Get started

NetApp Disaster Recovery

NetApp
February 04, 2026

Table of Contents

Get started

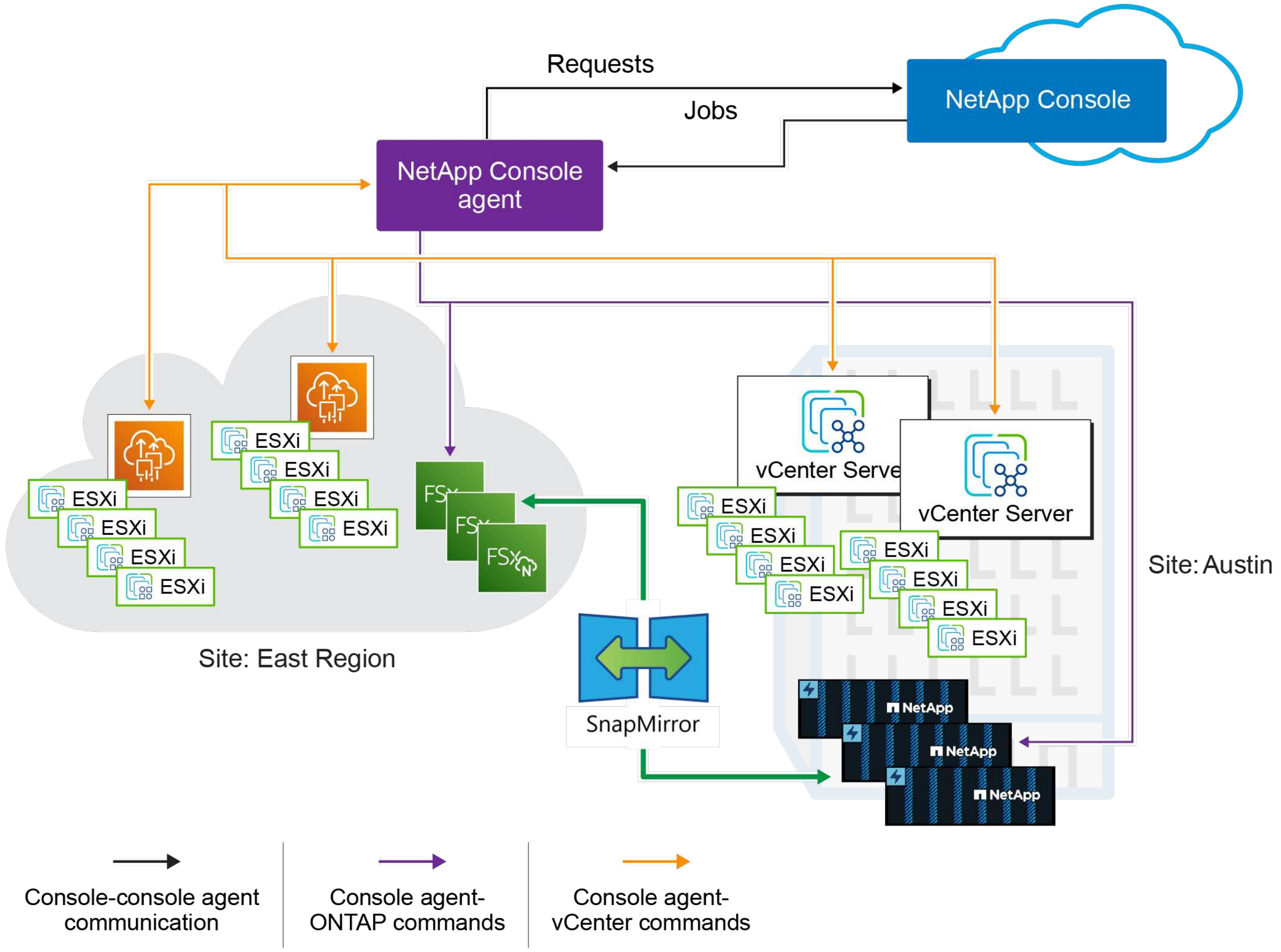
Learn about NetApp Disaster Recovery for VMware

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

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

- Amazon Elastic VMware Service (EVS) with Amazon FSx for NetApp ONTAP For details, refer to Introduction of NetApp Disaster Recovery using Amazon Elastic VMware Service and Amazon FSx for NetApp ONTAP.
- VMware Cloud (VMC) on AWS with Amazon FSx for NetApp ONTAP
- Azure VMware Solution (AVS) with NetApp Cloud Volumes ONTAP (iSCSI) (Private preview)
- Google Cloud VMware Engine (GCVE) with Google Cloud NetApp Volumes
- Another on-premises NFS and or VMFS-based (iSCSI/FC) VMware environment with ONTAP storage

NetApp Disaster Recovery uses ONTAP SnapMirror technology with integrated native VMware orchestration to protect VMware VMs and their associated on-disk OS images, while retaining all storage efficiency benefits of ONTAP. Disaster Recovery uses these technologies as the replication transport to the disaster recovery site. This enables industry-best storage efficiency (compression and deduplication) on primary and secondary sites.



NetApp Console

NetApp Disaster Recovery is accessible through the NetApp Console.

The NetApp Console provides centralized management of NetApp storage and data services across on-premises and cloud environments at enterprise grade. The Console is required to access and use NetApp data services. As a management interface, it enables you to manage many storage resources from one interface. Console administrators can control access to storage and services for all systems within the enterprise.

You don't need a license or subscription to start using NetApp Console and you only incur charges when you need to deploy Console agents in your cloud to ensure connectivity to your storage systems or NetApp data services. However, some NetApp data services accessible from the Console are licensed or subscription-based.

Learn more about the NetApp Console.

Benefits of using NetApp Disaster Recovery for VMware

NetApp Disaster Recovery offers the following benefits:

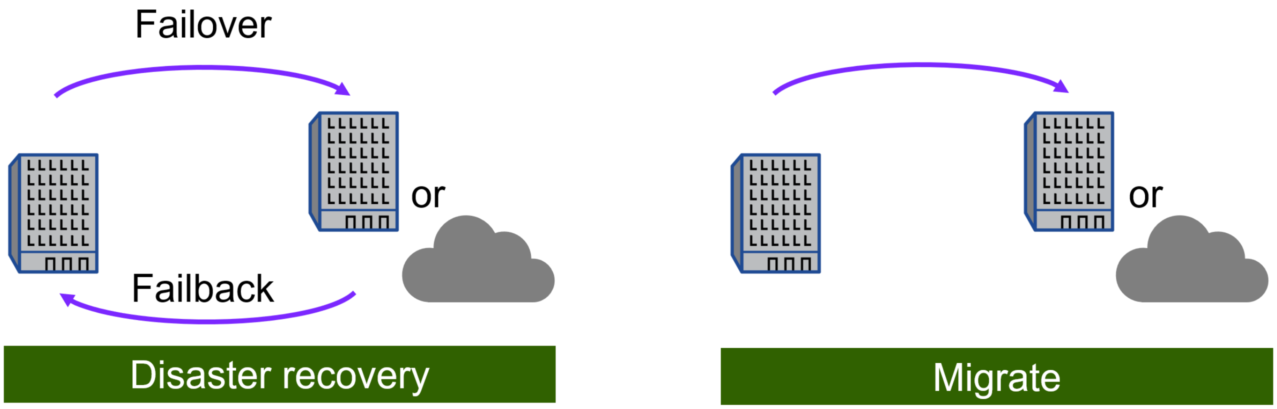
- Simplified user experience for vCenter discovery and recovery of applications with multiple point-in-time recovery operations.

