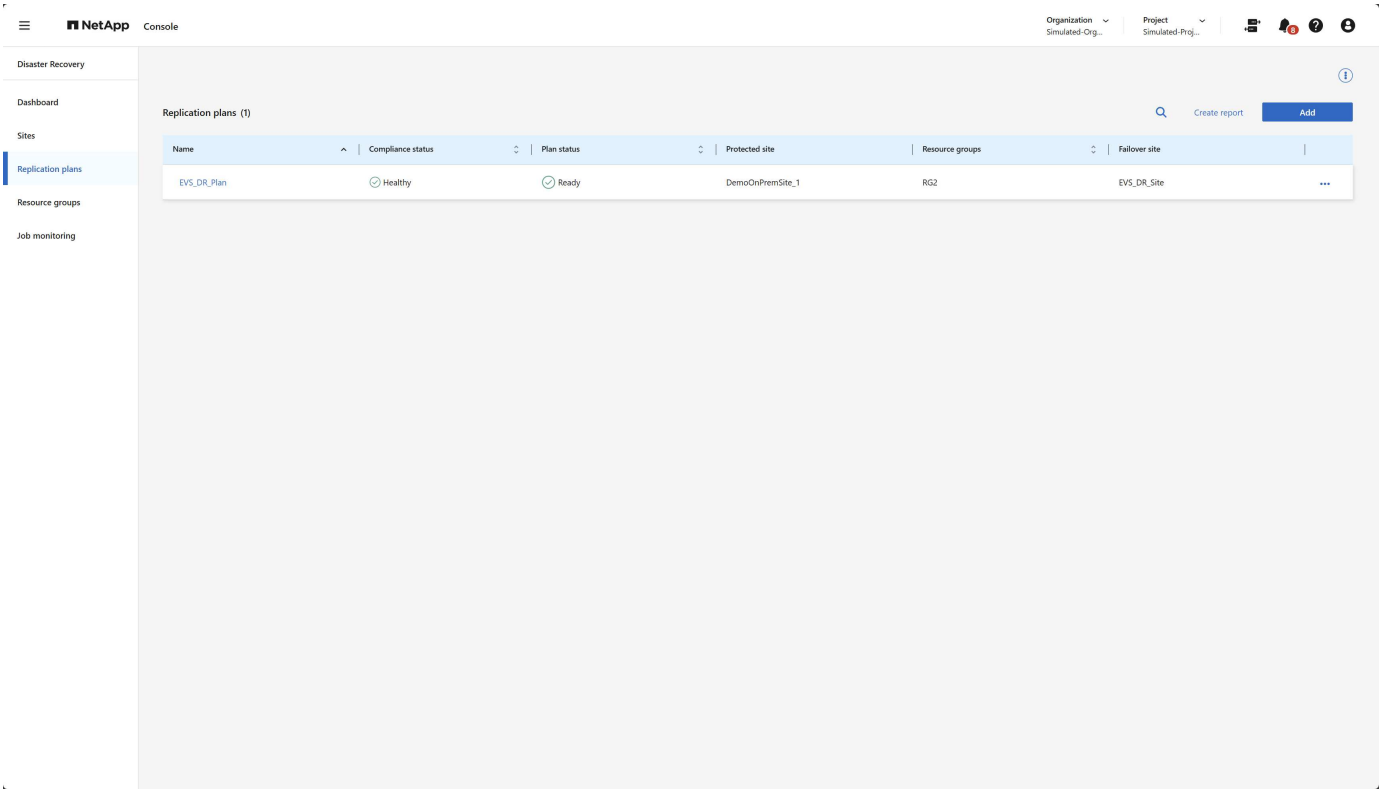
2. When you are satisfied that all settings are correct, select **Add plan** at the bottom of the screen.

Continue with Verify the replication plan.

Verify that everything is working in NetApp Disaster Recovery

After you add the replication plan in NetApp 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



NetApp 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 NetApp Disaster Recovery

Use NetApp 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.

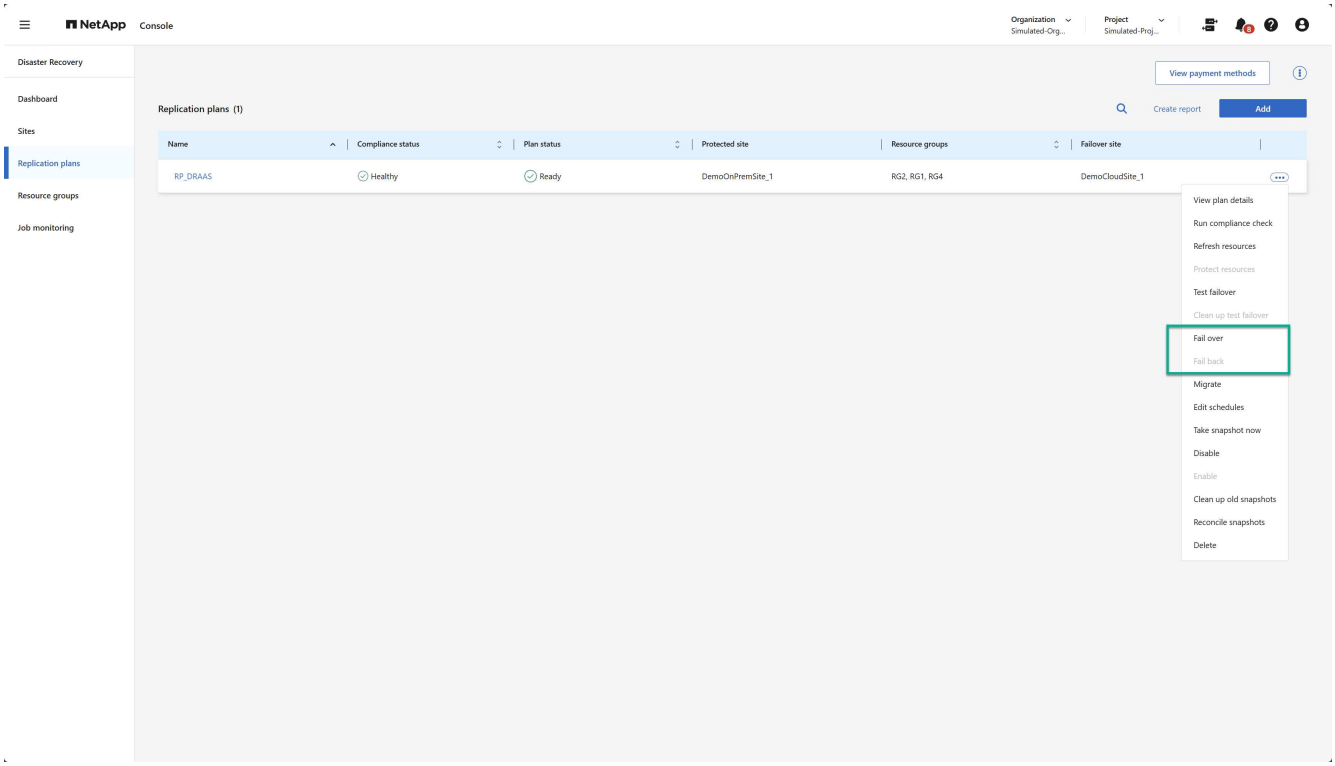
Failover is a manually initiated process.

