Use ONTAP to manage your data

ASA r2

NetApp
February 11, 2026

Table of Contents

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 128 TB. See the NetApp Hardware Universe for the most current storage limits for ASA r2 systems.

You add and map host initiators to the storage unit as part of the storage unit creation process. You can also add and map host initiators after you create the storage units.

Beginning with ONTAP 9.18.1, you can modify the snapshot reserve and enable automatic snapshot deletion when you create a storage unit. The snapshot reserve is the amount of space in the storage unit reserved specifically for snapshots. When snapshot reserve is set with automatic snapshot deletion, older snapshots are automatically deleted when space used by snapshots exceeds the snapshot reserve.

Learn more about snapshot reserve on ASA r2 systems.

Storage units are thin provisioned by default. Thin provisioning allows the storage unit to grow up to the size allocated but doesn't reserve the space in advance. Space is allocated dynamically from available free space as needed. This allows you to realize greater storage efficiency by *over provisioning* your available space. For

example, suppose you have 1 TB of free space and you need to create four 1 TB storage units. Instead of immediately adding 3 TB of additional storage capacity to your system, you can create the storage units, monitor space utilization, and increase your storage capacity as the the storage units consume actual space. Learn more about thin provisioning.

Steps

1. In System Manager, select **Storage**; then select + Add.
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.

   To optimize workload balancing across the storage availability zone, create an even number of storage units.

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

   If you are creating more than one storage unit, each unit is created with the same capacity. Multiply the number of storage units you are creating by the desired capacity to ensure you have enough usable space. If you don't have enough free space and you chose to over provision, monitor utilization closely to avoid running out of space and losing data.

5. 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 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, ONTAP creates a new host group automatically .

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

Option	Steps
Change the default Quality of Service (QoS) policy 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.	a. Under **Storage and optimization**, next to **Quality of service (QoS)**, select ⌄. b. Select an existing QoS policy.

Option	Steps
Create a new QoS policy	a. Under **Storage and optimization**, next to **Quality of service (QoS)**, select . b. Select **Define new policy**. c. Enter a name for the new QoS policy. d. Set a QoS limit, a QoS guarantee, or both. i. Optionally, under **Limit**, enter a maximum throughput limit, a maximum IOPS limit, or both. 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. ii. Optionally, under **Guarantee**, enter a minimum throughput, a minimum IOPS, or both. Setting a minimum throughput and IOPS for a storage unit guarantees that it meets minimum performance targets regardless of demand by competing workloads. e. Select **Add**.
Change the default performance service level.	a. Under **Storage and optimization**, next to the **Performance service level**, select . b. Select **Performance**. ASA r2 systems offer two performance levels. The default performance level is **Extreme**, which is the highest available level. You can lower the level to **Performance**.
Modify the default snapshot reserve and enable automatic snapshot deletion.	a. Under **Snapshot reserve %**, enter the numeric value for the percentage of the storage unit space you want to allocate to snapshots. b. Select **Automatically delete older snapshots**.
Add a new SCSI host	a. Under **Host information**, select **SCSI** for the connection protocol. b. Select the host operating system. c. Under **Host Mapping**, select **New hosts**. d. Select **FC** or **iSCSI**. e. Select existing host initiators or select **Add initiator** to add a new host initiator. 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".

Option	Steps
Create a new SCSI host group	a. Under **Host information**, select **SCSI** for the connection protocol. b. Select the host operating system. c. Under **Host Mapping**, select **New host group**. d. Enter a name for the host group; then select the hosts to add to the group.
Add a new NVMe subsystem	a. Under **Host information**, select **NVMe** for the connection protocol. b. Select the host operating system. c. Under **Host Mapping**, select **New NVMe subsystem**. d. Enter a name for the subsystem or accept the default name. e. Enter a name for the initiator. f. If you want to enable in-band authentication or Transport Layer Security (TLS), select ; then select your options. In-band authentication allows secure bidirectional and unidirectional authentication between your NVMe hosts and your ASA r2 system. TLS encrypts all data sent over the network between your NVMe/TCP hosts and your ASA r2 system. g. Select **Add initiator** to add more initiators. Format the host NQN 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

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
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**.	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.

Map the storage unit to a host

After creating ASA r2 storage units and adding host initiators, map hosts to 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 a create 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	a. Under **Snapshot to clone**, select **Use an existing snaphot**. b. Select the snapshot you want to use for the clone.
Create a new host group	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	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 polices 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	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	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	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.

Split consistency group clone

When you split a consistency group clone, you dissociate the clone from the source consistency group and allocate disk space for the clone. The clone becomes a standalone consistency group that can be used independently of the source consistency group.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group clone that you want you want to split.
3. Select **Split clone**.
4. Select **Split**.

Result

The clone is dissociated from the source consistency group and disk space is allocated for the clone.

Manage host groups

Create host groups on your ASA r2 system

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.

Delete a host group on your ASA r2 system

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. You might want to delete a host group if you no longer want the hosts in the group to have access to the storage units that are mapped to the group.

Steps

1. In System Manager, select **Storage**.
2. Under **Host mapping** select the host group you want to delete.
3. Select **Mapped storage**.
4. Select **More**; then select **Delete**.
5. Select to verify that you want to continue; then select **Delete**.

What's next?

The host group is deleted. The hosts that were in the group no longer have access to the storage units that were mapped to the host group.

Manage storage units

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.

Move storage units on ASA r2 storage systems

If a storage availability zone is running low on space, you can move storage units to another storage availability zone to balance the storage utilization across the cluster.

You can move a storage unit while the storage unit is online and serving data. The move operation is non-disruptive.

Before you begin

- You must be running ONTAP 9.16.1 or later.
- Your cluster must consist of four or more nodes.

Steps

1. In System Manager, select **Storage**; then select the storage unit you want to move.
2. Select ⋮; then select **Move**.
3. Select the storage availability zone you want to move the storage unit to; then select **Move**.

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.

Migrate storage VMs

Migrate a storage VM from an ASA cluster to an ASA r2 cluster

Beginning with ONTAP 9.18.1, you can non-disruptively migrate a storage virtual machine (VM) from any ASA cluster to any ASA r2 cluster. Migrating from an ASA cluster to an ASA r2 cluster allows you to adopt the simplified and streamlined architecture of ASA r2 systems for SAN-only environments.

Storage VM migration between ASA and ASA r2 storage systems is supported as follows:

From any of the following ASA systems:	To any of the following ASA r2 systems:
• ASA C800 • ASA C400 • ASA C250 • ASA A900 • ASA A800 • ASA A400 • ASA A250 • ASA A150 • ASA AFF A800 • ASA AFF A700 • ASA AFF A400 • ASA AFF A250 • ASA AFF A220	• ASA A1K • ASA C30 • ASA A90 • ASA A70 • ASA A50 • ASA A30 • ASA A20

For the most current list of ASA and ASA r2 systems, see NetApp Hardware Universe. ASA r2 systems are listed in NetApp Hardware Universe as "ASA A-Series/C-Series (New)".

You can migrate a storage VM to an ASA r2 cluster from an ASA cluster only. Migration from any other type of ONTAP system is not supported.

Before you begin

All nodes in the ASA r2 cluster and the ASA cluster must be running ONTAP 9.18.1 or later. The ONTAP 9.18.1 patch versions on the cluster nodes can vary.

Step 1: Verify the status of the ASA storage VM

Before you migrate a storage VM from an ASA system, there should be no NVMe namespaces or vVols present and each volume in the storage VM should contain only one LUN. Migration of NVMe namespaces and vVols is not supported. The architecture of ASA r2 systems requires that volumes contain a single LUN.

