# Set up snapshot replication

ASA r2

NetApp
January 13, 2026

# Table of Contents


Set up snapshot replication . . . 1
- Replicate snapshots to a remote cluster from ASA r2 storage systems . . . 1
  - Step 1: Create a cluster peer relationship . . . 1
  - Step 2: Optionally, create a custom replication policy . . . 2
  - Step 3: Create a replication relationship . . . 2
  - Step 4: Test replication failover . . . 5
- Learn about pre-defined ONTAP data protection policies . . . 5
- Break an asynchronous replication relationship on your ASA r2 system . . . 6

# Set up snapshot replication

## Replicate snapshots to a remote cluster from ASA r2 storage systems

Snapshot replication is a process in which consistency groups on your ASA r2 system are copied to a geographically remote location. After the initial replication, changes to consistency groups are copied to the remote location based upon a replication policy. Replicated consistency groups can be used for disaster recovery or data migration.

> Snapshot replication for an ASA r2 storage system is only supported to and from another ASA r2 storage system. You cannot replicate snapshots from an ASA r2 system to an ASA, AFF or FAS system or from an ASA, AFF or FAS system to an ASA r2 system.

To set up Snapshot replication, you need to establish a replication relationship between your ASA r2 system and the remote location. The replication relationship is governed by a replication policy. A default policy to replicate all snapshots is created during cluster set up. You can use the default policy or optionally, create a new policy.

Beginning with ONTAP 9.17.1, you can apply asynchronous replication policies to consistency groups in a hierarchical relationship. Asynchronous replication is not supported for consistency groups in hierarchical relationships in ONTAP 9.16.1.

Learn more about hierarchical (parent/child) consistency groups.

### Step 1: Create a cluster peer relationship

Before you can protect your data by replicating it to a remote cluster, you need to create a cluster peer relationship between the local and remote cluster.

#### Before you begin

The prerequisites for cluster peering are the same for ASA r2 systems as for other ONTAP systems. Review the prerequisites for cluster peering.

#### Steps

1. On the local cluster, in System Manager, select **Cluster > Settings**.
2. Under **Intercluster Settings** next to **Cluster peers** select ⋮, then select **Add a cluster peer**.
3. Select **Lauch remote cluster**; this generates a passphrase you'll use to authenticate with the remote cluster.
4. After the passphrase for the remote cluster is generated, paste it under **Passphrase** on the local cluster.
5. Select + Add; then enter the intercluster network interface IP address.
6. Select **Initiate cluster peering**.

#### What's next?

You have peered for local ASA r2 cluster with a remote cluster. You can now create a replication relationship.

## Step 2: Optionally, create a custom replication policy

The replication policy defines when updates performed on the ASA r2 cluster are replicated to the remote site. ONTAP include various pre-defined data protection policies that you can use for your replication relationships. If the pre-defined policies do not meet your needs, you can create a custom replication policy.

Learn about pre-defined ONTAP data protection policies.

**Steps**

1. In System Manager, select **Protection > Policies**; then select **Replication policies**.
2. Select + Add.
3. Enter a name for the replication policy or accept the default name; then enter a description.
4. Select the **Policy scope**.

   If you want to apply the replication policy to the entire cluster, select **Cluster**. If you want the replication policy applied only to the storage units in a specific storage VM, select **Storage VM**.

5. For the **Policy type**, select **Asynchronous**.

   With the asynchronous policy, data is copied to the remote site after it is written to the source. Synchronous replication is not supported for ASA r2 systems.

6. Under **Transfer snapshots from source**, accept the default transfer schedule or select a different one.
7. Select to transfer all snapshots or to create rules to determine which snapshots to transfer.
8. Optionally, enable network compression.
9. Select **Save**.

**What's next?**

You have created a replication policy and are now ready to create a replication relationship between your ASA r2 system and your remote location.

**For more information**

Learn more about storage VMs for client access.

## Step 3: Create a replication relationship

A snapshot replication relationship establishes a connection between your ASA r2 system and a remote location so that you can replicate consistency groups to a remote cluster. Replicated consistency groups can be used for disaster recovery or for data migration.

For protection against ransomware attacks, when you set up your replication relationship, you can select to lock the destination snapshots. Locked snapshots cannot be deleted accidentally or maliciously. You can use locked snapshots to recover data if a storage unit is compromised by a ransomware attack.

**Before you begin**

- Learn about replication policies.

  When you create a replication relationship, you must select the appropriate replication policy for your replication relationship. You can use a pre-defined policy or create a custom policy.

- If you want to lock your destination snapshots, you must initialize the Snapshot compliance clock before you create the replication relationship.

Create a replication relationship with or without locked destination snapshots.