Steps to access the failover operation

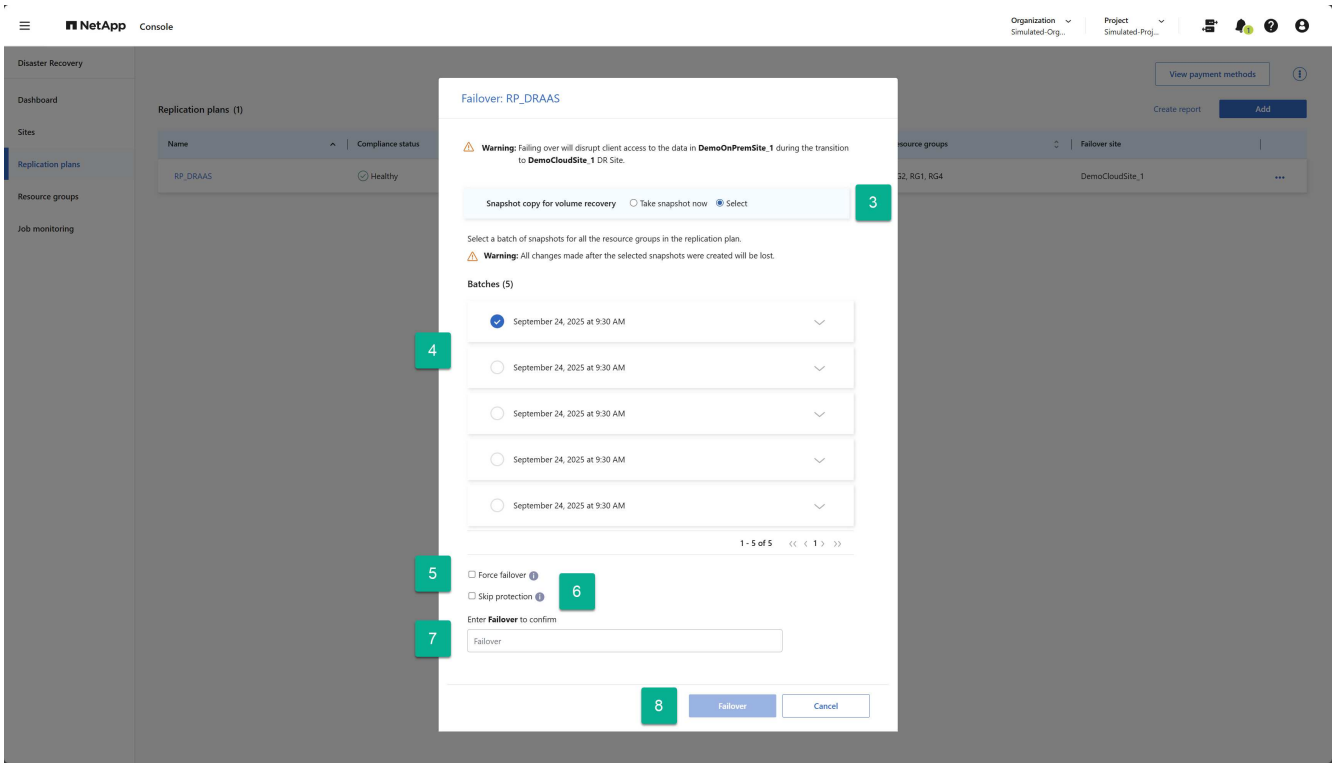
1. From the NetApp Console left navigation bar, select **Protection** > **Disaster Recovery**.
2. From the NetApp Disaster Recovery menu, select **Replication plans**.

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 NetApp 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 NetApp 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.

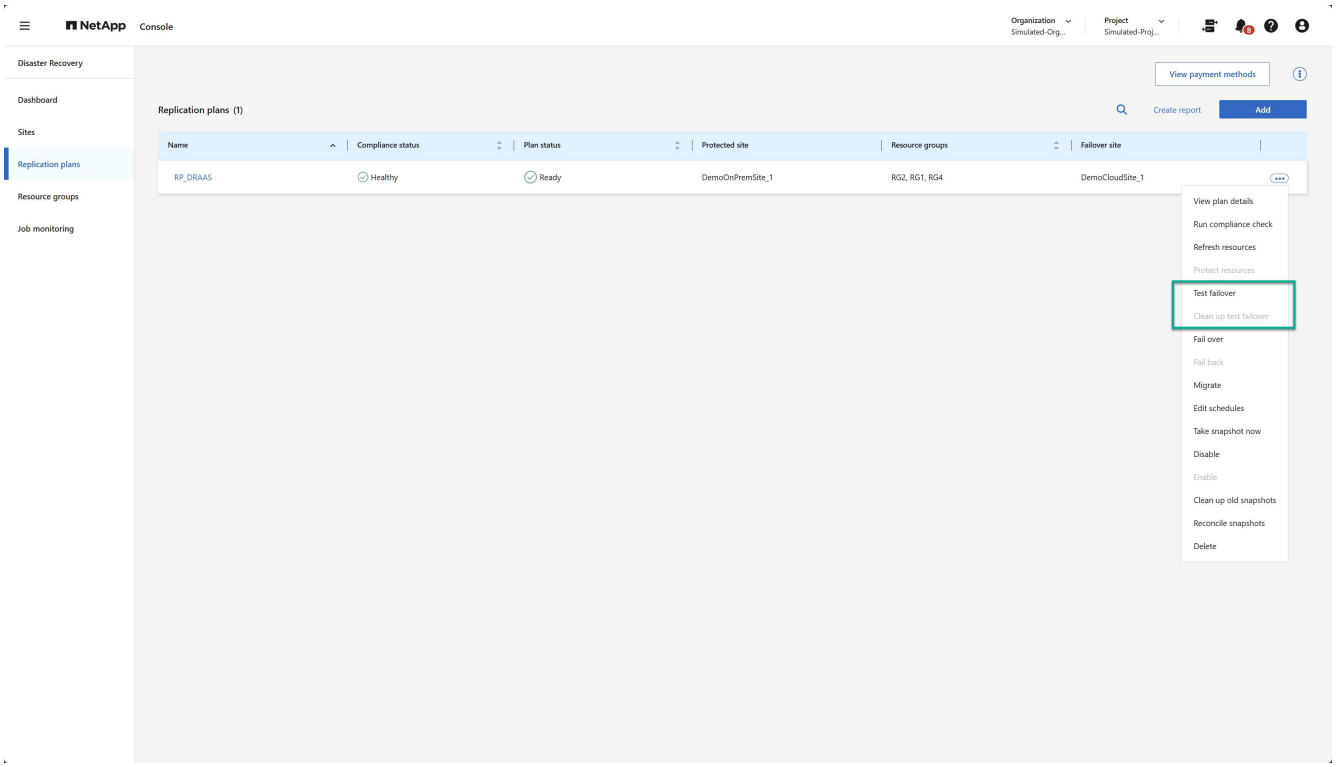
- The production site is still active and all VMs are still operating as expected.
- NetApp Disaster Recovery protection of the production VMs continues.

