



Protect your data

Workload Factory for NetApp Console

NetApp
October 07, 2026

This PDF was generated from <https://docs.netapp.com/us-en/data-services-workloads/fsx-storage/data-protection-overview.html> on October 07, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Protect your data	1
Types of data protection in NetApp Workload Factory	1
Types of data protection	1
Best practices for protecting your workload data	2
Protect your workload data with snapshots	2
Protect your workload data with NetApp Autonomous Ransomware Protection with AI	2
Protect your workload data with volume replication	2
Protect your workload data with backups	3
Recommendations for protecting your workload data	3
Use snapshots to protect data	3
Use snapshots to protect data in NetApp Workload Factory	3
Manage snapshot policies for volumes in NetApp Workload Factory	6
Manage snapshots of an FSx for ONTAP volume	10
Use backups to protect data in NetApp Workload Factory	12
Create an on-demand backup of a volume	12
Manage the backup schedule for an FSx for ONTAP file system	12
Restore a volume from a backup in NetApp Workload Factory	13
Use replication to protect data	14
Replicate data to FSx for ONTAP in NetApp Workload Factory	14
Replicate on-premises ONTAP cluster data in NetApp Workload Factory	19
Replicate a storage VM to another FSx for ONTAP file system	22
Track replication delays in NetApp Workload Factory	24
Manage your replication relationships in NetApp Workload Factory	24
Protect your FSx for ONTAP data with NetApp Autonomous Ransomware Protection with AI	29
Enable ARP/AI for a file system or a volume	30
Validate ransomware attacks	31
Recover data after a ransomware attack	31
Clone a volume in NetApp Workload Factory	32
Protect your FSx for ONTAP data with a cyber vault	32

Protect your data

Types of data protection in NetApp Workload Factory

FSx for ONTAP supports snapshots, NetApp Autonomous Ransomware Protection with AI, replication, and backups for data protection. We recommend that you use a combination of data protection types to prepare for the inevitable and safeguard your data.

Types of data protection

Data protection for your workloads helps ensure that you can recover from any data loss at any time. Learn about the types of data protection before you select the features you'll use.

Snapshots

A snapshot creates a read-only, point-in-time image of a volume within the source volume as a snapshot copy. You can use the snapshot copy to recover individual files, or to restore the entire contents of a volume. Snapshots are the basis of all the backup methods. The snapshot copy that is created on your volume is used to keep the replicated volume and backup file synchronized with changes made to the source volume.

NetApp Autonomous Ransomware Protection with AI

NetApp Autonomous Ransomware Protection with AI (ARP/AI) uses workload analysis in NAS (NFS/SMB) environments to detect and warn about abnormal activity that might be a ransomware attack. When an attack is suspected, ARP/AI also creates new, immutable snapshots in addition to the existing protection provided by scheduled snapshots.

Replication

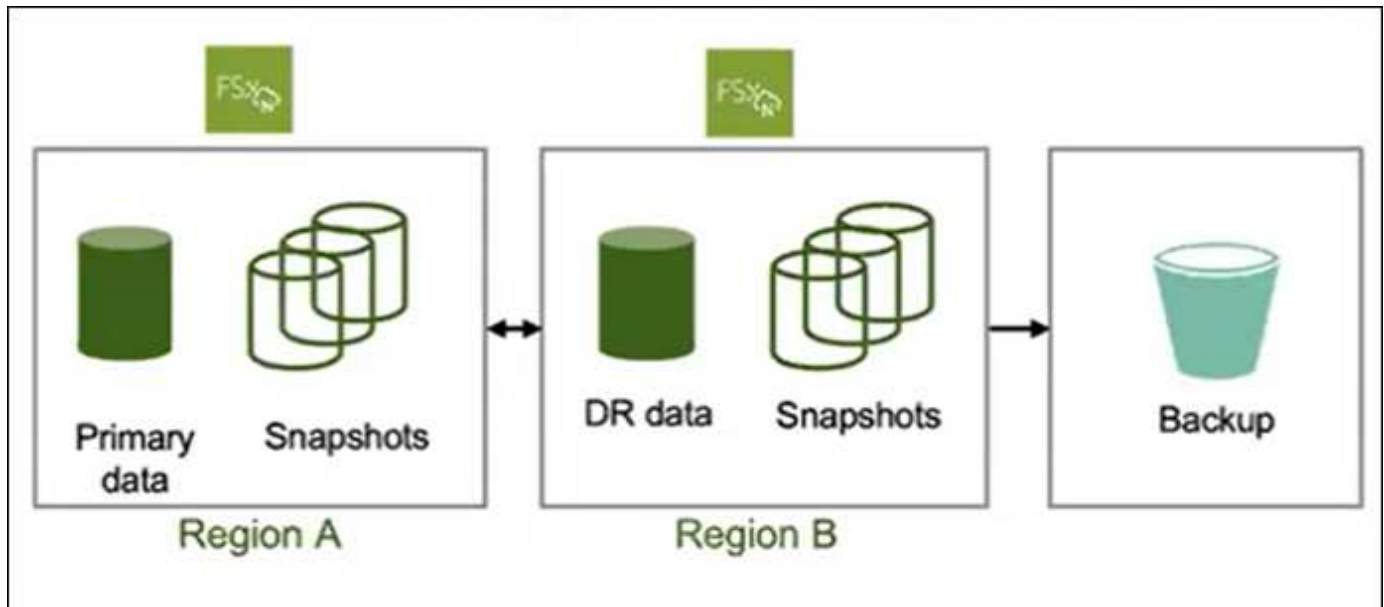
Replication creates a secondary copy of your data on another FSx for ONTAP file system and continually updates the secondary data. Your data is kept current and remains available whenever you need it, such as for disaster recovery.

You can choose to create both replicated volumes on another FSx for ONTAP file system and backup files in the cloud. Or you can choose just to create replicated volumes or backup files - it's your choice.

Backups

You can create backups of your data to the cloud for protection and for long-term retention purposes. If necessary, you can restore a volume, folder, or individual files from the backup to the same, or different, working file system.

The following diagram shows a visual representation of data protection for FSx for ONTAP storage using snapshots, replication across regions, and backup to object storage.



Best practices for protecting your workload data

FSx for ONTAP offers multiple data protection options which can be combined to achieve your selected recovery point and time objectives. For the best possible protection, we recommend that you use both volume snapshots and volume backups.

A recovery point objective (RPO) describes how recent the latest copy of your data is guaranteed to be, which depends on how frequently the copies are made. A recovery time objective (RTO) defines how long it takes to restore your data.

Protect your workload data with snapshots

Snapshots are virtual point-in-time versions of a volume that are taken on a scheduled basis. You can access snapshots using standard file system commands. Snapshots provide an RPO of as little as one hour. RTO depends on the amount of data to restore and is primarily limited by the volume throughput limit. Snapshots also allow users to restore specific files and directories, which decreases RTO even further. Snapshots only consume additional volume space for changes made to the volume.

Protect your workload data with NetApp Autonomous Ransomware Protection with AI

NetApp Autonomous Ransomware Protection with AI (ARP/AI) acts as an important additional layer of defense if anti-virus software has failed to detect an intrusion. Setting an ARP/AI policy enables it for all storage VMs and all existing and newly created volumes. Once enabled, ARP/AI detects and protects all volumes and storage VMs. If a file extension is flagged as abnormal, you should evaluate the alert.

Protect your workload data with volume replication

Volume replication creates a copy of the latest data of a volume including all its snapshots in a different region. If you cannot afford multi-hour RTOs of a full volume restore operation from a volume backup, consider performing a volume replication. While volume replication makes sure recent data is available in a different region for you to use, you need to adjust your clients to use the volume in the other region.

