ASA r2 documentation

ASA r2

NetApp
September 26, 2024

Table of Contents

ASA r2 documentation

Release notes

What's new in ONTAP 9.16.0 for ASA r2 systems

Learn about the new capabilities available in ONTAP 9.16.0 for ASA r2 systems.

Platforms

Update	Description
New platforms	The following new NetApp ASA r2 systems are available. These platforms deliver a unified hardware and software solution that creates a simplified experience specific to the needs of SAN-only customers. • ASA A1K • ASA A70 • ASA A90

System Manager

Update	Description
Streamlined support for SAN-only customers	System Manager is streamlined to provide support for essential SAN functionality while removing visibility of features and functions not supported in SAN environments.

Storage management

Update	Description
Simplified storage management	ASA r2 systems introduce the use of storage units with consistency groups for simplified storage management. • 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. • *A consistency group* is a collection of storage units that are managed as a single unit.

Data security

Update	Description
Onboard key manager and dual-layer encryption	ASA r2 systems support an onboard key manager and dual-layer (hardware and software) encryption.

Get started

Learn about ASA r2 storage systems

The new NetApp ASA r2 systems (ASA A1K, ASA A70, and ASA A90) deliver a unified hardware and software solution that creates a simplified experience specific to the needs of SAN-only customers.

ASA r2 systems support all SAN protocols (iSCSI, FC, NVMe/FC, NVMe/TCP) on a single HA-pair deployment. SCSI (iSCSI and FC) protocols use a symmetric active-active architecture for multipathing so that all paths between the hosts and storage are active/optimized. NVMe protocols support direct paths between the hosts and storage.

On an ASA r2 system, ONTAP software and System Manager are streamlined to provide support for essential SAN functionality while removing features and functions not supported in SAN environments.

ASA r2 systems introduce the use of storage units with consistency groups:

- 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.
- *A consistency group* is a collection of storage units that are managed as a single unit.

ASA r2 systems use storage units and consistency groups to simplify storage management and data protection. 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 individually, you can protect the entire database by backing up the consistency group.

To help secure your data against malicious attacks such as theft or ransomware, ASA r2 systems support an on-board key manager, dual-layer encryption, tamper-proof snapshots, multi-factor authentication and multi-admin verification.

ASA r2 systems do not support cluster mixing with current ASA, AFF, or FAS systems.

For more information

- Learn more about ASA r2 systems support and limitations in the NetApp Hardware Universe.
- Learn more about the new ASA r2 systems in comparison to the ASA systems.
- Learn more about the NetApp ASA.

Quick start for ASA r2 storage sytems

To get up and running with your ASA r2 system, you install your hardware components, set up your cluster, set up data access from your hosts to the storage system, and provision your storage.

Install and set up your hardware

Install and set up your ASA r2 system and deploy it as an HA pair in your ONTAP environment.

Set up your cluster

Use System Manager to guide you through a quick and easy process to set up your ONTAP cluster.

Set up data access

Connect your ASA r2 system to your SAN clients.

Provision your storage

Provision storage to begin serving data to your SAN clients.

What's next?

You can now use System Manager to protect your data by creating snapshots.

Install your ASA r2 system

Installation and setup workflow for ASA r2 storage systems

To install and configure your ASA r2 system, you review the hardware requirements, prepare your site, install and cable the hardware components, power on the system, and set up your ONTAP cluster.

Review the hardware installation requirements

Review the hardware requirements to install your ASA r2 storage system.

Prepare to install the ASA r2 storage system

To prepare to install your ASA r2 system, you need to get the site ready, check the environmental and electrical requirements, and ensure there's enough rack space. Then, unpack the equipment, compare its contents to the packing slip, and register the hardware to access support benefits.

Install the hardware for the ASA r2 storage system

To install the hardware, install the rail kits for your storage system and shelves, and then install and secure your storage system in the cabinet or telco rack. Next, slide the shelves onto the rails. Finally, attach cable management devices to the rear of the storage system for organized cable routing.

Cable the controllers and storage shelves for the ASA r2 storage system

To cable the hardware, first connect the storage controllers to your network and then connect the controllers to your storage shelves.

Power on the ASA r2 storage system

Before you power on the controllers, power on each NS224 shelf and assign a unique shelf ID to ensure each shelf is uniquely identified within the setup.

Installation requirements for ASA r2 storage systems

Review the equipment needed and the lifting precautions for your ASA r2 storage system and storage shelves.

Equipment needed for install

To install your ASA r2 storage system, you need the following equipment and tools.

- Access to a Web browser to configure your storage system
- Electrostatic discharge (ESD) strap
- Flashlight
- Laptop or console with a USB/serial connection
- Paperclip or narrow tipped ball point pen for setting NS224 storage shelf IDs
- Phillips #2 screwdriver

Lifting precautions

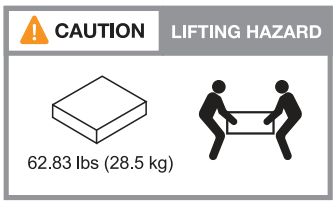
ASA r2 storage systems and NS224 storage shelves are heavy. Exercise caution when lifting and moving these items.

Storage system weights

Take the necessary precautions when moving or lifting your ASA r2 storage system.

ASA A1K

An ASA A1K storage system can weigh up to 62.83 lbs (28.5 kg). To lift the system, use two people or a hydraulic lift.

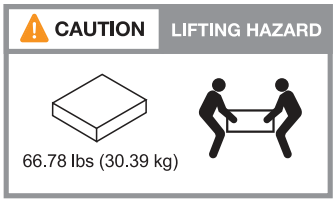


ASA A70 and ASA A90

An ASA A70 storage system or an ASA A90 storage system can weigh up to 151.68 lbs (68.8 kg). To lift the system, use four people or a hydraulic lift.

Storage shelf weight

An NS224 storage shelf can weigh up to 66.78 lbs (30.29 kg). To lift the storage shelf, use two people or a hydraulic lift. Keep all components in the storage shelf (both front and rear) to prevent unbalancing the shelf weight.



Related information

- Safety information and regulatory notices

What's next?

After you've reviewed the hardware requirements, you prepare to install your ASA r2 storage system.

Prepare to install an ASA r2 storage system

Prepare to install your ASA r2 storage system by getting the site ready, unpacking the boxes and comparing the contents of the boxes to the packing slip, and registering the system to access support benefits.

Step 1: Prepare the site

To install your ASA r2 storage system, ensure that the site and the cabinet or rack that you plan to use meet specifications for your configuration.

Steps

1. Use NetApp Hardware Universe to confirm that your site meets the environmental and electrical requirements for your ASA r2 storage system.
2. Make sure you have adequate rack space:
   - 4U in an HA configuration for the storage system
   - 2U for each NS224 storage shelf
3. Install any required network switches.

   See the Switch documentation for installation instructions and NetApp Hardware Universe for compatibility information.

Step 2: Unpack the boxes

After you've ensured that the site and the cabinet or rack that you plan to use for your ASA r2 storage system meet the required specifications, unpack all boxes and compare the contents to the items on the packing slip.

Steps

1. Carefully open all the boxes and lay out the contents in an organized manner.
2. Compare the contents you've unpacked with the list on the packing slip.

   You can get your packing list by scanning the QR code on the side of the shipping carton.

   The following items are some of the contents you might see in the boxes.

   Ensure that everything in the boxes matches the list on the packing slip. If there are any discrepancies, note them down for further action.

Hardware

- Bezel
- Cable management device
- Storage system
- Rail kits with instructions (optional)
- Storage shelf

Cables

- Management Ethernet cables (RJ-45 cables)
- Network cables
- Power cords
- Storage cables (if you ordered additional storage)
- USB-C serial port cable

Step 3: Register your storage system

After you've ensured that your site meets the requirements for your ASA r2 storage system specifications, and you've verified that you have all the parts you ordered, you should register your system.

Steps

1. Locate the serial number for your storage system.

   You can find the number on the packing slip, in your confirmation email, or on the controller's System Management module after you unpack it.

2. Go to the NetApp Support Site.
3. Determine whether you need to register your storage system:

If you are a…	Follow these steps…
Existing NetApp customer	a. Sign in with your username and password. b. Select **Systems** > **My Systems**. c. Confirm that the new serial number is listed. d. If it is not, follow the instructions for new NetApp customers.
New NetApp customer	a. Click **Register Now**, and create an account. b. Select **Systems** > **Register Systems**. c. Enter the storage system's serial number and requested details. After your registration is approved, you can download any required software. The approval process might take up to 24 hours.

What's next?

After you've prepared to install your ASA r2 hardware, you install the hardware for your ASA r2 storage system.

Install your ASA r2 storage system

After you prepare to install your ASA r2 storage system, install the hardware for the system. First, install the rail kits. Then install and secure your storage system in a cabinet or telco rack.