- 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. You can regularly test your DR failover plans without impacting production workloads.
- Faster time to value with dynamic changes in your IT environment and ability to address it in your disaster recovery plans.
- Ability to manage both the storage and virtual layers through backend orchestration of both ONTAP and VMware at the same time without the need for virtual server appliances (VSAs) that need to be deployed and maintained.
- DR solutions for VMware can be resource intensive. Many DR solutions replicate VMs at the VMware virtual layer using VSAs, which can consume more compute resources and lose the valuable storage efficiencies of ONTAP. Because Disaster Recovery uses ONTAP SnapMirror technology, it can replicate data from production datastores to the DR site using our incremental-forever replication model with all the native data compression and deduplication efficiencies of ONTAP.

What you can do with NetApp Disaster Recovery for VMware

NetApp Disaster Recovery provides you with full use of several NetApp technologies to accomplish the following goals:

- Replicate VMware apps on your on-premises production site to a disaster recovery remote site in the cloud or on-premises using SnapMirror replication.
- Migrate VMware workloads from your original site to another site.
- Conduct a failover test. When you do this, the service creates temporary virtual machines. Disaster Recovery makes a new FlexClone volume from the selected snapshot, and a temporary datastore, which is backed by the FlexClone volume, is mapped to the ESXi hosts. This process doesn’t consume additional physical capacity on on-premises ONTAP storage or FSx for NetApp ONTAP storage in AWS. The original source volume is not modified and replica jobs can continue even during disaster recovery.
- In case of disaster, fail over your primary site on demand to the disaster recovery site, which can be VMware Cloud on AWS with Amazon FSx for NetApp ONTAP or an on-premises VMware environment with ONTAP.
- After the disaster has been resolved, fail back on demand from the disaster recovery site to the primary site.
- Group VMs or datastores into logical resource groups for efficient management.



Configuration of the vSphere server is done outside of NetApp Disaster Recovery in vSphere Server.

Cost

NetApp doesn’t charge you for using the trial version of NetApp Disaster Recovery.

NetApp Disaster Recovery can be used either with a NetApp license or an annual subscription-based plan through Amazon Web Services.

Some releases include a technology preview. NetApp doesn’t charge you for any previewed workload capacity. See What’s new in NetApp Disaster Recovery for information about the latest technology previews.

Licensing

You can use the following license types:

- Sign up for a 30-day free trial.
- Purchase a pay-as-you-go (PAYGO) subscription with the Amazon Web Services (AWS) Marketplace or Microsoft Azure Marketplace. This license enables you to purchase a fixed protected capacity license without any long-term commitment.
- 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 the NetApp Console.

Licenses for all NetApp data services are managed through subscriptions in the NetApp Console. After you set up your BYOL, you can see an active license for the service in the Console.

The service is licensed based on the amount of data hosted on protected ONTAP volumes. The service determines which volumes should be considered for licensing purposes by mapping protected VMs to their vCenter datastores. Each datastore is hosted on an ONTAP volume or LUN. The used capacity reported by ONTAP for that volume or LUN is used for licensing determinations.

Protected volumes can host many VMs. Some might not be part of a NetApp Disaster Recovery resource group. Regardless, the storage consumed by all VMs on that volume or LUN is used against the license maximum capacity.

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

For details about setting up licensing for NetApp Disaster Recovery, refer to Set up NetApp Disaster Recovery licensing.

30-day free trial

You can try out NetApp Disaster Recovery by using a 30-day free trial.

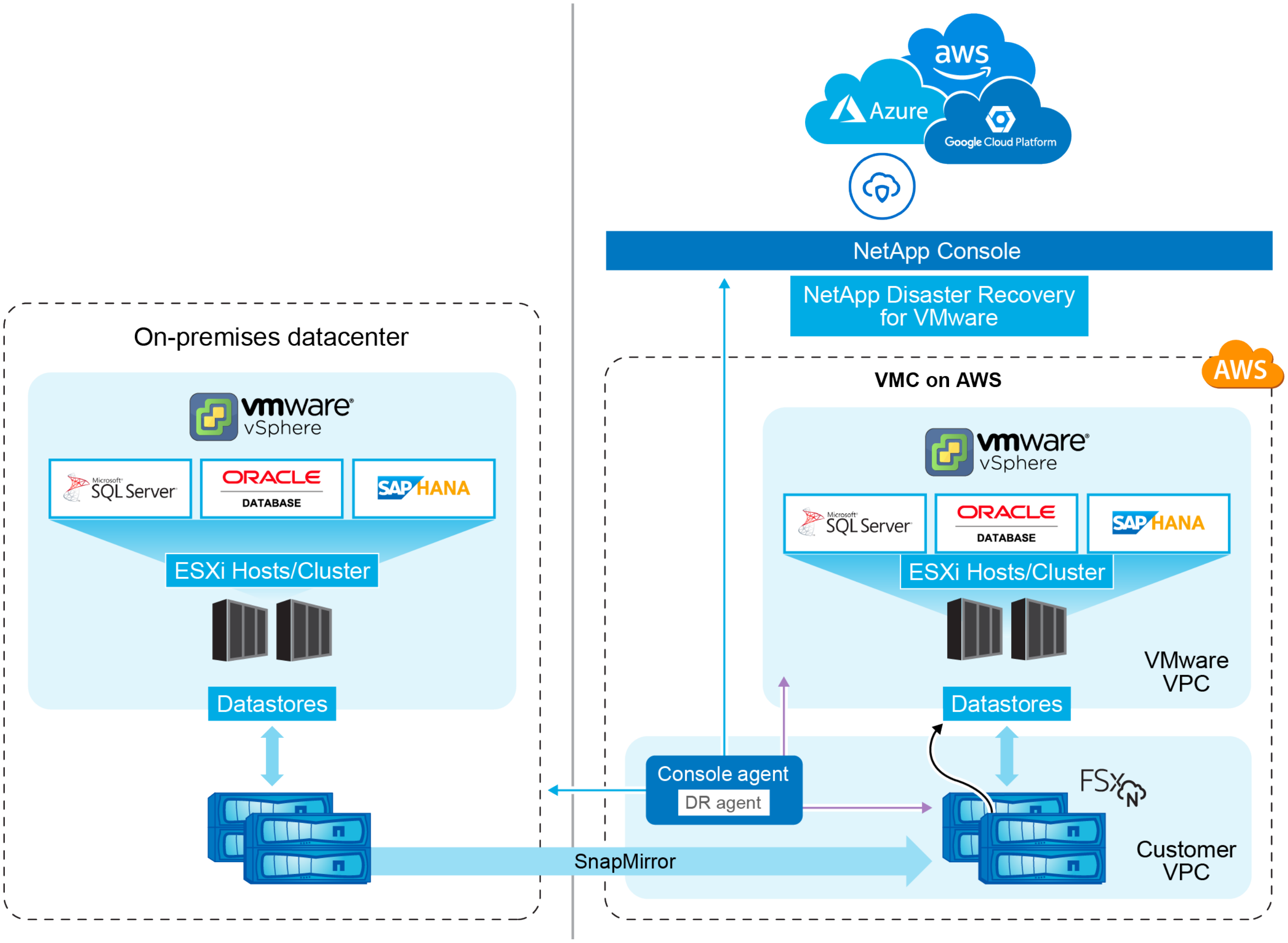
To continue after the 30-day trial, you’ll need to obtain a Pay-as-you-go (PAYGO) subscription from your cloud provider or purchase a BYOL license from NetApp.

