



Use ONTAP to manage your data

ASA r2

NetApp
September 26, 2024

Table of Contents

- Use ONTAP to manage your data 1
- ASA r2 storage system video demonstrations 1
- Manage your storage 1
- Protect your data 11
- Secure your data 26

Use ONTAP to manage your data

ASA r2 storage system video demonstrations

View short videos that demonstrate how to use ONTAP System Manager to quickly and easily perform common task on your ASA r2 storage systems.

[Configure SAN protocols on your ASA r2 system](#)

[Video transcript](#)

[Provision SAN storage on your ASA r2 system](#)

[Video transcript](#)

[Replicate data to a remote cluster from an ASA r2 system](#)

[Video transcript](#)

Manage your storage

Provision ONTAP SAN storage on the ASA r2 systems

When you provision storage, you enable your SAN hosts to read from and write data to ASA r2 storage systems. To provision storage, you use ONTAP System Manager to create storage units, add host initiators, and map the host to a storage unit. You also need to perform steps on the host to enable read/write operations.

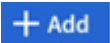
Create storage units

On an ASA r2 system, a storage unit makes storage space available to your SAN hosts for data operations. A storage unit refers to a LUN for SCSI hosts or an NVMe namespace for NVMe hosts. If your cluster is configured to support SCSI hosts, you are prompted to create a LUN. If your cluster is configured to support NVMe hosts, you are prompted to create an NVMe namespace. An ASA r2 storage unit has a maximum capacity of 128TB.

See the [NetApp Hardware Universe](#) for the most current storage limits for ASA r2 systems.

Host initiators are added and mapped to the storage unit as part of the storage unit creation process. You can also [add host initiators](#) and [map](#) them to your storage units after the storage units are created.

Steps

1. In System Manager, select **Storage**; then select  .
2. Enter a name for the new storage unit.
3. Enter the number of units you want to create.

If you create more than one storage unit, each unit is created with the same capacity, host operating system, and host mapping.



4. Enter the storage unit capacity; then select the host operating system.


- Accept the auto-selected **host mapping** or select a different host group for the storage unit to be mapped to.

Host mapping refers to the host group that the new storage unit will be mapped to. If there is a pre-existing host group for the type of host you selected for your new storage unit, the pre-existing host group is auto-selected for your host mapping. You can accept the host group that is auto-selected for your host mapping or you can select a different host group.

If there is no pre-existing host group for hosts running on the operating system you specified, a new host group is automatically created by ONTAP.

- If you want to do any of the following, select **More Options** and complete the required steps.

Option	Steps
<p>Change the default Quality of Service (QoS) policy</p> <p>If the default QoS policy has not previously been set on the storage virtual machine (VM) on which the storage unit is being created, this option is not available.</p>	<ol style="list-style-type: none"> Under Storage and optimization, next to Quality of service (QoS), select  . Select an existing QoS policy.
<p>Create a new QoS policy</p>	<ol style="list-style-type: none"> Under Storage and optimization, next to Quality of service (QoS), select  . Select Define new policy. Enter a name for the new QoS policy. Set a QoS limit, a QoS guarantee, or both. <ol style="list-style-type: none"> Optionally, under Limit, enter a maximum throughput limit, a maximum IOPS limit, or both. <p>Setting a maximum throughput and IOPS for a storage unit restricts its impact on system resources so that it does not degrade the performance of critical workloads.</p> Optionally, under Guarantee, enter a minimum throughput, a minimum IOPS, or both. <p>Setting a minimum throughput and IOPS for a storage unit guarantees that it meets minimum performance targets regardless of demand by competing workloads.</p> Select Add.