Before you begin

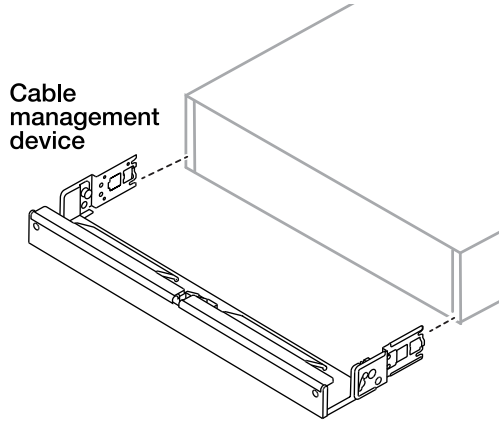
- Make sure you have the instructions packaged with the rail kit.
- Be aware of the safety concerns associated with the weight of the storage system and storage shelf.
- Understand that the airflow through the storage system enters from the front where the bezel or end caps are installed and exhausts out the rear where the ports are located.

Steps

1. Install the rail kits for your storage system and storage shelves, as needed, using the instructions included with the kits.
2. Install and secure your storage system in the cabinet or telco rack:
   a. Position the storage system onto the rails in the middle of the cabinet or telco rack, and then support the storage system from the bottom and slide it into place.
   b. Secure the storage system to the cabinet or telco rack using the included mounting screws.
3. Install the storage shelf:
   a. Position the back of the storage shelf onto the rails, and then support the shelf from the bottom and slide it into the cabinet or telco rack.

      If you are installing multiple storage shelves, place the first storage shelf directly above the controllers. Place the second storage shelf directly under the controllers. Repeat this pattern for any additional storage shelves.

   b. Secure the storage shelf to the cabinet or telco rack using the included mounting screws.
4. Attach the cable management devices to the rear of the storage system.



5. Attach the bezel to the front of the storage system.

What's next?

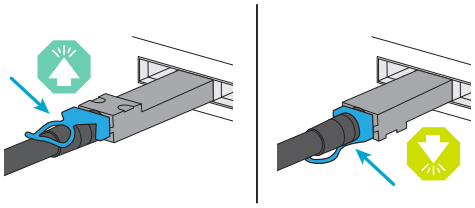
After you've installed the hardware for your ASA r2 system, you cable the controllers and storage shelves for your ASA r2 system.

Cable the hardware for your ASA r2 storage system

After you install the rack hardware for your ASA r2 storage system, install the network cables for the controllers, and connect the cables between the controllers and storage shelves.

Before you begin

Check the illustration arrow in the cabling diagrams for the proper cable connector pull-tab orientation.



- As you insert the connector, you should feel it click into place; if you do not feel it click, remove it, turn the cable head over and try again.
- If connecting to an optical switch, insert the small form-factor pluggable (SFP) transceiver into the controller port before cabling to the port.

Step 1: Connect the storage controllers to your network

Connect your controllers directly to each other and to your host network.

Before you begin

Contact your network administrator for information about connecting your storage system to the host network switches.

About this task

These procedures show common configurations. The specific cabling depends on the components ordered for your storage system. For comprehensive configuration and slot priority details, see NetApp Hardware Universe.

ASA A1K

Connect your storage controllers to each other to create the ONTAP cluster connections, and then connect the Ethernet ports on each controller to your host network.

Steps

1. Use the Cluster/HA interconnect cable to connect ports e1a to e1a and ports e7a to e7a.

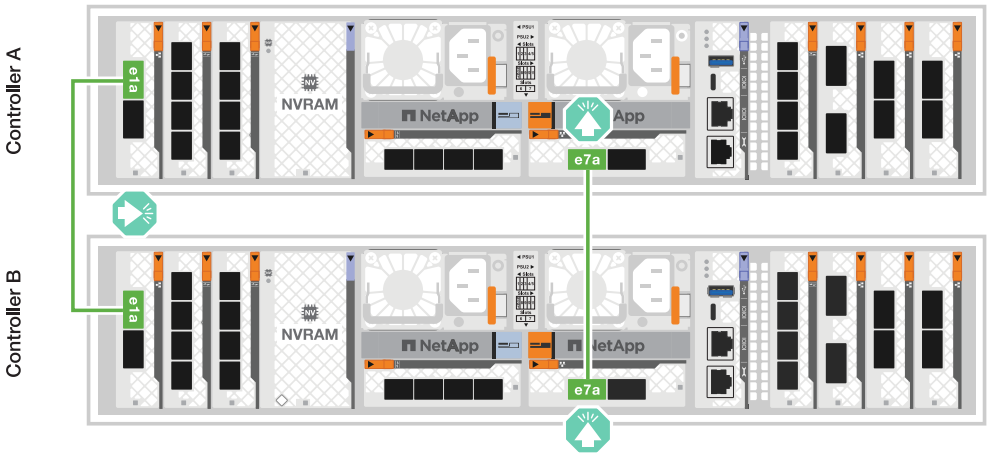
   The cluster interconnect traffic and the HA traffic share the same physical ports.

   a. Connect port e1a on Controller A to port e1A on Controller B.

   b. Connect port e7a on Controller A to port e1A on Controller B.

   Cluster/HA interconnect cables

2. Connect the Ethernet module ports to your host network.

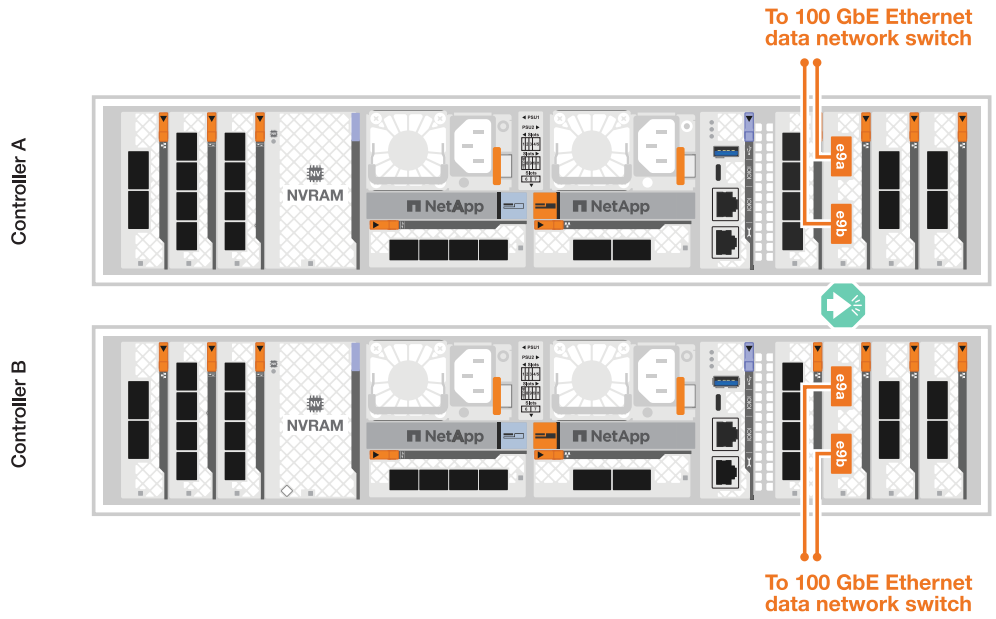
   The following are some typical host network cabling examples. See NetApp Hardware Universe for your specific system configuration.

   a. Connect ports e9a and e9b to your Ethernet data network switch as shown.

   For maximum system performance for cluster and HA traffic, do not use ports e1b and e7b ports for host network connections. Use a separate host card to maximize performance.