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

How NetApp Disaster Recovery works

NetApp Disaster Recovery is a service hosted within the NetApp Console software as a service (SaaS) environment. 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 VMware Cloud on AWS, 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.

NetApp 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.



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.

Components of Disaster Recovery

Disaster Recovery uses the following components to provide disaster recovery for VMware workloads:

- **NetApp Console**: The user interface for managing your disaster recovery plans. You can use the NetApp Console to create and manage replication plans, resource groups, and failover operations across your on-premises and cloud environments.
- **Console agent**: A lightweight software component that runs in your cloud-hosted network or your on-premises VMware environment. It communicates with the NetApp Console and manages the replication of data between your on-premises environment and the disaster recovery site. The Console agent is installed on a virtual machine in your VMware environment.
- **ONTAP storage clusters**: The ONTAP storage clusters are the primary storage systems that host your VMware workloads. The ONTAP storage clusters provide the underlying storage infrastructure for your

disaster recovery plans. Disaster Recovery uses ONTAP storage APIs to manage ONTAP storage clusters such as on-premises arrays, and cloud-based solutions, such as Amazon FSx for NetApp ONTAP.

- **vCenter servers**: The VMware vCenter is the management server for your VMware environment. It manages the ESXi hosts and their associated datastores. The Console agent communicates with the VMware vCenter to manage the replication of data between your on-premises environment and the disaster recovery site. This includes registering ONTAP LUNs and volumes as datastores, reconfiguring VMs, and starting and stopping VMs.

The Disaster Recovery protection workflow

When a replication plan is assigned to a resource group, Disaster Recovery performs a discovery check of all the components in the resource group and plan to ensure that the plan can be activated.

If this check is successful, Disaster Recovery performs the following initialization steps:

1. For each VM in the target resource group, identify the hosting VMware datastore.
2. For each VMware datastore found, identify the hosting ONTAP FlexVol volume or LUN.
3. For each ONTAP volume and LUN found, determine if there is an existing SnapMirror relationship between the source volumes and a destination volume in the destination site.
   a. If there is no pre-existing SnapMirror relationship, create any new destination volumes and create a new SnapMirror relationship between each unprotected source volume.
   b. If there is a pre-existing SnapMirror relationship, use that relationship to perform all replication operations.

After Disaster Recovery creates and initializes all relationships, at each scheduled backup, the service perform the following data protection steps:

1. For each VM flagged as “application consistent,” use VMtools to place the supported application into a backup state.
2. Create a new snapshot of all ONTAP volumes hosting protected VMware datastores.
3. Perform a SnapMirror update operation to replicate those snapshots to the destination ONTAP cluster.
4. Determine if the number of retained snapshots has exceeded the maximum snapshot retention defined in the replication plan and delete any extraneous snapshots from both the source and destination volumes.

Supported protection targets and datastore types

Datastore types supported
NetApp Disaster Recovery supports the following datastore types:

- NFS datastores hosted on ONTAP FlexVol volumes residing on ONTAP clusters.
- VMware vSphere virtual machine file system (VMFS) datastores using the iSCSI or FC protocol

Protection targets supported

- VMware Cloud (VMC) on AWS with Amazon FSx for NetApp ONTAP
- Another on-premises, NFS-based VMware environment with ONTAP storage or an on-premises FC/iSCSI VMSF
- Amazon Elastic VMware Service
- Azure VMware Solution (AVS) with NetApp Cloud Volumes ONTAP (iSCSI) (Private preview)

- Google Cloud VMware Engine (GCVE) with Google Cloud NetApp Volumes

Terms that might help you with NetApp Disaster Recovery

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

- **Datastore**: A VMware vCenter data container, which uses a file system to hold VMDK files. Typical datastore types are NFS, VMFS, vSAN or vVol. Disaster Recovery supports NFS and VMFS datastores. Each VMware datastore is hosted on a single ONTAP volume or LUN. Disaster Recovery supports NFS and VMFS datastores hosted on FlexVol volumes residing on ONTAP clusters.
- **Replication plan**: A set of rules about how often backups occur and how to handle failover events. Plans are assigned to one or more resource groups.
- **Recovery point objective (RPO)**: The maximum amount of data loss that is acceptable in the event of a disaster. RPO is defined in the replication plan's frequency of data replication or replication schedule.
- **Recovery time objective (RTO)**: The maximum amount of time that is acceptable to recover from a disaster. RTO is defined in the replication plan and is the time it takes to fail over to the DR site and restart all VMs.
- **Resource group**: A logical container that enables you to manage multiple VMs as a single unit. A VM can be in only one resource group at a time. You can create a resource group for each application or workload that you want to protect.
- **Site**: A logical container typically associated with a physical datacenter or cloud location hosting one or more vCenter clusters and ONTAP storage.

NetApp Disaster Recovery prerequisites

Before using NetApp Disaster Recovery, ensure your environment meets the ONTAP storage, VMware vCenter cluster, and NetApp Console requirements.

Software versions

Component	Minimum version
Amazon FSx for NetApp ONTAP	Latest available version
Google Cloud VMware Engine using Google Cloud NetApp Volumes	Latest available version
ONTAP software	ONTAP 9.10.0 or later
VMware Cloud for AWS	Latest available version
VMware on-premises vCenter	7.0u3 or later

Google Cloud prerequisites and considerations

With Disaster Recovery on Google Cloud VMware Engine using Google Cloud NetApp Volumes, ensure you configure the correct permissions and adhere to the noted considerations.