Steps

1. Verify that no NVMe namespaces are present in the storage VM:

   ```
   vserver nvme namespace show -vserver <storage_VM>
   ```

   If entries are displayed, the NVMe objects must be converted to LUNs or removed. See the `vserver nvme namespace delete` and the `vserver nvme subsystem delete` commands in the ONTAP command reference for more information.

2. Verify that there are no vVols present in the storage VM:

   ```
   lun show -verser <storage_VM> -class protocol-endpoint,vvol
   ```

   If any vVols are present, they should be copied to another storage VM and then deleted from the storage VM to be migrated. See the `lun copy` and `lun delete` commands in the ONTAP command reference for more information.

3. Verify that each volume in the storage VM contains a single LUN:

   ```
   lun show -verser <storage_VM>
   ```

   If a volume contains more than one LUN, use the `volume create` and `lun move` commands to create a 1:1 volume-to-LUN ratio. See the ONTAP command reference for more information.

What's next?

You are ready to create a cluster peer relationship between your ASA and ASA r2 clusters.

Step 2: Create a cluster peer relationship between your ASA and ASA r2 clusters

Before you can migrate a storage VM from an ASA cluster to an ASA r2 cluster, you need to create a peer relationship. A peer relationship defines network connections that enable ONTAP clusters and storage VMs to exchange data securely.

Before you begin

You must have created intercluster LIFs on every node in the clusters being peered using one of the following methods.

- Configure intercluster LIFs on shared data ports
- Configure intercluster LIFs on dedicated data ports
- Configure intercluster LIFs in custom IPspaces

Steps

1. On the ASA r2 cluster, create a peer relationship with the ASA cluster and generate a passphrase:

```
cluster peer create -peer-addrs <ASA_cluster_LIF_IPs> -generate
-passphrase
```

   The following example creates a cluster peer relationship between cluster 1 and cluster 2 and creates a system-generated passphrase:

```
cluster1::> cluster peer create -peer-addrs 10.98.191.193 -generate
-passphrase
Passphrase: UCa+6lRVICXeL/gq1WrK7ShR
            Peer Cluster Name: cluster2
            Initial Allowed Vserver Peers: -
            Expiration Time: 6/7/2017 09:16:10 +5:30
            Intercluster LIF IP: 10.140.106.185
Warning: make a note of the passphrase - it cannot be displayed again.
```

2. Copy the generated passphrase.
3. On the ASA cluster, create a peer relationship with the ASA r2 cluster:

```
cluster peer create -peer-addrs <ASA_r2_LIF_IPs>
```

4. Enter the passphrase generated on the ASA r2 cluster.
5. Verify that the cluster peer relationship is created:

```
cluster peer show
```

   The following example displays the expected output for successfully peered clusters.

```
cluster1::> cluster peer show

Peer Cluster Name   Cluster Serial Number   Availability
Authentication
-----------------   ---------------------   --------------
--------------
cluster2             1-80-123456             Available      ok
```

Result

The ASA and ASA r2 clusters are peered and storage VM data can be securely transferred.

What's next?

You are ready to prepare your ASA storage VM for migration.

Step 3: Prepare for storage VM migration from an ASA to an ASA r2 cluster

Before you migrate a storage virtual machine (VM) from an ASA cluster to an ASA r2 cluster, you must run a migration pre-check and fix any required issues. You cannot perform the migration until the pre-check passes successfully.

Step

1. From your ASA r2 cluster, execute the migration pre-check:

   ```
   vserver migrate start -vserver <storage_VM> -source-cluster
   <asa_cluster> -check-only true
   ```

   If you need to fix any issues to prepare your ASA cluster for migration, the issue and the corrective action is displayed. Fix the issue and repeat the pre-check until it completes successfully.

What's next?

You are ready to migrate your storage VM from your ASA cluster to an ASA r2 cluster.

Step 4: Migrate an ASA storage VM to an ASA r2 cluster

After you have prepared your ASA cluster and created the necessary cluster peer relationship with the ASA r2 cluster, you can begin the storage VM migration.

When performing a storage VM migration, it is a best practice to leave 30% CPU headroom on both the ASA cluster and the ASA r2 cluster to enable the CPU workload to execute.

About this task

After the storage VM migration, clients are automatically cut over to the ASA r2 cluster and the storage VM on the ASA cluster is automatically removed. Automatic cutover and automatic storage VM removal are enabled by default. You can optionally disable them both and perform the cutover and the storage VM removal manually.

Before you begin

- The ASA r2 cluster must have enough free space to hold the migrated storage VM.
- If the ASA storage VM contains encrypted volumes, the onboard key manager or the external key manager on the ASA r2 system must be configured at the cluster level.
- The following operations cannot be running on the source ASA cluster:
  - Failover operations
  - WAFLIRON
  - Fingerprint
  - Volume move, rehost, clone, create, convert or analytics

Steps

1. From the ASA r2 cluster, start the storage VM migration:

```
vserver migrate start -vserver <storage_VM_name> -source-cluster
<ASA_cluster>
```

To disable automatic cutover, use the `-auto-cutover false` parameter. To disable the automatic removal of the ASA storage VM, use the `-auto-source-cleanup false` parameter.

2. Monitor the status of the migration

```
vserver migrate show -vserver <storage_VM_name>
```

When the migration is complete, the **status** displays as **migration-complete**.

> If you need to pause or cancel the migration before automatic cutover begins, use the `vserver migrate pause` and the `vserver migrate abort` commands. You must pause the migration before cancelling it. You cannot cancel the migration after cutover starts.

Result

The storage VM is migrated from the ASA cluster to the ASA r2 cluster. The storage VM's name and UUID, the data LIF name, IP address, and object names, such as the volume name, remain unchanged. The UUID of the migrated objects in the storage VM are updated.

What's next?

If you disabled automatic cutover and automatic storage VM removal, manually cut over your ASA clients to your ASA r2 cluster and remove the storage VM from the ASA cluster.

Cutover clients and clean up source storage VM after migration to an ASA r2 system

After a storage virtual machine (VM) is migrated from an ASA cluster to an ASA r2 cluster, by default, clients are automatically cut over to the ASA r2 cluster and the storage VM on the ASA cluster is automatically removed. If you chose to disable automatic cutover and removal of the ASA storage VM during the migration, you need to perform these steps manually after the migration is complete.

Manually cut over clients to an ASA r2 system after a storage VM migration

If you disable automatic client cutover during the migration of a storage VM from an ASA cluster to an ASA r2 cluster, after the migration is successfully complete, perform the cutover manually so the ASA r2 storage VM can serve data to clients.

Steps

1. On the ASA r2 cluster, manually execute client cutover:

```
vserver migrate cutover -vserver <storage_VM_name>
```

2. Verify that the cutover operation is complete:

```
vserver migrate show
```

Result

Data is being served to your clients from the storage VM on your ASA r2 cluster.

What's next?

You are now ready to remove the storage VM from the source ASA cluster.

Manually remove an ASA storage VM after migration to an ASA r2 cluster

If you disable automatic source cleanup during the migration of a storage VM from an ASA cluster to an ASA r2 cluster, after the migration is complete, remove the storage VM from the ASA cluster to free the storage space.

Before you begin

Your clients should be serving data from the ASA r2 cluster.

Steps

1. From the ASA cluster, verify that the status of the ASA storage VM is **Ready for source cleanup**:

```
vserver migrate show
```

2. Remove the ASA storage VM:

```
vserver migrate source-cleanup -vserver <storage_VM_name>
```

Result

The storage VM on your ASA cluster is removed.