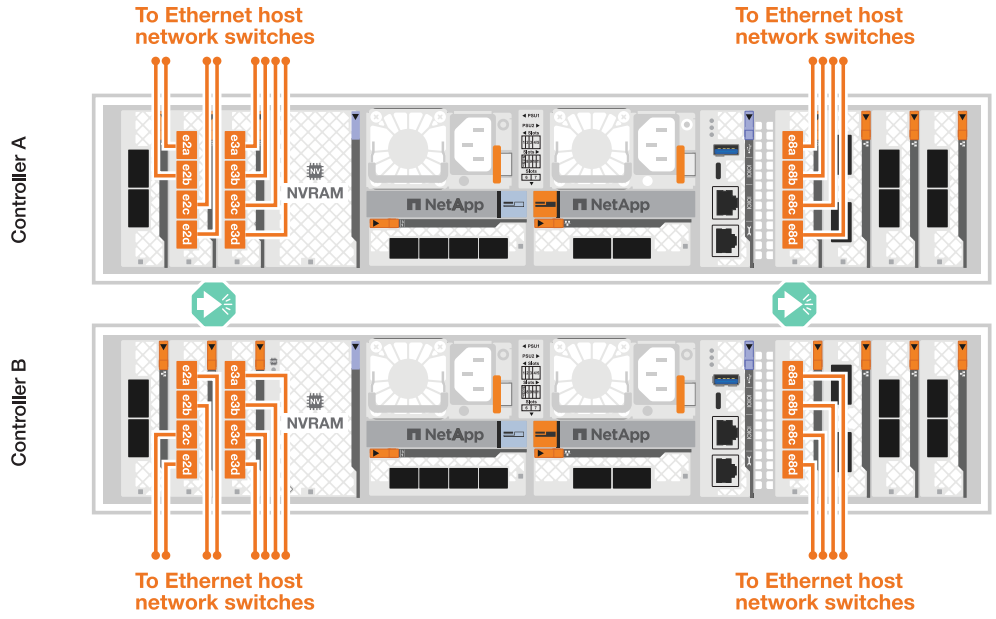
   100 GbE cable



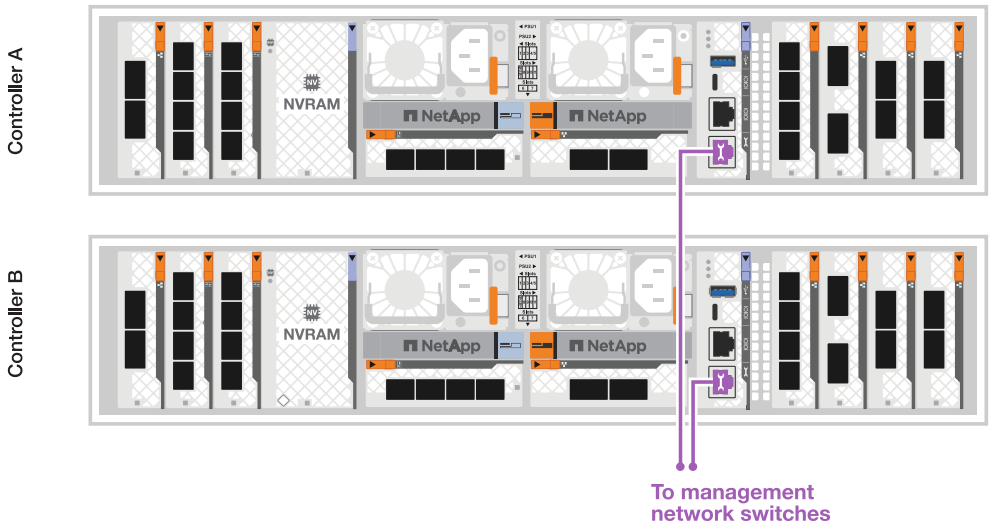
b. Connect your 10/25 GbE host network switches.

10/25 GbE Host



3. Use the 1000BASE-T RJ-45 cables to connect the controller management (wrench) ports to the management network switches.

1000BASE-T RJ-45 cables



Do not plug in the power cords yet.

ASA A70 and ASA A90

Connect your storage controllers to each other to create the ONTAP cluster connections, and then connect the Ethernet ports on each controller to your host network.

Steps

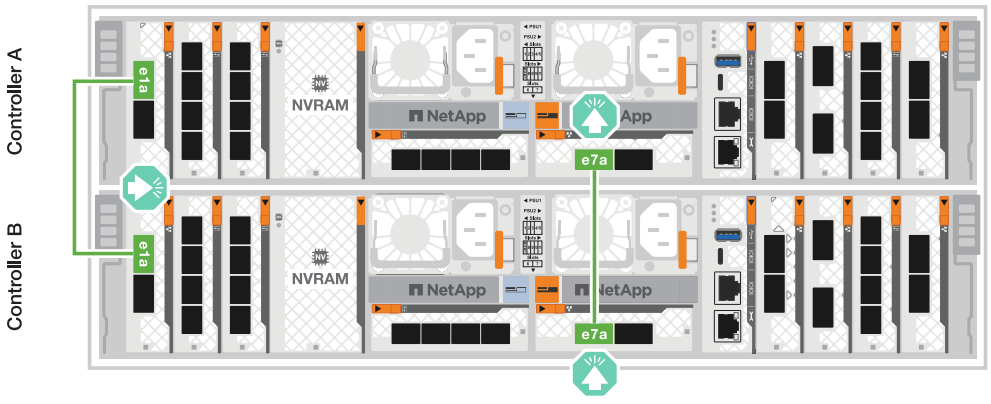
1. Use the the Cluster/HA interconnect cable to connect to connect ports e1a to e1a and ports e7a to e7a.

   The cluster interconnect traffic and the HA traffic share the same physical ports.

   a. Connect port e1a on Controller A to port e1A on Controller B.

   b. Connect port e7a on Controller A to port e1A on Controller B.

   Cluster/HA interconnect cables



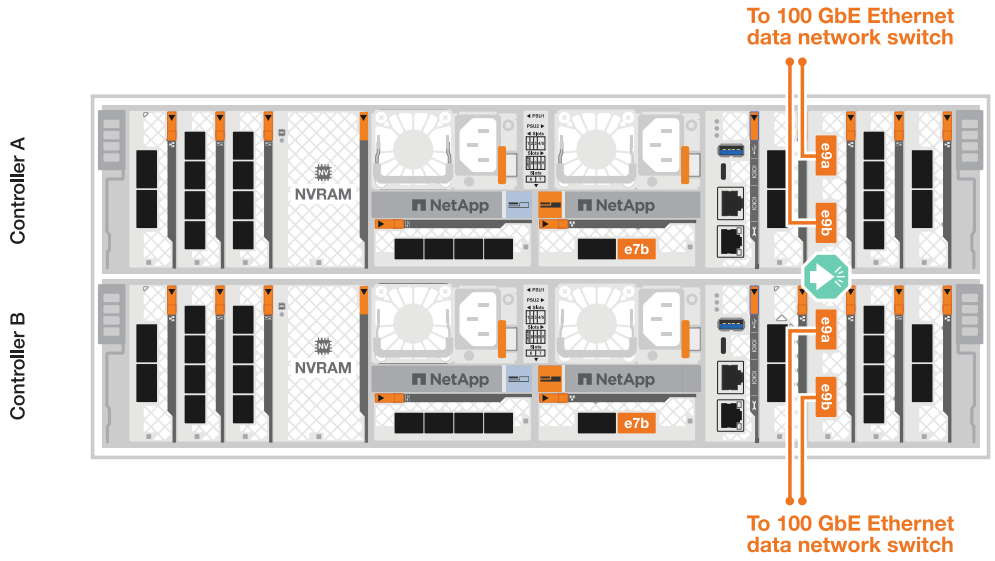
2. Connect the Ethernet module ports to your host network.

   The following are some typical host network cabling examples. See NetApp Hardware Universe for your specific system configuration.

a. Connect ports e9a and e9b to your Ethernet data network switch as shown.

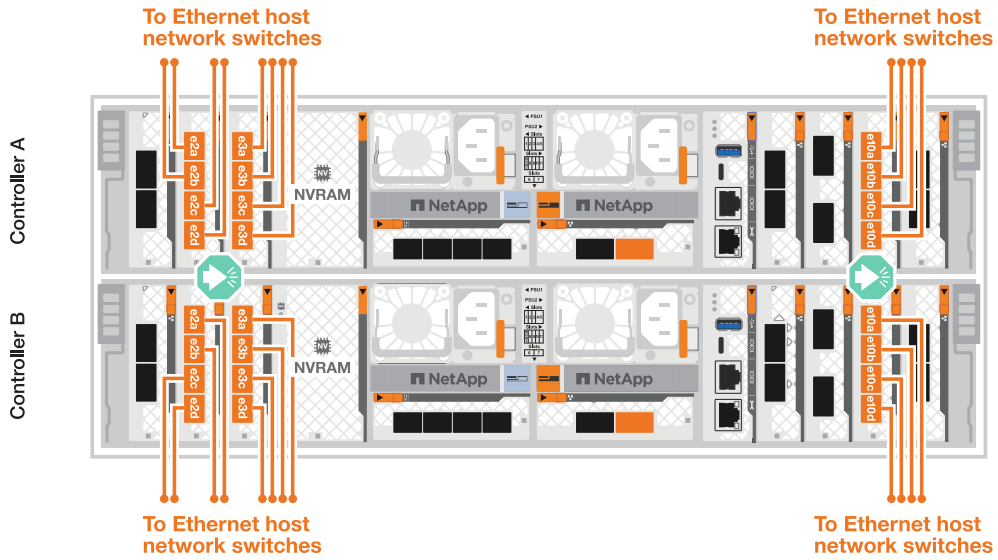
> For maximum system performance for cluster and HA traffic, do not use ports e1b and e7b ports for host network connections. Use a separate host card to maximize performance.