- Contact the Google SRE team to allow-list the:
  - sync API to transfer snapshots from on-premises storage to Google Cloud NetApp Volumes.
  - the Google project with the VMware engine for creating, mounting, and unmounting datastores.
- You must File a request to allow-list your volumes hybrid replication.
- Be aware of the Google Cloud NetApp Volumes quota and limits.
- You can only add one volume or datastore to a replication plan.
- Review the limitations.

Failover considerations

- Failover is only supported using the latest snapshot. If necessary, you can create a new snapshot during failover (that is, the selective snapshot option must be disabled).
- You can't create a new snapshot after failover.
- You can't retain and reconcile snapshots after failover.

Failback considerations

- Failback is only possible with the selective snapshot option. You can't perform a failback by taking a new snapshot.
- If you remove cluster peering between on-premises storage and Google Cloud NetApp Volumes storage clusters, you must manually clear the cluster and storage VM peering entry from the on-premises cluster. For more information, see Delete a vserver peer relationship.

Google Cloud permissions

The service principal in Google Cloud should be assigned the following roles or equivalent permissions:

- Compute Admin role
- Google Cloud Permissions for NetApp Console
- Google Cloud NetApp Volumes Admin
- VMware Engine Service Admin

NetApp Console permissions

The NetApp Console user must have the following roles:

- Google Cloud NetApp Volumes admin
- SnapCenter admin
- Disaster Recovery failover admin

ONTAP storage prerequisites

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

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

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

VMware vCenter clusters prerequisites

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

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

NetApp Console prerequisites

Get started with the NetApp Console

If you haven't already done so, sign up to the NetApp Console and create an organization.

Gather credentials for ONTAP and VMware

- Amazon FSx for ONTAP and AWS credentials must be added to the system within the NetApp Console project that manages NetApp Disaster Recovery.
- NetApp Disaster Recovery requires vCenter credentials. You enter the vCenter credentials when you're adding a site in NetApp Disaster Recovery.

  For a list of vCenter privileges needed, refer to vCenter privileges needed for NetApp Disaster Recovery. For instructions on how to add a site, refer to Add a site.

Create the NetApp Console agent

The Console agent is a software component that enables the Console to communicate with your ONTAP storage and VMware vCenter clusters. It is required for Disaster Recovery to function properly. The agent resides in your private network (either an on-premises data center or a cloud VPC) and communicates with your ONTAP storage instances and any additional server and application components. For Disaster Recovery, this is access to your managed vCenter clusters.

A Console agent must be set up in the NetApp Console. When you use the agent, it will include the appropriate capabilities for the Disaster Recovery service.

- NetApp Disaster Recovery works only with the standard mode agent deployment. See Getting started with the NetApp Console in standard mode.
- Ensure both the source and destination vCenter clusters use the same Console agent.
- Type of Console agent needed:
  - **On-premises to on-premises disaster recovery**: Install the on-premises Console agent in the disaster recovery site. Using this method, a failure of the primary site doesn't prevent the service from restarting your virtual resources at the DR site. Refer to Install and set up the Console agent on premises.

    Disaster Recovery also supports using multiple Console agents with on-premises configurations. For this scenario, the Console agents direct actions to vCenters and ONTAP array clusters, and the source and target would each have their own Console agent. Using multiple Console agents is recommended to reduce latency and improve recovery time if a Console agent or site fails.
  - **On-premises to AWS**: Install the Console agent for AWS in your AWS VPC. Refer to Console agent installation options in AWS.

    > For on-premises to on-premises, use the on-premises Console agent. For on-premises to AWS, use the AWS Console agent, which has access to the source on-premises vCenter and the destination on-premises vCenter.
  - The installed Console agent must be able to access any VMware vCenter cluster instances and ESXi hosts managed by those vCenter clusters that Disaster Recovery will manage.
- All ONTAP arrays to be managed by NetApp Disaster Recovery must be added to any system within the NetApp Console project that will be used to manage NetApp Disaster Recovery.

  See Discover on-premises ONTAP clusters.
- For information about setting up an intelligent proxy for NetApp Disaster Recovery, see Set up your infrastructure for NetApp Disaster Recovery.

Workload prerequisites

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

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

More information

- Required vCenter privileges
- Prerequisites for Amazon EVS with NetApp Disaster Recovery

Quick start for NetApp Disaster Recovery

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

1 **Review prerequisites**

Ensure your system meets these requirements.

2 **Set up NetApp Disaster Recovery**

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

3 **What's next?**

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

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

Set up your infrastructure for NetApp Disaster Recovery

To use NetApp Disaster Recovery, perform a few steps to set it up both in Amazon Web Services (AWS) and in the NetApp Console.

Review prerequisites to ensure that your system is ready.

You can use NetApp Disaster Recovery in the following infrastructures:

- Hybrid cloud DR that replicates an on-premises VMware plus ONTAP datacenter to an AWS DR infrastructure based on VMware Cloud on AWS and Amazon FSx for NetApp ONTAP.
- Private cloud DR that replicates an on-premises VMware plus ONTAP vCenter to another on-premises VMware plus ONTAP vCenter.

Hybrid cloud with VMware Cloud and Amazon FSx for NetApp ONTAP

This method consists of an on-premises production vCenter infrastructure using datastores hosted on ONTAP FlexVol volumes using an NFS protocol. The DR site consists of one or more VMware Cloud SDDC instances using datastores hosted on FlexVol volumes provided by one or more FSx for ONTAP instances using an NFS protocol.

The production and DR sites are connected by an AWS-compatible secure connection. Common connection typs are a secure VPN (private or AWS provided), AWS Direct Connect, or other approved interconnect methods.

For Disaster Recovery involving AWS cloud infrastructure, you must use the Console agent for AWS. The agent should be installed in the same VPC as the FSx for ONTAP instance. If additional FSx for ONTAP instances were deployed in other VPCs, the VPC hosting the agent must have access to the other VPCs.

AWS availability zones

AWS supports deploying solutions in one or more availability zones (AZ) within a given region. Disaster Recovery uses two AWS hosted services: VMware Cloud for AWS and AWS FSx for NetApp ONTAP.

- **VMware Cloud for AWS**: Supports the deployment in a single-AZ or in a dual-AZ stretch-cluster SDDC environment. Disaster Recovery supports a single-AZ SDDC deployment only for Amazon VMware Cloud for AWS.
- **AWS FSx for NetApp ONTAP**: When this is deployed in a dual-AZ configuration, each volume is owned by a single FSx system. Each volume is owned by a single FSx system. The volume’s data is mirrored to the second FSx system. The FSx for ONTAP systems can be deployed in either single- or dual-AZ deployments. Disaster Recovery supports both single- and multi-AZ FSx for FSx for ONTAP deployments.