ASA r2 storage limits

For optimal performance, configuration and support, you should be aware ofASA r2 storage limits.

For a complete list of the most current ASA r2 storage limits, see NetApp Hardware Universe.

ASA r2 systems support the following storage limits:

	Maximum per HA pair	Maximum per cluster
Consistency groups	256	256
Enterprise applications	100	350
Nodes	2	12
Replication groups	50	50
Storage availability zone size	2 PB	2 PB

	Maximum per HA pair	Maximum per cluster
Storage units	10,000	30,000
Storage unit size	128 TB	128 TB
Storage units per consistency group	256	256
Child consistency groups per parent consistency group	64	64
Storage virtual machines	• 256 (ONTAP 9.18.1 and later) • 32 (ONTAP 9.17.1 and earlier)	• 256 (ONTAP 9.18.1 and later) • 32 (ONTAP 9.17.1 and earlier)
Virtual machines	800	1200

Limits for SnapMirror asynchronous relationships

The following limits apply to storage units and consistency groups in a SnapMirror asynchronous replication relationship. For a complete list of the most current ASA r2 storage limits, NetApp Hardware Universe.

Limit maximum	Per HA pair	Per cluster
Consistency groups	250	750
Storage units	4,000	6,000

Limits for SnapMirror active sync relationship

The following limits apply to storage units and consistency groups in a SnapMirror active sync replication relationship. SnapMirror active sync is supported beginning with ONTAP 9.17.1 on two-node clusters only. Beginning with ONTAP 9.18.1, SnapMirror active sync is supported on four-node clusters.

For a complete list of the most current ASA r2 storage limits, NetApp Hardware Universe.

Limit maximum	Per HA pair
Consistency groups	50
Storage units	400

Protect your data

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

Create a snapshot to back up data on your ASA r2 system. 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.

Beginning with ONTAP 9.18.1,you can set the snapshot reserve percentage and enable automatic snapshot deletion when creating a consistency group with new storage units. The snapshot reserve is the amount of space in the storage unit reserved specifically for snapshots. When snapshot reserve is set with automatic snapshot deletion, older snapshots are automatically deleted when space used by snapshots exceeds the snapshot reserve. If snapshot reserve and automatic snapshot deletion is enabled on a parent consistency group, it is enabled on all existing child consistency groups. If new child consistency groups are added they do not inherit the snapshot reserve and snapshot deletion settings of the parent.

Learn more about snapshot reserve on ASA r2 storage systems.

Beginning with ONTAP 9.16.1, you when you create consistency groups using new storage units, you can configure up to five child consistency group.
Learn more about child consistency groups on ASA r2 systems.

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 by default. You can optionally assign a different capacity to each unit.

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

Option	Steps
Assign a different capacity to each storage unit	Select **Add a different capacity**.
Change the default performance service level	Under **Performance service level**, select a different service level. ASA r2 systems offer two performance levels. The default performance level is **Extreme**, which is the highest available level. You can lower the performance level to **Performance**.
Modify the default snapshot reserve and enable automatic snapshot deletion	a. Under **Snapshot reserve %**, enter the numeric value for the percentage of the storage unit's space that you want allocated to snapshots. b. Select **Automatically delete older snapshots**.
Create a child consistency group	Select **Add child consistency group**.

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

What's next?

You have created a consistency group containing the storage units you want to protect. Now you can 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. Now you can

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

  You can create an on-demand snapshot of a storage unit 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	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	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.

Manage snapshot reserve

Learn about ONTAP snapshot reserve on ASA r2 storage

The snapshot reserve is the amount of space in the storage unit reserved specifically for snapshots. When snapshot reserve is set with automatic snapshot deletion, older snapshots are automatically deleted when space used by snapshots exceeds the snapshot reserve. This prevents snapshots from consuming space in your storage unit intended for user data.

Snapshot reserve is set as a percentage of the total storage unit size. For example, if the storage unit is 50 GB and you set the snapshot reserve to 10%, the amount of space reserved for snapshots is 5 GB. When the amount of space used by snapshots grows to 5 GB, older snapshots are automatically deleted to make room for new snapshots. If the storage unit size increases to 100 GB, then the snapshot reserve increases to 10 GB. The maximum snapshot reserve you can set is 200%. If your storage unit grows to the maximum size of 128 TB, a 200% snapshot reserve allows you to take 2 complete snapshots.

By default, snapshot reserve is set to 0% and snapshot auto-delete is not enabled.

Beginning with ONTAP 9.18.1, you can modify the default snapshot reserve during or after the creation of storage units and during the creation of consistency groups. You can also modify the default snapshot reserve on existing storage virtual machines (VMs). In ONTAP 9.17.1 and earlier, you cannot modify these settings.

Snapshot reserve is set to the same percentage for all storage units in a consistency group at the time the consistency group is created. Snapshot reserve must be individually set on any storage units added later.

Modify snapshot reserve on an ASA r2 storage system

The snapshot reserve is the amount of space in the storage unit reserved specifically for snapshots. By default, snapshot reserve is set to 0%. Beginning with ONTAP 9.18.1, you can modify the storage unit's default snapshot reserve and enable automatic snapshot deletion. Automatic deletion of snapshots is disabled by default. When a snapshot reserve value is set and automatic snapshot deletion is enabled, older snapshots are automatically deleted when space used by snapshots exceeds the snapshot reserve. This prevents snapshots from consuming space in your storage unit intended for user data.

Learn more about snapshot reserve on ASA r2 storage systems.

Modify snapshot reserve on storage units

To set different snapshot reserve values, configure each storage unit individually. To use the same value for all storage units, modify the snapshot reserve on the storage VM.

Steps

1. In System Manager, select **Storage**.
2. Hover over the name of the storage unit for which you want to set the snapshot reserve.
3. Select ⋮, then select **Edit**.
4. Under **Snapshot reserve %**, enter the numeric value for the percentage of the storage unit's space that you want allocated to snapshots.
5. Verify that **Automatically delete older snapshots** is selected.
6. Select **Save**.

Result

The snapshot reserve is set to the percentage you specified. If the amount of space consumed by snapshots reaches the reserve, older snapshots are automatically deleted.

Modify snapshot reserve on a storage VM

To set the same snapshot reserve for all storage units in a storage VM, apply the desired percentage to the storage VM. . When snapshot reserve is applied to the storage VM, it is applied to all newly created storage units within the storage VM. It is not applied to storage units created before you modified the setting.

Steps

1. In System Manager, select **Cluster > Storage VMs**; then select **Settings**.
2. Under **Policies**, next to **Snapshots**, select ⋮ ; then select **Set/edit snapshot reserve default**.
3. Under **Snapshot reserve %**, enter the numeric value for the percentage of the storage unit's space that you want allocated to snapshots.
4. Verify that **Automatically delete older snapshots** is selected.
5. Select **Save**.

Result

The snapshot reserve for newly created storage units is set to the percentage you specified. If the amount of space consumed by snapshots in those storage units reaches the reserve, older snapshots are automatically deleted.

Create an intercluster storage VM peer relationship on ASA r2 storage systems

A peer relationship defines network connections that enable clusters and storage virtual machine (VM) to exchange data securely. Create peer relationships between storage VMs on different clusters to enable data protection and disaster recovery using SnapMirror.

Learn more about peer relationships.

Before you begin

You must have established a cluster peer relationship between the local and remote clusters before you can create a storage VM peer relationship. Create a cluster peer relationship if you have not already done so.