100 GbE cable



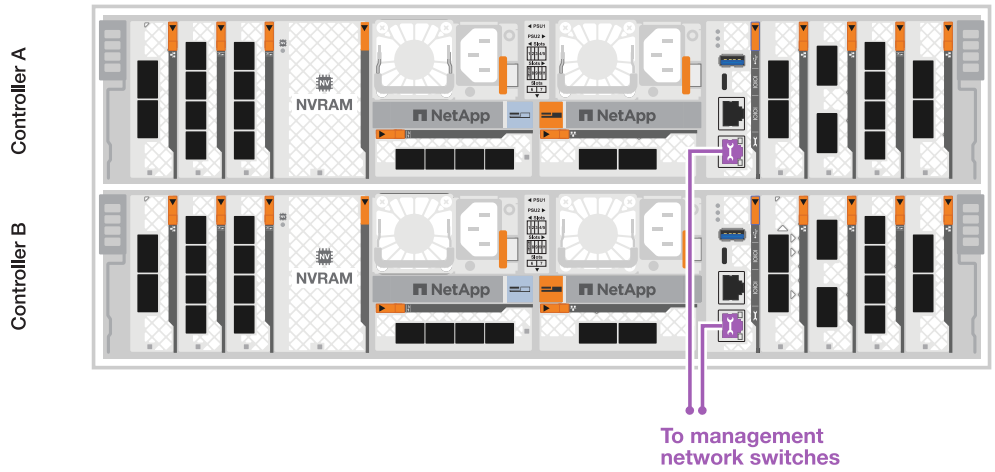
b. Connect your 10/25 GbE host network switches.

4-ports, 10/25 GbE Host



3. Use the 1000BASE-T RJ-45 cables to connect the controller management (wrench) ports to the management network switches.

1000BASE-T RJ-45 cables



Do not plug in the power cords yet.

Step 2: Connect the storage controllers to the storage shelves

The following cabling procedures show how to connect your controllers to one shelf and to two shelves. You can directly connect up to four shelves to your controllers.

ASA A1K

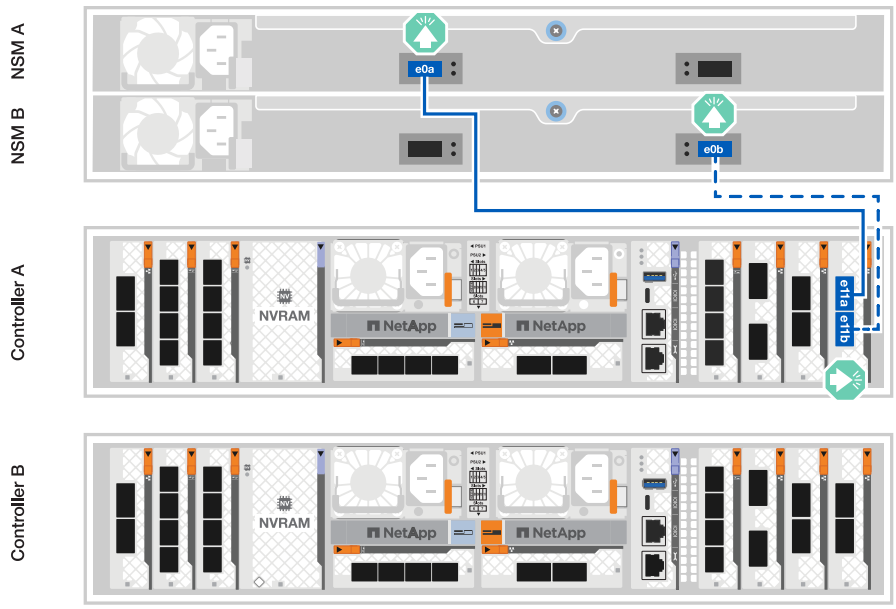
Choose one of the following cabling options that matches your setup.

Option 1: Connect the controllers to one NS224 storage shelf

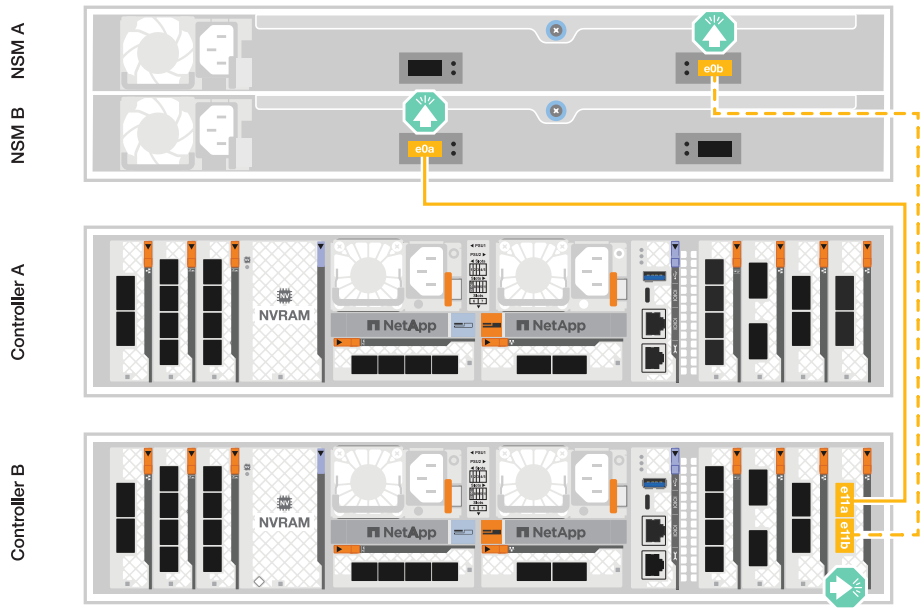
Connect each controller to the NSM modules on the NS224 shelf. The graphics show cabling from each of the controllers: Controller A cabling is shown in blue and Controller B cabling is shown in yellow.

Steps

1. On controller A, connect the following ports:
   a. Connect port e11a to NSM A port e0a.
   b. Connect port e11b to port NSM B port e0b.



2. On controller B, connect the following ports:
   a. Connect port e11a to NSM B port e0a.
   b. Connect port e11b to NSM A port e0b.