Option	Steps
Add a new SCSI host	<p>a. Under Host information, select SCSI for the connection protocol.</p> <p>b. Select the host operating system.</p> <p>c. Under Host Mapping, select New hosts.</p> <p>d. Select FC or iSCSI.</p> <p>e. Select existing host initiators or select Add initiator to add a new host initiator.</p> <p>An example of a valid FC WWPN is "01:02:03:04:0a:0b:0c:0d". Examples of valid iSCSI initiator names are "iqn.1995-08.com.example:string" and "eui.0123456789abcdef".</p>
Create a new SCSI host group	<p>a. Under Host information, select SCSI for the connection protocol.</p> <p>b. Select the host operating system.</p> <p>c. Under Host Mapping, select New host group.</p> <p>d. Enter a name for the host group; then select the hosts to add to the group.</p>
Add a new NVMe subsystem	<p>a. Under Host information, select NVMe for the connection protocol.</p> <p>b. Select the host operating system.</p> <p>c. Under Host Mapping, select New NVMe subsystem.</p> <p>d. Enter a name for the subsystem or accept the default name.</p> <p>e. Enter a name for the initiator.</p> <p>f. If you want to enable in-band authentication or Transport Layer Security (TLS), select ; then select your options.</p> <p>In-band authentication allows secure bidirectional and unidirectional authentication between your NVMe hosts and your ASA r2 system.</p> <p>TLS encrypts all data sent over the network between your NVMe/TCP hosts and your ASA r2 system.</p> <p>g. Select Add initiator to add more initiators.</p> <p>The host NQN should be formatted as <nqn.yyyy-mm> followed by a fully qualified domain name. The year should be equal to or later than 1970. The total maximum length should be 223. An example of a valid NVMe initiator is nqn.2014-08.com.example:string</p>

7. Select **Add**.

What's next?

Your storage units are created and mapped to your hosts. You can now [create snapshots](#) to protect the data on your ASA r2 system.

For more information

Learn more about [how ASA r2 systems use storage virtual machines](#).

Add host initiators

You can add new host initiators to your ASA r2 system at any time. Initiators make the hosts eligible to access storage units and perform data operations.

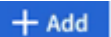
Before you begin

If you want to replicate the host configuration to a destination cluster during the process of adding your host initiators, your cluster must be in a replication relationship. Optionally, you can [create a replication relationship](#) after your host is added.

Add host initiators for SCSI or NVMe hosts.

SCSI hosts

Steps

1. Select **Host**.
2. Select **SCSI**; then select  **Add** .
3. Enter the host name, select the host operating system and enter a host description.
4. If you want to replicate the host configuration to a destination cluster, select **Replicate host configuration**; then select the destination cluster.

Your cluster must be in a replication relationship to replicate the host configuration.

5. Add new or existing hosts.

Add new hosts	Add existing hosts
<ol style="list-style-type: none">a. Select New hosts.b. Select FC or iSCSI; then select the host initiators.c. Optionally, select Configure host proximity. Configuring host proximity enables ONTAP to identify the controller nearest to the host for data path optimization and latency reduction. This is only applicable if you have replicated data to a remote location. If you have not set up snapshot replication, you do not need to select this option.d. If you need to add new initiators, select Add initiators.	<ol style="list-style-type: none">a. Select Existing hosts.b. Select the host you want to add.c. Select Add.

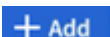
6. Select **Add**.

What's next?

Your SCSI hosts are added to your ASA r2 system and you are ready to map your hosts to your storage units.

NVMe hosts

Steps

1. Select **Host**.
2. Select **NVMe**; then select  **Add** .
3. Enter a name for the NVMe subsystem, select the host operating system and enter a description.
4. Select **Add initiator**.

What's next?

Your NVMe hosts are added to your ASA r2 system and you are ready to map your hosts to your storage units.

Create host groups

On an ASA r2 system, a *host group* is the mechanism used to give hosts access to storage units. A host group refers to an igroup for SCSI hosts or to an NVMe subsystem for NVMe hosts. A host can only see the storage units that are mapped to the host groups to which it belongs. When a host group is mapped to a storage unit, the hosts that are members of the group, are then able to mount (create directories and file structures on) the storage unit.

Host groups are automatically or manually created when you create your storage units. You can optionally use the following steps to create host groups before or after storage unit creation.

Steps

1. From System Manager, select **Host**.
2. Select the hosts you want to add to the host group.

After you select the first host, the option to add to a host group appears above the list of hosts.

3. Select **Add to host group**.
4. Search for and select the host group to which you want to add the host.


What's next?

You have created a host group and you can now map it to a storage unit.

Map the storage unit to a host

After you have created your ASA r2 storage units and added host initiators, you need to map your hosts to your storage units to begin serving data. Storage units are mapped to hosts as part of the storage unit creation process. You can also map existing storage units to new or existing hosts at any time.

Steps

1. Select **Storage**.
2. Hover over the name of the storage unit you want to map.
3. Select ; then select **Map to hosts**.
4. Select the hosts you want to map to the storage unit; then select **Map**.

What's next?

Your storage unit is mapped to your hosts and you are ready to complete the provisioning process on your hosts.

Complete host-side provisioning

After you have created your storage units, added your host initiators and mapped your storage units, there are steps you must perform on your hosts before they can read and write data on your ASA r2 system.