Steps

1. In System Manager, select **Protection > Overview**.
2. Under **Storage VM peers** select **Add a storage VM peer**.
3. Select the storage VM on the local cluster; then select the storage VM on the remote cluster.
4. Select **Add a storage VM peer**.

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. 2. Search for and select the source consistency group. 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 . 2. Search for and select the source consistency group. 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.

Set up SnapMirror active sync

SnapMirror active sync setup workflow

ONTAP SnapMirror active sync data protection enables business services to continue operating even through a complete site failure, supporting applications to fail over transparently using a secondary copy. There is no manual intervention or custom scripting required to trigger a failover with SnapMirror active sync.

While the System Manager procedures for configuring SnapMirror active sync are different on ASA r2 systems than NetApp FAS, AFF, and ASA systems running the unified ONTAP personality, the requirements, architecture and operation of SnapMirror active sync is the same.

Learn more about ONTAP personalities.

> Beginning with ONTAP 9.18.1, SnapMirror active sync is supported on four-node configurations. In ONTAP 9.17.1, SnapMirror active sync is supported on two-node configurations only.

Learn more about SnapMirror active sync.

Learn more about disaster recovery with SnapMirror active sync on your ASA r2 system

On ASA r2 systems, SnapMirror active sync supports symmetric active/active configurations. In a symmetric active/active configuration, both sites can access local storage for active I/O.

Learn more about symmetric active/active configurations.

Prepare to configure SnapMirror active sync.

To prepare to configure SnapMirror active sync on your ASA r2 system you should review the configuration prerequisites, confirm support for your host operating systems, and be aware of object limits that might impact specific configuration.

Confirm your cluster configuration.

Before you configure SnapMirror active sync, you should confirm that your ASA r2 clusters are in the proper peering relationships and meet other configuration requirements.

Install ONTAP Mediator.

You can use ONTAP Mediator or ONTAP Cloud Mediator to monitor the health of your cluster and enable

business continuity. If you are using ONTAP Mediator, you must install it on your host. If you are using ONTAP Cloud Mediator, you can skip this step.

Configure ONTAP Mediator or ONTAP Cloud Mediator using self-signed certificates.

You must configure ONTAP mediator or ONTAP cloud mediator before you can begin using it with SnapMirror active sync for cluster monitoring.

Configure SnapMirror active sync.

Configure SnapMirror active sync to create a copy of your data at a secondary site and enable your host applications to automatically and transparently fail over in the event of a disaster.

Prepare to configure SnapMirror active sync on ASA r2 systems

To prepare to configure SnapMirror active sync on your ASA r2 system you should review the configuration prerequisites, confirm support for your hosts operating systems, and be aware of object limits that might impact specific configuration.

Steps

1. Review the SnapMirror active sync prerequisites.
2. Confirm that your host operating systems are supported for SnapMirror active sync.
3. Review the object limits that might impact your configuration.
4. Verify host protocol support for SnapMirror active sync on your ASA r2 system.

   Support for SnapMirror active sync on ASA r2 systems varies based upon ONTAP version and host protocol.

Beginning with ONTAP…	SnapMirror active sync supports…
9.17.1	• iSCSI • FC • NVMe/FC • NVMe/TCP
9.16.0	• iSCSI • FC

NVMe protocol limitations with SnapMirror active sync on ASA r2 systems

Before you configure SnapMirror active sync on an ASA r2 system with NVMe hosts, you should be aware of certain NVMe protocol limitations.

All NVMe storage units in the NVMe subsystem must be members of the same consistency group and must all be part of the same SnapMirror active sync relationship.

The NVMe/FC and NVMe/TCP protocols are supported with SnapMirror active sync as follows:

- Only on 2-node clusters
- Only on ESXi hosts
- Only with symmetric active/active configurations

  Asymmetric active/active configurations are not supported with NVMe hosts.

SnapMirror active sync with NVMe does not support the following:

- Subsystems mapped to more than one consistency group

  A consistency group can be mapped with multiple subsystems, but each subsystem can be mapped to only one consistency group.

- Expansion of consistency groups in a SnapMirror active sync relationship
- Mapping NVMe storage units that are not in a SnapMirror active sync relationship to replicated subsystems
- Removing a storage unit from a consistency group
- Consistency group geometry change
- Microsoft Offloaded Data Transfer (ODX)

What's next?

After you have completed the preparation necessary to enable SnapMirror active sync, you should confirm your cluster configuration.

Confirm your ASA r2 cluster configuration before configuring SnapMirror active sync

SnapMirror active sync relies on peered clusters to protect your data in the event of a failover. Before you configure SnapMirror active sync, you should confirm that your ASA r2 clusters are in a supported peering relationship and meet other configuration requirements.

Steps

1. Confirm that a cluster peering relationship exists between the clusters.

   > The default IPspace is required by SnapMirror active sync for cluster peer relationships. A custom IPspace isn't supported.

   Create a cluster peer relationship.

2. Confirm that a peer relationship exists between the storage virtual machines (VMs) on each cluster.

   Create an intercluster storage VM peer relationship.

3. Confirm that at least one LIF is created on each node in the cluster.

   Create a LIF.

4. Confirm that the necessary storage units are created and mapped to host groups.

   Create a storage unit and map the storage unit to a host group.

5. Rescan the application host to discover any new storage units.

What's next?

After you have confirmed your cluster configuration, you are ready to install ONTAP Mediator.

Install ONTAP Mediator on ASA r2 systems

To install ONTAP Mediator for your ASA r2 system, you should follow the same procedure used to install ONTAP Mediator for all other ONTAP systems.

Installing ONTAP Mediator includes preparing for installation, enabling access to repositories, downloading the ONTAP Mediator package, verifying the code signature, installing the package on the host and performing post-installation tasks.

To install ONTAP Mediator, follow this workflow

What's next

After ONTAP Mediator is installed you should configure ONTAP Mediator using self-signed certificates.

Configure ONTAP Mediator or ONTAP Cloud Mediatior on ASA r2 systems

You must configure ONTAP Mediator or ONTAP Cloud Mediator before you can begin using SnapMirror active sync for cluster monitoring. ONTAP Mediator and ONTAP Cloud Mediator both provide a persistent and fenced store for high availability (HA) metadata used by the ONTAP clusters in a SnapMirror active sync relationship. Additionally, both mediators provide a synchronous node health query functionality to aid in quorum determination and serves as a ping proxy for controller liveliness detection.

Before you begin

If you are using ONTAP Cloud Mediator, verify that your ASA r2 system meets the necessary prerequisites.

Steps

1. In System Manager, select **Protection > Overview**.
2. In the right pane under **Mediators**, select **Add a mediator**.
3. Select the **Mediator type**.
4. For a **Cloud** mediator enter the organization ID, client ID and client secret. For an **On-premises** mediator enter the IP address, port, mediator user name and mediator password.
5. Select the cluster peer from the list of eligible cluster peers or select **Add a cluster peer** to add a new one.
6. Add the certificate information
   - If you are using a self signed certificate, copy the content of the `intermediate.crt` file and paste it into the **Certificate** field, or select **Import** to navigate to the `intermediate.crt` file and import the certificate information.
   - If you are using a third-party certificate, enter the certificate information into the **Certificate** field.
7. Select **Add**.

What's next?

After you have initialized the mediator, you can configure SnapMirror active sync to create a copy of your data at a secondary site and enable your host applications to automatically and transparently failover in the event of

a disaster.

Configure SnapMirror active sync on ASA r2 systems

Configure SnapMirror active sync to create a copy of your data at a secondary site and enable your host applications to automatically and transparently failover in the event of a disaster.