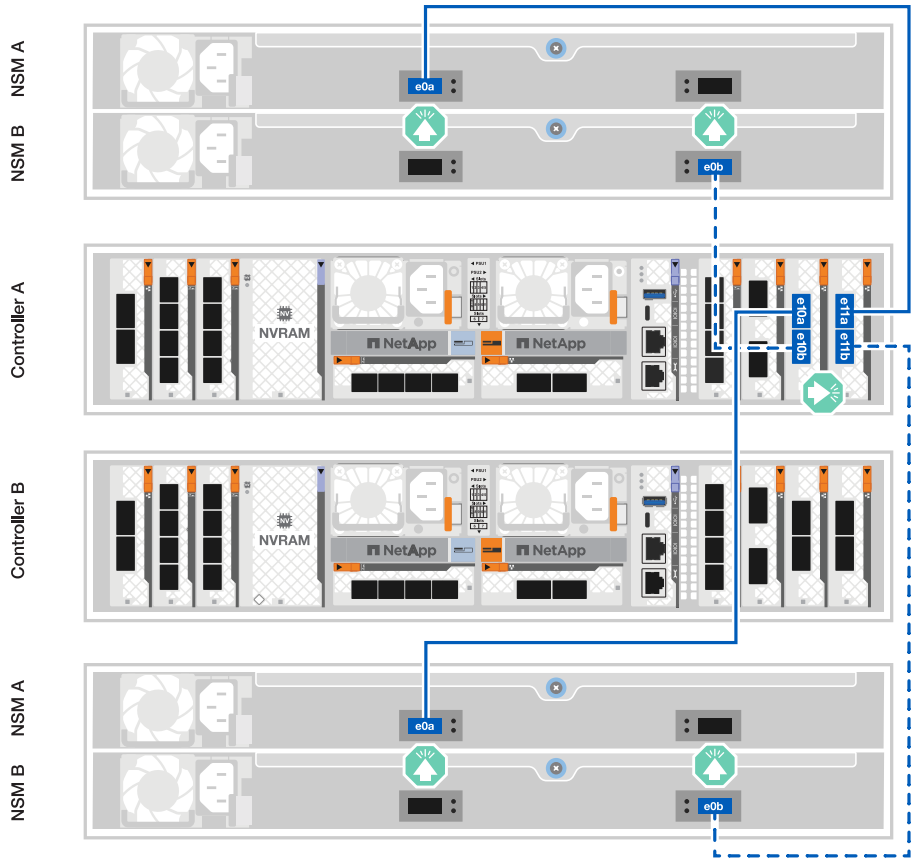


Option 2: Connect the controllers to two NS224 storage shelves

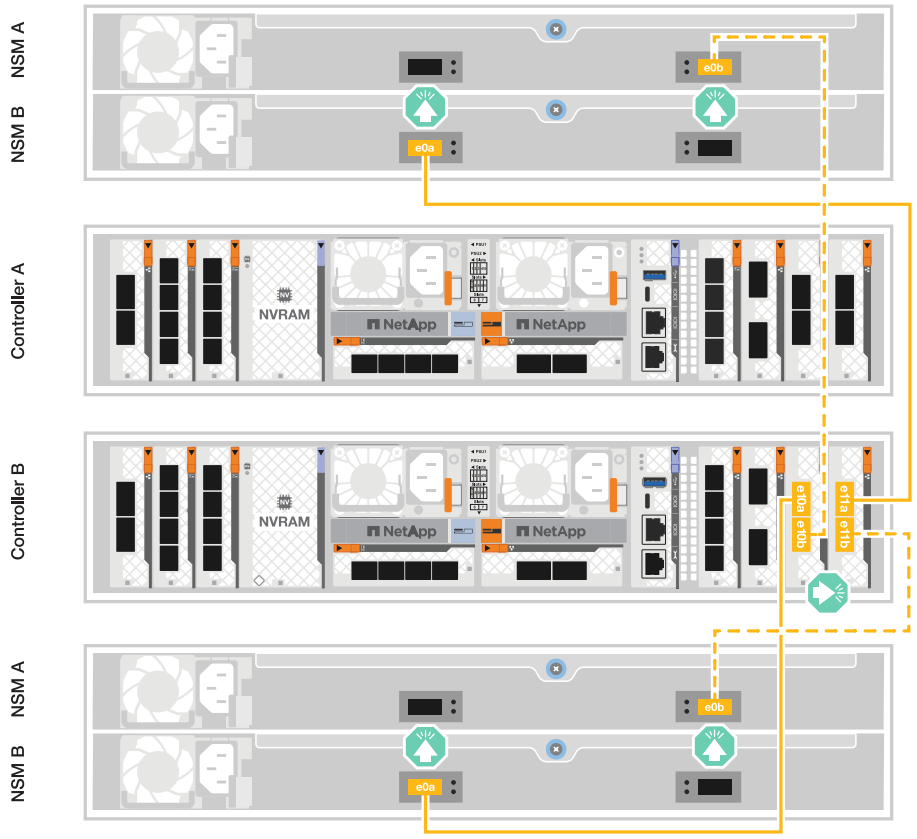
Connect each controller to the NSM modules on both NS224 shelves. The graphics show cabling from each of the controllers: Controller A cabling is shown in blue and Controller B cabling is shown in yellow.

Steps

1. On controller A, connect the following ports:
   a. Connect port e11a to shelf 1 NSM A port e0a.
   b. Connect port e11b to shelf 2 NSM B port e0b.
   c. Connect port e10a to shelf 2 NSM A port e0a.
   d. Connect port e10b to shelf 1 NSM A port e0b.



2. On controller B, connect the following ports:
   a. Connect port e11a to shelf 1 NSM B port e0a.
   b. Connect port e11b to shelf 2 NSM A port e0b.
   c. Connect port e10a to shelf 2 NSM B port e0a.
   d. Connect port e10b to shelf 1 NSM A port e0b.



ASA A70 and ASA A90

Choose one of the following cabling options that matches your setup.

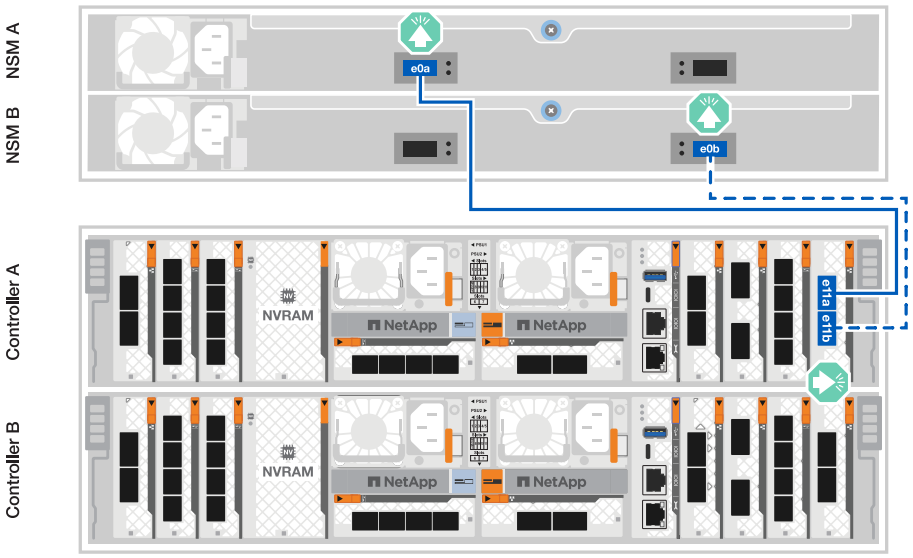
Option 1: Connect the controllers to one NS224 storage shelf

Connect each controller to the NSM modules on the NS224 shelf. The graphics show cabling from each of the controllers: Controller A cabling is shown in blue and Controller B cabling is shown in yellow.

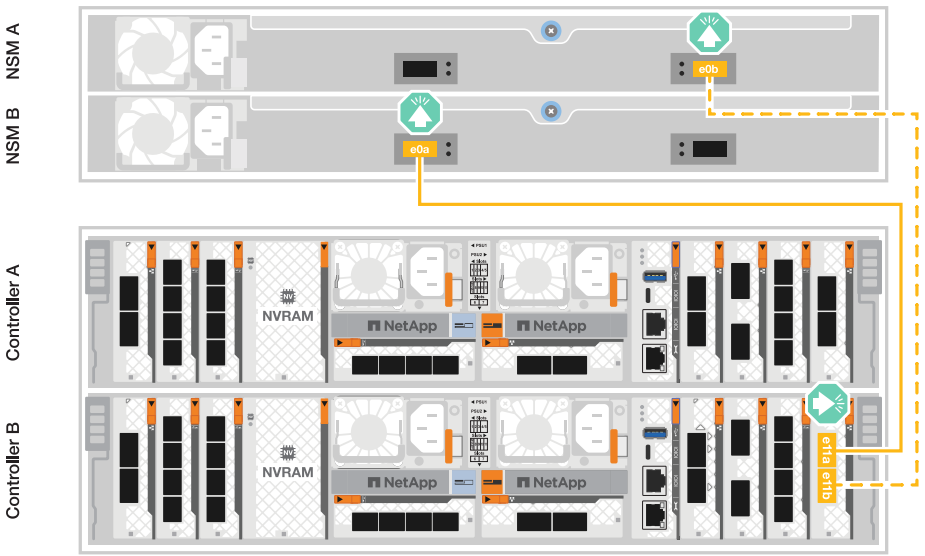
100 GbE QSFP28 copper cables

Steps

1. Connect controller A port e11a to NSM A port e0a.
2. Connect controller A port e11b to port NSM B port e0b.



3. Connect controller B port e11a to NSM B port e0a.
4. Connect controller B port e11b to NSM A port e0b.



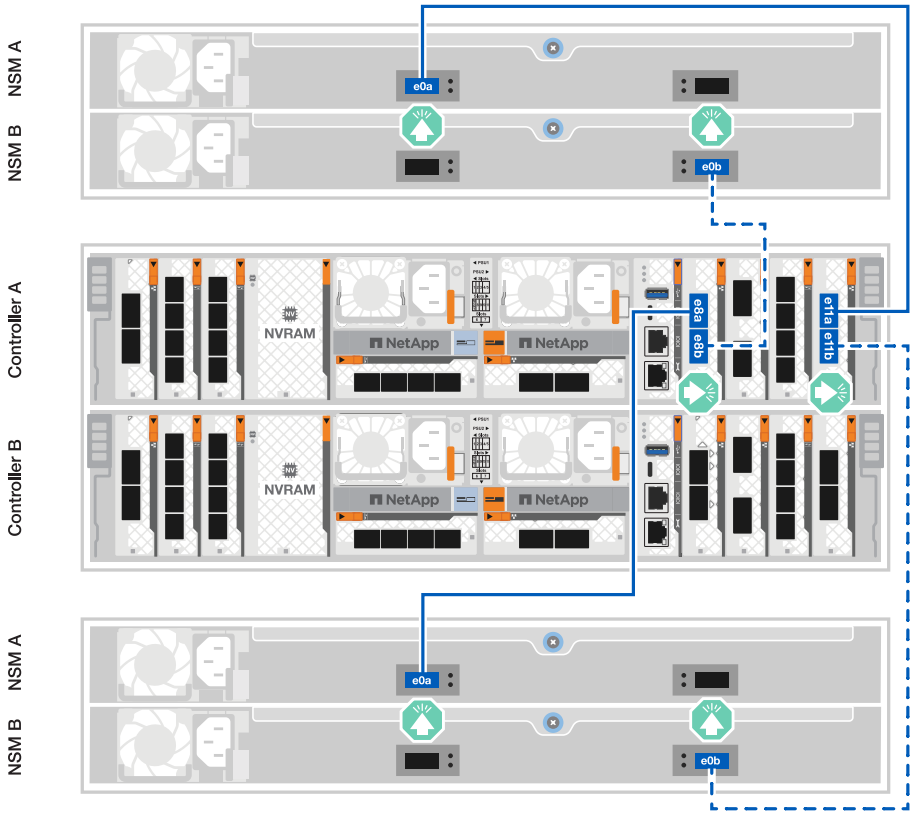
Option 2: Connect the controllers to two NS224 storage shelves

Connect each controller to the NSM modules on both NS224 shelves. The graphics show cabling from each of the controllers: Controller A cabling is shown in blue and Controller B cabling is shown in yellow.