Protect your workload data with backups

Volume backups provide independent point-in-time copies of your volume. They can be used to store old backups and provide the necessary second copy of your data. Daily, weekly, and monthly backup schedules allow for RPOs starting at one day. Volume backups can only be restored as a whole. Creating a volume from a backup (RTO) can take hours to many days, depending on the size of the backup.

Recommendations for protecting your workload data

Consider the following recommendations for protecting your workload data.

- Use volume replication for disaster recovery: if your application requires a low RTO, consider using volume replication to replicate your data to another region.
- Use volume backups in conjunction with snapshots: using the two features together ensures that you're able to restore your files from snapshots and perform full restores in case of volume loss using backups.
- Define a volume backup policy: make sure that the backup policy satisfies your company requirements for backup age and frequency. We recommend keeping a minimum of two daily backups for each volume.
- Define a snapshot schedule: older snapshots are less likely to be used to restore data. We recommend that you define a snapshot schedule that takes into consideration the diminishing returns of keeping older snapshots against the cost for additional snapshot capacity.
- Enable an ARP/AI policy for your file system or individual volumes to add an additional layer of protection to protect your data from ransomware attacks.

Use snapshots to protect data

Use snapshots to protect data in NetApp Workload Factory

Protect volume data from accidental deletion or corruption by creating and managing snapshots in NetApp Workload Factory. You can create an on-demand snapshot of a volume, define a snapshot policy to automate snapshot creation and retention for storage VMs, and restore a volume from an existing snapshot to recover data at a specific point in time.

Create an on-demand snapshot of a volume

Create a manual snapshot of an FSx for ONTAP volume in NetApp Workload Factory. Snapshots are point-in-time versions of your volume's content.

Snapshots are resources of volumes and are instant captures of your data that consume space only for modified data. Because data changes over time, snapshots usually consume more space as they get older.

FSx for ONTAP volumes use just-in-time copy-on-write so that any unmodified files in snapshots don't consume any of the volume's capacity.



Snapshots aren't copies of your data. If you want to make copies of your data, consider using the volume backups or volume replication features.

Before you begin

You must associate a link to create a manual snapshot of a volume. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system that contains the volume to create a snapshot for and then select **Manage**.
4. In the file system overview, select the **Volumes** tab.
5. From the **Volumes** tab, select the actions menu for the volume to protect with snapshots.
6. Select **Data protection actions** and then **Manage snapshots**.
7. From the Manage snapshots page, select **Create snapshot**.
8. In the Create a snapshot dialog, do the following:
 - a. Enter a snapshot name in the **Snapshot name** field.
 - b. Optionally, select a label or create a new label.
 - c. Set the **Retention period** as a number of hours, days, months, or years.
 - d. Optional: **Make this snapshot immutable** to prevent the snapshot from being deleted during the retention period.

Accept the statement regarding immutable snapshots.
9. Select **Create**.

Create a snapshot policy for storage VMs

Create a custom snapshot policy for storage VMs in Workload Factory to manage snapshot creation and retention. A snapshot policy defines how the system creates snapshots for a storage VM. You can create a snapshot policy for a storage VM in an FSx for ONTAP file system. You can also share the policy across multiple storage VMs.

You can create a custom snapshot policy that differs from the three built-in snapshot policies for FSx for ONTAP:

- `default`
- `default-1weekly`
- `none`

By default, every volume is associated with the file system's `default` snapshot policy. We recommend using this policy for most workloads.

Customizing a policy lets you specify when to create snapshots, how many copies to retain, and how to name them.

Before you begin

- Once a snapshot policy is created, its association with the storage VM(s) cannot be modified, but you can always add or remove the policy from volumes.
- Consider the following about snapshot capacity before you use snapshots:
 - For most datasets, an additional capacity of 20% is enough to keep snapshots for up to four weeks. As data gets older, its use for restorations becomes less likely.

- Overwriting all the data in a snapshot consumes significant volume capacity, which factors into provisioning volume capacity.
- To create a custom snapshot policy, you must associate a link. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system with the volume and then select **Manage**.
4. In the file system overview, select the **Storage VMs** tab.
5. From the **Storage VMs** tab, select the actions menu for the volume to protect with scheduled snapshots, then **Advanced actions**, and then **Manage snapshot policies**.
6. On the Snapshot policy management page, select **Create snapshot policy**.
7. In the **Snapshot policy name** field, enter a name for the snapshot policy.
8. Optionally, enter a description for the snapshot policy.
9. Under **Policy schedule and copies**, select when to create snapshots. For example, every minute or hourly.

You can select more than one frequency.

10. Under **Number of copies**, enter the number of copies to retain.

The maximum number of copies is 1,023.

11. Optional: Under **Naming convention**, enter a **Prefix** for the policy.
12. **Retention label** is automatically populated.

This label refers to the SnapMirror, or replication label that is used to select only specified snapshots for replication from the source to the target file system.

13. Optional: Enable **Immutable snapshots** for any schedules you need, set the **Retention period** for each schedule, and accept the statement to continue.

Enabling immutable snapshots locks all snapshots in this snapshot policy to prevent the snapshots from being deleted during the retention period.

14. **Share across storage VMs**: Enabled by default. When enabled, the snapshot policy is shared across all storage VMs in the file system. Disable to create a snapshot policy for a single storage VM.
15. Select **Create**.

Restore a volume from a snapshot

You can restore data from a snapshot to an existing volume or to a new volume. The restore operation enables point-in-time recovery when a volume contains deleted or corrupted files.

The creation of a new volume from a snapshot makes a copy of an entire volume within a few seconds independent of volume size. The newly created copy represents a new volume.

Before you begin

Consider the following limitations before you create a volume from a snapshot:

- You can only restore a volume from a snapshot if you have an existing snapshot copy of the volume.
- Changes to permission models: If you use this operation to switch the network-attached storage (NAS) protocol type, it might also switch the permission model that the security style provides. You might experience file access permission issues, which you can only fix manually with administrator access using the NAS client tools for permissions setting.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system with the volume and then select **Manage**.
4. In the file system overview, select the **Volumes** tab.
5. From the **Volumes** tab, select the actions menu for the volume to restore from a snapshot.
6. Select **Data protection actions** and then **Manage snapshots**.
7. From the Manage snapshots page, select the actions menu for the snapshot to restore, and then select **Restore**.
8. In the Restore volume from a snapshot dialog, select from the following options:
 - Toggle to select **Restore as a new volume**.

In the **Restored volume name** field, enter a unique name for the volume to restore.

- Restore data from a snapshot to an existing volume. This operation permanently deletes any data that was modified after the snapshot creation time.

Accept the statement to proceed.

9. Select **Restore**.

Manage snapshot policies for volumes in NetApp Workload Factory

Manage snapshot policies for FSx for ONTAP volumes in Workload Factory. A snapshot policy defines how the system creates snapshots for a volume.

Snapshot management operations like assigning, changing, and deleting snapshot policies for volumes in an FSx for ONTAP file system are managed at the storage VM level. Snapshot policies can be shared with a single storage VM or with all storage VMs.

Some management tasks require you to associate a link with the FSx for ONTAP file system. [Learn about Workload Factory links](#).

By default, every volume is associated with the file system's `default` snapshot policy. We recommend using this policy for most workloads.

Assign a snapshot policy to a volume

You can assign a snapshot policy to a single volume to create scheduled snapshots for the volume.