On ASA r2 systems, SnapMirror active sync supports symmetric active/active configurations. In a symmetric active/active configuration, both sites can access local storage for active I/O.

If you are using the iSCSI or FC protocol and use ONTAP tools for VMware Sphere, you can optionally use ONTAP Tools for VM ware to configure SnapMirror active sync.

Before you begin

Create a consistency group on the primary site with new storage units. If you want to create a non-uniform symmetric active/active configuration, also create a consistency group on the secondary site with new storage units.

Learn more about non-uniform symmetric active/active configurations.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the name of the consistency group you want to protect with SnapMirror active sync.
3. Select and then select **Protect**.
4. Under **Remote protection**, select **Replicate to a remote cluster**.
5. Select an existing cluster peer or choose to **Add a new one**.
6. Select the storage VM.
7. For the replication policy, select **AutomatedFailOverDuplex**.
8. If you are creating a non-uniform symmetric active/active configuration, select **Destination settings**; then input the name of the new destination consistency group you create before beginning this procedure.
9. Select **Save**.

Result

SnapMirror active sync is configured to protect your data so that you can continue operations with near zero recovery point objective (RPO) and near zero recovery time objective (RTO) in the event of a disaster.

Manage SnapMirror active sync

Reconfigure ONTAP Mediator or ONTAP Cloud Mediator to use a third-party certificate on ASA r2 systems

If you configure ONTAP Mediator or ONTAP Cloud Mediator with a self-signed certificate, you can reconfigure the mediator to use a third-party certificate. Third party certificates might be preferred or required by your organization for security reasons.

Step 1: Remove the mediator configuration

To reconfigure the mediator, you must first remove its current configuration from the cluster.

Steps

1. In System Manager, select **Protection > Overview**.
2. In the right pane, under **Mediators**, select ⋮ next to the cluster peer with the mediator configuration that you want to remove; then select **Remove**.

   If you have multiple mediators installed, and you want to remove all configurations, select ⋮ next to **Mediators**; then select **Remove**.

3. Select **Remove** to confirm that you want to remove the mediator configuration.

Step 2: Remove the self-signed certificate

After the mediator configuration is removed, you should remove the associated self-signed certificate from the cluster.

Steps

1. Select **Cluster > Settings**.
2. Under **Security**, select **Certificates**.
3. Select the certificate that you want to remove.
4. Select ⋮; then select **Delete**.

Step 3: Reinstall the mediator with a third-party certificate

After you have removed the associated self-signed certificate, you can reconfigure the mediator with the third-party certificate.

Steps

1. Select **Protection > Overview**.
2. In the right pane, under **Mediators**, select **Add a mediator**.
3. Select the **Mediator type**.
4. For a **Cloud** mediator enter the organization ID, client ID and client secret. For an **On-premises** mediator enter the IP address, port, mediator user name, and mediator password.
5. Select a cluster peer from the list of eligible cluster peers or select **Add a cluster peer** to add a new one.
6. Under **Certificate**, enter the third-party certificate information.
7. Select **Add**.

Result

The ONTAP Mediator or ONTAP Cloud Mediator is reconfigured to use the third-party certificate. You can now use the mediator to manage SnapMirror active sync relationships.

Perform a planned failover of ASA r2 clusters in a SnapMirror active sync relationship

SnapMirror active sync offers continuous availability for business-critical applications by creating a copy of your data at a secondary site and enabling your host applications to automatically and transparently fail over in the event of a disaster. You might need to

perform a planned failover of your SnapMirror active sync relationship to test the failover process or to perform maintenance on the primary site.

Before you begin

- The SnapMirror active sync relationship must be in sync.
- You cannot initiate a planned failover when a nondisruptive operation, such as a storage unit move, is in process.
- ONTAP Mediator or ONTAP Cloud Mediator must be configured, connected, and in quorum.

Steps

1. Select **Protection > Replication**.
2. Select the SnapMirror active sync relationship you want to fail over.
3. Select ⋮; then select **Failover**.

What's next

Use the `snapmirror failover show` command in the ONTAP command line interface (CLI) to monitor the status of the failover.

Reestablish the SnapMirror active sync relationship after an unplanned failover of your ASA r2 clusters

On ASA r2 systems, SnapMirror active sync supports symmetric active/active configurations. In a symmetric active/active configuration both sites can access local storage for active I/O. If the source cluster fails or is isolated, the mediator triggers an automatic unplanned failover (AUFO) and serves all I/O from the destination cluster until the source cluster recovers.

If you experience an AUFO of your SnapMirror active sync relationship, you should reestablish the relationship and resume operations on the original source cluster after it comes back online.

Before you begin

- The SnapMirror active sync relationship must be in sync.
- You cannot initiate a planned failover when a nondisruptive operation, such as a storage unit move, is in process.
- The ONTAP Mediator must be configured, connected, and in quorum.
- To recover lost I/O paths or update I/O path states on your hosts, you need to perform a storage/adapter rescan on the hosts after the primary storage cluster resumes operation.

Steps

1. Select **Protection > Replication**.
2. Select the SnapMirror active sync relationship you need to reestablish.
3. Wait for the relationship status to display **InSync**.
4. Select ⋮; then select **Failover** to resume operations on the original primary cluster.

Delete a SnapMirror active sync relationship on your ASA r2 system

If you no longer require near zero RPO and RTO for a business application, you should remove SnapMirror active sync protection by deleting the associated SnapMirror active

sync relationship. If you are running ONTAP 9.16.1 on an ASA r2 system, you might also need to delete the SnapMirror active sync relationship before you can make certain geometry changes to consistency groups in a SnapMirror active sync relationship.

Step 1: Terminate host replication

If the host group from the source cluster is replicated to the destination cluster and destination consistency groups are mapped to the replicated host group, you must terminate host replication on the source cluster before you can delete the SnapMirror active sync relationship.

Steps

1. In System Manager, select **Host**.
2. Next to a host containing the host group you want to stop replicating, selet ⋮, and then select **Edit**.
3. Deselect **Replicate host configuration**, and then select **Update**.

Step 2: Delete the SnapMirror active sync relationship

To remove SnapMirror active sync protection from a consistency group, you must delete the SnapMirror active sync relationship.

Steps

1. In System Manager, select **Protection > Replication**.
2. Select **Local destinations** or **Local sources**.
3. Next to the SnapMirror active sync relationship that you want to remove, select ⋮; then select **Delete**.
4. Select **Release the source consistency group base snapshots**.
5. Select **Delete**.

Result

The SnapMirror active sync relationship is removed and the source consistency group base snapshots are released. The storage units in the consistency group are no longer protected by SnapMirror active sync.

What's next?

Set up snapshot replication to copy the consistency group to a geographically remote location for backup and disaster recovery.

Remove ONTAP Mediator or ONTAP Cloud Mediator from your ASA r2 system

You can use only one type of mediator at a time for SnapMirror active sync on your ASA r2 system. If you choose to change your mediator type, you must remove your current instance before you install another instance.

Steps

You must use the ONTAP command line interface (CLI) to remove ONTAP Mediator or ONTAP Cloud Mediator.

ONTAP Mediator

1. Remove ONTAP Mediator:

   ```
   snapmirror mediator remove -mediator-address <address> -peer-cluster
   <peerClusterName>
   ```

   Example:

   ```
   snapmirror mediator remove -mediator-address 12.345.678.90 -peer
   -cluster cluster_xyz
   ```

ONTAP Cloud Mediator

1. Remove ONTAP Cloud Mediator:

   ```
   snapmirror mediator remove -peer-cluster <peerClusterName> -type cloud
   ```

   Example:

   ```
   snapmirror mediator remove -peer-cluster cluster_xyz -type cloud
   ```

Related information

- snapmirror mediator remove

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 consistency groups

Learn about 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.