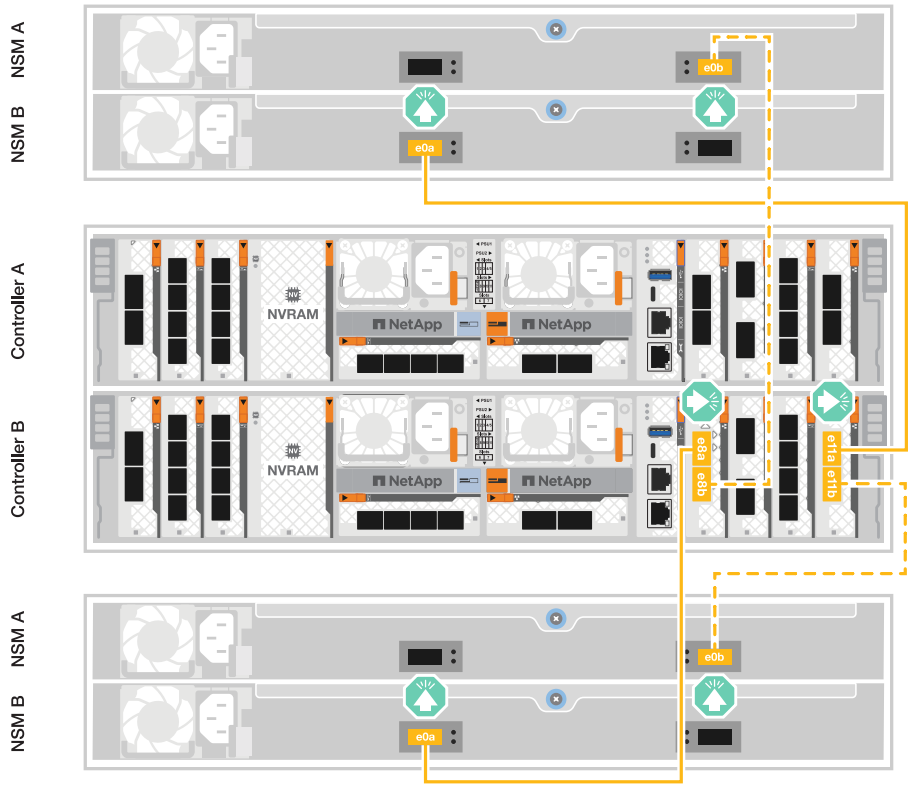
100 GbE QSFP28 copper cables

Steps

1. On on controller A, connect the following ports:
   a. Connect port e11a to shelf 1, NSM A port e0a.
   b. Connect port e11b to shelf 2, NSM B port e0b.
   c. Connect port e8a to shelf 2, NSM A port e0a.
   d. Connect port e8b to shelf 1, NSM B port e0b.



2. On controller B, connect the following ports:
   a. Connect port e11a to shelf 1, NSM B port e0a.
   b. Connect port e11b to shelf 2, NSM A port e0b.
   c. Connect port e8a to shelf 2, NSM B port e0a.
   d. Connect port e8b to shelf 1, NSM A port e0b.



What's next?

After you've connected the storage controllers to your network and then connected the controllers to your storage shelves, you power on the ASA r2 storage system.

Power on your ASA r2 storage system

After you install the rack hardware for your ASA r2 storage system and install the cables for the controllers and storage shelves, you should power on your storage shelves and controllers.

Step 1: Power on the shelf and assign shelf ID

Each NS224 shelf is distinguished by a unique shelf ID. This ID ensures that the shelf is distinct within your storage system setup. By default, shelf IDs are assigned as '00' and '01', but you may need to adjust these IDs to maintain uniqueness across your storage system.

About this task

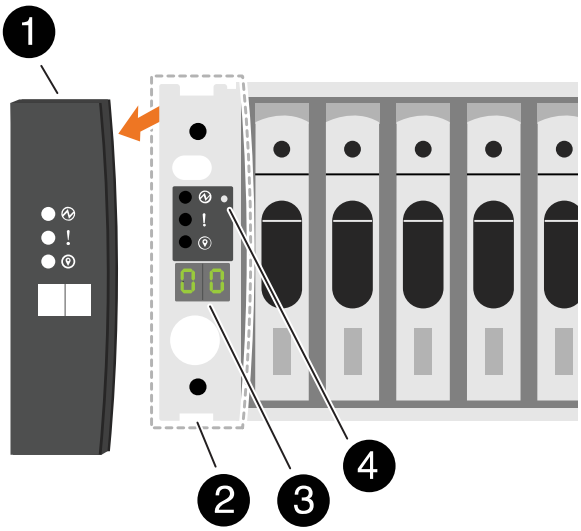
- A valid shelf ID is 00 through 99.
- You must power cycle a shelf (unplug both power cords, wait the appropriate amount of time, and then plug them back in) for the shelf ID to take effect.

Steps

1. Power on the shelf by connecting the power cords first to the shelf, securing them in place with the power cord retainer, and then connecting the power cords to power sources on different circuits.

   The shelf powers on and boots automatically when plugged into the power source.

2. Remove the left end cap to access the shelf ID button behind the faceplate.



1	Shelf end cap
2	Shelf faceplate
3	Shelf ID number
4	Shelf ID button

3. Change the first number of the shelf ID:
   a. Insert the straightened end of a paperclip or narrow tipped ball point pen into the small hole to press the shelf ID button.
   b. Press and hold the shelf ID button until the first number on the digital display blinks, and then release the button.

      It can take up to 15 seconds for the number to blink. This activates the shelf ID programming mode.

      If the ID takes longer than 15 seconds to blink, press and hold the shelf ID button again, making sure to press it in all the way.

   c. Press and release the shelf ID button to advance the number until you reach the desired number from 0 to 9.

      Each press and release duration can be as short as one second.

      The first number continues to blink.

4. Change the second number of the shelf ID:
   a. Press and hold the button until the second number on the digital display blinks.

      It can take up to three seconds for the number to blink.

The first number on the digital display stops blinking.

b. Press and release the shelf ID button to advance the number until you reach the desired number from 0 to 9.

   The second number continues to blink.

5. Lock in the desired number and exit the programming mode by pressing and holding the shelf ID button until the second number stops blinking.

   It can take up to three seconds for the number to stop blinking.

   Both numbers on the digital display start blinking and the amber LED illuminates after about five seconds, alerting you that the pending shelf ID has not yet taken effect.

6. Power-cycle the shelf for at least 10 seconds to make the shelf ID take effect.
   a. Unplug the power cord from both power supplies on the shelf.
   b. Wait 10 seconds.
   c. Plug the power cords back into the shelf power supplies to complete the power cycle.

      A power supply is powered on as soon as the power cord is plugged in. Its bicolored LED should illuminate green.

7. Replace the left end cap.

Step 2: Power on the controllers

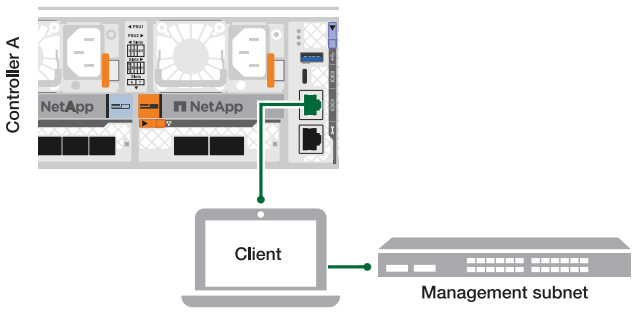
After you've turned on your storage shelves and assigned them unique IDs, turn on the power to the storage controllers.

Steps

1. Connect your laptop to the serial console port. This will allow you to monitor the boot sequence when the controllers are turned on.
   a. Set the serial console port on the laptop to 115,200 baud with N-8-1.

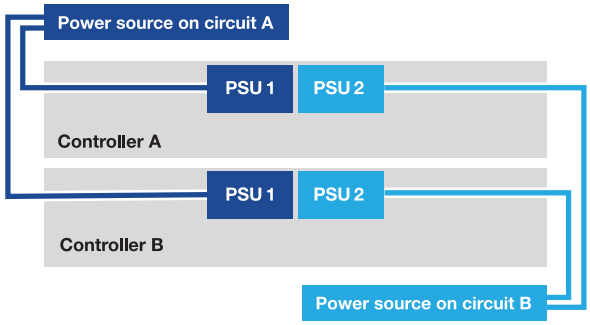
      See your laptop's online help for instructions on how to configure the serial console port.

   b. Connect the console cable to the laptop, and connect the serial console port on the controller using the console cable that came with your storage system.
   c. Connect the laptop to the switch on the management subnet.



   d. Assign a TCP/IP address to the laptop, using one that is on the management subnet.

