Create replication plans for Amazon EVS

NetApp Disaster Recovery

NetApp
January 08, 2026

Table of Contents

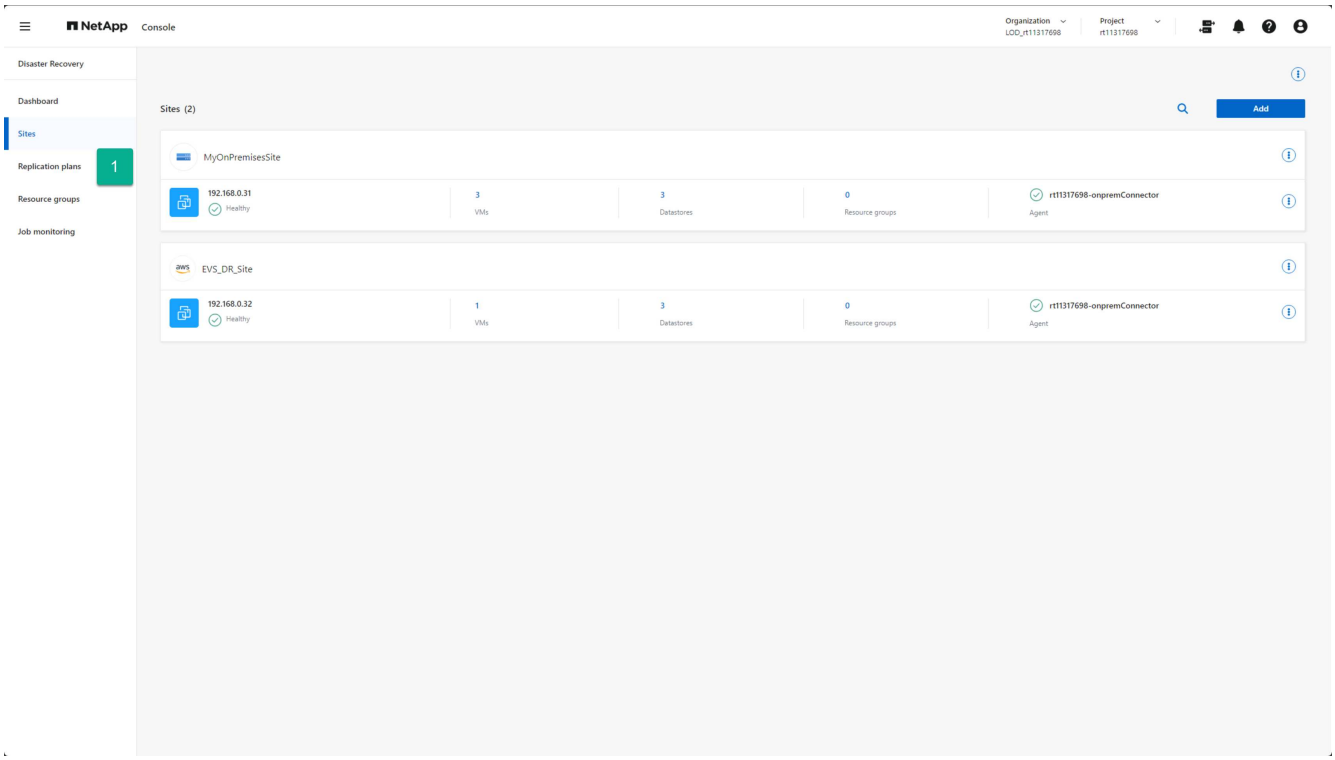
Create replication plans for Amazon EVS

Create replication plans in NetApp Disaster Recovery overview

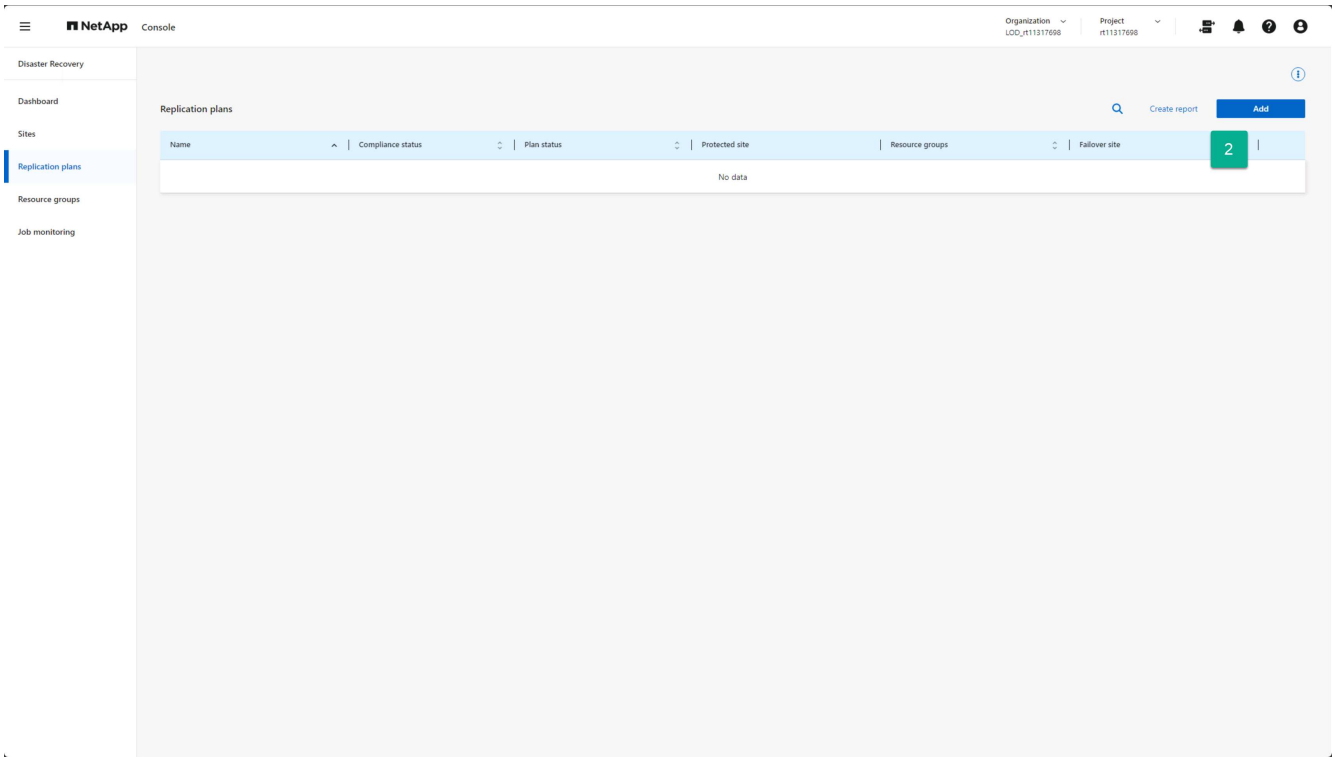
After you have vCenters to protect on the on-premises site and you have an Amazon EVS site configured to use Amazon