Before you begin

You must associate a link to assign a snapshot policy. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. Select the actions menu of the file system that contains the volume to assign a snapshot policy to and then select **Manage**.
5. In the file system overview, select the **Storage VMs** tab.
6. From the **Storage VMs** tab, select the actions menu for the storage VM containing the volume to protect with scheduled snapshots, then **Advanced actions**, and then **Manage snapshot policies**.
7. On the Snapshot policy management page, select the actions menu of the snapshot policy and then select **Assign policy to volume**.
8. In the Assign snapshot policy dialog, select a snapshot policy to assign to the volume and review the policy schedule.

If the policy contains immutable snapshots, and you want use it, accept the statement.

9. Select **Assign**.

Result

The snapshot policy is assigned to the volume.

Change a snapshot policy

You can change the snapshot policy name, schedule, and number of copies to retain, and enable or disable immutable snapshots. It isn't possible to enable or disable policy sharing across storage VMs. This option is available only during snapshot policy creation.

Before you begin

To display existing snapshot policies, you must associate a link. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. Select the actions menu of the file system and then select **Manage**.
5. In the file system overview, select the **Storage VMs** tab.
6. From the **Storage VMs** tab, select the actions menu for the storage VM containing the volume to protect with scheduled snapshots, then **Advanced actions**, and then **Manage snapshot policies**.
7. On the Snapshot policy management page, select the actions menu for the snapshot policy to change and then select **Edit**.
8. In the Edit snapshot policy dialog, make the necessary changes to the snapshot policy.

9. Select **Apply**.

Result

The snapshot policy is updated.

Enable immutable snapshots

Lock snapshots to prevent them from being deleted during the retention period.

Before you begin

You must associate a link to enable immutable snapshots. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu of the volume to lock snapshots for.
4. Select **Data protection actions, Snapshots**, then **Make a snapshot immutable**.
5. In the Make a snapshot immutable dialog, do the following:
 - a. **Snapshot name**: Select the snapshot to lock.
 - b. Set the **Retention period** in number of hours, days, months, or years.
 - c. Accept the statement.
6. Select **Apply**.

Result

The volume snapshot is now locked.

Enable long-term snapshot retention in NetApp Workload Factory

In NetApp Workload Factory, you can enable snapshots for long-term retention, which lets you replicate specific snapshots for long-term disaster recovery.

Long-term retention enables business services to continue operating even in the event of a complete site failure, supporting transparent failover of applications using a secondary copy.

The same steps apply for enabling and editing snapshots for long-term retention.

When an on-premises ONTAP cluster is the target for the replication relationship, changing snapshots for long-term retention isn't supported.



Editing long-term retention isn't available when replicating storage VM data and configuration settings.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.

3. From the **FSx for ONTAP** menu, select **Inventory** and then select the actions menu of the file system to update and then select **Manage**.
4. From the file system overview, select the **Replication relationships** tab.
5. In the Replication relationships tab, select the actions menu of the replication relationship schedule to change.
6. Select **Edit long-term retention**.
7. In the Edit long-term retention dialog, enable or disable snapshots for long-term retention.
8. If you select to disable snapshots for long-term retention, select **Apply** to complete this operation.
9. If you select to enable snapshots for long-term retention, choose between selecting an existing policy or creating a new policy.
 - a. To use an existing policy, select it from the dropdown menu.
 - b. To create a new policy, provide the following:
 - i. **Policy name**: Enter a policy name.
 - ii. **Snapshot policies**: Select one or more snapshot policies.
 - iii. **Copies to retain**: Enter the number of snapshot copies to retain on the target file system.
10. Select **Apply**.

Remove a snapshot policy from a volume

Remove a snapshot policy from a volume because you no longer want snapshots of the volume or because you want to delete a snapshot policy that is assigned to multiple volumes. To [delete a snapshot policy](#) that is assigned to more than one volume, you must manually remove it from all volumes.

Before you begin

You must associate a link to remove a snapshot policy. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **Inventory** and then select the actions menu of the file system to update and then select **Manage**.
4. In the file system overview, select the **Storage VMs** tab.
5. From the **Storage VMs** tab, select the actions menu for the storage VM containing the volume to protect with scheduled snapshots, then **Advanced actions**, and then **Manage snapshot policies**.
6. On the Snapshot policy management page, select the actions menu of the snapshot policy and then select **Assign policy to volume**.
7. In the Assign snapshot policy dialog, select **None** to remove the snapshot policy.
8. Select **Assign**.

Result

The snapshot policy is removed from the volume.

Delete a snapshot policy

Delete a snapshot policy when you no longer need it.

When a snapshot policy is assigned to more than one volume, you must manually [remove it](#) from all volumes to delete the snapshot policy. Alternatively, you can [assign a different snapshot policy](#) to the volumes.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **Inventory** and then select the actions menu of the file system to update and then select **Manage**.
4. In the file system overview, select the **Storage VMs** tab.
5. From the **Storage VMs** tab, select the actions menu of the storage VM with the snapshot policy to delete, then **Advanced actions**, and then **Manage snapshot policies**.
6. On the Snapshot policy management page, select the actions menu for the snapshot policy to delete and then select **Delete**.
7. In the Delete dialog, select **Delete** to delete the policy.

Manage snapshots of an FSx for ONTAP volume

Edit snapshot settings, enable directory access, and delete snapshots to manage your snapshots and data protection in Workload Factory.

Edit a snapshot

Edit the name, label, and retention period of a snapshot. If the snapshot isn't already immutable, you can make the snapshot immutable.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu for the volume with the snapshot to edit.
4. Select **Data protection actions** and then **Manage snapshots**.
5. From the Manage snapshots page, select the actions menu for the snapshot to edit, and then select **Edit**.
6. In the Edit a snapshot dialog, you may edit the following:
 - a. Change the name.
 - b. Change the label.
 - c. Change the retention period.
 - d. Optional: **Make this snapshot immutable** to prevent the snapshot from being deleted during the retention period.

If the snapshot is already immutable, you can't edit this setting.

Accept the statement regarding immutable snapshots.

7. Select **Apply**.

Access a snapshot

Enable snapshot directory access to give users the ability access snapshots autonomously.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu for the volume with the snapshot to access.
4. Select **Data protection actions** and then **Manage snapshots**.
5. From the Manage snapshots page, select the actions menu for the snapshot to access, and then select **Access**.
6. In the Access snapshot dialog, select to **Enable snapshot directory access** to access this volume snapshot and all snapshots of the volume.
 - For NFS volumes: Select **NFS access path** to view the NFS path for the snapshot.
 - For SMB/CIFS volumes: Select **SMB access path** to view the SMB path for the snapshot.
7. Copy the access path.
8. Select **Apply**.

Restore data from a snapshot

You have the option to restore data from a snapshot to an existing volume or to a new volume.

[Restore a volume from a snapshot](#)

Delete a snapshot

Delete a snapshot to free up space.

Immutable snapshots cannot be deleted until the retention period ends.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu for the volume with the snapshot to delete.
4. Select **Data protection actions** and then **Manage snapshots**.
5. From the Manage snapshots page, select the actions menu for the snapshot to delete, and then select **Delete**.
6. In the Delete snapshot dialog, type "delete".
7. Select **Delete** to confirm deletion.

Related information

- [Create a snapshot](#)

- [Create a snapshot policy](#)
- [Restore a volume from a snapshot](#)

Use backups to protect data in NetApp Workload Factory

Protect your volume data from accidental deletion, corruption, and other data loss events by creating and restoring backups in NetApp Workload Factory. You can set up a backup schedule, create an on-demand backup of a volume outside your regularly scheduled backups, and you can restore a volume from an existing backup to any FSx for ONTAP file system in your AWS account.