Steps

1. For FC and FC/NVMe, zone your FC switches by WWPN.

Use one zone per initiator and include all target ports in each zone.

2. Discover the new storage unit.
3. Initialize the storage unit and create a file system.

4. Verify that your host can read and write data on the storage unit.

What's next?

You have completed the provisioning process and are ready to begin serving data. You can now [create snapshots](#) to protect the data on your ASA r2 system.

For more information

For more details about host-side configuration, see the [ONTAP SAN host documentation](#) for your specific host.


Clone data on ASA r2 storage systems

Data cloning creates copies of storage units and consistency groups on your ASA r2 system using ONTAP System Manager that can be used for application development, testing, backups, data migration or other administrative functions.

Clone storage units

When you clone a storage unit, you create a new storage unit on your ASA r2 system that is a point-in-time, writable copy of the storage unit you cloned.

Steps

1. In System Manager, select **Storage**.
2. Hover over the name of the storage unit you want to clone.
3. Select ; then select **Clone**.
4. Accept the default name for the new storage unit that will be created as a clone or enter a new one.
5. Select the host operating system.

A new snapshot is created for the clone by default.

6. If you want to use an existing snapshot, create a new host group, or add a new host, select **More Options**.

Option	Steps
Use an existing snapshot	<ol style="list-style-type: none">a. Under Snapshot to clone, select Use an existing snapshot.b. Select the snapshot you want to use for the clone.
Create a new host group	<ol style="list-style-type: none">a. Under Host mapping, select New host group.b. Enter a name for the new host group; then select the host initiators to include in the group.
Add a new host	<ol style="list-style-type: none">a. Under Host mapping, select New hosts.b. Enter the a name for the new host; then select FC or iSCSI.c. Select the host initiators from the list of existing initiators or select Add to add new initiators for the host.

7. Select **Clone**.

What's next?

You have created a new storage unit that is identical to the storage unit you cloned. You are now ready to use the new storage unit as needed.

Clone consistency groups

When you clone a consistency group, you create a new consistency group that's identical in structure, storage units, and data to the consistency group you cloned. Use a consistency group clone to perform application testing or to migrate data. Suppose, for example, you need to migrate a production workload out of a consistency group. You can clone the consistency group to create a copy of your production workload to maintain as a backup until the migration is complete.


The clone is created from a snapshot of the consistency group being cloned. The snapshot used for the clone is taken at the point in time that the cloning process is initiated by default. You can modify the default behavior to use a pre-existing snapshot.

Storage unit mappings are copied as part of the cloning process. Snapshot policies are not copied as part of the cloning process.

You can create clones from consistency groups stored locally on your ASA r2 system or from consistency groups that have been replicated to remote locations.

Clone using local snapshot

Steps


1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to clone.
3. Select , then select **Clone**.
4. Enter a name for consistency group clone or accept the default name.
5. Select the host operating system.
6. If you want to dissociate the clone from the source consistency group and allocate disk space, select **Split clone**.
7. If you want to use an existing snapshot, create a new host group or add a new host for the clone, select **More Options**.

Option	Steps
Use an existing snapshot	<ol style="list-style-type: none">a. Under Snapshot to clone, select Use an existing snapshot.b. Select the snapshot you want to use for the clone.
Create a new host group	<ol style="list-style-type: none">a. Under Host mapping, select New host group.b. Enter a name for the new host group; then select the host initiators to include in the group.
Add a new host	<ol style="list-style-type: none">a. Under Host mapping, select New hosts.b. Enter the name new host name; then select FC or iSCSI.c. Select the host initiators from the list of existing initiators or select Add initiator to add new initiators for the host.

8. Select **Clone**.

Clone using remote snapshot

Steps

1. In System Manager, select **Protection > Replication**.
2. Hover over the **Source** you want to clone.
3. Select , then select **Clone**.
4. Select the source cluster and storage VM; then enter a name for the new consistency group or accept the default name.
5. Select the snapshot to clone; then select **Clone**.

What's next?

You have cloned a consistency group from your remote location. The new consistency group is locally available on your ASA r2 system to use as needed.

What's next?

To protect your data, you should [create snapshots](#) of the cloned consistency group.

Modify storage units on ASA r2 storage systems

To optimize performance on your ASA r2 system, you might need to modify your storage units to increase their capacity, update QoS policies or to change the hosts that are mapped to the units. For example, if a new, critical application workload is added to an existing storage unit, you might need to change the Quality of Service (QoS) policy applied to the storage unit to support the performance level needed for the new application.