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.

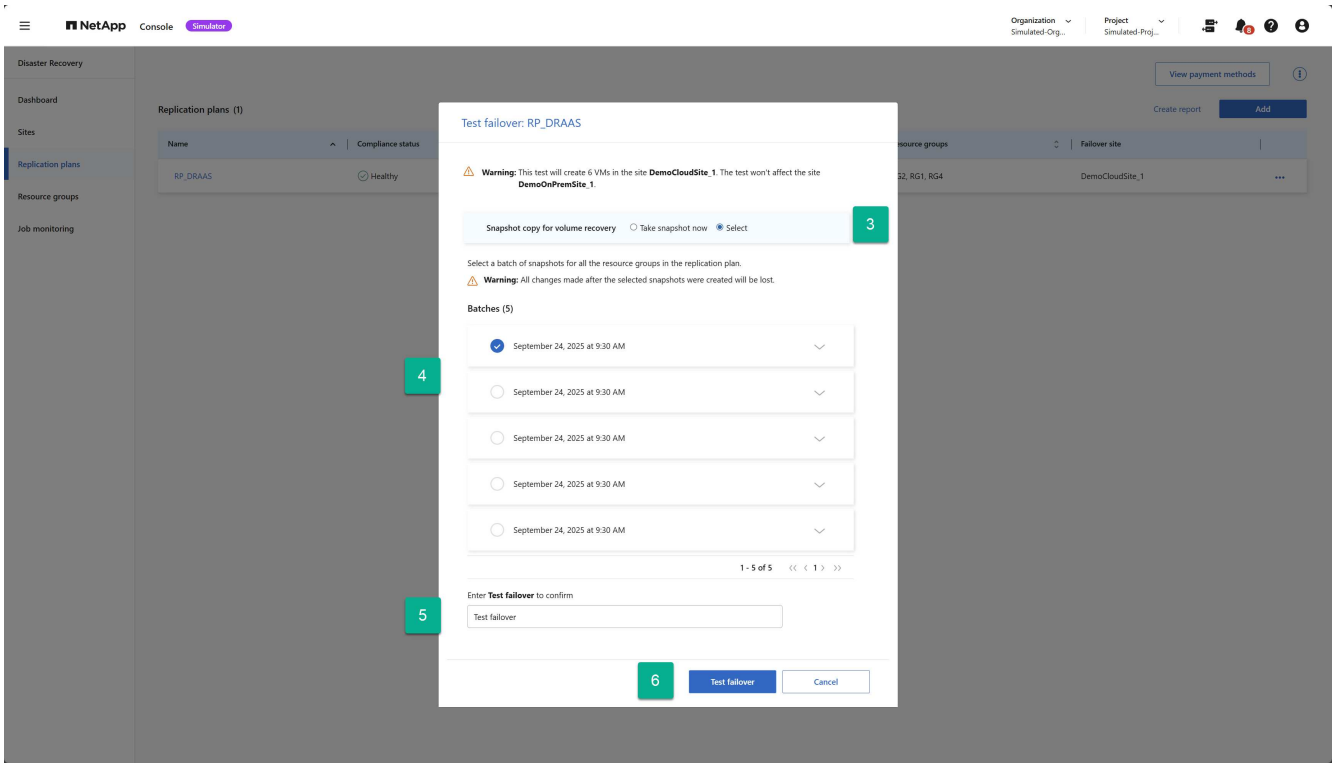
The steps for executing a test failover are identical to those used to execute a real failover except that you use the Test failover operation on the replication plan's context menu.

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**.

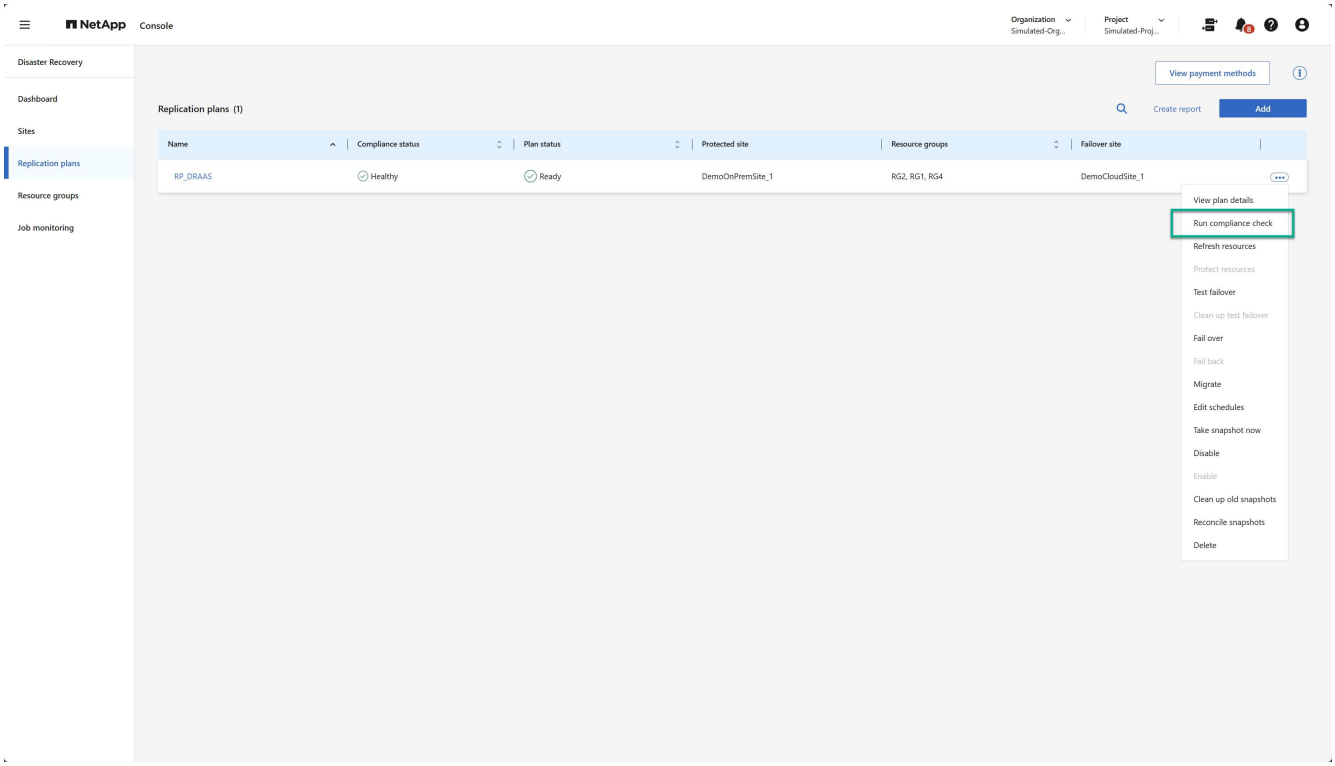


Run a compliance check

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:



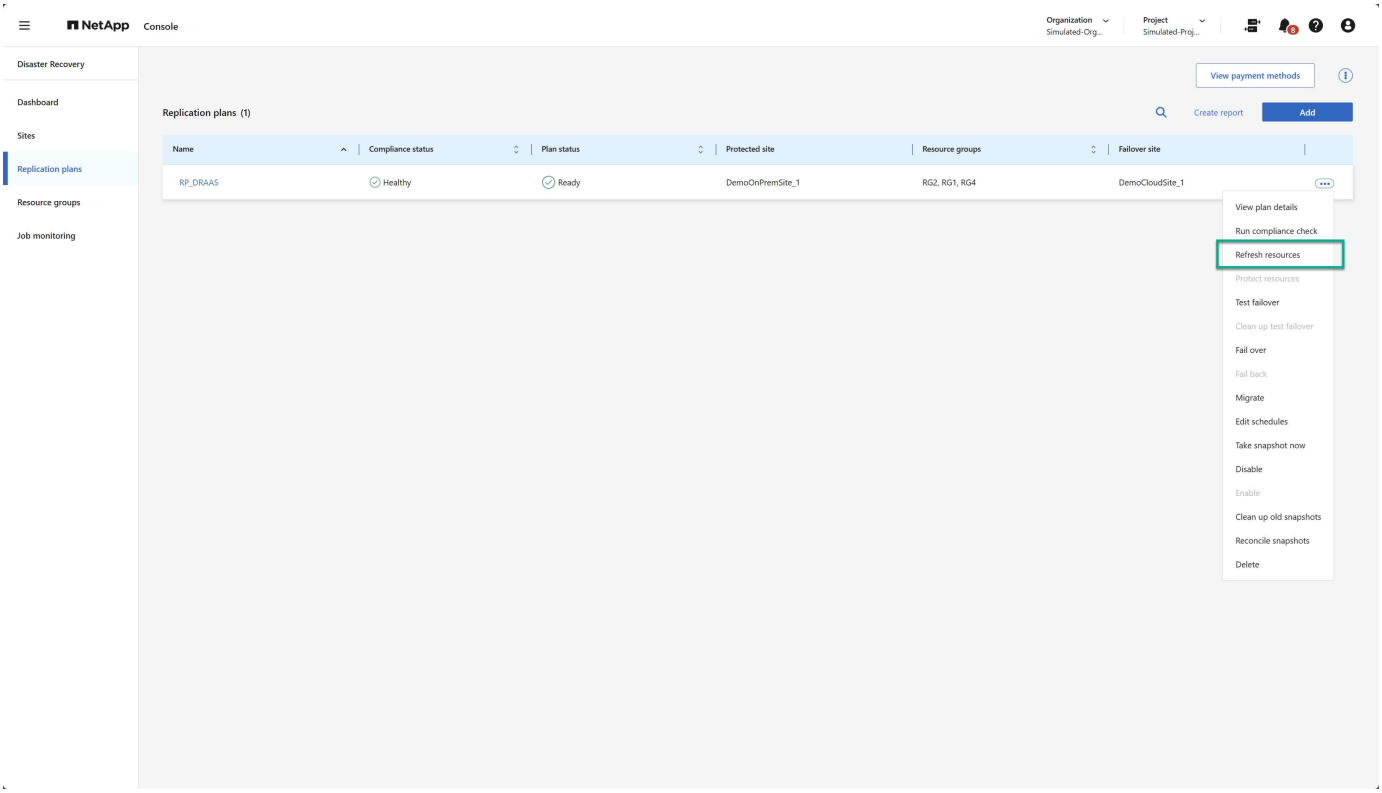
3. To change how often NetApp Disaster Recovery automatically runs compliance checks, select **Edit schedules** option from the replication plan's Actions menu.

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 NetApp 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:

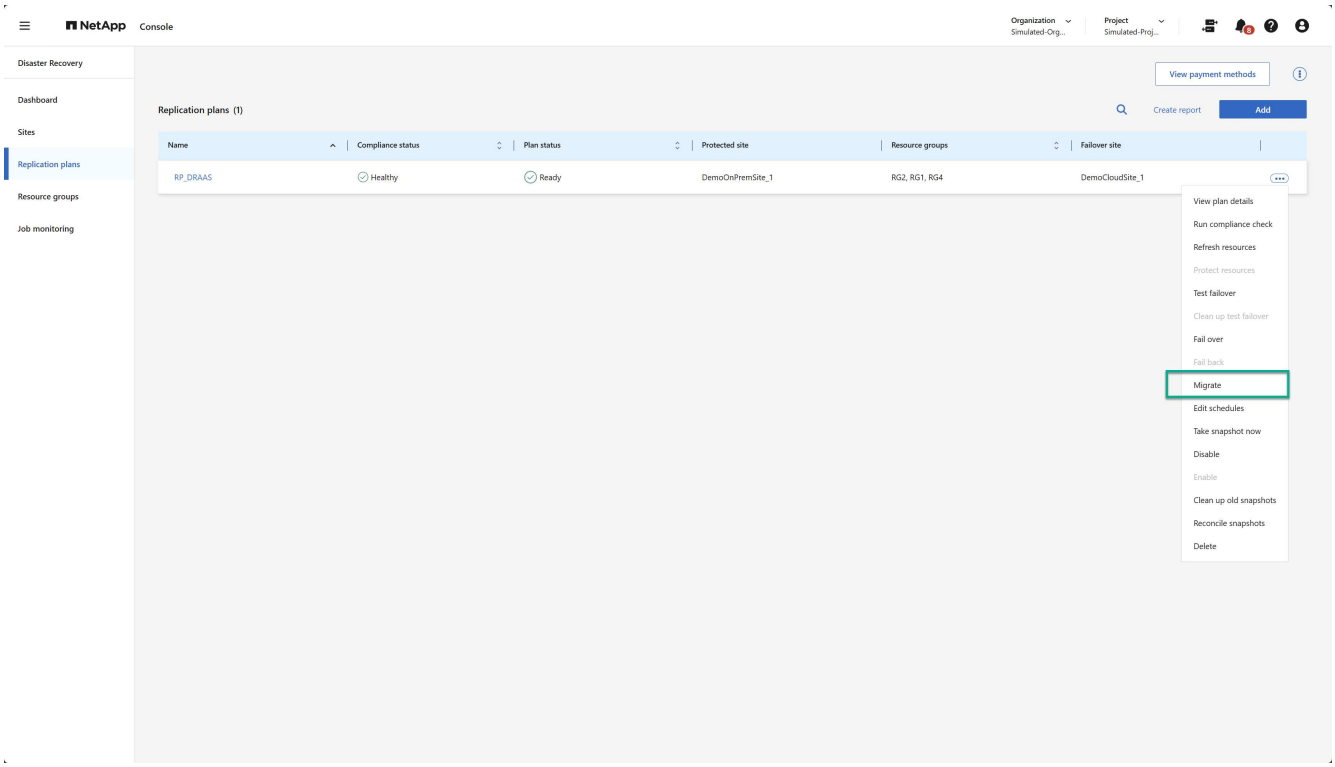
- vCenter refresh: Perform a vCenter refresh anytime VMs are added or deleted from or moved out of a vCenter cluster:
- Replication plan refresh: Perform a replication plan refresh anytime a VM is moved between datastores in the same source vCenter cluster.