Create an on-demand backup of a volume

Create a manual backup of a volume outside regularly scheduled backups in NetApp Workload Factory.

About this task

Volume backups are per volume, so each backup contains only the data in a particular volume.

Volume backups are incremental which means that only the data on the volume that has changed after your most recent backup is saved. This minimizes the time required to create the backup and the storage required for the backup, which saves on storage costs by not duplicating data.

Before you begin

To take backups of your volumes, both your volume and your file system must have enough available SSD storage capacity to store the backup snapshot. When taking a backup snapshot, the additional storage capacity consumed by the snapshot cannot cause the volume to exceed 98% SSD storage utilization. If this happens, the backup will fail.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu for the volume to back up.
4. Select **Data protection actions**, **Volume backups**, and then **Manual backup**.
5. In the Manual backup dialog, enter a name for the backup.
6. Select **Back up**.

Manage the backup schedule for an FSx for ONTAP file system

Manage the backup schedule for an FSx for ONTAP file system in NetApp Workload Factory.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system to update the backup schedule for and then select **Manage**.

4. Under Information, select the pencil icon next to **Volume backups**. The pencil icon appears next to the dropdown arrow when the mouse hovers over the **Volume backups** row.
5. In the **Volume backups** dialog, provide the following:
 - a. **Daily automatic backups**: Enable or disable the feature. If you disable the feature, select **Apply**. If you enable the feature, complete the following steps.
 - b. **Automatic backup retention period**: Enter the number of days to retain automatic backups.
 - c. **Daily automatic backup window**: Select either **No preference** (a daily backup start time is Selected for you) or **Select start time for daily backups** and specify a start time.
 - d. **Weekly maintenance window**: Select either **No preference** (a weekly maintenance window start time is selected for you) or **Select start time for 30-minute weekly maintenance window** and specify a start time.
6. Select **Apply**.

Restore a volume from a backup in NetApp Workload Factory

In NetApp Workload Factory, you can restore a volume from a backup to any FSx for ONTAP file system in your AWS account.

Workload Factory determines if you have enough capacity for the restore and can automatically add SSD storage tier capacity if you don't.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu for the volume to restore from a backup.
4. Select **Data protection actions**, **Volume backups**, and then **Restore from a backup**.
5. In the Restore from a backup dialog, provide the following:
 - a. **Target file system**: Select the target file system from the dropdown menu.
 - b. **Target storage VM**: Select the target storage VM from the dropdown menu.
 - c. **Backup name**: Select the backup name from the dropdown menu.
 - d. **Restored volume name**: Enter the restored volume name.
6. Verify file system capacity for the restore operation.

When file system capacity is limited, the following might occur:

- The restore can push used capacity over the threshold you specified. You can complete the restore operation. Consider [manually adding SSD storage tier capacity](#) or selecting for Workload Factory to automatically add SSD storage tier capacity.
- The restore requires additional SSD capacity. You must select for Workload Factory to automatically add SSD storage tier capacity to proceed.

7. Select **Restore**.

Use replication to protect data

Replicate data to FSx for ONTAP in NetApp Workload Factory

Replicate data in NetApp Workload Factory to protect against data loss if the region where your data resides experiences a disaster. Data replication is supported between FSx for ONTAP file systems and on-premises ONTAP systems or Cloud Volumes ONTAP. Workload Factory also supports cascading replication to extend data protection to tertiary systems or migrate your data.

When replicating storage VM data and configuration settings, you must first create and initialize the replication relationship and then wait for the data to sync at least once before completing the cut over operation.

Standard replication

Replication protects your data if a disaster affects your region; it can also be used for migration purposes.

Replication includes creating and initializing a replication relationship. To set up replication, create the replication relationship. To transfer the data between the source and target storage systems, initialize the replication relationship. When migrating storage VM data and configuration settings, you must also complete the cutover operation.

Replicated volumes in the target file system are data protection (DP) volumes and follow the naming format: `{OriginalVolumeName}_copy`.

If you replicate a source volume with immutable files, the target volume and file system remain locked until the source volume's retention period ends. The immutable files feature is available when you [create a volume](#) for an FSx for ONTAP file system.



You can replicate one source (read/write) volume or one data protection (DP) volume. Cascading replication is supported, but a third hop isn't. Learn more about [cascading replication](#).

Migration use cases

For migration, you can choose to replicate storage VM data and configuration settings for one storage VM. If you migrate data and configuration settings together, make sure the last replication for the volume finished within the last 24 hours. You must select all volumes in the same storage VM to use this feature. The tiering policy for all volumes defaults to the tiering policy of the source volume, which is recommended for migration use cases.

Workload Factory supports migration replication for storage VMs between the following storage systems.

- On-premises ONTAP systems and FSx for ONTAP file systems
- Cloud Volumes ONTAP and FSx for ONTAP file systems
- FSx for ONTAP and FSx for ONTAP file systems
 - First to first generation
 - Second to second generation

To migrate storage VM data and configuration settings, you must complete three operations.

1. [Create the replication relationship](#), select **Migration** as the use case and select **Replicate storage VM configuration**.
2. [Initialize the replication relationship](#) to transfer the data from the source to the target storage system.
3. [Cut over replication for migration use cases](#) to permanently migrate data and configuration settings from the source file system to the target FSx for ONTAP file system.

Step 1: Create the replication relationship

Replicate data between two FSx for ONTAP file systems, between an on-premises ONTAP system and an FSx for ONTAP file system, or between Cloud Volumes ONTAP and an FSx for ONTAP file system.

Before you begin

Review these requirements before you begin.

- Ensure that one FSx for ONTAP file system is available to use for the target in the replication relationship.
- Open TCP ports 11104 and 11105 for secure data transfer and management between storage systems. ICMP is optional, but can help with network checks and troubleshooting.
- The FSx for ONTAP file system you use for the replication relationship must have an associated link. [Learn how to associate an existing link or to create and associate a new link](#). After you associate the link, return to this operation.
- For replication from an on-premises ONTAP system to an FSx for ONTAP file system, make sure you have discovered the on-premises ONTAP system.
- Replication isn't supported for volumes in a state other than available, created, or misconfigured, and when the ONTAP version isn't compatible.
- For migration use cases ensure that the last replication for the volume completed in the last 24 hours before you create a replication relationship with storage VM data and configuration settings.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the FSx for ONTAP page, select the file system that contains the volume(s) to replicate.
4. Either replicate all volumes in a file system or replicate select volumes.
 - To replicate all volumes in a file system: From the file system overview, select **Replicate data**.
 - To replicate select volumes: From the file system overview, select the **Volumes** tab.

In the Volumes table, select one or more volumes and then select **Replicate data**.

5. On the Replicate data page, under Replication target, provide the following:

Unresolved directive in fsx-storage/create-replication.adoc - include::_include/create-replication.adoc[]

8. Select **Create**.

Result

The replication relationship appears in the **Replication relationships** tab in the target FSx for ONTAP file system.

If you created a replication relationship for migration purposes, you must cut over all the volumes and their

associated storage VM to complete migration of storage VM data and configuration settings to the target FSx for ONTAP file system.

Step 2: Initialize the replication relationship

Initialize a replication relationship between source and target volumes to transfer the snapshot and all data blocks in NetApp Workload Factory.

Initialization performs a *baseline* transfer: it makes a snapshot of the source volume, then transfers the snapshot and all the data blocks it references to the target volume.

Before you begin

Consider when you choose to complete this operation. Initialization can be time-consuming. You might want to run the baseline transfer in off-peak hours.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.

Unresolved directive in fsx-storage/create-replication.adoc - include::_include/initialize-replication.adoc[]

3. In the Initialize relationship dialog, select **Initialize**.

When the replication status shows **Idle**, the data transfer is complete.