Beginning with ONTAP 9.16.1, you can use System Manager to create hierarchical consistency groups on your ASA r2 system. In an hierarchical structure, one or more consistency groups are configured as children under a parent consistency group.

Hierarchical consistency groups allow you to apply individual snapshot policies to each child consistency group and to replicate the snapshots of all the child consistency groups to a remote cluster as a single unit by replicating the parent. This simplifies data protection and management for complex data structures. For example, suppose you create a parent consistency group called `SVM1_app` which contains two child consistency groups: `SVM1app_data` for application data and `SVM1app_logs` for application logs. Snapshots of `SVM1app_data` are taken every 15 minutes and snapshots of `SVM1app_logs` are taken every hour. The parent consistency group, `SVM1_app`, has a SnapMirror policy that replicates the snapshots of both `SVM1app_data` and `SVM1app_logs` to a remote cluster every 24 hours. The parent consistency group `SVM1_app` is managed as a single unit and the child consistency groups are managed as separate units.

Consistency groups in replication relationships

Beginning with ONTAP 9.17.1, you can make the following geometry changes to consistency groups in an asynchronous replication relationship or in a SnapMirror active sync relationship without breaking or deleting the relationship. When a geometry change occurs on the primary consistency group, the change is replicated to the secondary consistency group.

- Modify the size of a storage unit by adding or removing storage units.
- Promote a single consistency group to a parent consistency group.
- Demote a parent consistency group to a single consistency group.
- Detach a child consistency group from a parent consistency group.
- Create a child consistency group using an existing consistency group.

In ONTAP 9.16.1, you must break the asynchronous replication relationship and delete the SnapMirror active sync relationship before making geometry changes to the consistency group.

Protect consistency groups on your ASA r2 system with snapshots

Create snapshots of the consistency groups in your ASA r2 storage system to protect the data in the storage units that are part of the consistency group. If you no longer need to protect the data in any of the storage units in the consistency group, you can remove snapshot protection from the consistency group.

If you no longer need to protect the data from specific storage units in the consistency group, you can remove

those storage units from the consistency group.

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	a. Select + Add ; then enter the new policy name. b. Select the policy scope. c. Under **Schedules** select + Add . d. Select the name that appears under **Schedule name**; then select ⌄. e. Select the policy schedule. f. Under **Maximum snapshots**, enter the maximum number of snapshots that you want to retain of the consistency group. g. Optionally, under **SnapMirror label** enter a SnapMirror label. h. Select **Save**.

6. 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.

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.

Modify the size of consistency groups on your ASA r2 system

Increase or decrease the size of a consistency group by modifying the number of 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 new or existing storage units to the consistency group.

Beginning with ONTAP 9.18.1, you can set snapshot reserve and automatic snapshot deletion to limit the amount of space used by snapshots in your storage units. When you add a storage unit to an existing consistency group, snapshot reserve and automatic snapshot deletion are set as follows by default.

If you add…	The snapshot reserve percentage is set to…	Automatic snapshot deletion is…
New storage units	0	Disabled
Existing storage units	Unchanged	Unchanged

You can modify the default settings for new storage units when you create the storage units. You can also modify existing storage units to update their current settings.

Learn more about snapshot reserve on ASA r2 storage systems.

Before you begin

If you are running ONTAP 9.16.1 and the consistency group you want to expand is in an SnapMirror active sync relationship, you must delete the SnapMirror active sync relationship before you can add storage units. If you are running ONTAP 9.16.1 and the consistency group is in an asynchronous replication relationship, you must break the relationship before you can expand the consistency group. Deleting the SnapMirror active sync relationship or breaking the asynchronous relationship before expanding a consistency group is not required in ONTAP 9.17.1 and later releases.

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 hosts 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

Remove a storage unit from a consistency group to delete it, manage it as part of a different consistency group, or stop protecting its data. 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 consistency groups on your ASA r2 system

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. If the consistency group was in a replication relationship, the replicated copies remain on the remote cluster.

Before you begin

If you are running ONTAP 9.16.1, and the consistency group you want to delete is in a SnapMirror active sync relationship, you must delete the SnapMirror active sync relationship before you delete the consistency group. Deleting this relationship before modifying a consistency group is not required in ONTAP 9.17.1 and later releases.

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 hierarchical consistency groups on your ASA r2 system

Beginning with ONTAP 9.16.1, you can use System Manager to create hierarchical consistency groups on your ASA r2 system. In an hierarchical structure, one or more consistency groups are configured as children under a parent consistency group. You can apply individual snapshot policies to each child consistency group and replicate the snapshots of all the child consistency groups to a remote cluster as a single unit by replicating the parent. This simplifies data protection and management for complex data structures.

Promote an existing consistency group into a parent consistency group

If you promote an existing consistency group to a parent, a new child consistency group is created and the storage units belonging to the promoted consistency group are moved to the new child consistency group. Storage units cannot be directly associated with a parent consistency group.

Before you begin

If you are running ONTAP 9.16.1 and the consistency group you want to promote is in a SnapMirror active sync relationship, you must delete the SnapMirror active sync relationship before the consistency group can be promoted. If you are running ONTAP 9.16.1 and the consistency group is in an asynchronous replication relationship, you must break the relationship before you can promote the consistency group. Deleting the

SnapMirror active sync relationship or breaking the asynchronous relationship before promoting a consistency group is not required in ONTAP 9.17.1 and later releases.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the consistency group you want convert into a parent consistency group.
3. Select ⋮; then select **Promote to parent consistency group**.
4. Enter a name for the new child consistency group or accept the default name; then select the consistency group component type.
5. Select **Promote**.

What's next?

You can create additional child consistency groups under the parent consistency group. You can also set up snapshot replication to copy the parent and child consistency groups to a geographically remote location for backup and disaster recovery.

Demote a parent consistency group to a single consistency group

When you demote a parent consistency group to a single consistency group, the storage units of the associated child consistency groups are added to the parent consistency group. The child consistency groups are deleted and the parent is then managed as a single consistency group.

Before you begin

If you are running ONTAP 9.16.1 and the consistency group you want to demote is in a SnapMirror active sync relationship, you must delete the SnapMirror active sync relationship before the consistency group can be demoted. If you are running ONTAP 9.16.1 and the consistency group is in an asynchronous replication relationship, you must break the relationship before you can demote the consistency group. Deleting the SnapMirror active sync relationship or breaking the asynchronous relationship before expanding a consistency group is not required in ONTAP 9.17.1 and later releases.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the parent consistency group you want to demote.
3. Select ⋮; then select **Demote to a single consistency group**.
4. Select **Demote**

What's next?

Add a snapshot policy to the demoted consistency group to protect the storage units that were previously managed by the child consistency groups.

Create a child consistency group

Creating child consistency groups allows you to apply individual snapshot policies to each child. Beginning with ONTAP 9.17.1, you can also apply individual replication policies directly to each child. In ONTAP 9.16.1, replication policies can be applied only at the parent level.

You can create a child consistency group from a new or existing consistency group.

From a new consistency group

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Hover over the parent consistency group you want to add a child consistency group to.
3. Select ⋮; then select **Add a new child consistency group**.
4. Enter a name for the child consistency group or accept the default name; then select the consistency group component type.
5. Select to add existing storage units to the child consistency group or to create new storage units.

   If you create new storage units, enter the number of units you want to create and the capacity per unit; then enter the host information.

   If you create more than one storage 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**.