Increase capacity

Increase the size of a storage unit before it reaches full capacity to prevent a loss of data access that can occur if the storage unit runs out of writeable space. The capacity of a storage unit can be increased to 128 TB which is the maximum size allowed by ONTAP.

Modify host mappings

Modify the hosts that are mapped to a storage unit to assist in balancing workloads or reconfiguring system resources.

Modify QoS policy

Quality of service (QoS) policies guarantee that the performance of critical workloads is not degraded by competing workloads. You can use QoS policies to set a QoS throughput *limit* and a QoS throughput *guarantee*.


- QoS throughput limit

The QoS throughput *limit* restricts the impact of a workload on system resources by limiting the throughput for the workload to a maximum number of IOPS or MBps, or IOPS and MBps.

- QoS throughput guarantee

The QoS throughput *guarantee* ensures that critical workloads meet minimum throughput targets, regardless of demand by competing workloads, by guaranteeing that the throughput for the critical workload does not fall below a minimum number of IOPS or MBps, or IOPS and MBps.

Steps

1. In System Manager, select **Storage**.
2. Hover over the name of the storage unit you want to edit.
3. Select ; then select **Edit**.
4. Update the storage unit parameters as needed to increase capacity, change the QoS policy, and update the host mapping.

What's next?

If you have increased the size of your storage unit, you must rescan the storage unit on the host for the host to

recognize the change in size.


Delete storage units on ASA r2 storage systems

Delete a storage unit if you no longer need to maintain the data contained in the unit. Deleting storage units that are no longer needed can help you free space needed for other host applications.

Before you begin

If the storage unit you want to delete is in a consistency group that is in replication relationship, you must [remove the storage unit from the consistency group](#) before you delete it.

Steps

1. In System Manager, select **Storage**.
2. Hover over the name of the storage unit you want to delete.
3. Select ; then select **Delete**.
4. Acknowledge that the deletion cannot be undone.
5. Select **Delete**.

What's next?

You can use the space freed from the deleted storage unit to [increase the size](#) of storage units that need additional capacity.

ASA r2 storage limits

For optimal performance, configuration and support, you should be aware of your ASA r2 storage limits.

ASA r2 systems support the following:

Max nodes per cluster	2
Max storage unit size	128 TB

For more information

For a complete list of the most current ASA r2 storage limits, see [NetApp Hardware Universe](#).

Protect your data

Create snapshots to back up your data on ASA r2 storage systems

To back up data on your ASA r2 system, you need to create a snapshot. You can use ONTAP System Manager to create a manual snapshot of a single storage unit, or to create a consistency group and schedule automatic snapshots of multiple storage units at the same time.

Step 1: Optionally, create a consistency group

A consistency group is a collection of storage units that are managed as a single unit. Create consistency groups to simplify storage management and data protection for application workloads spanning multiple storage units. For example, suppose you have a database consisting of 10 storage units in a consistency group, and you need to back up the entire database. Instead of backing up each storage unit, you can back up the entire database by simply adding snapshot data protection to the consistency group.

Create a consistency group using new storage units or create a consistency group using existing storage units.

Use new storage units

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select **+ Add** ; then select **Using new storage units**.
3. Enter a name for the new storage unit, the number of units, and the capacity per unit.

If you create more than one unit, each unit is created with the same capacity and the same host operating system. To assign a different capacity to each unit, select **More options**; then select **Add a different capacity**.

4. Select the host operating system and host mapping.
5. Select **Add**.

What's next?

You have created a consistency group containing the storage units you want to protect. You are now ready to create a snapshot.

Use existing storage units

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select **+ Add** ; then select **Using existing storage units**.
3. Enter a name for the consistency group; then search for and select the storage units you want to include in the consistency group.
4. Select **Add**.

What's next?

You have created a consistency group containing the storage units you want to protect. You are now ready to create a snapshot.

Step 2: Create a snapshot

A snapshot is a local, read-only copy of your data that you can use to restore storage units to specific points in time.

Snapshots can be created on demand, or they can be created automatically in regular intervals based on a [snapshot policy and schedule](#). The snapshot policy and schedule specifies when to create the snapshots, how many copies to retain, how to name them, and how to label them for replication. For example, a system might create one snapshot every day at 12:10 a.m., retain the two most recent copies, name them “daily” (appended with a timestamp), and label them “daily” for replication.