Step 3: Cut over replication for migration use cases

After creating the replication relationship for a migration use case, you must cut over replication to complete migration of storage VM data and configuration settings to the target FSx for ONTAP file system. Cutover replication permanently migrates data and storage VM configuration settings from the source file system to the target FSx for ONTAP file system. During the cutover, data gets replicated for the last time. The source storage VM goes offline when the cutover begins.

Plan for the cutover operation

Consider the following when planning for the cutover operation for migration use cases.

- **Replication version support:** Source and target storage systems must have the same major ONTAP version. For example, if the source system is running ONTAP version 9.18.1, then the target system must also run a version of 9.18.1.
- **Storage VM configuration settings:**
 - The cutover operation doesn't migrate all storage VM configuration settings to the target storage VM. For example, iSCSI, broadcast-domain MTU, and DNS settings do not migrate. Update these settings manually on the target storage VM after cutover. For more details, refer to the [Update configuration settings after cutover](#) section.
 - If your storage VM uses domain-tunnel authentication, set up and enable a domain tunnel on the target file system before you start the migration.
- **Clones:** Clones get migrated as individual volumes, and therefore, will consume more space on the target FSx for ONTAP file system. Consider deleting the clones before cutover to avoid increased capacity on the target.

- **Cache volumes:** For ONTAP FlexCache 9.17.x or below. Source storage VMs that contain cache volumes aren't supported for cutover. Remove the ONTAP FlexCache relationship before cutover to avoid migration failures.
- **AWS S3 access points:** Cutover replication for migration use cases isn't supported for volumes with S3 access points. Delete S3 access points from the source volume to avoid migration failures.
- **ONTAP S3 configurations:** Cutover replication for migration use cases isn't supported for vservers with ONTAP S3 configurations. Remove ONTAP S3 configurations including object-store-server, buckets, users, groups, or policies on the vserver, to avoid migration failures.
- **LUN serial numbers and iSCSI target IQN:** LUN serial numbers and the iSCSI target IQN change during cutover.

Before you begin

Review these requirements before you begin.

- Stop any client access to your storage VM before you cut over replication.
- Ensure all source volumes are not serving any data before you cut over replication.
- Ensure the data is synced between the source and target volumes before you cut over replication.
- The FSx for ONTAP file system you use for the replication relationship must have an associated link. [Learn how to associate an existing link or to create and associate a new link](#). After you associate the link, return to this operation.
 - The following ports must be open in the security group associated with the FSx for ONTAP file system for link connectivity: port 443 (HTTPS) and port 22 (SSH).

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.

Unresolved directive in fsx-storage/create-replication.adoc - include::_include/cutover-replication.adoc[]

8. Select **Cut over**.

Result

After initiating cutover, the source storage VM goes offline.

Update configuration settings after cutover

After you cut over replication for migration use cases, update the following storage VM configuration settings on the target storage VM.

- For iSCSI:
 - Recreate the igroup
 - Update LUN mapping
 - Log in to each SAN client and update iSCSI/MPIO settings for the new target and remove the old vserver target IPs
- Validate broadcast-domain MTU settings are as expected
- Validate DNS settings are as expected

- Recreate cache relationships (ONTAP FlexCache relationships) if there were cache volumes in the source storage VM.

If needed, [modify the tiering policy](#) for the target volume(s) after cutover.

Cascade replication for data protection volumes

NetApp Workload Factory supports replicating data protection volumes, also called *cascade deployments*. A *cascade deployment* consists of a chain of relationships in which a source volume is mirrored to a secondary volume (first hop), and the secondary volume is mirrored to a tertiary volume (second hop). If the secondary volume becomes unavailable, you can synchronize the relationship between the primary and tertiary volumes without performing a new baseline transfer.

This feature is supported for FSx for ONTAP file systems with ONTAP version 9.6 and higher. Refer to [ONTAP documentation for compatible ONTAP versions](#).

Learn more about [how cascade deployments work](#).

Before you begin

Consider the following before you begin:

- Be aware that volumes that are part of a cascade configuration can take longer to resynchronize.
- If the source volume of the relationship is a data protection volume and is a target of another relationship, reversing the replication relationship isn't supported.
- One replica of a data protection volume (or a second hop) is supported. It isn't considered best practice to create a second replica of a data protection volume (or a third hop).
- Open TCP ports 11104 and 11105 for secure data transfer and management between storage systems. ICMP is optional, but can help with network checks and troubleshooting.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system that contains the volume(s) to replicate and then select **Manage**.
4. From the file system overview, select the **Volumes** tab.
5. In the Volumes table, select one or more data protection volumes (DP/replicated volumes), and then select **Replicate data**.
6. On the Replicate data page, under Replication target, provide the following:

Unresolved directive in fsx-storage/create-replication.adoc - include::_include/create-replication.adoc[]

1. Select **Create**.

Result

The replicated volume or volumes replicate and appear in the **Replication relationships** tab in the target FSx for ONTAP file system.

Related information

[Modify the tiering policy](#) for the target volume(s) after cutover.

Replicate on-premises ONTAP cluster data in NetApp Workload Factory

Discover and replicate on-premises ONTAP data in NetApp Workload Factory so it can be used as a backup in the cloud.

About this task

To use data from an on-premises ONTAP cluster, you'll first need to discover the on-premises ONTAP cluster. After you've discovered an on-premises ONTAP cluster, you can use the data for any of the following use cases.

Use cases

- **Backup and migration to cloud:** Replicated on-premises ONTAP volume data to an FSx for ONTAP file system can be used as a backup in the cloud.
- **Data tiering:** After replication, infrequently accessed on-premises ONTAP volume data can be tiered from the SSD storage tier to the capacity pool storage tier.

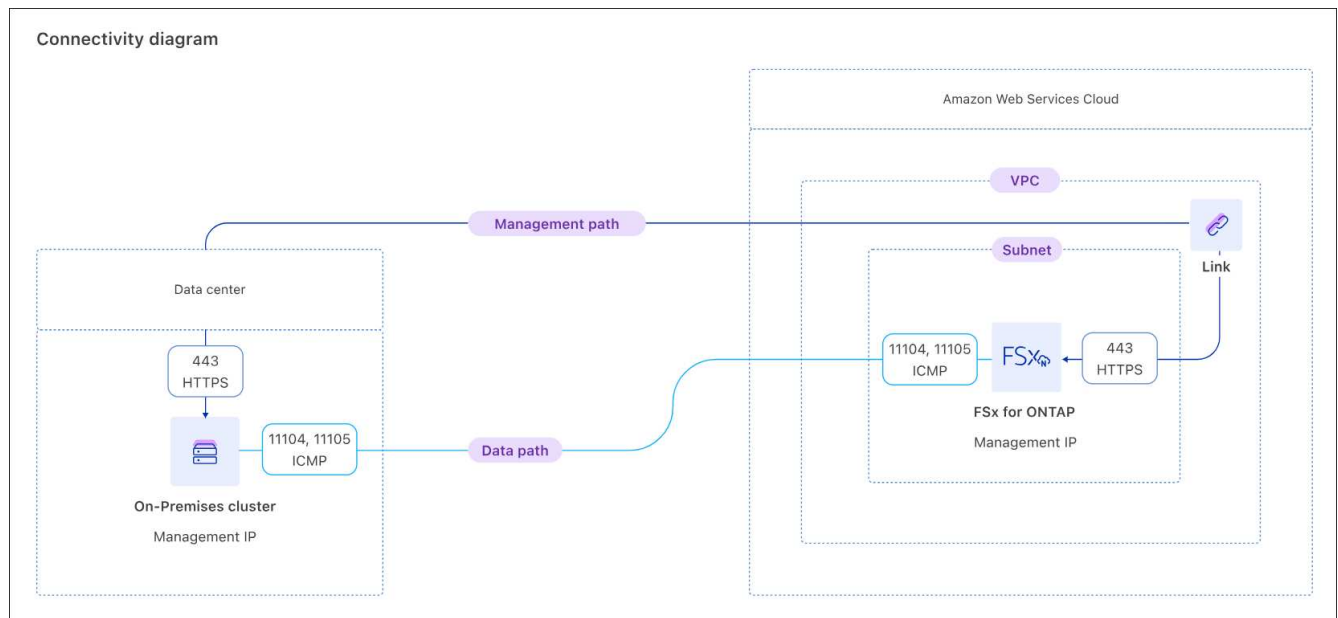
Discover an on-premises ONTAP cluster

Discover an on-premises ONTAP cluster in NetApp Workload Factory so that you can replicate the data to an Amazon FSx for NetApp ONTAP file system.

