Release notes

NetApp Disaster Recovery

NetApp
March 09, 2026

Table of Contents

Release notes

What's new in NetApp Disaster Recovery

Learn what's new in NetApp Disaster Recovery.

09 March 2026

Version 4.3.1

Exclude a datastore from replication plans

When you create a replication plan in Disaster, you can now exclude specific datastores from replication. For situations where a VM is configure to use multiple datastore, this allows you to limit which ones are replicated.

For details, see Create a replication plan.

Removed password validation from vCenter password

Disaster Recovery removed password restrictions on vCenter passwords to allow passwords that contain spaces.

For more information, see Add on-premises and Amazon EVS vCenter clusters in NetApp Disaster Recovery.

New replication plan submenu

Disaster Recover now includes new menu options to trigger vCenter refreshes from the replication plan dashboard. You can access the submenu from the replication plan dashboard's action menu: select **Plan Health** then **Refresh Source vCenter / Refresh Target vCenter**.

For more information, see Modify a replication plan.

Improved network discovery

Disaster Recovery now includes improved network discovery to support a broader array of network configurations.

16 February 2026

Version 4.3.0

Improved user interface

The Disaster Recovery UI has been refreshed to improve performance and user experience based on feedback.

API Swagger documentation

The Disaster Recovery API Swagger documentation can now be accessed in a regular browser; incognito mode is no longer required. To access the API documentation, browse to the Disaster Recovery dashboard, select the top-right context menu  then **API Documentation** to open the Swagger documentation. You

can also bookmark the URL.

12 January 2026

Version 4.2.9

Support for multiple Console agents in on-premises environments

If you're using Disaster Recovery on-premises, you can now deploy a Console agent for each vCenter instance, improving resiliency.

For example, if you have two sites (Sites A and B), Site A can have Console agent A attached to vCenter 1, ONTAP deployment 1 and ONTAP deployment 2. Site B can have Console agent B attached to vCenter 2 and ONTAP deployments 3 and 4.

For information about the Console agent in Disaster Recovery, see Create the Console agent.

Add VMs after failover for replication plans using datastore-based protection

When failover is triggered, any replication plan using datastore-based protection includes VMs that have been added to the datastore, provided they have been discovered. You must provide mapping details for the added VMs before failover completes.

For more information, see Fail over applications.

New email notifications

Disaster Recovery now provides email notifications for the following events:

- Approaching capacity usage limit
- Completed report generation
- Job failures
- License expiration or violations

Swagger improvements

You can now access the Swagger documentation from within Disaster Recovery. In Disaster Recovery, select **Settings** then **API documentation** to link to the Swagger, or visit this URL in your browser's incognito/private mode: https://snapcenter.cloudmanager.cloud.netapp.com/api/api-doc/draas.

Improved user interfaces

Disaster Recovery now provides improved warnings and error resolutions. This release fixes an error that prevented canceled jobs from displaying in the user interface. Canceled jobs are now visible. There's also a new warning when the same destination network is mapped to multiple different source networks.

Retain VM folder structure added as default in replication plans

When you create a replication, the new default is to retain the VM folder structure. If the recovery target does not have the original folder hierarchy, Disaster Recovery creates it. You can deselect this option to disregard the original folder hierarchy.

For more information, see Create a replication plan.

09 December 2025

Version 4.2.8P1

Folder hierarchy retention

By default, Disaster Recovery retains the VM inventory hierarchy (folder structure) on failover. If the recovery target doesn't have the required folder, Disaster Recovery creates it.

You can now override this setting by designating a new parent VM folder or by unchecking the **Retain original folder hierarchy** option.

For more information, see Create a replication plan.

Streamlined Console agent updating

Disaster Recovery now supports a streamlined process for using multiple Console agents in a working environment. To switch between Console agents, you must edit your vCenter configuration, rediscover the credentials, and refresh the replication plans to use the new Console agent.

For more information, see Switch Console agents.