Migrate

While NetApp 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:

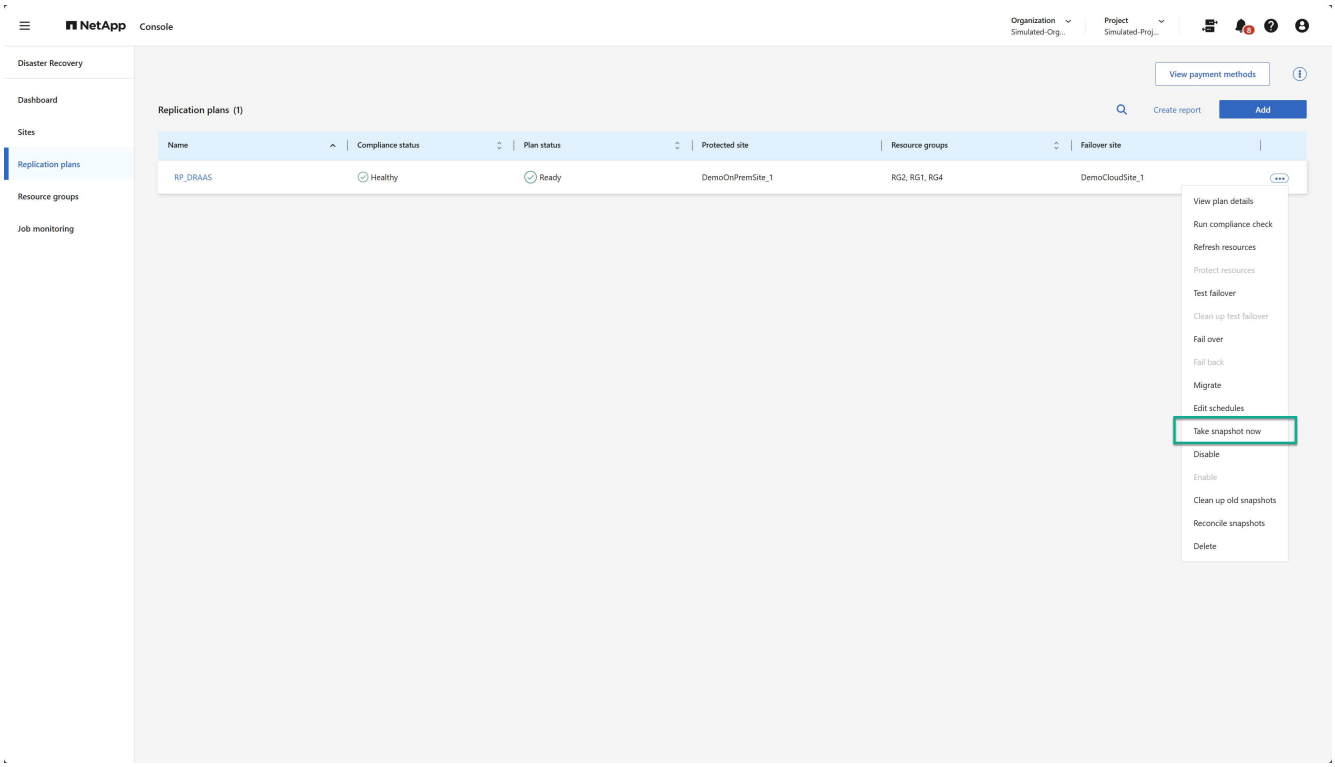


3. Enter information in the Migrate dialog box.

Take a snapshot now

At any time, you can take an immediate snapshot of the replication plan. This snapshot is included in the NetApp 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:

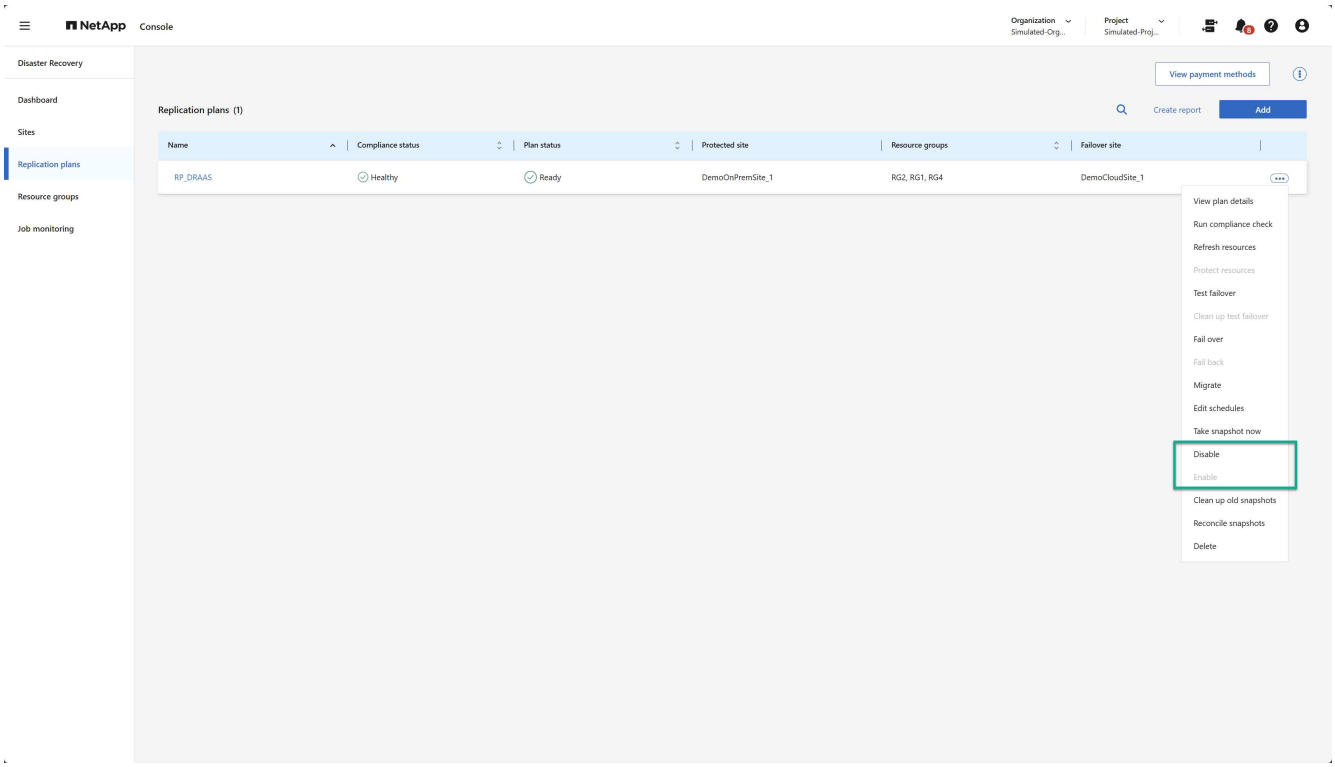


Disable or enable replication plan

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.