Types of snapshots

You can create an on-demand snapshot of a single storage unit or of a consistency group. You can create automated snapshots of a consistency group containing multiple storage units. You cannot create automated snapshots of a single storage unit.

- On-demand snapshots

An on-demand snapshot of a storage unit can be created at any time. The storage unit does not need to be a member of a consistency group to be protected by an on-demand snapshot. If you create an on-demand snapshot of a storage unit that is a member of a consistency group, the other storage units in the consistency group are not included in the on-demand snapshot. If you create an on-demand snapshot of a consistency group, all the storage units in the consistency group are included in the snapshot.


- Automated snapshots

Automated snapshots are created using snapshot policies. To apply a snapshot policy to a storage unit for automated snapshot creation, the storage unit must be a member of a consistency group. If you apply a snapshot policy to a consistency group, all the storage units in the consistency group are protected with automated snapshots.

Create a snapshot of a consistency group or a storage unit.

Snapshot of a consistency group

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the name of the consistency group you want to protect.
3. Select  ; then select **Protect**.
4. If you want to create an immediate snapshot on-demand, under **Local protection**, select **Add a snapshot now**.



Local protection creates the snapshot on the same cluster containing the storage unit.

- a. Enter a name for the snapshot or accept the default name; then optionally, enter a SnapMirror label.

The SnapMirror label is used by the remote destination.

5. If you want to create automated snapshots using a snapshot policy, select **Schedule snapshots**.
 - a. Select a snapshot policy.

Accept the default snapshot policy, select an existing policy, or create a new policy.

Option	Steps
Select an existing snapshot policy	Select  next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	<ol style="list-style-type: none">a. Select  Add ; then enter the snapshot policy parameters.b. Select Add policy.


6. If you want to replicate your snapshots to a remote cluster, under **Remote protection**, select **Replicate to a remote cluster**.
 - a. Select the source cluster and storage VM; then select the replication policy.

The initial data transfer for replication starts immediately by default.

7. Select **Save**.

Snapshot of storage unit

Steps

1. In System Manager, select **Storage**.
2. Hover over the name of the storage unit you want to protect.
3. Select  ; then select **Protect**.

If you want to create an immediate snapshot on-demand, under **Local protection**, select **Add a snapshot now**.



Local protection creates the snapshot on the same cluster containing the storage unit.

4. Enter a name for the snapshot or accept the default name; then optionally, enter a SnapMirror label.

The SnapMirror label is used by the remote destination.

5. If you want to create automated snapshots using a snapshot policy, select **Schedule snapshots**.
 - a. Select a snapshot policy.

Accept the default snapshot policy, select an existing policy, or create a new policy.

Option	Steps
Select an existing snapshot policy	Select  next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	<ol style="list-style-type: none">a. Select  Add ; then enter the snapshot policy parameters.b. Select Add policy.

6. If you want to replicate your snapshots to a remote cluster, under **Remote protection**, select **Replicate to a remote cluster**.
 - a. Select the source cluster and storage VM; then select the replication policy.

The initial data transfer for replication starts immediately by default.

7. Select **Save**.

What's next?

Now that your data is protected with snapshots, you should [set up snapshot replication](#) to copy your consistency groups to a geographically remote location for backup and disaster recovery.

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 from an ASA r2 storage system is supported only to another ASA r2 storage system. You cannot replicate snapshots from an ASA r2 system to a current ASA, AFF or FAS 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.

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.

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 **Launch 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**.

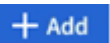
What's next?

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

Step 2: Optionally, create a replication policy

The snapshot replication policy defines when updates performed on the ASA r2 cluster are replicated to the remote site.

Steps

1. In System Manager, select **Protection > Policies**; then select **Replication policies**.
2. Select .
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. Select the **Policy type**.

Option	Steps
Copy data to the remote site after it is written to the source.	<ol style="list-style-type: none"> a. Select Asynchronous. b. Under Transfer snapshots from source, accept the default transfer schedule or select a different one. c. Select to transfer all snapshots or to create rules to determine which snapshots to transfer. d. Optionally, enable network compression.
Write data to the source and remote sites simultaneously.	<ol style="list-style-type: none"> a. Select Synchronous.

6. 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

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	<ol style="list-style-type: none">1. Select Local destinations, then select .2. Search for and select the source consistency group. <p>The <i>source</i> consistency group refers to the consistency group on your local cluster that you want to replicate.</p>

Option	Steps
Local sources	<ol style="list-style-type: none"> 1. Select Local sources, then select  . 2. Search for and select the source consistency group. The <i>source</i> consistency group refers to the consistency group on your local cluster that you want to replicate. 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.