BEST PRACTICE: For AWS DR site configuration, NetApp recommends using single-AZ deployments for both VMware Cloud and AWS FSx for ONTAP instances. Because AWS is being used for DR, there is no advantage to introducing multiple AZs. Multi-AZs can increase costs and complexity.

On-premises to AWS

AWS provides the following methods to connect private datacenters to the AWS cloud. Each solution has its benefits and cost considerations.

- **AWS Direct Connect**: This is an AWS cloud interconnect located in the same geographic area as your private datacenter and provided by an AWS partner. This solution provides a secure, private connection between your local datacenter and the AWS cloud without the need for a public internet connection. This is the most direct and efficient connection method offeredy by AWS.
- **AWS Internet Gateway**: This provides public connectivity between AWS cloud resources and external compute resources. This type of connection is typically used to provide service offerings to external customers, such as HTTP/HTTPS service where security is not a requirement. There is no quality-of-service control, security, or guarantee of connectivity. For this reason, this connection method is not recommended for connecting a production datacenter to the cloud.
- **AWS Site-Site VPN**: This virtual private network connection can be used to provide secure access connections along with a public internet service provider. The VPN encrypts and decrypts all data traveling to and from the AWS cloud. VPNs can be either software- or hardware-based. For enterprise applications, the public internet service provider (ISP) should offer quality-of-service guarantees to ensure that adequate bandwidth and latency are provide for DR replication.

BEST PRACTICE: For AWS DR site configuration, NetApp recommends using AWS Direct Connect. This solution provides the highest performance and security for enterprise applications. If it is not available, a high-performance public ISP connection along with a VPN should be used. Ensure that the ISP offers commercial QoS service levels to ensure adequate network performance.

VPC-to-VPC interconnections

AWS offers the following types of VPC-to-VPC interconnections. Each solution has its benefits and cost considerations.

- **VPC Peering**: This is a private connection between two VPCs. It is the most direct and efficient connection method offered by AWS. VPC peering can be used to connect VPCs in the same or different AWS regions.
- **AWS Internet Gateway**: This is typically used to provide connections between AWS VPC resources and non-AWS resources and endpoints. All traffic follows a "hair-pin" path where VPC traffic destined to another VPC exits the AWS infrastructure through the internet gateway and returns to the AWS infrastructure through the same or different gateway. This is not a suitable VPC connection type for enterprise VMware solutions.
- **AWS Transit Gateway**: This is a centralized router-based connection type that enables each VPC to connect to a single, central gateway, which acts as a central hub for all VPC-to-VPC traffic. This can also be connected to your VPN solution to enable on-premises datacenter resources to access AWS VPC-hosted resources. This type of connection typically requires an additional cost to implement.

BEST PRACTICE: For DR solutions involving VMware Cloud and a single FSx for ONTAP VPC, NetApp recommends that you use the VPC peer connection. If multiple FSx for ONTAP VPCs are deployed, then we recommend using an AWS Transit Gateway to reduce the management overhead of multiple VPC peer connections.

Get ready for on-premises-to-cloud protection using AWS

To set up NetApp Disaster Recovery for on-premises-to-cloud protection using AWS, you need to set up the following:

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

Set up AWS FSx for NetApp ONTAP

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

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

Set up VMware Cloud on AWS SDDC

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

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

Private cloud

You can use NetApp Disaster Recovery to protect VMware VMs hosted on one or more vCenter clusters by replicating VM datastores to another vCenter cluster either in the same private datacenter or to a remote private or collocated datacenter.

For on-premises to on-premises situations, install the Console agent at one of the physical sites.

Disaster Recovery supports site-to-site replication using Ethernet and TCP/IP. Ensure that adequate bandwidth is available to support data change rates on the production site VMs so that all changes can be replicated to the DR site within the Recovery Point Objective (RPO) time frame.

Get ready for on-premises-to-on-premises protection

Ensure that the following requirements are met before you set up NetApp Disaster Recovery for on-premises-to-on-premises protection:

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

Intelligent proxy support

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

When a proxy is configured, NetApp Disaster Recovery attempts to communicate directly with VMware or ONTAP and uses the configured proxy if direct communication fails.

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

For more information about general proxy set up in the NetApp Console, see Configure the Console agent to use a proxy server.

Access NetApp Disaster Recovery

You use the NetApp Console to log in to the NetApp Disaster Recovery service.

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

Specific tasks require specific user roles.
Learn about user roles and permissions in NetApp Disaster Recovery.
Learn about NetApp Console access roles for all services.