Before you begin

Make sure you have the following before you begin:

- An FSx for ONTAP file system for replication.
- A connected link to associate with the discovered on-premises cluster. If you don't have a link, you'll need to [create one](#).
- ONTAP user credentials with required permissions.
- On-premises ONTAP version 9.8 and above.
- Connectivity as shown in the following diagram.



Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **On-premises ONTAP**.
4. Select **Discover**.
5. Review the prerequisites and select **Next**.
6. On the Discover ONTAP on-premises page, provide the following under **Cluster configuration**:
 - a. **Link**: Select a link. The link will be associated with the on-premises cluster to create connectivity between the cluster and Workload Factory.

If you haven't created a link, follow the instructions and then return to this operation and select the link.

- b. **Cluster IP address**: Provide the IP address for the on-premises ONTAP cluster to replicate.
- c. **ONTAP credentials**: Provide the following:
 - GovCloud accounts: Enter ARN with ONTAP credentials.
 - All other accounts: Enter the ONTAP credentials for the on-premises ONTAP cluster. Make sure the user has the required permissions.

7. Select **Discover** to start the discovery process.

Result

The on-premises ONTAP cluster is discovered and now appears in the **On-Premises ONTAP** tab.

You can now view the data in your on-premises ONTAP cluster and [replicate the data to an FSx for ONTAP file system](#).

Replicate volume data from an on-premises ONTAP cluster

Replicate volume data from an on-premises ONTAP cluster to an FSx for ONTAP file system. After replication, the data can be used to enrich AI knowledge bases.

Before you begin

- You must discover an on-premises ONTAP cluster to replicate its volume data.
- You must have an available FSx for ONTAP file system to be the target for the replication.
- Both the on-premises ONTAP cluster and the FSx for ONTAP file system you use for the replication relationship must have an associated link. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **On-premises ONTAP**.
4. To find volumes by storage VM, you can **Select storage VM** from the dropdown.
5. Select one or more volumes to replicate and then select **Replicate**.
6. On the Create replication page, under Replication target, provide the following:
 - a. **FSx for ONTAP file system**: Select credentials, region, and FSx for ONTAP file system name for the target FSx for ONTAP file system.
 - b. **Storage VM name**: Select the storage VM from the dropdown menu.
 - c. **Volume name**: The target volume name is generated automatically with the following format `{OriginalVolumeName}_copy`. You can use the auto-generated volume name or enter another volume name.
 - d. **Tiering data**: Select the tiering policy for the data stored in the target volume.
 - **Auto**: The default tiering policy when creating a volume using the Workload Factory FSx for ONTAP user interface. Tiers all cold data that includes user data and snapshots to the capacity pool storage tier for a specific time period.
 - **Snapshot only**: Tiers only snapshot data to the capacity pool storage tier.
 - **None**: Keeps all your volume's data on the primary storage tier.
 - **All**: Marks all user data and snapshot data as cold and stores it in the capacity pool storage tier.

Note that some tiering policies have an associated minimum cooling period which sets the time, or *cooling days*, that user data in a volume must remain inactive for the data to be considered "cold" and moved to the capacity pool storage tier. The cooling period starts when data is written to the disk.

For more information about volume tiering policies, refer to [Volume storage capacity](#) in AWS FSx for NetApp ONTAP documentation.

- e. **Max transfer rate**: Select **Limited** and enter the max transfer limit in MiB/s. Alternatively, select **Unlimited**.

Without a limit, network and application performance might decline. Alternatively, we recommend an unlimited transfer rate for FSx for ONTAP file systems for critical workloads, for example, those that are used primarily for disaster recovery.

7. Under Replication settings, provide the following:
 - a. **Replication interval**: Select the frequency that snapshots are transferred from the source volume to the target volume.

- b. **Long-term retention:** Optionally, enable snapshots for long-term retention.

If you enable long-term retention, then select an existing policy or create a new policy to define the snapshots to replicate and the number to retain.

- For an existing policy, select **Choose an existing policy** and then select the existing policy from the dropdown menu.
- For a new policy, select **Create a new policy** and provide the following:
 - **Policy name:** Enter a policy name.
 - **Snapshot policies:** In the table, select the snapshot policy frequency and the number of copies to retain. You can select more than one snapshot policy.

8. Select **Create**.

Result

The replication relationship appears in the **Replication relationships** tab in the target FSx for ONTAP file system.

Remove an on-premises ONTAP cluster from NetApp Workload Factory

Remove an on-premises ONTAP cluster from NetApp Workload Factory when needed.

Before you begin

You must [delete all existing replication relationships](#) for any volumes in the on-premises ONTAP cluster before removing the cluster so that no broken relationships remain.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **On-premises ONTAP**.
4. Select the on-premises ONTAP cluster to remove.
5. Select the actions menu and select **Remove from Workload Factory**.

Result

The on-premises ONTAP cluster is removed from NetApp Workload Factory.

Replicate a storage VM to another FSx for ONTAP file system

Replicating a storage VM to another FSx for ONTAP file system in NetApp Workload Factory provides a protective layer of data access in case of data loss. This operation replicates all volumes in one storage VM to another FSx for ONTAP file system.

Before you begin

To replicate a storage VM to another FSx for ONTAP file system, you must associate a link. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system with the storage VM to replicate and then select **Manage**.
4. In the file system overview under Storage VMs, select **Manage**.
5. On the Manage storage VMs screen, select the actions menu of the storage VM to replicate an SVM for, then select **Advanced actions > Replicate storage VM**.
6. On the Replicate data page, under Replication target, provide the following:
 - a. **FSx for ONTAP file system**: Select credentials, region, and FSx for ONTAP file system name for the target FSx for ONTAP file system.
 - b. **Storage VM name**: Select the storage VM from the dropdown menu.
 - c. **Volume name**: The target volume name is generated automatically with the following format `{OriginalVolumeName}_copy`.
 - d. **Tiering policy**: Select the tiering policy for the data stored in the target volume.

Auto is the default tiering policy when creating a volume using the Workload Factory FSx for ONTAP user interface. For more information about volume tiering policies, refer to [Volume storage capacity](#) in AWS FSx for NetApp ONTAP documentation.
 - e. **Max transfer rate**: Select **Limited** and enter the max transfer limit in MB/s. Alternatively, select **Unlimited**.

Without a limit, network and application performance might decline. Alternatively, we recommend an unlimited transfer rate for FSx for ONTAP file systems for critical workloads, for example, those that are used primarily for disaster recovery.
7. Under Replication settings, provide the following:
 - a. **Replication interval**: Select the frequency that snapshots are transferred from the source volume to the target volume.
 - b. **Long-term retention**: Optionally, enable snapshots for long-term retention.