6. Select **Add**.

From an existing consistency group

Before you begin

If the consistency group you would like to use is already the child of another consistency group, you must detach it from the existing parent consistency group before you can move it to a new parent consistency group.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select the existing consistency group that you would like to make a child consistency group.
3. Select ⋮; then select **Move under different consistency group**.
4. Enter a new name for the child consistency group or accept the default name; then select the consistency group component type.
5. Select the existing consistency group that you would like to make the parent consistency group or select to create a new parent consistency group.

   If you select to create a new parent consistency group, enter a name for the parent consistency group or accept the default name; then select the consistency application component type.

6. Select **Move**.

What's next

After you create a child consistency group, you can apply individual snapshot protection policies to each child consistency group. You can also set up replication policies on the parent and child consistency groups to replicate the consistency groups to a remote location.

Detach a child consistency group from a parent consistency group

When you detach a child consistency group from a parent consistency group, the child consistency group is removed from the parent consistency group and is managed as a single consistency group. The replication policy applied to the parent is no longer applied to the detached child consistency group.

Before you begin

If you are running ONTAP 9.16.1 and the consistency group you want to detach is in a SnapMirror active sync relationship, you must delete the SnapMirror active sync relationship before the consistency group can be detached. If you are running ONTAP 9.16.1 and the consistency group is in an asynchronous replication relationship, you must break the relationship before you can detach the consistency group. Deleting the SnapMirror active sync relationship or breaking the asynchronous relationship before expanding a consistency group is not required in ONTAP 9.17.1 and later releases.

Steps

1. In System Manager, select **Protection > Consistency groups**.
2. Select the parent consistency group.
3. Select over the child consistency group you want to detach.
4. Select ⋮; then select **Detach from parent**.
5. Enter a new name for the consistency group you are detaching or accept the default name; then select the consistency group application type.
6. Select **Detach**.

What's next?

Set up a replication policy to replicate the snapshots of the detached child consistency group to a remote cluster.

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 + Add.
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.

ⓘ In ASA r2 systems, SEDs are supported only for NVMe based SSD's.

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	a. Select **Onboard Key Manager** to add the key servers. b. Enter a passphrase.

Option	Steps
Configure an external key manager	a. Select **External key manager** to add the key servers. b. Select + Add to add the key servers. c. Add the KMIP server CA certificates. d. Add the KMIP client certificates.

4. Select **Dual-layer encryption** to enable software encryption.
5. 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.

Migrate ONTAP data encryption keys between key managers on your ASA r2 system

You can manage your data encryption keys using either the ONTAP onboard key manager on your ASA r2 system or an external key manager (or both). External key managers can only be enabled at the storage VM level. At the ONTAP cluster level, you can enable either the onboard key manager or an external key manager.

If you enable your key manager at the…	You can use…
Cluster level only	Either the onboard key manager or an external key manager
Storage VM level only	An external key manager only
Both the cluster and storage VM level	One of the following key manager combinations: • Option 1 Cluster level: Onboard key manager Storage VM level: External key manager • Option 2 Cluster level: External key manager Storage VM level: External key manager

Migrate keys between key managers at the ONTAP cluster level

Beginning with ONTAP 9.16.1 you can use the ONTAP command line interface (CLI) to migrate keys between key managers at the cluster level.

From onboard to external

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Create an inactive external key manager configuration:

```
security key-manager external create-config
```

3. Switch to the external key manager:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type KMIP
```

4. Delete the onboard key manager configuration:

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type OKM
```

5. Set the privilege level to admin:

```
set -privilege admin
```

From external to onboard

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Create an inactive onboard key manager configuration:

```
security key-manager onboard create-config
```

3. Enable the onboard key manager configuration:

```
security key-manager keystore enable -vserver <storage_vm_name>
-type OKM
```

4. Delete the external key manger configuration

```
security key-manager keystore delete-config -vserver
<storage_vm_name> -type KMIP
```

5. Set the privilege level to admin:

```
set -privilege admin
```

Migrate keys between key managers across ONTAP cluster and storage VM levels

You can use the ONTAP command line interface (CLI) to migrate keys between the key manager at the cluster level and a key manager at the storage VM level.

Steps

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Migrate the keys:

```
security key-manager key migrate -from-vserver <storage_vm_name> -to
-vserver <storage_vm_name>
```

3. Set the privilege level to admin:

```
set -privilege admin
```

Protect against ransomware attacks

Create tamper-proof snapshots to 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

1. Select **Cluster > Overview**.
2. In the **Nodes** section, select **Initialize SnapLock Compliance Clock**.
3. Select **Initialize**.
4. Verify that the compliance clock is initialized.
   a. Select **Cluster > Overview**.
   b. 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.

Enable autonomous ransomware protection with AI on your ASA r2 storage systems

Beginning with ONTAP 9.17.1, you can use Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) to protect the data on your ASA r2 system. ARP/AI quickly detects potential ransomware threats, automatically creates an ARP snapshot to protect your data, and displays a warning message in System Manager to alert you of suspicious activity.

ARP improves cyber resiliency by adopting a machine-learning model for anti-ransomware analytics that detects constantly evolving forms of ransomware with 98% accuracy for SAN environments. ARP's machine-learning model is pre-trained on a large dataset of files both before and after a simulated ransomware attack. This resource-intensive training is done outside ONTAP, and the pre-trained model that results from this training is included on-box with ONTAP. This model is not accessible or modifiable. ARP/AI is active immediately after enablement; there is no learning period.

> No ransomware detection or prevention system can completely guarantee safety from a ransomware attack. Although an attack might go undetected, ARP/AI acts as an important additional layer of defense if anti-virus software fails to detect an intrusion.

About this task

- ARP/AI support is included with the ONTAP One license.
- ARP/AI is not supported on storage units protected by SnapMirror active sync, SnapMirror synchronous or SnapLock.
- Beginning with ONTAP 9.18.1, ARP/AI is enabled by default on all newly created storage units 12 hours after upgrading to ONTAP 9.18.1 or initializing a new ONTAP 9.18.1 ASA r2 cluster.
- After you have enabled ARP/AI, you should enable automatic updates for your security files to automatically receive new security updates.

Enable ARP/AI on all storage units in the cluster

If you are running ONTAP 9.17.1, you can enable ARP/AI on all storage units created in the cluster by default.

In ONTAP 9.18.1 and later, ARP/AI is enabled by default on all new storage units. If you have storage units created in ONTAP 9.17.1 for which ARP/AI is not enabled, you can enable it manually.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Anti-ransomware**, select ⋮ and then select **Enable on all existing storage units**.
3. Select **Enable**.

Enable ARP/AI on all storage units in a storage VM

If you are running ONTAP 9.17.1, you can enable ARP/AI on all storage units created in a storage virtual machine (VM) by default. This means that any new storage units created in the storage VM will have ARP/AI enabled automatically. You can also apply ARP/AI to existing storage units in the storage VM.

In ONTAP 9.18.1 and later, ARP/AI is enabled by default on all new storage units. If you have storage units created in ONTAP 9.17.1 for which ARP/AI is not enabled, you can enable it manually.

Steps

1. In System Manager, select **Cluster > Storage VMs**.
2. Select the storage VM on which you want to enable ARP/AI.
3. In the **Security** section, next to **Anti-ransomware**, select ⋮; then select **Edit anti-ransomware settings**.
4. Select **Enable anti-ransomware**.

   This enables ARP/AI on all future storage units created on the selected storage VM by default.

5. To apply ARP to existing storage units on the selected storage VM, select **Apply this change to all applicable existing storage units on this storage VM**.
6. Select **Save**.