Protect your Kubernetes applications on ASA r2 storage systems

Use Astra Control Center to protect your Kubernetes applications. Astra Control Center allows you to migrate applications and data from one Kubernetes cluster to another, replicate applications to a remote system using NetApp SnapMirror technology, and clone applications from staging to production.

For more information

[Learn more about protecting Kubernetes applications using Astra Control.](#)

Restore data on ASA r2 storage systems

Data in a consistency group or storage unit that is protected by snapshots can be restored if it is lost or corrupted.

Restore a consistency group


Restoring a consistency group replaces the data in all the storage units in the consistency group with the data from a snapshot. Changes made to the storage units after the snapshot was created are not restored..

You can restore a consistency group from a local or remote snapshot.

Restore from a local snapshot


Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Double-click the consistency group containing the data you need to restore.

The consistency group details page opens.
3. Select **Snapshots**.
4. Select the snapshot you want to restore; then select .
5. Select **Restore consistency group from this snapshot**; then select **Restore**.

Restore from a remote snapshot

Steps

1. In System Manager, select **Protection > Replication**.
2. Select **Local destinations**.
3. Select the **Source** you want to restore, then select .
4. Select **Restore**.
5. Select the cluster, storage VM, and consistency group to which you want to restore data.
6. Select the snapshot you want to restore from.
7. When prompted, enter "restore"; then select **Restore**.

Result

Your consistency group is restored to the point in time of the snapshot used for restoration.


Restore a storage unit

Restoring a storage unit replaces all the data in the storage unit with the data from a snapshot. Changes made to the storage unit after the snapshot was created are not restored.

Steps

1. In System Manager, select **Storage**.
2. Double-click the storage unit containing the data you need to restore.

The storage unit details page opens.

3. Select **Snapshots**.
4. Select the snapshot you want to restore.
5. Select ; then select **Restore**.
6. Select **Use this snapshot to restore the storage unit**; then select **Restore**.

Result

Your storage unit is restored to the point in time of the snapshot used for restoration.

Manage ONTAP consistency groups on ASA r2 storage systems


A consistency group is a collection of storage units that are managed as a single unit. Use consistency groups for simplified storage management. For example, suppose you have a database consisting of 10 storage units in a consistency group, and you need to back up the entire database. Instead of backing up each storage unit, you can back up the entire database by simply adding snapshot data protection to the consistency group. Backing up the storage units as a consistency group instead of individually also provides a consistent backup of all the units, while backing up units individually could potentially create inconsistencies.

Add snapshot data protection to a consistency group





When you add snapshot data protection to a consistency group, local snapshots of the consistency group are taken at regular intervals based on a pre-defined schedule.

You can use snapshots to [restore data](#) that is lost or corrupted.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to protect.
3. Select ; then select **Edit**.
4. Under **Local protection**, select **Schedule snapshots**.
5. Select a snapshot policy.

Accept the default snapshot policy, select an existing policy, or create a new policy.

Option	Steps
Select an existing snapshot policy	Select  next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	<ol style="list-style-type: none"> Select  Add ; then enter the new policy name. Select the policy scope. Under Schedules select  Add . Select the name that appears under Schedule name; then select  . Select the policy schedule. Under Maximum snapshots, enter the maximum number of snapshots that you want to retain of the consistency group. Optionally, under SnapMirror label enter a SnapMirror label. Select Save.

6. Select **Edit**.


What's next

Now that your data is protect with snapshots, you should [set up snapshot replication](#) to copy your consistency groups to a geographically remote location for backup and disaster recovery.

Remove snapshot data protection from a consistency group

When you remove snapshot data protection from a consistency group, snapshots are disabled for all the storage units in the consistency group.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to stop protecting.
3. Select  ; then select **Edit**.
4. Under **Local protection**, deselect Schedule snapshots.
5. Select **Edit**.

Result

Snapshots will not be taken for any of the storage units in the consistency group.


Add storage units to a consistency group

Expand the amount of storage managed by a consistency group by adding storage units to the consistency group.

You can add existing storage units to your consistency group or you can create new storage units to add to the consistency group.


Add existing storage units

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to expand.
3. Select ; then select **Expand**.
4. Select **Using existing storage units**.
5. Select the storage units to add to the consistency group; then select **Expand**.

Add new storage units

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to expand.
3. Select ; then select **Expand**.
4. Select **Using new storage units**.
5. Enter the number of units you want to create and the capacity per unit.