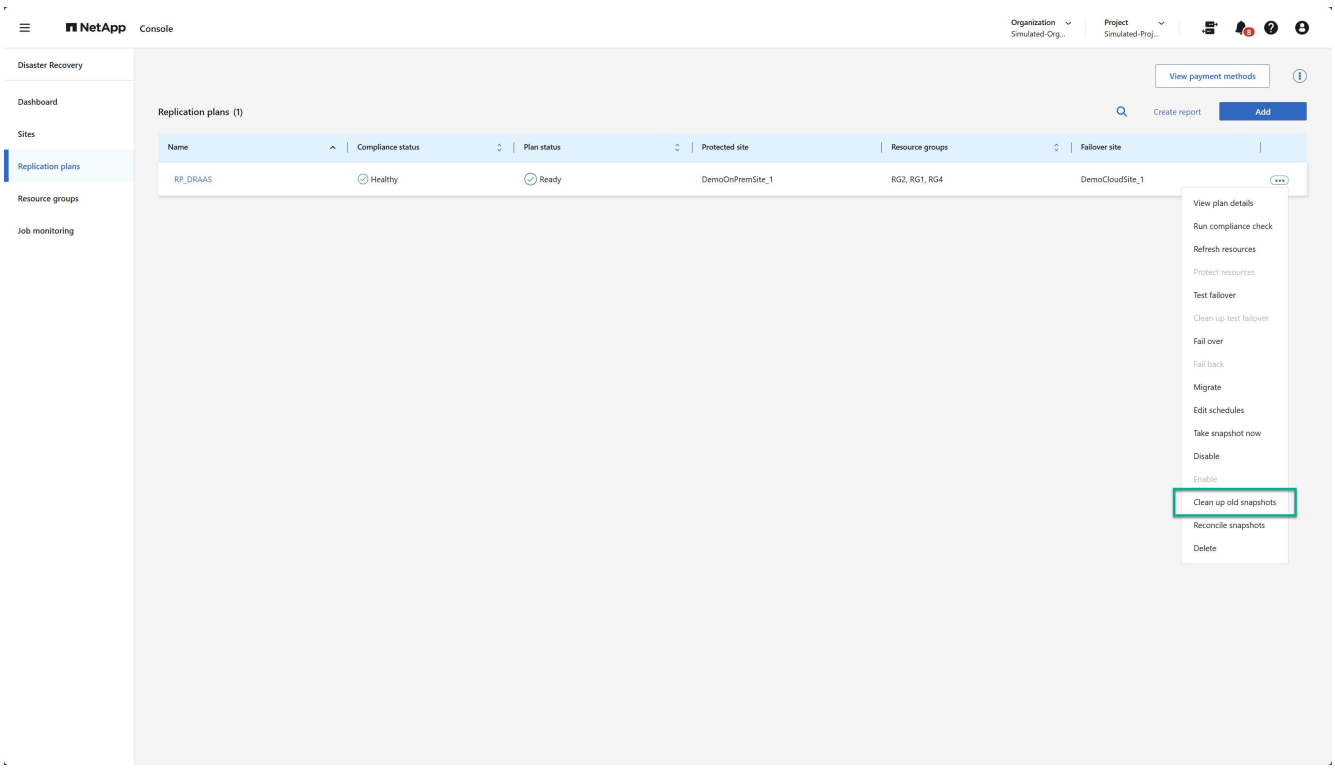
   When the replication plan is active, the **Enable** command is grayed out. When the replication plan is disabled, the **Disable** command is grayed out.



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.

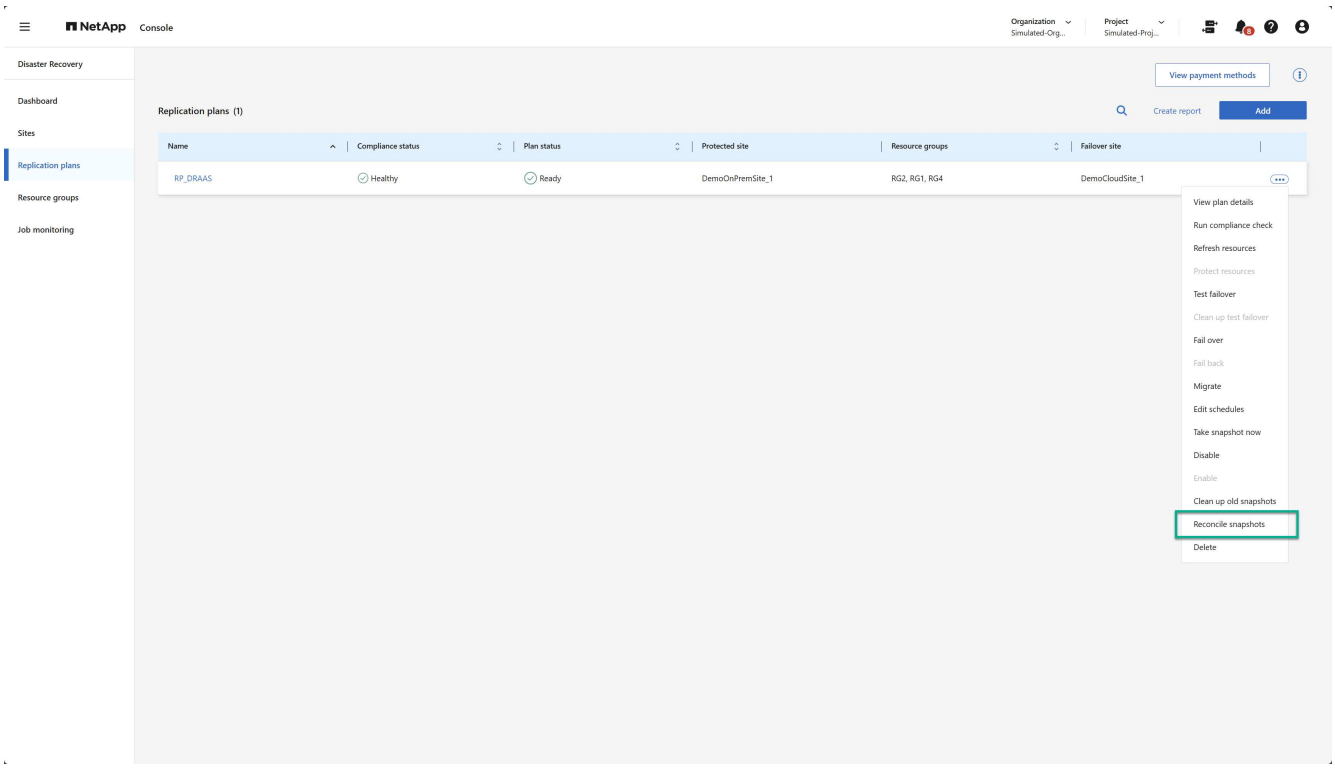
1. Select the **Actions** option ••• next to the replication plan.
2. To remove these older snapshots manually, select **Clean up old snapshots** from the replication plan's Actions menu.



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.