2. Plug the power cords into the controller power supplies, and then connect them to power sources on different circuits.



   - The storage system begins to boot. Initial booting may take up to eight minutes.
   - The LEDs flash on and the fans start, which indicates that the controllers are powering on.
   - The fans might be very noisy when they first start up. The fan noise during start-up is normal.
3. Secure the power cables using the securing device on each power supply.

What's next?

After you've turned on your ASA r2 storage system, you set up an ONTAP ASA r2 cluster.

Set up your ASA r2 system

Set up an ONTAP cluster on your ASA r2 storage system

ONTAP System Manager guides you through a quick and easy workflow to set up an ONTAP ASA r2 cluster.

During cluster setup, your default data storage virtual machine (VM) is created. Optionally, you can enable the Domain Name System (DNS) to resolve host names, set your cluster to use the Network Time Protocol (NTP) for time synchronization and enable encryption of data at rest.

Before you begin

Gather the following information:

- Cluster management IP address

  The cluster management IP address is a unique IPv4 address for the cluster management interface used by the cluster administrator to access the admin storage VM and manage the cluster. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.

- Network subnet mask

  During cluster setup, ONTAP recommends a set of network interfaces appropriate for your configuration. You can adjust the recommendation if necessary.

- Network gateway IP address
- Partner node IP address
- DNS domain names
- DNS name server IP addresses

- NTP server IP addresses
- Data subnet mask

Steps

1. Discover you cluster network
   a. Connect your laptop to the management switch and access the network computers and devices.
   b. Open File Explorer.
   c. Select **Network**; then right-click and select **Refresh**.
   d. Select either ONTAP icon; then accept any certificates displayed on your screen.

      System Manager opens.

2. Under **Password**, create a strong password for the admin account.

   The password must be at least eight characters long and must contain at least one letter and one number.

3. Reenter the password to confirm and then select **Continue**.
4. Under **Network addresses**, enter a storage system name or accept the default name.

   If you change the default storage system name, the new name must begin with a letter and must be fewer than 44 characters. You can use a period (.), hyphen (-) or underscore (_) in the name.

5. Enter the cluster management IP address, subnet mask, gateway IP address and the IP address of the partner node; then select **Continue**.
6. Under **Network services**, select the desired options to **Use the Domain Name System (DNS) for resolving host names** and to **Use the Network Time Protocol (NTP) to keep times synchronized**.

   If you choose to use the DNS, enter the DNS domain and name servers. If you choose to use NTP, enter the NTP servers; then select **Continue**.

7. Under **Encryption**, enter a passphrase for the Onboard Key Manager (OKM).

   Encryption of data at rest using an Onboard Key Manager (OKM) is selected by default. If you want to use an external key manager, update the selections.

   Optionally, you can configure your cluster for encryption after cluster setup is complete.

8. Select **Initialize**.

   When setup is complete, you are redirected to the cluster's management IP address.

9. Under **Network**, select **Configure protocols**.

To configure IP (iSCSI and NVMe/TCP), do this…	To configure FC and NVMe/FC, do this…
a. Select **IP**; then select **Configure IP interfaces**. b. Select **Add a subnet**. c. Enter a name for the subnet, then enter the subnet IP addresses. d. Enter the subnet mask, and optionally enter a gateway; then select **Add**. e. Select the subnet you just created; then select **Save**. f. Select **Save**.	a. Select **FC**; then select **Configure FC interfaces** and/or **Configure NVMe/FC interfaces**. b. Select the FC and/or NVMe/FC ports; then select **Save**.

10. Optionally, download and run ActiveIQ Config Advisor to confirm your configuration.

    ActiveIQ Config Advisor is a tool for NetApp systems that checks for common configuration errors.

What's next?

You are ready to set up data access from your SAN clients to your ASA r2 system.

Enable data access from SAN hosts to your ASA r2 storage system

To set up data access, you should ensure that specific parameters and settings on your SAN client that are critical for proper operation with ONTAP are configured correctly. If you are using VMware, you should migrate your virtual machines.

Set up data access from SAN hosts

The configuration necessary to set up data access to your ASA r2 system from your SAN hosts varies depending on the host operating system and the protocol. Correct configuration is important for best performance and successful failover.

See the ONTAP SAN host documentation for VMware vSphere SCSI clients, VMware vSphere NVMe clients and other SAN clients to properly configure your hosts to connect to your ASA r2 system.

Migrate VMware virtual machines

If you need to migrate your VM workload from an ASA storage system to an ASA r2 storage system, NetApp recommends that you use VMware vSphere vMotion to perform a live, non-disruptive migration of your data.

What's next?

You are ready to provision storage to enable your SAN hosts to read and write data to storage units.

Use ONTAP to manage your data

ASA r2 storage system video demonstrations

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

Configure SAN protocols on your ASA r2 system

Video transcript

Provision SAN storage on your ASA r2 system

Video transcript

Replicate data to a remote cluster from an ASA r2 system

Video transcript

Manage your storage

Provision ONTAP SAN storage on the ASA r2 systems

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

Create storage units

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

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

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

Steps

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

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

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 for your host mapping or you can select a different host group.

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

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.
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**.

Option	Steps
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".
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. The host NQN should be formatted as <nqn.yyyy-mm> followed by a fully qualified domain name. The year should be equal to or later than 1970. The total maximum length should be 223. An example of a valid NVMe initiator is nqn.2014-08.com.example:string

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.

Create host groups

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

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

Steps

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

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

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

What's next?

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

Map the storage unit to a host

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

Steps

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

What's next?

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

Complete host-side provisioning

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

Steps

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

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

2. Discover the new storage unit.
3. Initialize the storage unit and 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.

Modify storage units on ASA r2 storage systems

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

Increase capacity

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

Modify host mappings

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

Modify QoS policy

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

- QoS throughput limit

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

- QoS throughput guarantee

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

Steps

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

What's next?

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

recognize the change in size.

Delete storage units on ASA r2 storage systems

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

Before you begin

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

Steps

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

What's next?

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

ASA r2 storage limits

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

ASA r2 systems support the following:

Max nodes per cluster	2
Max storage unit size	128 TB

For more information

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

Protect your data

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

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

Step 1: Optionally, create a consistency group

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

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

Use new storage units

Steps

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

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

What's next?

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

Use existing storage units

Steps

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

What's next?

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

Step 2: Create a snapshot

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

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

Types of snapshots

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

- On-demand snapshots

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

- Automated snapshots

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

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

Snapshot of a consistency group

Steps

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

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

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

      The SnapMirror label is used by the remote destination.

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

   a. Select a snapshot policy.

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

Option	Steps
Select an existing snapshot policy	Select ⌄ next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	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.

Replicate snapshots to a remote cluster from ASA r2 storage systems

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

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

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

Step 1: Create a cluster peer relationship

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

Steps

1. On the local cluster, in System Manager, select **Cluster > Settings**.
2. Under **Intercluster Settings** next to **Cluster peers** select ⋮, then select **Add a cluster peer**.
3. Select **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 replication policy

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

Steps

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

Option	Steps
Copy data to the remote site after it is written to the source.	a. Select **Asynchronous**. b. Under **Transfer snapshots from source**, accept the default transfer schedule or select a different one. c. Select to transfer all snapshots or to create rules to determine which snapshots to transfer. d. Optionally, enable network compression.
Write data to the source and remote sites simultaneously.	a. Select **Synchronous**.

6. Select **Save**.

What's next?

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

For more information

Learn more about storage VMs for client access.

Step 3: Create a replication relationship

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

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

Before you begin

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

Create a replication relationship with or without locked destination snapshots.

With locked snapshots

Steps

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

   You must select a *vault* replication policy.

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

   The initial data transfer begins immediately by default.

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

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

11. Select **Save**.

Without locked snapshots

Steps

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

Option	Steps
Local destinations	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. The *source* consistency group refers to the consistency group on your local cluster that you want to replicate. 3. Under **Replication destination**, select the cluster to replicate to; then select the storage VM.

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

   The initial data transfer begins immediately by default.

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

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

6. Select **Save**.

What's next?

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

Step 4: Test replication failover

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

Steps

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

What's next?

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

Protect your Kubernetes applications on ASA r2 storage systems

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

For more information

Learn more about protecting Kubernetes applications using Astra Control.

Restore data on ASA r2 storage systems

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

Restore a consistency group

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

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

Restore from a local snapshot

Steps

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

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

Restore from a remote snapshot

Steps

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

Result

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

Restore a storage unit

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

Steps

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

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

Result

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

Manage ONTAP consistency groups on ASA r2 storage systems

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

Add snapshot data protection to a consistency group

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

You can use snapshots to restore data that is lost or corrupted.

Steps

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

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

Option	Steps
Select an existing snapshot policy	Select ⌄ next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	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 **Edit**.

What's next

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

Remove snapshot data protection from a consistency group

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

Steps

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

Result

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

Add storage units to a consistency group

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

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

Add existing storage units

Steps

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

Add new storage units

Steps

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

   If you create more that 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

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

Steps

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

Result

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

What's next

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

Delete a consistency group

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

Before you begin

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

Steps

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

What's next?