If you create more than one unit, each unit is created with the same capacity and the same host operating system. To assign a different capacity to each unit, select **Add a different capacity** to assign a different capacity to each unit.

6. Select **Expand**.

What's next

After you create a new storage unit, you should [add host initiators](#) and [map the newly created storage unit to a host](#). Adding host initiators makes hosts eligible to access the storage units and perform data operations. Mapping a storage unit to a host allows the storage unit to begin serving data to the host it is mapped to.

What's next?

Existing snapshots of the consistency group won't include your newly added storage units. You should [create an immediate snapshot](#) of your consistency group to protect your newly added storage units until the next scheduled snapshot is automatically created.

Remove a storage unit from a consistency group

You should remove a storage unit from a consistency group if you want to delete the storage unit, if you want to manage it as part of a different consistency group, or if you no longer need to protect the data it contains. Removing a storage unit from a consistency group breaks the relationship between the storage unit and the consistency group, but does not delete the storage unit.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Double-click the consistency group from which you want to remove a storage unit.
3. In the **Overview** section, under **Storage units**, select the storage unit you want to remove; then select **Remove from consistency group**.

Result

The storage unit is no longer a member of the consistency group.

What's next

If you need to continue data protection for the storage unit, add the storage unit to another consistency group.


Delete a consistency group

If you no longer need to manage the members of a consistency group as a single unit, you can delete the consistency group. After a consistency group is deleted, the storage units previously in the group remain active on the cluster.

Before you begin

If the consistency group you want to delete is in a replication relationship, you must break the relationship before you delete the consistency group. After you delete a previously replication consistency group, the storage units that were in the consistency group remain active on the cluster and their replicated copies remain on the remote cluster.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want to delete.
3. Select ; then select **Delete**.
4. Accept the warning, then select **Delete**.

What's next?

After you delete a consistency group, the storage units previously in the consistency group are no longer protected by snapshots. Consider adding these storage units to another consistency group to protect them against data loss.

Manage ONTAP data protection policies and schedules on ASA r2 storage systems

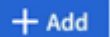
Use snapshot policies to protect data in your consistency groups on an automated schedule. Use policy schedules within snapshot policies to determine how often snapshots are taken.

Create a new protection policy schedule

A protection policy schedule defines how often a snapshots policy is executed. You can create schedules to run in regular intervals based on a number of days, hours, or minutes. For example, you can create a schedule to run every hour or to run only once per day. You can also create schedules to run at specific times on specific days of the week or month. For example, you can create a schedule to run at 12:15am on the 20th of every month.

Defining various protection policy schedules gives you the flexibility to increase or decrease the frequency of snapshots for different applications. This enables you to provide a greater level of protection and a lower risk of data loss for your critical workloads than what might be needed for less critical workloads.

Steps

1. Select **Protection > Policies**; then select **Schedule**.
2. Select .
3. Enter a name for the schedule; then select the schedule parameters.

4. Select **Save**.

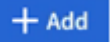
What's next?

Now that you have created a new policy schedule, you can use the newly created schedule within your policies to define when snapshots are taken.

Create a snapshot policy

A snapshot policy defines how often snapshots are taken, the maximum number of snapshots allowed, and how long snapshots are retained.

Steps

1. In System Manager, select **Protection > Policies**; then select **Snapshot policies**.
2. Select  **Add**.
3. Enter a name for the snapshot policy.
4. Select **Cluster** to apply the policy to the entire cluster. Select **Storage VM** to apply the policy to an individual storage VM.
5. Select **Add a schedule**; then enter the snapshot policy schedule.
6. Select **Add policy**.


What's next?

Now that you have created a snapshot policy, you can apply it to a consistency group. Snapshots will be taken of the consistency group based on the parameters you set in your snapshot policy.

Apply a snapshot policy to a consistency group

Apply a snapshot policy to a consistency group to automatically create, retain, and label snapshots of the consistency group.

Steps

1. In System Manager, select **Protection > Policies**; then select **Snapshot policies**.
2. Hover over the name of the snapshot policy you want to apply.
3. Select ; then select **Apply**.
4. Select the consistency groups to which you want to apply the snapshot policy; then select **Apply**.

What's next?

Now that your data is protected with snapshots, you should [set up a replication relationship](#) to copy your consistency groups to a geographically remote location for backup and disaster recovery.