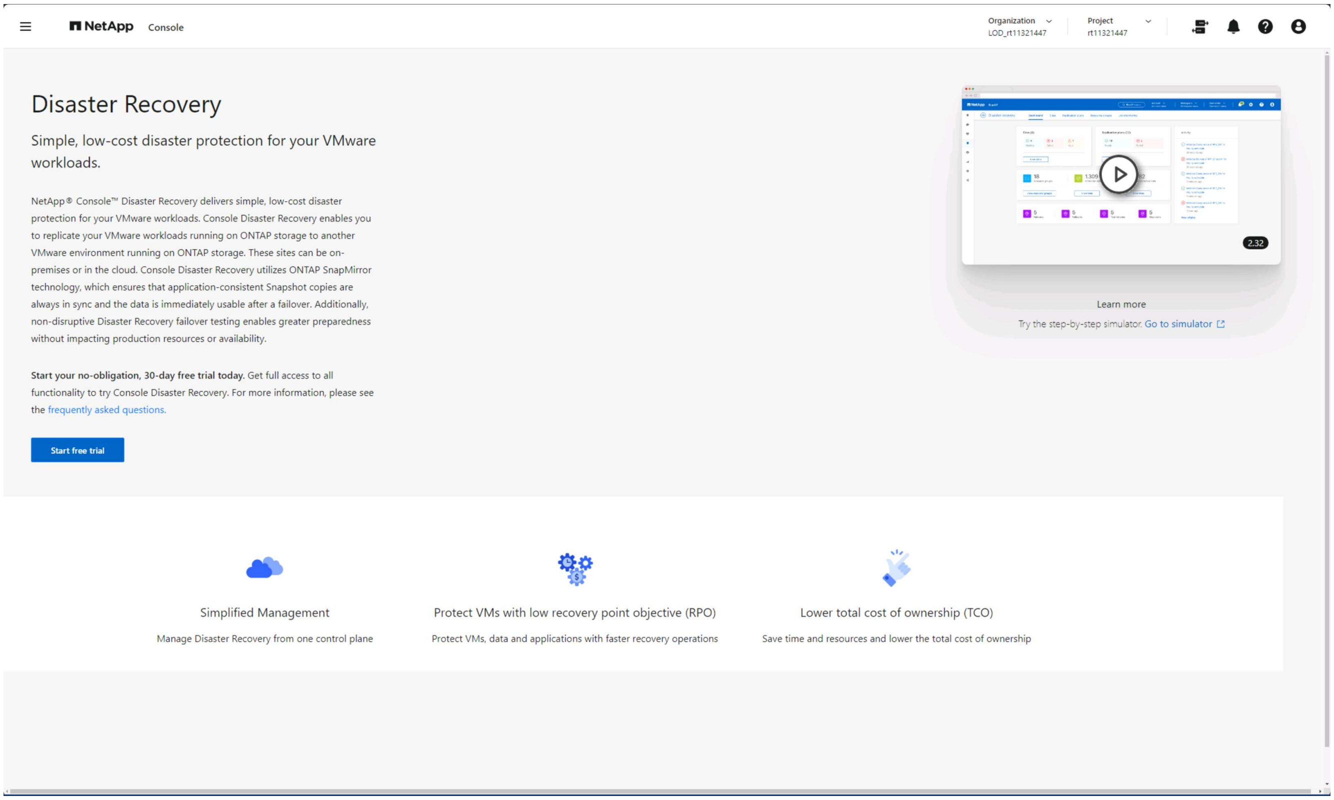
Steps

1. Open a web browser and go to the NetApp Console.

   The NetApp Console login page appears.

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

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



Disaster Recovery

Simple, low-cost disaster protection for your VMware workloads.

NetApp® Console™ Disaster Recovery delivers simple, low-cost disaster protection for your VMware workloads. Console Disaster Recovery enables you to replicate your VMware workloads running on ONTAP storage to another VMware environment running on ONTAP storage. These sites can be on-premises or in the cloud. Console Disaster Recovery utilizes ONTAP SnapMirror technology, which ensures that application-consistent Snapshot copies are always in sync and the data is immediately usable after a failover. Additionally, non-disruptive Disaster Recovery failover testing enables greater preparedness without impacting production resources or availability.

Start your no-obligation, 30-day free trial today. Get full access to all functionality to try Console Disaster Recovery. For more information, please see the frequently asked questions.

Try the step-by-step simulator. Go to simulator

Simplified Management

Manage Disaster Recovery from one control plane

Protect VMs with low recovery point objective (RPO)

Protect VMs, data and applications with faster recovery operations

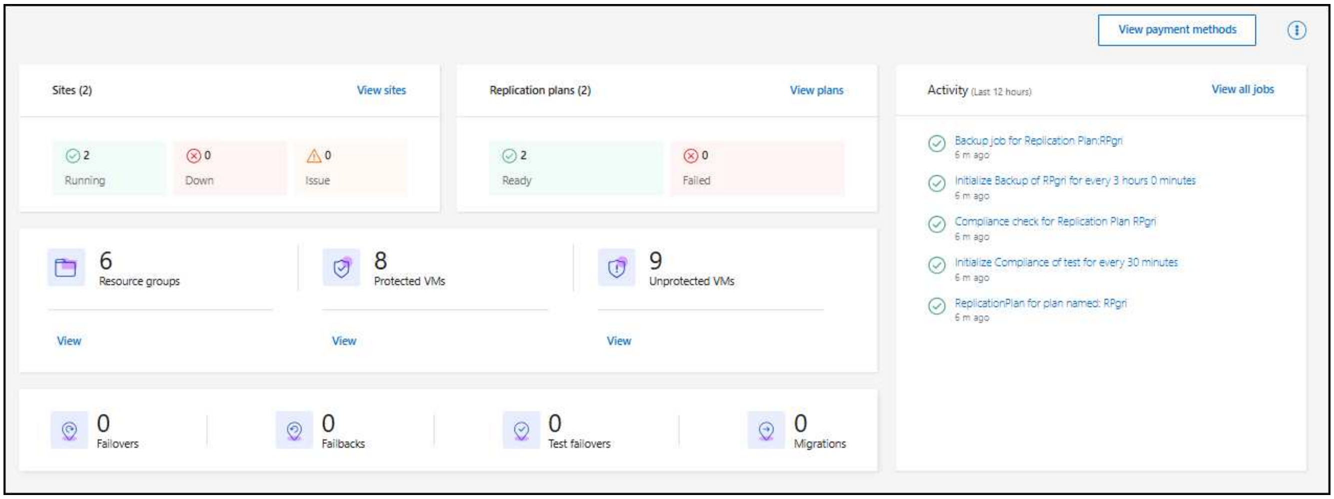
Lower total cost of ownership (TCO)

Save time and resources and lower the total cost of ownership

   Otherwise, the NetApp Disaster Recovery Dashboard appears.

   - If you haven’t yet added a NetApp Console agent, you’ll need to add one. To add the agent, refer to Learn about Console agents.

- If you are a NetApp Console user with an existing agent, when you select "Disaster recovery," a message appears about signing up.
- If you are already using the service, when you select "Disaster recovery," the Dashboard appears.



Backup job for Replication Plan:RPgri
6 m ago

Initialize Backup of RPgri for every 3 hours 0 minutes
6 m ago

Compliance check for Replication Plan RPgri
6 m ago

Initialize Compliance of test for every 30 minutes
6 m ago

ReplicationPlan for plan named: RPgri
6 m ago

Set up licensing for NetApp Disaster Recovery

With NetApp Disaster Recovery, you can use different licensing plans including a free trial, a pay-as-you-go subscription, or bring your own license.

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

Learn about user roles and permissions in NetApp Disaster Recovery.
Learn about access roles for all services.

Licensing options
You can use the following licensing options:

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

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

Learn more about subscriptions.

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

- View any resource, such as a workload or replication plan.

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

Try it out using a 30-day free trial

You can try NetApp Disaster Recovery out by using a 30-day free trial.

> ⓘ No capacity limits are enforced during the trial.