01 December 2025

Version 4.2.8

Support for Google Cloud VMware Engine using Google Cloud NetApp Volumes

NetApp Disaster Recovery now supports Google Cloud VMware Engine using Google Cloud NetApp Volumes for migration, failover, failback, and testing operations. This integration enables seamless disaster recovery workflows between on-premises environments and Google Cloud.

Ensure you review the prerequisites and limitations for Google Cloud.

10 November 2025

Version 4.2.7

Cascading failover support

You can now configure a cascading relationship in ONTAP and use any leg of that replication relationship for disaster recovery.

Downgrade VMware hardware support during registration

Disaster Recovery now supports downgrading VMware hardware to an earlier version of vSphere during registration. This is useful when the source ESX host is running a later version than the disaster recovery site.

For more information, see Create a replication plan in NetApp Disaster Recovery.

Graceful shutdown

Disaster Recovery now gracefully shuts down VMs instead of powering them off. If a given VM takes more than ten minutes to power down, Disaster Recovery powers it off.

Pre-backup scripting support

You can now inject custom scripting into the failover workflow to run before creating a backup. Pre-backup scripting enables you to control the VM's state before a snapshot is replicated and prepare a VM for a transition. For example, you can inject a script that unmounts an NFS mount that will be remounted using a different script after failover.

For more information, see Create a replication plan in NetApp Disaster Recovery.

06 October 2025

Version 4.2.6

BlueXP disaster recovery is now NetApp Disaster Recovery

BlueXP disaster recovery has been renamed to NetApp Disaster Recovery.

BlueXP is now NetApp Console

The NetApp Console, built on the enhanced and restructured BlueXP foundation, provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration, that is highly secure and compliant.

For details on what has changed, see the NetApp Console release notes.

Other updates

- Support for Amazon Elastic VMware Service (EVS) with Amazon FSx for NetApp ONTAP was in a public preview. With this release, it is now generally available. For details, refer to Introduction of NetApp Disaster Recovery using Amazon Elastic VMware Service and Amazon FSx for NetApp ONTAP.
- Storage discovery improvements, including reduced discovery times for on-premises deployments
- Identity and Access Management (IAM) support, including role-based access control (RBAC) and enhanced user permissions
- Private Preview support for Azure VMware solution and Cloud Volumes ONTAP. With this support, you can now configure disaster recovery protection from on-premises to the Azure VMware solution using Cloud Volumes ONTAP storage.

04 August 2025

Version 4.2.5P2

NetApp Disaster Recovery updates

This release includes the following updates:

- Improved the VMFS support to handle the same LUN presented from multiple storage virtual machines.
- Improved the test teardown cleanup to handle the datastore already being unmounted and or deleted.
- Improved subnet mapping so that it now validates that the gateway entered is contained within the network provided.
- Corrected an issue that could cause the replication plan to fail if the VM name contains ".com".

- Removed a restriction preventing the destination volume from being the same as the source volume when creating the volume as part of the replication plan creation.
- Added support for a pay-as-you-go (PAYGO) subscription to NetApp Intelligent Services in the Azure Marketplace and added a link to the Azure Marketplace in the free trial dialog.

  For details, see NetApp Disaster Recovery licensing and Set up licensing for NetApp Disaster Recovery.

14 July 2025

Version 4.2.5

User roles in NetApp Disaster Recovery

NetApp Disaster Recovery now employs roles to govern the access that each user has to specific features and actions.

The service uses the following roles that are specific to NetApp Disaster Recovery.

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

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

For details, see User roles and permissions in NetApp Disaster Recovery.

Learn about access roles for all services.