FSx for NetApp ONTAP that you can use as a DR destination, you can create a replication plan (RP) to protect any set of VMs hosted on the vCenter cluster within your on-premises site.

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

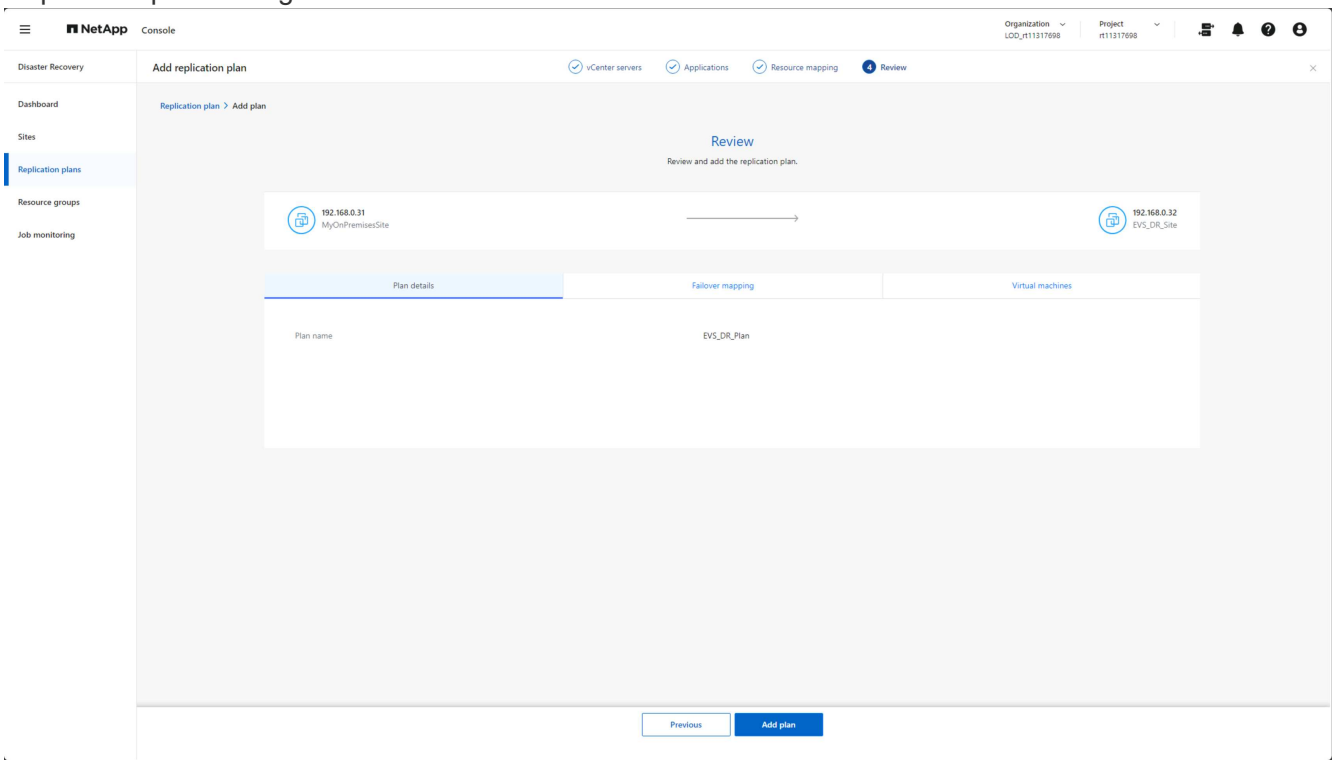
After you add the replication plan information in NetApp Disaster Recovery, verify that the information you entered is correct.