**With locked snapshots**

**Steps**

1. In System Manager, select **Protection > Consistency groups**.
2. Select a consistency group.
3. Select ⋮; then select **Protect**.
4. Under **Remote protection**, select **Replicate to a remote cluster**.
5. Select the **Replication policy**.

   You must select a *vault* replication policy.

6. Select **Destination settings**.
7. Select **Lock destination snapshots to prevent deletion**
8. Enter the maximum and minimum data retention period.
9. To delay the start of the data transfer, deselect **Start transfer immediately**.

   The initial data transfer begins immediately by default.

10. Optionally, to override the default transfer schedule, select **Destination settings**, then select **Override transfer schedule**.

    Your transfer schedule must be a minimum of 30 minutes to be supported.

11. Select **Save**.

**Without locked snapshots**

**Steps**

1. In System Manager, select **Protection > Replication**.
2. Select to create the replication relationship with local destination or local source.

| Option | Steps |
| --- | --- |
| Local destinations | 1. Select **Local destinations**, then select Replicate.<br>2. Search for and select the source consistency group.<br><br>The *source* consistency group refers to the consistency group on your local cluster that you want to replicate. |

| Option | Steps |
| --- | --- |
| Local sources | 1. Select **Local sources**, then select Replicate .<br>2. Search for and select the source consistency group.<br>3. Under **Replication destination**, select the cluster to replicate to; then select the storage VM. |

3. Select a replication policy.
4. To delay the start of the data transfer, select **Destination settings**; then deselect **Start transfer immediately**.

   The initial data transfer begins immediately by default.

5. Optionally, to override the default transfer schedule, select **Destination settings**, then select **Override transfer schedule**.

   Your transfer schedule must be a minimum of 30 minutes to be supported.

6. Select **Save**.

**What's next?**

Now that you have created a replication policy and relationship, your initial data transfer begins as defined in your replication policy. You can optionally test your replication failover to verify that successful failover can occur if your ASA r2 system goes offline.

## Step 4: Test replication failover

Optionally, validate that you can successfully serve data from replicated storage units on a remote cluster if the source cluster is offline.

**Steps**

1. In System Manager, select **Protection > Replication**.
2. Hover over the replication relationship you want to test, then select ⋮.
3. Select **Test failover**.
4. Enter the failover information, then select **Test failover**.

**What's next?**

Now that your data is protected with snapshot replication for disaster recovery, you should encrypt your data at rest so that it can't be read if a disk in your ASA r2 system is repurposed, returned, misplaced or stolen.

# Learn about pre-defined ONTAP data protection policies

The replication policy defines when updates performed on the ASA r2 cluster are replicated to the remote site. ONTAP includes various pre-defined data protection policies that you can use for your replication relationships.

If the pre-defined policies do not meet your needs, you can create a custom replication policy.

ASA r2 systems do not support synchronous replication.

ASA r2 systems support the following pre-defined protection policies.

| Policy | Description | Policy type |
|---|---|---|
| Asynchronous | A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots with an hourly transfer schedule. | Asynchronous |
| AutomatedFailOverDuplex | Policy for SnapMirror synchronous with zero RTO guarantee and bi-directional sync replication. | SnapMirror active sync |
| CloudBackupDefault | Vault policy with daily rule. | Asynchronous |
| DailyBackup | Vault policy with a daily rule and a daily transfer schedule. | Asynchronous |
| DPDefault | SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system. | Asynchronous |
| MirrorAllSnapshots | SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system. | Asynchronous |
| MirrorAllSnapshotsDiscardNetwork | SnapMirror asynchronous policy for mirroring all snapshots and the latest active file system excluding the network configurations. | Asynchronous |
| MirrorAndVault | A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots. | Asynchronous |
| MirrorAndVaultDiscardNetwork | A unified SnapMirror asynchronous and vault policy for mirroring the latest active file system and daily and weekly snapshots excluding the network configurations. | Asynchronous |
| MirrorLatest | SnapMirror asynchronous policy for mirroring the latest active file system. | Asynchronous |
| Unified7year | Unified SnapMirror policy with 7-year retention. | Asynchronous |
| XDPDefault | Vault policy with daily and weekly rules. | Asynchronous |

# Break an asynchronous replication relationship on your ASA r2 system

In certain situations, you might need to break an asynchronous replication relationship. For example, if are running ONTAP 9.16.1 and you want to increase the size of a consistency group that is in an asynchronous replication relationship, you must break the relationship before you can modify the consistency group's size.

**Steps**

1. In System Manager, select **Protection > Replication**.
2. Select **Local destinations** or **Local sources**.
3. Next to the relationship that you want to break, select ⋮; then select **Break**.
4. Select **Break**.

**Result**

The asynchronous relationship between the primary and secondary consistency group is broken.

## Copyright information



## Trademark information