Edit, delete, or disable a snapshot policy

Edit a snapshot policy to modify the policy name, maximum number of snapshots, or the SnapMirror label. Delete a policy to remove it and its associated back up data from your cluster. Disable a policy to temporarily stop the creation or transfer of snapshots specified by the policy.

Steps

1. In System Manager, select **Protection > Policies**; then select **Snapshot policies**.
2. Hover over the name of the snapshot policy you want to edit.

3. Select ; then select **Edit**, **Delete**, or **Disable**.


Result

You have modified, deleted or disabled the snapshot policy.

Edit a replication policy

Edit a replication policy to modify the policy description, transfer schedule, and rules. You can also edit the policy to enable or disable network compression.

Steps

1. In System Manager, select **Protection > Policies**.
2. Select **Replication policies**.
3. Hover over the replication policy that you want to edit; then select .
4. Select **Edit**.
5. Update the policy; then select **Save**.

Result

You have modified the replication policy.

Secure your data

Encrypt data at rest on ASA r2 storage systems

When you encrypt data at rest, it can't be read if a storage medium is repurposed, returned, misplaced, or stolen. You can use ONTAP System Manager to encrypt your data at the hardware and software level for dual-layer protection.

NetApp Storage Encryption (NSE) supports hardware encryption using self-encrypting drives (SEDs). SEDs encrypt data as it is written. Each SED contains a unique encryption key. Encrypted data stored on the SED can't be read without the SED's encryption key. Nodes attempting to read from an SED must be authenticated to access the SED's encryption key. Nodes are authenticated by obtaining an authentication key from a key manager, then presenting the authentication key to the SED. If the authentication key is valid, the SED will give the node its encryption key to access the data it contains.

Use the ASA r2 onboard key manager or an external key manager to serve authentication keys to your nodes.

In addition to NSE, you can also enable software encryption to add another layer of security to your data.

Steps

1. In System manager, select **Cluster > Settings**.
2. In the **Security** section, under **Encryption**, select **Configure**.
3. Configure the key manager.

Option	Steps
Configure the Onboard key Manager	<ol style="list-style-type: none"> Select Onboard Key Manager to add the key servers. Enter a passphrase.
Configure an external key manager	<ol style="list-style-type: none"> Select External key manager to add the key servers. Select + Add to add the key servers. Add the KMIP server CA certificates. Add the KMIP client certificates.

- Select **Dual-layer encryption** to enable software encryption.
- Select **Save**.

What's next?

Now that you have encrypted your data at rest, if you are using the NVMe/TCP protocol, you can [encrypt all the data sent over the network](#) between your NVMe/TCP host and your ASA r2 system.


Protect against ransomware attacks on ASA r2 storage systems

For enhanced protection against ransomware attacks, replicate snapshots to a remote cluster, then lock the destination snapshots to make them tamper-proof. Locked snapshots cannot be deleted accidentally or maliciously. You can use locked snapshots to recover data if a storage unit is ever compromised by a ransomware attack.

Initialize the Snaplock compliance clock

Before you can create tamper-proof snapshots, you must initialize the Snaplock compliance clock on your local and destination clusters.

Steps

- Select **Cluster > Overview**.
- In the **Nodes** section, select **Initialize SnapLock Compliance Clock**.
- Select **Initialize**.
- Verify that the compliance clock is initialized.
 - Select **Cluster > Overview**.
 - In the **Nodes** section, select ; then select **SnapLock Compliance Clock**.

What's next?

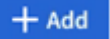

After you have initialized the Snaplock compliance clock on your local and destination clusters, you are ready to [create a replication relationship with locked snapshots](#).

Secure NVMe connections on your ASA r2 storage systems

If you are using the NVMe protocol, you can configure in-band authentication to enhance

your data security. In-band authentication allows secure bidirectional and unidirectional authentication between your NVMe hosts and your ASA r2 system. In-band authentication is available for all NVMe hosts. If you are using the NVMe/TCP protocol, you can further enhance your data security by configuring transport layer security (TLS) to encrypt all data sent over the network between your NVMe/TCP hosts and your ASA r2 system.

Steps

1. Select **Hosts**; then select **NVMe**.
2. Select  .
3. Enter the host name; then select the host operating system.
4. Enter a host description; then select the storage VM to connect to the host.
5. Select  next to the host name.
6. Select **In-band authentication**.
7. If you are using the NVMe/TCP protocol, select **Require Transport Layer Security (TLS)**.
8. Select **Add**.

Result

The security of your data is enhanced with in-band authentication and/or TLS.

Copyright information

Copyright © 2024 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.