If you enable long-term retention, then select an existing policy or create a new policy to define the snapshots to replicate and the number to retain.

 - i. For **Choose an existing policy**, select an existing policy from the dropdown menu.
 - ii. For **Create a new policy**, provide the following:
 - A. **Policy name**: Enter a policy name.
 - B. **Snapshot policies**: In the table, select the snapshot policy frequency and the number of copies to retain. You can select more than one snapshot policy.
8. Select **Create**.

Result

All volumes within the storage VM are replicated to the target file system.

Track replication delays in NetApp Workload Factory

Turn on tracking to monitor replication delays across your account. Workload Factory alerts you when delays go beyond a set threshold. By default, the threshold is 150% of the replication interval to allow normal transfer time and reduce false alarms. You can adjust the threshold to match your RPO and get notifications when delays exceed it. You can also export the data to a CSV file for further analysis.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From **FSx for ONTAP**, select the actions menu of the file system to update and then select **Manage**.
4. From the file system overview, select the **Replication relationships** tab.
5. Select **Enable tracking**.
6. In the Enable replication lag history dialog, select **Enable**.
7. Back in the Replication lag history tile, select **Customize threshold** to set your preferred threshold.
8. In the Customize lag time threshold dialog, enter the threshold in hours and minutes.
9. Optionally, select **Enable lag time notifications** to receive notifications when replication lags exceed the threshold.

Notifications come in an email and include:

- Source file system
- Source volume
- Target file system
- Target volume
- Lag time threshold that was exceeded
- Link to the replication relationship

10. Select **Apply**.

Related information

[Manage replication relationships](#)

Manage your replication relationships in NetApp Workload Factory

Manage your replication relationships in NetApp Workload Factory. You can pause, resume, reverse, stop, and delete replication relationships between source and target volumes. You can also change the replication schedule of the source volume, and limit the max transfer rate for your replication relationships.

Change the replication schedule of a source volume

Change the replication schedule of the source volume in a replication relationship in NetApp Workload Factory.

Choose how frequently snapshots from the source volume are transferred to the replicated volume to match your required point objectives (RPOs).

When an on-premises ONTAP cluster is the target for the replication relationship, changing the replication schedule isn't supported.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship schedule to change.
7. Select **Edit replication interval**.
8. In the Edit replication interval dialog, select the frequency of snapshot transfer from the source volume. You may select between the following frequencies:
 - Every 5 minutes
 - Hourly
 - Every 8 hours
 - Daily
 - Weekly
9. Select **Apply**.

Limit the max transfer rate of a replication relationship

Limiting the max transfer rate is optional but recommended. Without a limit, network and application performance might decline.

Alternatively, we recommend an unlimited transfer rate for FSx for ONTAP file systems for critical workloads, for example, those that are used primarily for disaster recovery.

Before you begin

Consider how much bandwidth to allocate for replication.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to limit the max transfer rate for.

7. Select **Edit max transfer rate**.
8. In the Edit max transfer rate dialog, select **Limited** and enter the max transfer limit in MB/s.

Alternatively, select **Unlimited**.
9. Select **Apply**.

Manually update snapshot data in a replication relationship

A replication relationship has a set replication schedule, but you can manually update snapshot data transferred between source and target volumes in NetApp Workload Factory at any time.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to update.
7. Select **Update**.
8. In the Update dialog, select **Update**.

Pause a replication relationship

Pause a replication relationship to stop scheduled replication updates from the source volume to the target volume. The target volume transitions from read-only to read/write. Both volumes continue to share the latest replication snapshot as a new baseline for later resynchronization.

Before you begin

If you pause when a transfer is in progress, the transfer is not affected, and the relationship becomes "Quiescing" until the transfer completes. If the current transfer aborts, it is now a future transfer and will not restart.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to pause.
7. Select **Pause (Quiesce)**.
8. In the **Quiesce relationship** dialog, select **Quiesce**.

Result

The relationship pauses and its status shows as "Paused".

Resume a paused replication relationship

When you resume a replication relationship, any changes to the destination volume while the replication was stopped are deleted. The target volume transitions from read/write to read-only, and receives updates from the source volume at the scheduled replication interval again.



Any data written to the original source volume between the last data replication and the time that the source volume is disabled is not preserved.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to resume.
7. Select **Resume**.
8. In the Resume relationship dialog, select **Resume**.

Result

The relationship resumes and its status shows as "Replicated".

Reverse a replication relationship

Reverse a replication relationship so that the target volume becomes the source volume.

Reverse operations are supported for the following:

- Two FSx for ONTAP file systems
- One FSx for ONTAP file system and one on-premises ONTAP system

After you stop replication and make changes to the target volume, you can replicate those changes back to the source volume. This process is common in a disaster recovery scenario in which you operate on the target volume for a while and want to switch roles of the volumes.

When you reverse and resume a replication, it switches the source and target roles of your volumes; the target volume becomes the new source volume, and the source volume becomes the new target volume. The reverse operation also overwrites the contents of the new target volume with the contents of the new source volume. If you reverse a replication twice, the original replication direction re-establishes.

NOTE:

- Any data written to the original source volume between the last data replication and the time that the source volume is disabled is not preserved.
- Reversing replication isn't available when replicating storage VM data and configuration settings.

Before you begin

Make sure that you know the current and future roles of your source and target volumes because changes on the new target volume are overwritten with the new source volume. If used incorrectly, you can experience unintended data loss.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to reverse.
7. Select **Reverse relationship**.
8. In the Reverse relationship dialog, select **Reverse**.

Stop a replication relationship

Stop a replication relationship in NetApp Workload Factory. When you stop a replication relationship, scheduled replication updates from the source volume to the target volume pause. The target volume transitions from read-only to read/write.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage**.
3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to stop.
7. Select **Break**.
8. In the Break replication dialog, select **Break**.

Result

The replication status of the volume changes to **Broken**. The target volume becomes writable.

Delete a replication relationship

Delete a replication relationship in NetApp Workload Factory. When you delete a replication relationship, it removes the replication relationship between the source and target volume. After the replication relationship deletes, both volumes continue to exist independently with the current data they contain.

When you delete a replication relationship, FSx for ONTAP also deletes the common replication snapshots of the source and target volume.

Steps

1. Log in to the [NetApp Console](#).
- 2.

Select the menu , **Workloads > Storage**.

3. From the Storage menu, select **Inventory**.
4. In the **Inventory**, select the actions menu of the file system to update and then select **Manage**.
5. From the file system overview, select the **Replication relationships** tab.
6. In the Replication relationships tab, select the actions menu of the replication relationship to delete.
7. Select **Delete**.
8. In the Delete relationship dialog, select **Delete**.

Protect your FSx for ONTAP data with NetApp Autonomous Ransomware Protection with AI

Protect your data with NetApp Autonomous Ransomware Protection with AI (ARP/AI). It monitors activity in NAS (NFS/SMB) and SAN environments to detect unusual behavior that could signal a ransomware attack. If a threat is detected, ARP/AI automatically creates new immutable snapshots so you can restore your data.

About this task

Use ARP/AI to protect against denial-of-service attacks where the attacker withholds data until a ransom is paid. ARP/AI offers real-time ransomware detection based on:

- Identification of the incoming data as encrypted or plaintext.
- Analytics that detect:
 - **Entropy**: An evaluation of the randomness of data in a file (used in both NAS and SAN environments)
 - **File extension types**: An extension that does not conform to the normal extension type (used in NAS environments only)
 - **File IOPS**: A surge in abnormal volume activity with data encryption (used in NAS environments only)

ARP/AI can detect the spread of most ransomware attacks after only a small number of files are encrypted, take action automatically to protect data, and alert you that a suspected attack is happening.