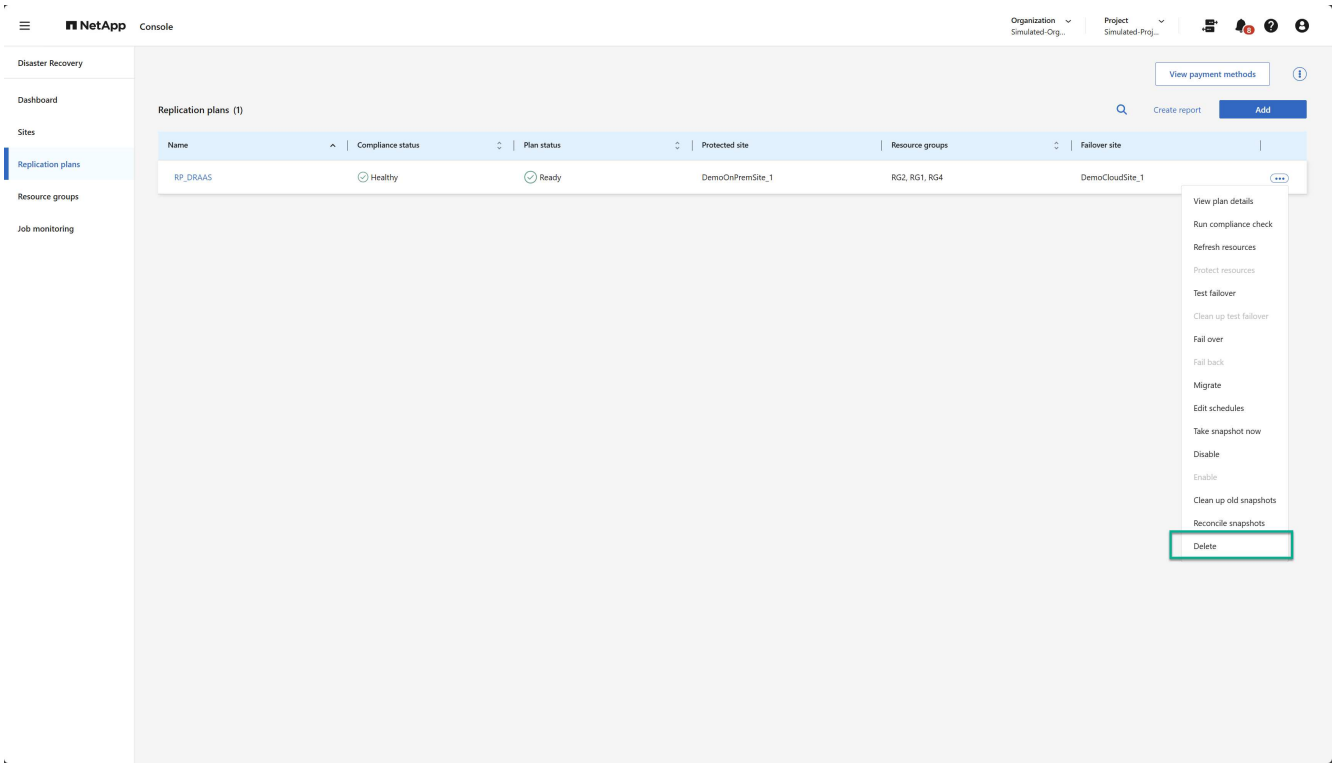
1. Select the **Actions** option ••• next to the replication plan.
2. To delete snapshots from the source cluster that do not exist on the destination cluster, select **Reconcile snapshots** from the replication plan's Actions menu.



Delete replication plan

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

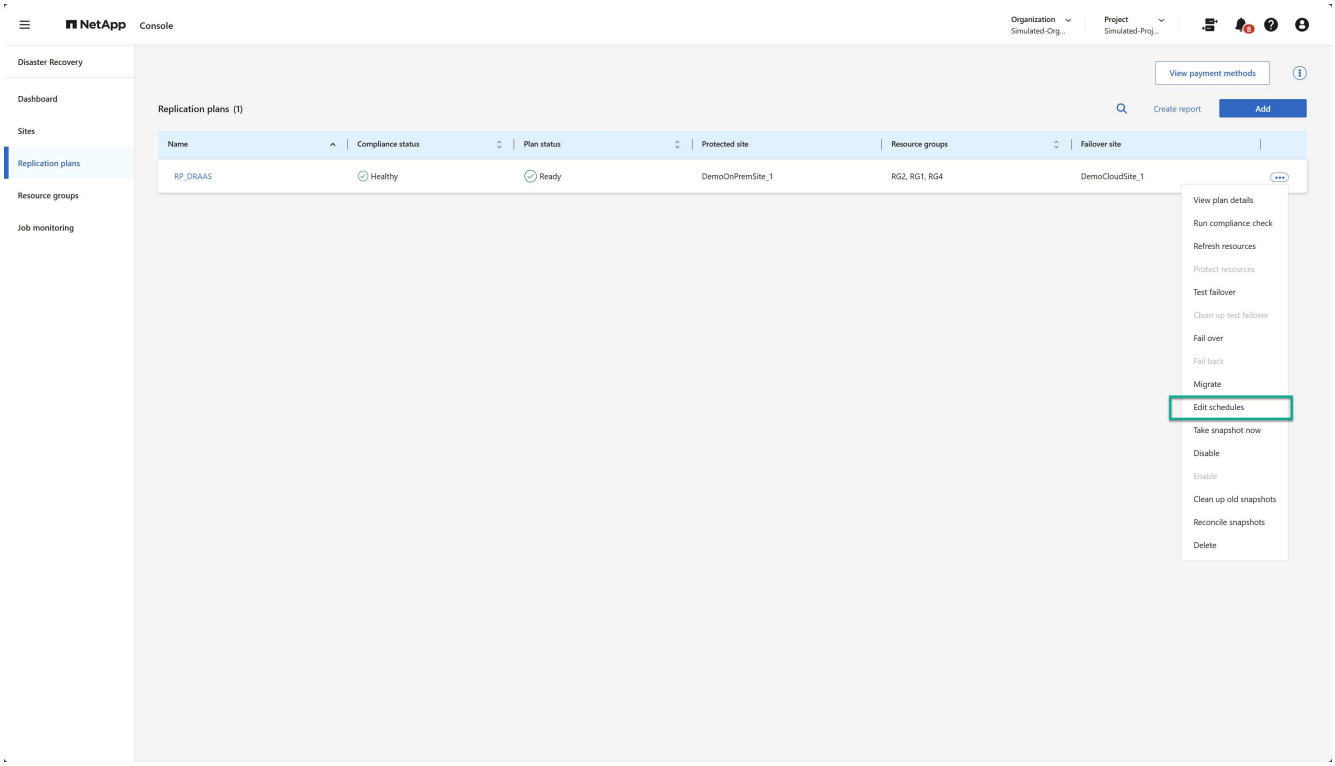
1. Select the **Actions** option ••• next to the replication plan.
2. To delete the replication plan, select **Delete** from the replication plan's context menu.