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



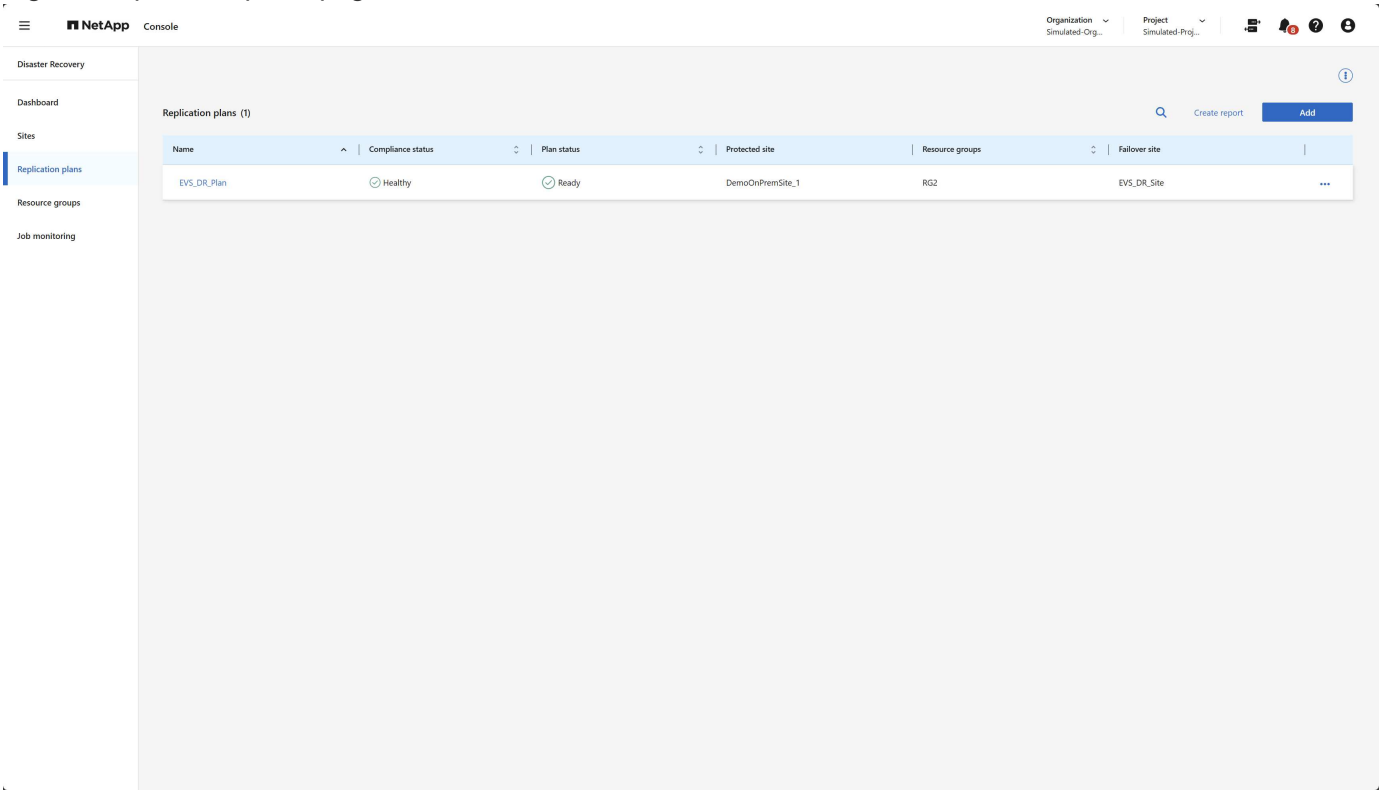
2. When you are satisfied that all settings are correct, select **Add plan** at the bottom of the screen.

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

Copyright information

Trademark information