The ARP/AI feature automatically updates according to the ONTAP version that Amazon FSx for NetApp ONTAP runs so you don't have to make manual updates.

Learning and active modes

ARP/AI behavior depends on the protocol and volume type:

- **NAS volumes (NFS/SMB)**: ARP/AI starts working as soon as you enable it. It uses a pre-trained AI model to detect ransomware threats immediately.
- **SAN volumes (beginning with ONTAP 9.17.1)**: ARP/AI provides immediate protection, even during the first evaluation period. During this 2-4 week period, the system learns normal encryption activity and sets alert thresholds. At the same time, it continues to monitor your data, detect threats, and send alerts.
- **Active mode**: When active mode is on, FSx for ONTAP creates ARP/AI snapshots to help protect your data when it detects a possible threat.

If the system flags a file extension as unusual, review the alert. You can respond to the alert to protect your

data, or mark it as a false positive if the activity is expected.

When you mark an alert as a false positive, the system updates its alert settings. For example, if a new file extension triggers an alert and you mark it as a false positive, you will not receive an alert the next time the system sees that file extension.

Unsupported configurations

The following configurations don't support the use of ARP/AI.

- NVMe volumes
- iSCSI volumes with ONTAP versions earlier than 9.17.1

Enable ARP/AI for a file system or a volume

Turning on ARP/AI for a file system automatically protects all current and new NAS volumes (NFS/SMB). Starting with ONTAP 9.17.1, it also supports SAN volumes (iSCSI). You can also turn on ARP/AI for specific volumes.

If ARP/AI detects a real attack after it is enabled, Workload Factory automatically creates a snapshot policy. This policy can create up to six snapshots every four hours. Each snapshot is locked for 2-5 days.

Before you begin

To enable ARP/AI for a file system or a volume, you must associate a link. [Learn how to associate an existing link or to create and associate a new link](#). After the link associates, return to this operation.

Enable ARP/AI for a file system

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **Inventory** and then select the actions menu of the file system to enable ARP/AI and then select **Manage**.
4. Under Information, select the pencil icon next to **Autonomous Ransomware Protection**. The pencil icon appears next to the arrow when the mouse hovers over the **Autonomous Ransomware Protection** row.
5. From the NetApp Autonomous Ransomware Protection with AI (ARP/AI) page, do the following:
 - a. Enable or disable the feature.
 - b. **Automatic snapshot creation**: Select the maximum number of snapshots to retain and the interval of time between taking snapshots. The default is 6 snapshots every 4 hours.
 - c. **Immutable snapshots**: Select the default retention period in hours and the maximum number of days to retain immutable snapshots. Enable this option to ensure that snapshots cannot be deleted or modified until the specified retention period ends.
 - d. **Detection**: Optionally, select any of the following parameters to automatically scan and detect anomalies.
6. Accept the statement to proceed.
7. Select **Apply** to save the changes.

Enable ARP/AI for a volume

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu of the volume to enable ARP/AI, then **Data protection actions**, and then **Manage ARP/AI**.
4. In the Manage ARP/AI dialog, do the following:
 - a. Enable or disable the feature.
 - b. **Detection**: Optionally, select any of the following parameters to automatically scan and detect anomalies.
5. Accept the statement to proceed.
6. Select **Apply** to save the changes.

Validate ransomware attacks

Determine if an attack is a false alarm or a genuine ransomware incident.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **Inventory** and then select the file system to validate ransomware attacks for.
4. From the file system overview, select the **Volumes** tab.
5. Select **Analyze attacks** from the Autonomous Ransomware Protection tile.
6. Download the attack events report to review if any files or folders were compromised and then decide if an attack has occurred.
7. If no attack occurred, select **False alarm** for the volume in the table and then select **Close**.
8. If an attack has occurred, select **Real attack** for the volume in the table. The Restore compromised volume data dialog opens. You can proceed to [recover your data](#) immediately or select **Close** and come back to complete the recovery process later.

Recover data after a ransomware attack

When the system detects a possible attack, it creates and locks a snapshot of the volume at that moment.

If the attack is later confirmed, you can restore affected files or the entire volume from the snapshot.

Locked snapshots cannot be deleted until the retention period expires. If the attack is later identified as a false alarm, the locked snapshot is deleted.

Because the system identifies the affected files and the time of the attack, you can recover only the affected files from available snapshots instead of restoring the entire volume.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Storage > FSx for ONTAP**.
3. From the **FSx for ONTAP** menu, select **Inventory** and then select the file system to recover data for.
4. From the file system overview, select the **Volumes** tab.
5. Select **Analyze attacks** from the Autonomous Ransomware Protection tile.
6. If an attack has occurred, select **Real attack** for the volume in the table.
7. In the Restore compromised volume data dialog, follow the instructions to restore at the file-level or at the volume-level. In most cases, you'll restore files rather than an entire volume.
8. After you complete the restore, select **Close**.

Result

The compromised data has been restored.

Clone a volume in NetApp Workload Factory

Clone a volume in NetApp Workload Factory to make a read/write volume of the original volume for testing.

The clone reflects the current, point-in-time state of the data. You can also use clones to give additional users access to data without giving them access to production data.

About this task

Volume cloning is only supported for FlexClone volumes.

When a volume is cloned, a writeable volume is created with references to snapshots from the parent volume. Clone creation occurs in seconds. The cloned data doesn't reside on the volume clone but instead resides on the parent volume. Any new data written to the volume after clone creation resides on the clone.

For a cloned volume to contain all data from the parent volume and any new data added to the clone after creation, you'll need to [split the clone](#) from the parent volume. Additionally, you can't delete a parent volume if it has a clone. A clone must be split before a parent volume can be deleted.

Steps

1. Log in to the [NetApp Console](#).
2. Select the menu , **Workloads > Volumes explorer**.
3. Select the actions menu of the volume to clone.
4. Select **Data protection actions**, then **Clone volume**.
5. In the Clone volume dialog, enter a name for the volume clone.
6. Select **Clone**.

Protect your FSx for ONTAP data with a cyber vault

A cyber vault volume is an isolated, secure storage location used to store backup copies of your data, protecting it from ransomware attacks and other cyber threats. As part of

vault creation, you'll create a cyber vault volume, disable all client protocols, and set up a replication relationship between the source volume and the cyber vault volume, and create immutable snapshots on the cyber vault volume.

What is a cyber vault?

A cyber vault is a specific data protection technique that involves storing critical data in an isolated environment, separate from the primary IT infrastructure.

The cyber vault is an "air-gapped", immutable, and indelible data repository that is immune to threats affecting the main network, such as malware, ransomware, or even insider threats. A cyber vault can be achieved with immutable and indelible snapshots.

Air-gapping backups that use traditional methods involve creating space and physically separating the primary and secondary media. By moving the media offsite and/or severing connectivity, bad actors have no access to the data. This protects the data but can lead to slower recovery times.

FSx for ONTAP cyber vaults

Amazon FSx for NetApp ONTAP is supported as a cyber vault source and target.

Implementation

Workload Factory provides assistance in creating a cyber vault architecture. After you contact NetApp to express your interest in implementing a cyber vault, a NetApp specialist contacts you to discuss your requirements.

Send an email to ng-FSx-CyberVault@netapp.com to get started.

Related information

For more information about cyber vaults and how to set up this architecture, refer to the [ONTAP cyber vault documentation](#).

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.