Other updates in NetApp Disaster Recovery

- Enhanced network discovery
- Scalability improvements:
  - Filtering for the required metadata instead of all the details
  - Discovery improvements to retrieve and update VM resources faster
  - Memory optimization and performance optimization for data retrieval and data updates
  - vCenter SDK client creation and pool management improvements
- Stale data management on the next scheduled or manual discovery:
  - When a VM is deleted in the vCenter, NetApp Disaster Recovery now automatically removes it from the replication plan.
  - When a datastore or network is deleted in the vCenter, NetApp Disaster Recovery now deletes it from the replication plan and resource group.
  - When a cluster, host, or datacenter is deleted in the vCenter, NetApp Disaster Recovery now deletes it from the replication plan and resource group.
- You can now access Swagger documentation in your browser's incognito mode. You can access it from within NetApp Disaster Recovery from the Settings option > API Documentation or directly at the following URL in your browser's incognito mode: Swagger documentation.

- In some situations after a failback operation, the iGroup was left behind after the operation completed. This update removes the iGroup if it is stale.
- If the NFS FQDN was used in the replication plan, NetApp Disaster Recovery now resolves it to an IP address. This update is useful if the FQDN is not resolvable in the disaster recovery site.
- UI alignment improvements
- Log improvements to capture the vCenter sizing details after the successful discovery

30 June 2025

Version 4.2.4P2

Discovery improvements

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

23 June 2025

Version 4.2.4P1

Subnet mapping improvements

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

09 June 2025

Version 4.2.4

Windows Local Administrator Password Solution (LAPS) support

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

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

For details, refer to Create a replication plan.

13 May 2025

Version 4.2.3

Subnet mapping

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

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

For example:

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

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

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

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

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

Skip protection

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

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

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

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

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

SnapMirror schedule updates in the replication plan

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

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

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

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

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

16 April 2025

Version 4.2.2

Scheduled discovery for VMs

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

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

For details, refer to Add vCenter server sites.

Resource group datastore support

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

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

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

For details, refer to Create a replication plan.

Notifications of free trial or license expiration

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

Notification of service updates

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

10 March 2025

Version 4.2.1

Intelligent proxy support

The NetApp Console agent supports intelligent proxy. Intelligent proxy is a lightweight, secure, and efficient way to connect your on-premises system to NetApp Disaster Recovery. It provides a secure connection between your system and NetApp Disaster Recovery 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 the intelligent proxy for NetApp Disaster Recovery, see Set up your infrastructure for NetApp Disaster Recovery.

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

End the free trial any time

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

See End the free trial.

19 February 2025

Version 4.2

ASA r2 support for VMs and datastores on VMFS storage

This release of NetApp Disaster Recovery provides support for ASA r2 for VMs and datastores on VMFS storage. On an ASA r2 system, ONTAP software supports essential SAN functionality while removes features not supported in SAN environments.

This release supports the following features for ASA r2:

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

The support for ASA r2 in NetApp Disaster Recovery uses ONTAP 9.16.1.

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

30 October 2024

Reporting

You can now generate and download reports to help you analyze your landscape. Predesigned reports

summarize failovers and failbacks, show replication details on all sites, and show job details for the past seven days.

Refer to Create disaster recovery reports.

30-day free trial

You can now sign up for a 30-day free trial of NetApp Disaster Recovery. Previously, free trials were for 90 days.

Refer to Set up licensing.

Disable and enable replication plans

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

Here's how:

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

Folder mapping

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

For details, refer to Create a replication plan.

VM details available for failover, failback, and test failover

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

Refer to Fail over applications to a remote site.

VM boot delay with ordered boot sequence

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

For details, refer to Create a replication plan.

VM operating system information

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

For details, refer to Create a replication plan.

VM name aliasing

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

For details, refer to Create a replication plan.

Clean up old snapshots

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

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

Reconcile snapshots

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

For details, refer to Manage replication plans.

20 September 2024

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

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

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

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

02 August 2024

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

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

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

Job cancel

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

Refer to Monitor jobs.

17 July 2024

Failover test schedules

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

Here's how:

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

Replication plan updates

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

Here's how:

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

05 July 2024

This NetApp Disaster Recovery release includes the following updates:

Support for AFF A-series

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

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

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

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

Replication plan updates

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

Edit replication plans

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

Refer to Manage plans.

Edit VMs

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

Refer to Manage VMs.

Fail over updates

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

Refer to Fail over applications to a remote site.