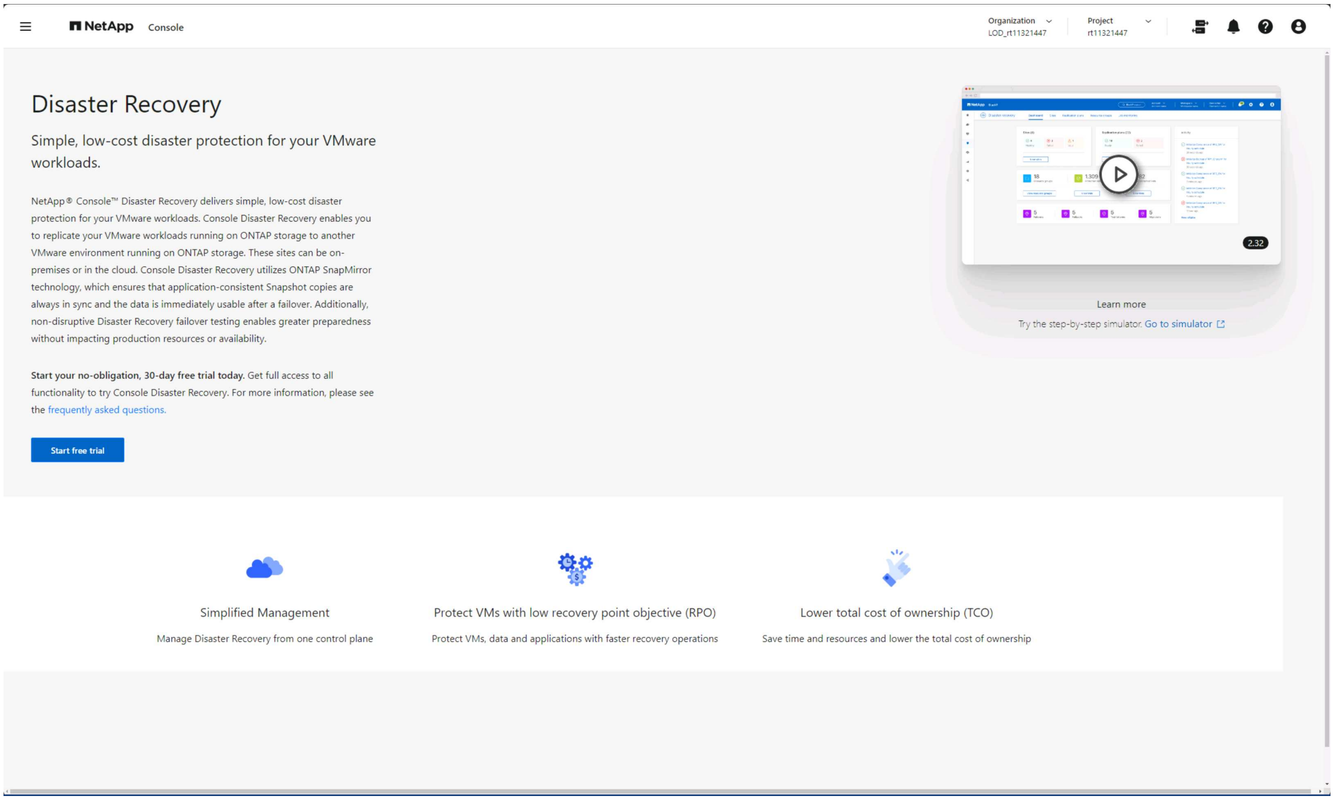
To continue after the trial, you'll need to purchase a BYOL license or PAYGO AWS subscription. You can get a license at any time and you will not be charged until the trial ends.

During the trial, you have full functionality.

Steps

1. Log in to the NetApp Console.
2. From the NetApp Console left navigation, select **Protection** > **Disaster recovery**.

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



Disaster Recovery

Simple, low-cost disaster protection for your VMware workloads.

NetApp® Console™ Disaster Recovery delivers simple, low-cost disaster protection for your VMware workloads. Console Disaster Recovery enables you to replicate your VMware workloads running on ONTAP storage to another VMware environment running on ONTAP storage. These sites can be on-premises or in the cloud. Console Disaster Recovery utilizes ONTAP SnapMirror technology, which ensures that application-consistent Snapshot copies are always in sync and the data is immediately usable after a failover. Additionally, non-disruptive Disaster Recovery failover testing enables greater preparedness without impacting production resources or availability.

Start your no-obligation, 30-day free trial today. Get full access to all functionality to try Console Disaster Recovery. For more information, please see the frequently asked questions.

Try the step-by-step simulator. Go to simulator

Simplified Management

Manage Disaster Recovery from one control plane

Protect VMs with low recovery point objective (RPO)

Protect VMs, data and applications with faster recovery operations

Lower total cost of ownership (TCO)

Save time and resources and lower the total cost of ownership

3. If you haven't already added a Console agent for other services, add one.

   To add a Console agent, refer to Learn about Console agents.

4. After you set up the agent, in the NetApp Disaster Recovery landing page, the button to add the agent changes to a button for starting a free trial. Select **Start free trial**.
5. Begin by adding vCenters.

For details, see Add vCenter sites.

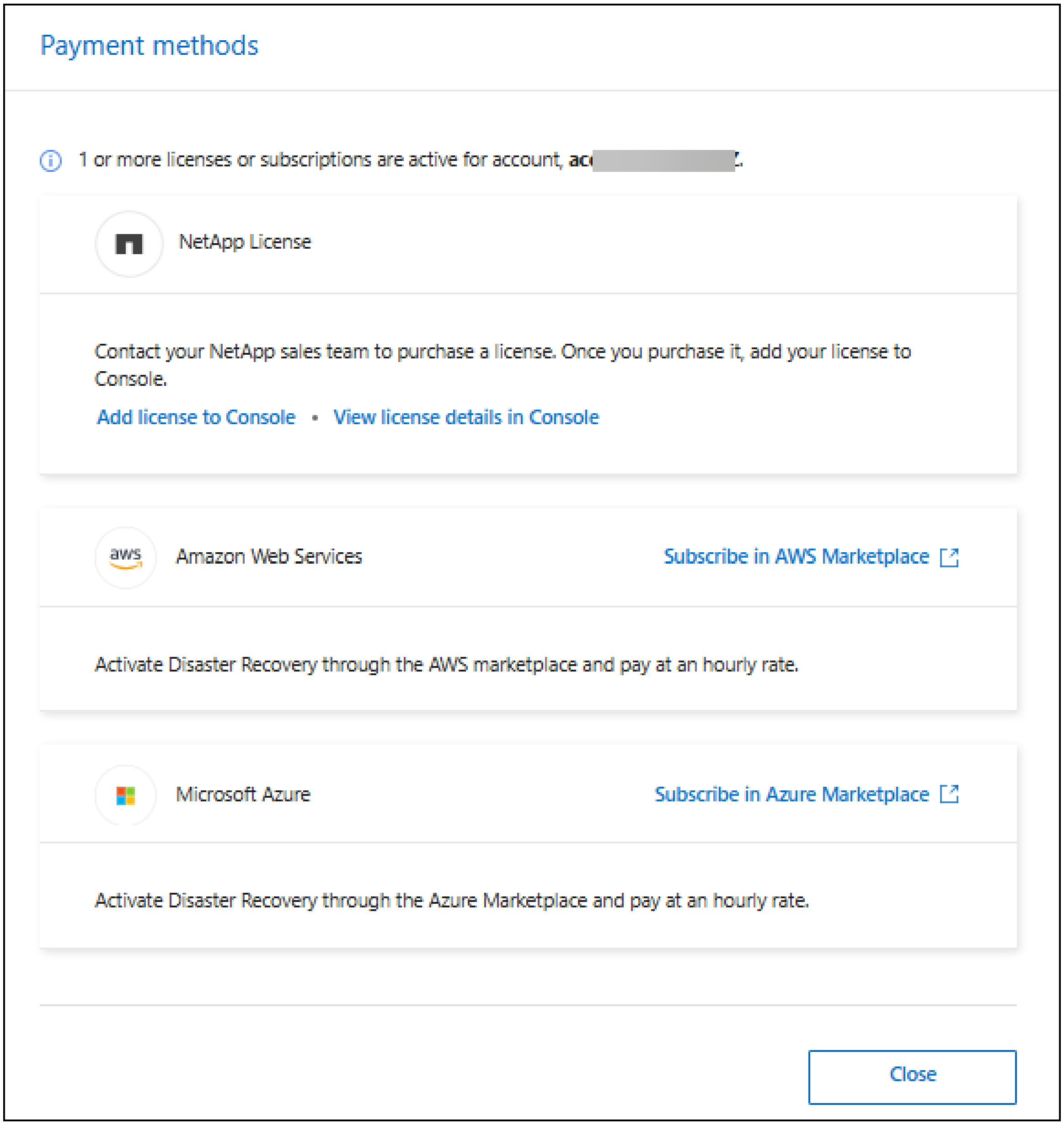
After the trial ends, subscribe through one of the Marketplaces