Result

All new storage units you create on the storage VM are protected against ransomware attacks by default, and suspicious activity is reported to you in System Manager.

Enable ARP/AI on specific storage units in a storage VM

If you are running ONTAP 9.17.1, and you do not want ARP/AI enabled on all the storage units in an storage VM, you can select the specific units you want enabled.

In ONTAP 9.18.1 and later, ARP/AI is enabled by default on all new storage units. If you have storage units created in ONTAP 9.17.1 for which ARP/AI is not enabled, you can enable it manually.

Steps

1. In System Manager, select **Storage**.
2. Select the storage units for which you want to enable ARP/AI.
3. Select ⋮; then select **Enable anti-ransomware**.
4. Select **Enable**.

Result

The storage units you selected are protected against ransomware attacks, and suspicious activity is reported to you in System Manager.

Disable default autonomous ransomware protection on your ASA r2 storage systems

When you initialize a new ONTAP 9.18.1 ASA r2 cluster or upgrade your cluster to ONTAP 9.18.1, ARP/AI is automatically enabled by default on all new storage units after a 12-hour grace period. If you don't disable ARP/AI during the grace period, it is enabled cluster-wide for new storage units when the grace period ends.

Storage units created in ONTAP 9.17.1 must be manually enabled for ARP/AI.

Steps

You can disable the default enablement during or after the initial 12-hour grace period.

System Manager

1. Select **Cluster > Settings**.
2. Disable ARP:
   - To disable during the 12-hour grace period:
     a. Under **Anti-ransomware**, select **Don't enable** and then select **Disable**.
   - To disable after the 12-hour grace period:
     a. Under **Anti-ransomware**, select  and then deselect **Enable for new storage units**.
     b. Select **Save**

CLI

1. Check the default enablement status:

```
security anti-ransomware auto-enable show
```

2. Disable default enablement for existing and new volumes:

```
security anti-ransomware auto-enable modify -default-existing-volume
-state false -default-new-volume-state false
```

Modify ARP/AI snapshot retention periods on ASA r2 storage systems

If Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) detects abnormal activity on one or more of your ASA r2 system storage units, it automatically creates an ARP snapshot to protect the storage unit's data. Depending upon your storage capacity and the business requirements for your data, you might want to increase or decrease the default ARP snapshot retention period. For example, you might want to increase the retention period for business critical applications so that, if needed, you have longer retention periods for data recovery, or you might want to decrease the retention period for non-critical applications to save storage space.

The default retention period for the ARP snapshot varies depending on the action you take in response to the

abnormal activity.

If you take this action…	ARP snapshots are retained by default for…
Mark as false positive	12 hours
Mark as potential ransomware attack	7 days
Do not take immediate action	10 days

The default retention periods can be modified using the ONTAP command line interface (CLI). See Modify options for ONTAP automatic snapshots for steps to change the default retention period.

Respond to autonomous ransomware protection with AI alerts on ASA r2 storage systems

If Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) detects abnormal activity on one or more of your ASA r2 system storage units, a warning is generated on the System Manager dashboard. You should view the warning, verify the activity and, if necessary, take action to stop any potential threat to your data.

If an ARP/AI warning message is displayed, before you take action, you should use the appropriate application integrity checker to verify the integrity of the data on the storage unit. Verifying the storage unit's data integrity helps you determine if the activity is acceptable or if it is a potential ransomware attack.

If the abnormal activity is …	Then do this…
Acceptable	Mark the activity as a false positive.
A potential ransomware attack	Mark the activity as a potential ransomware attack.
Indeterminate	Do not take immediate action. Monitor the storage unit to for up to 7 days. If the storage unit continues to operate normally, mark the activity as a false positive. If the storage unit continues to exhibit abnormal activity, mark the activity as a potential ransomware attack.

Steps

1. In System Manager, select **Dashboard**.

   If ARP has detected abnormal activity on one or more storage units, a message appears under **Warnings**.

2. Select the warning message.
3. Under **Events overview**, select the **Warnings** message that indicates the number of storage units with abnormal activity.
4. Under **Storage units with abnormal activity**, select the storage unit.
5. Select **Security**.

   If there is abnormal activity on the storage unit, a message is displayed under **Anti-ransomware**.

6. Select **Choose an action**.
7. Select **Mark as false positive** or select **Mark as potential ransomware attack**.

What's next?

If you know of surges in your storage unit activity, either one-time surges or a surge that is characteristic of a new normal, you should report them as safe. Manually reporting these surges as safe helps to improve the accuracy of ARP's threat assessments. Learn how to report known ARP/AI surges.

Pause or resume autonomous ransomware protection with AI on your ASA r2 storage systems

Beginning with ONTAP 9.17.1, you can use Autonomous Ransomware Protection with Artificial Intelligence (ARP/AI) to protect the data on your ASA r2 system. If you are planning an unusual workload event, you can temporarily suspend ARP/AI analysis to prevent false positive detections of ransomware attacks. After your workload event is complete, you can resume ARP/AI analysis.

Pause ARP/AI

Before you begin an unusual workload event, you might need to temporarily suspend the ARP/AI analysis to prevent false positive detections of ransomware attacks.

Steps

1. In System Manager, select **Storage**.
2. Select the storage units for which you want to pause ARP/AI.
3. Select **Pause anti-ransomware**.

Result

ARP/AI analysis is paused for the selected storage units, and no suspicious activity is reported to you in System Manager until you resume ARP/AI.

Resume ARP/AI

If you pause ARP/AI during an unusual workload, after your workload is complete, you should resume it to protect your data against ransomware attacks.

Steps

1. In System Manager, select **Storage**.
2. Select the storage units for which you want to resume ARP/AI.
3. Select **Resume anti-ransomware**.

Result

Analysis of potential ransomware attacks is resumed, and suspicious activity is reported to you in System Manager.

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 + Add .
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.

Secure IP connections on your ASA r2 storage systems

If you are using the IP protocol on your ASA r2 system, you can configure IP security (IPsec) to enhance your data security. IPsec is an internet standard that provides data-in-flight encryption, authentication for the traffic flowing between the network endpoints at an IP level, and protection against replay and malicious man-in-the-middle attacks on your data.

For ASA r2 systems, IPsec is available for iSCSI and NVMe/TCP hosts.

On certain ASA r2 systems, several of the cryptographic operations, such as encryption and integrity checks, can be offloaded to a supported network interface controller (NIC) card. The throughput for operations offloaded to the NIC card is approximately 5% or less. This can significantly improve the performance and throughput of the network traffic protected by IPsec.

Beginning with ONTAP 9.18.1, IPsec hardware offload supported is extended to IPv6 traffic.

The following NIC cards are supported for hardware offload on the following ASA r2 systems and ONTAP versions:

Supported NIC card	ASA r2 systems	ONTAP Version
X50135A (2p, 40G/100G Ethernet Controller)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.17.1 and later
X60135A (2p, 40G/100G Ethernet Controller)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.17.1 and later

Supported NIC card	ASA r2 systems	ONTAP Version
X50131A - (2p, 40G/100G/200G/400G Ethernet Controller)	• ASA A1K • ASA A90 • ASA A70	ONTAP 9.16.1 and later
X60132A - (4p, 10G/25G Ethernet Controller)	• ASA A50 • ASA A30 • ASA A20	ONTAP 9.16.1 and later

See the NetApp Hardware Universe for more information about the supported systems and cards.

What's next?

IPsec is configured on your ASA r2 system the same way as on other ONTAP systems. For more information, see Prepare to configure IP security for the ONTAP network.

Copyright information

Trademark information