Edit schedules

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

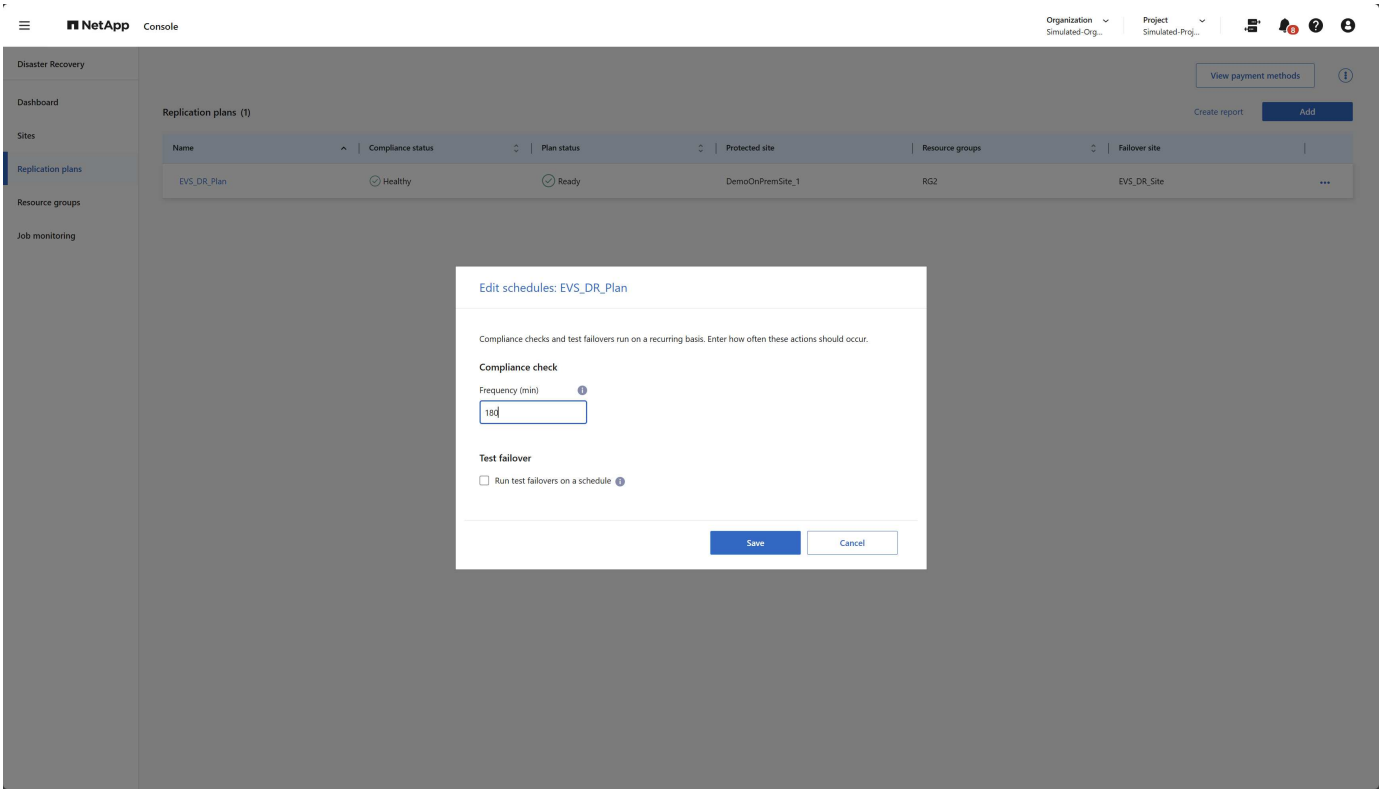
1. Select the **Actions** option ••• next to the replication plan.
2. To change these schedules for either of these two operations, select **Edit schedules** for the replication plan.



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:



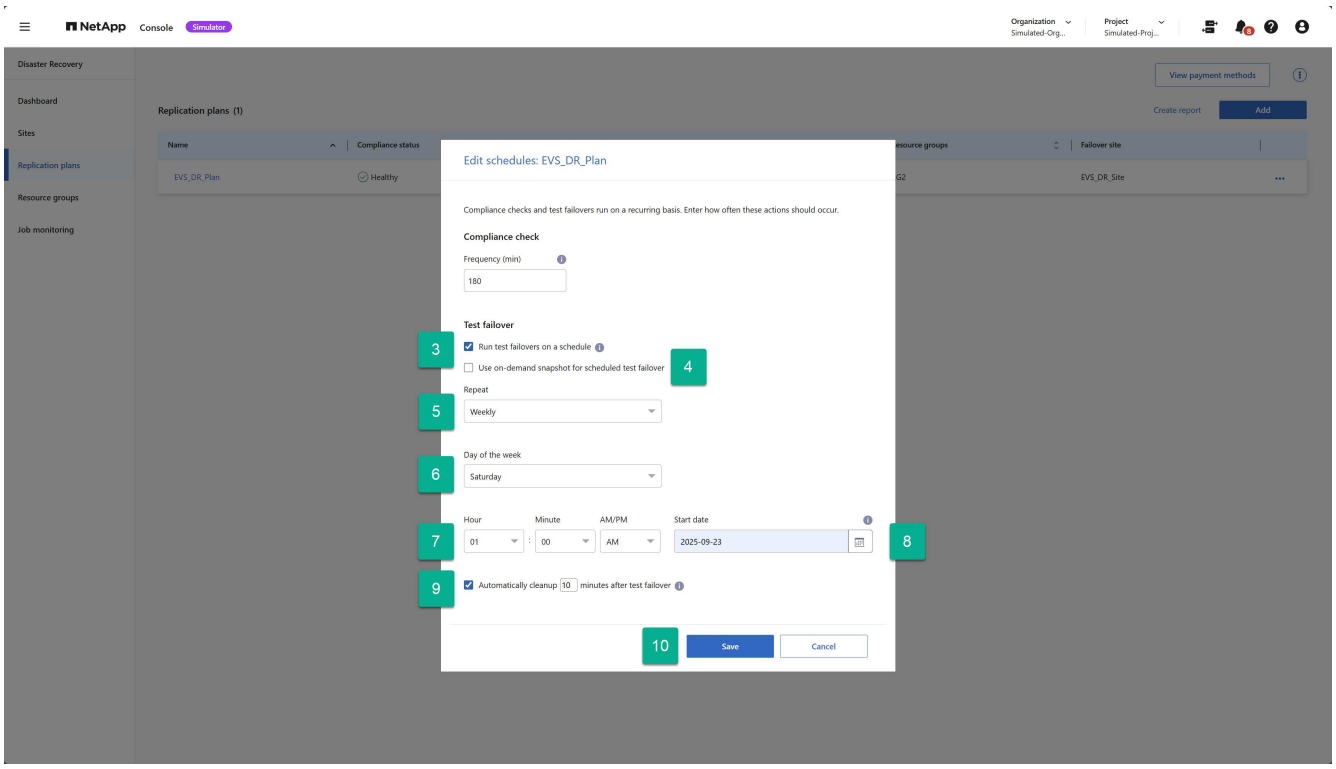
Schedule automated test failovers

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**.



Copyright information

Trademark information