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

Steps

1. In the NetApp Disaster Recovery, you see a message that the free trial is expiring. In the message, select **Subscribe or purchase a license**.

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



Payment methods

ⓘ 1 or more licenses or subscriptions are active for account, ac[redacted].

NetApp License

Contact your NetApp sales team to purchase a license. Once you purchase it, add your license to Console.

Add license to Console • View license details in Console

Amazon Web Services — Subscribe in AWS Marketplace

Activate Disaster Recovery through the AWS marketplace and pay at an hourly rate.

Microsoft Azure — Subscribe in Azure Marketplace

Activate Disaster Recovery through the Azure Marketplace and pay at an hourly rate.

2. Select **Subscribe in AWS Marketplace** or **Subscribe in Azure Marketplace**.
3. Use AWS Marketplace or Microsoft Azure Marketplaceto subscribe to **NetApp Disaster Recovery**.

4. When you return to NetApp Disaster Recovery, a message states that you are subscribed.

   You can view subscription details in the NetApp Console subscription page. Learn more managing subscriptions with the NetApp Console.

After the trial ends, purchase a BYOL license through NetApp

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

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

Add the license to the NetApp Console*
After you've purchased your NetApp Disaster Recovery license from a NetApp Sales Rep, you can manage the license in the Console.

Learn about adding licenses with the NetApp Console.

Update your 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 NetApp Disaster Recovery UI. You can update your NetApp 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 the NetApp Console and in Notifications.

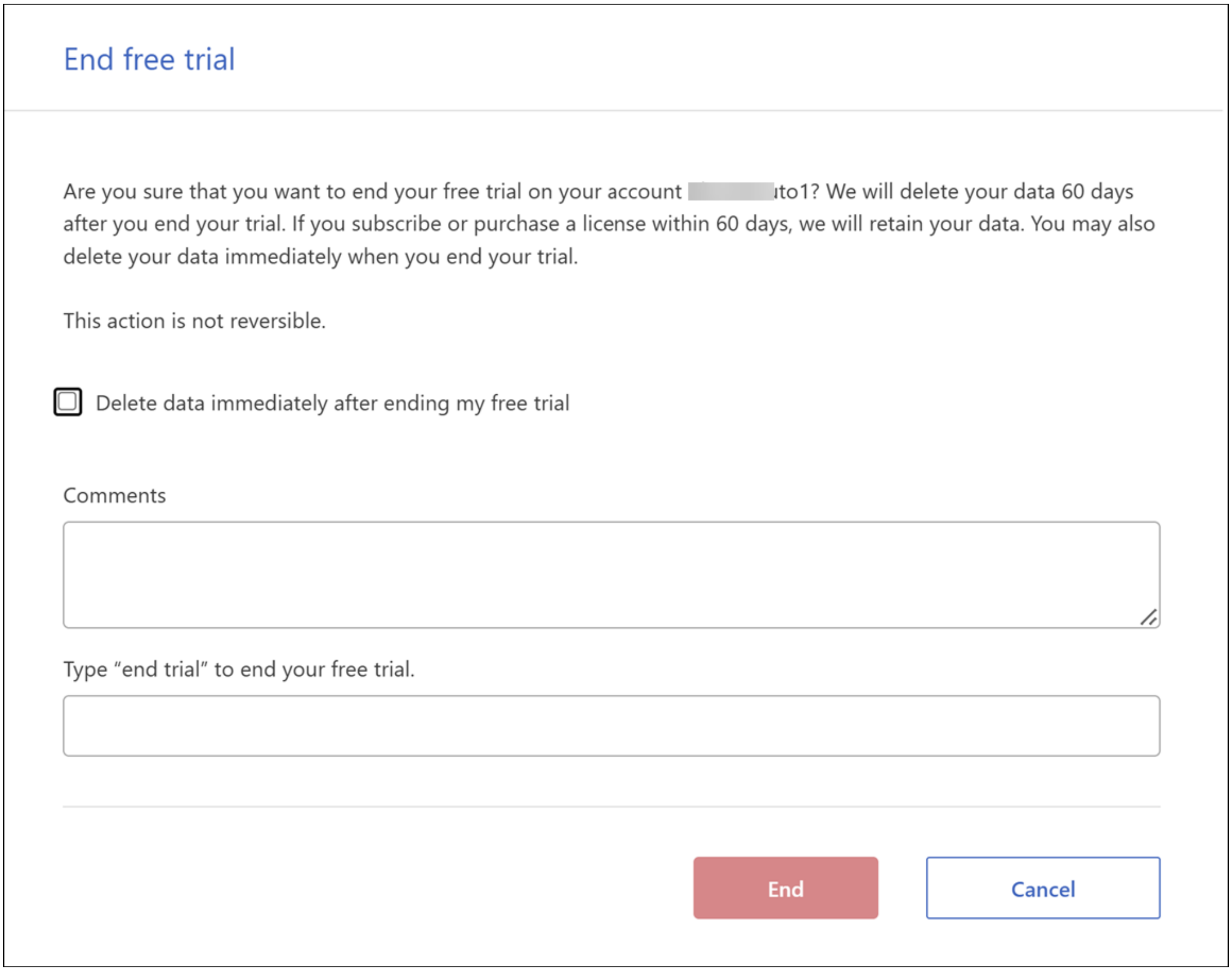
Learn about updating licenses with the NetApp Console.

End the free trial

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

Steps

1. In NetApp Disaster Recovery, select **Free trial - View details**.
2. In the drop-down details, select **End free trial**.



End free trial

Are you sure that you want to end your free trial on your account [redacted]ıto1? We will delete your data 60 days after you end your trial. If you subscribe or purchase a license within 60 days, we will retain your data. You may also delete your data immediately when you end your trial.

This action is not reversible.

☐ Delete data immediately after ending my free trial

Comments

Type “end trial” to end your free trial.

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

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

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

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

Copyright information

Trademark information