Failover test schedules

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

Refer to Manage plans.

Updates to prerequisite information

NetApp Disaster Recovery prerequisites information has been updated.

Refer to NetApp Disaster Recovery prerequisites.

15 May 2024

This NetApp Disaster Recovery release includes the following updates:

Replicating VMware workloads from on-premises to on-premises

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

Licensing updates

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

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

Learn more about NetApp Disaster Recovery.

05 March 2024

This is the General Availability release of NetApp Disaster Recovery, which includes the following updates.

Licensing updates

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

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

For details about managing licenses for **all** NetApp Console data services, refer to Manage licenses for all NetApp Console data services.

Edit schedules

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

For details, refer to Create the replication plan.

01 February 2024

This NetApp Disaster Recovery preview release includes the following updates:

Network enhancement

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

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

For details, refer to Create a replication plan.

Custom scripts

Can now be included as post failover processes. With custom scripts, you can have NetApp Disaster Recovery run your script after a failover process. For example, you can use a custom script to resume all database

transactions after the failover is complete.

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

SnapMirror relationship

You can now create a SnapMirror relationship while developing the replication plan. Previously, you had to create the relationship outside of NetApp Disaster Recovery.

For details, refer to Create a replication plan.

Consistency groups

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

For details, refer to Create a replication plan.

VM power-on delay option

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

For details, refer to Create a replication plan.

Application-consistent Snapshot copies

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

For details, refer to Create a replication plan.

11 January 2024

This preview release of NetApp Disaster Recovery includes the following updates:

Dashboard more quickly

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

Learn about NetApp Disaster Recovery.

20 October 2023

This preview release of NetApp Disaster Recovery includes the following updates.

Protect on-premises, NFS-based VMware workloads

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

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

Learn more about NetApp Disaster Recovery.

27 September 2023

This preview release of NetApp Disaster Recovery includes the following updates:

Dashboard updates

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

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

Replication plan updates

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

  Refer to Create a replication plan.

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

  Refer to Create a replication plan.

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

  Refer to Manage resources.

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

    Refer to Create a replication plan.

01 August 2023

NetApp Disaster Recovery preview

NetApp Disaster Recovery preview is a cloud-based disaster recovery service that automates disaster recovery workflows. Initially, with the NetApp Disaster Recovery preview, you can protect your on-premises,

NFS-based VMware workloads running NetApp storage to VMware Cloud (VMC) on AWS with Amazon FSx for ONTAP.

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

Learn more about NetApp Disaster Recovery.

This release includes the following updates:

Resource groups update for boot order

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

Replication verification

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

Replication plan shows recovery point objective (RPO) transfer schedules

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

Job Monitor update

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

18 May 2023

This is the initial release of NetApp Disaster Recovery.

Cloud-based disaster recovery service

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

Learn more about NetApp Disaster Recovery.

Limitations in NetApp Disaster Recovery

Known limitations identify platforms, devices, or functions that are not supported by this

release of the service, or that do not interoperate correctly with it.

Wait until failback completes before running discovery

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

NetApp Console might not discover Amazon FSx for NetApp ONTAP

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

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

If you need to remove the ONTAP FSx cluster from NetApp Disaster Recovery, complete the following steps:

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

Refer to Manage existing Console agents.

1. In the NetApp Console Systems page, add the Amazon FSx for ONTAP system again and provide the FSx credentials.

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

2. From NetApp Disaster Recovery, select **Sites**, on the vCenter row select the **Actions** option , and from the Actions menu, select **Refresh** to refresh the FSx discovery in NetApp Disaster Recovery.

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

Limitations with Google Cloud NetApp Volumes

- After running a failover test, you have to wait at least 52 hours to delete the clone volume. You must delete the volume manually. After 52 hours, you can test failover again.
- If any part of the mount operation fails, failover will not succeed and the jobs will time out. It takes up to three days for Google to look into the issue, during which all datastore-related operations on the vCenter are blocked.

Copyright information

Trademark information