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

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

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

Create a new protection policy schedule

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

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

Steps

1. Select **Protection > Policies**; then select **Schedule**.
2. Select + 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.

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.
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.

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.

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.

Administer and monitor

Manage client access to storage VMs on ASA r2 storage systems

Storage units on an ASA r2 system are contained inside storage virtual machines (VMs). Storage VMs are used to serve data to your SAN clients. Use ONTAP System Manager to create a LIF (network interface) for your SAN clients to connect to a storage VM and access data in the storage units. You can optionally use subnets to simplify LIF creation and IPspaces to provide your storage VMs with their own secure storage, administration, and routing.

Create IPspaces

An IPspace is a distinct IP address space in which storage VMs reside. When you create IPspaces, you enable your storage VMs to have their own secure storage, administration, and routing. You also enable clients in administratively separate network domains to use overlapping IP addresses from the same IP address subnet range.

You must create an IPspace before you can create a subnet.

Steps

1. Select **Network > Overview**.
2. Under **IPspaces**, select + Add.
3. Enter a name for the IPspace or accept the default name.

   An IPspace name cannot be “all” because “all” is a system-reserved name.

4. Select **Save**.

What’s next?

Now that you have created an IPspace, you can use it to create a subnet.

Create subnets

A subnet allows you to allocate specific blocks of IPv4 or IPv6 addresses to use when you create a LIF (network interface) . A subnet simplifies LIF creation by allowing you to specify the subnet name instead of a specific IP address and network mask for each LIF.

Before you begin

- You must be a cluster administrator to perform this task.
- The broadcast domain and IPspace where you plan to add the subnet must already exist.

Steps

1. Select **Network > Overview**.
2. Select **Subnets**; then select + Add.
3. Enter the subnet name.

All subnet names must be unique within an IPspace.

4. Enter the subnet IP address and subnet mask.
5. Specify the IP address range for the subnet.

   When you specify the IP address range for the subnet, do not overlap IP addresses with other subnets. Network issues can occur when subnet IP addresses overlap and different subnets or hosts attempt to use the same IP address.

6. Select the broadcast domain for the subnet.
7. Select **Add**.

What's next?

You have created a subnet which you can now use to simplify the creation of your LIFs.

Create a LIF (network interface)

A LIF (network interface) is an IP address associated with a physical or logical port. Create LIFs on the ports you want to use to access data. Storage VMs serve data to clients through one or more LIFs. If there is a component failure, a LIF can fail over or be migrated to a different physical port, so that network communication is not interrupted.

When an IP data LIF is created, it can service both iSCSI and NVMe/TCP traffic by default. Separate data LIFs must be created for FC and NVMe/FC traffic.

Before you begin

- You must be a cluster administrator to perform this task.
- The underlying physical or logical network port must have been configured to the administrative `up` status.
- If you are planning to use a subnet name to allocate the IP address and network mask value for a LIF, the subnet must already exist.
- A LIF handling intracluster traffic between nodes should not be on the same subnet as a LIF handling management traffic or a LIF handling data traffic.

Steps

1. Select **Network > Overview**.
2. Select **Network interfaces**; then select + Add.
3. Select the interface type and protocol; then select the storage VM.
4. Enter a name for the LIF or accept the default name.
5. Select the home node for the network interface; then enter the IP address and subnet mask.
6. Select **Save**.

Result

You have created a LIF for data access.

Modify a LIF (network interfaces)

LIFs can be disabled or renamed as needed. You can also change the LIF IP address and subnet mask.

Steps

1. Select **Network > Overview**; then select **Network interfaces**.
2. Hover over the network interface you want to edit; then select ⋮.
3. Select **Edit**.
4. You can disable the network interface, rename the network interface, change the IP address, or change the subnet mask.
5. Select **Save**.

Result

Your LIF has been modified.

Manage cluster networking on ASA r2 storage systems

You can use ONTAP System Manager to perform basic storage network administration on your ASA r2 system. For example, you can add a broadcast domain or reassign ports to a different broadcast domain.

Add a broadcast domain

Use broadcast domains to simplify management of your cluster network by grouping network ports that belong to the same layer 2 network. Storage virtual machines (VMs) can then use the ports in the group for data or management traffic.

The “Default” broadcast domain and the “Cluster” broadcast domain are created during cluster setup. The “Default” broadcast domain contains ports that are in the “Default” IPspace. These ports are used primarily to serve data. Cluster management and node management ports are also in this broadcast domain. The “Cluster” broadcast domain contains ports that are in the “Cluster” IPspace. These ports are used for cluster communication and include all cluster ports from all nodes in the cluster.

You can create additional broadcast domains after your cluster has been initialized. When you create a broadcast domain, a failover group that contains the same ports is automatically created.

About this task

The maximum transmission unit (MTU) of the ports added to a broadcast domain are updated to the MTU value set in the broadcast domain.

Steps

1. In System Manager, select **Network > Overview**.
2. Under **Broadcast** domains, select + Add.
3. Enter a name for the broadcast domain or accept the default name.

   All broadcast domain names must be unique within an IPspace.

4. Select the IPspace for the broadcast domain.

   If you don’t specify an IPspace name, the broadcast domain is created in the "Default" IPspace.

5. Enter the maximum transmission unit (MTU).

   MTU is the largest data packet that can be accepted in your broadcast domain.

6. Select the desired ports; then select **Save**.

Result

You have added a new broadcast domain.

Reassign ports to a different broadcast domain

Ports can belong to only one broadcast domain. If you want to change the broadcast domain to which a port belongs, you need to reassign the port from its existing broadcast domain to a new broadcast domain.

Steps

1. In System Manager, select **Network > Overview**.
2. Under **Broadcast Domains**, select ⋮ next to the domain name; then select **Edit**.
3. Deselect the Ethernet ports that you want to reassign to another domain.
4. Select the broadcast domain to which you want to reassign the port; then select **Reassign**.
5. Select **Save**.

Result

You have reassigned ports to a different broadcast domain.

Create a VLAN

A VLAN consists of switch ports grouped together into a broadcast domain. VLANs enable you to increase security, isolate problems, and limit available paths within your IP network infrastructure.

Before you begin

The switches deployed in the network must either comply with IEEE 802.1Q standards or have a vendor-specific implementation of VLANs.

About this task

- A VLAN can’t be created on an interface group port that contains no member ports.
- When you configure a VLAN over a port for the first time, the port might go down, resulting in a temporary disconnection of the network. Subsequent VLAN additions to the same port do not affect the port state.
- You should not create a VLAN on a network interface with the same identifier as the native VLAN of the switch. For example, if the network interface e0b is on native VLAN 10, you should not create a VLAN e0b-10 on that interface.

Steps

1. In System Manager, select **Network > Ethernet ports**; then select + VLAN.
2. Select the node and broadcast domain for the VLAN.
3. Select the port for the VLAN.

   The VLAN can’t be attached to a port hosting a cluster LIF or to ports assigned to the cluster IPspace.

4. Enter a VLAN ID.
5. Select **Save**.

Result

You have created a VLAN to increase security, isolate problems, and limit available paths within your IP

network infrastructure.

Monitor usage and increase capacity

Monitor cluster and storage unit performance on ASA r2 storage systems

Use ONTAP System Manager to monitor the overall performance of your cluster and the performance of specific storage units to determine how latency, IOPS and throughput are impacting your critical business applications. Performance can be monitored over various spans of time ranging from one hour to one year.

For example, suppose a critical application is experiencing high latency and low throughput. When uou view cluster performance for the last five business days, you notice a decrease in performance at the same time each day. You use this information to determine that the critical application is competing for cluster resources when a non-critical process begins running in the background. You are then able to modify your QoS policy to limit the impact of the non-critical workload on system resources and to ensure that your critical workload meets minimum throughput targets.

Monitor cluster performance

Use cluster performance metrics to determine whether you need to shift workloads to minimize latency and maximize IOPS and throughput for your critical applications.

Steps

1. In System Manager, select **Dashboard**.
2. Under **Performance**, view the latency, IOPS, and throughput for the cluster by hour, day, week, month, or year.
3. Select  to download the performance data.

What's next?

Use your cluster performance metrics to analyze if you need to modify your QoS policies or make other adjustments to your application workloads to maximize your overall cluster performance.

Monitor storage unit performance

Use storage unit performance metrics to determine the impact of specific applications on latency, IOPS and throughput.

Steps

1. In System Manager, select **Storage**.
2. Select the storage unit you want to monitor; then select **Overview**.
3. Under **Performance**, view the latency, IOPS, and throughput for the storage unit by hour, day, week, month, or year.
4. Select  to download the performance data.

What's next?

Use your storage unit performance metrics to analyze if you need to modify the QoS policies assigned to your storage units to decrease latency and maximize IOPS and throughput.

Monitor cluster and storage unit utilization on ASA r2 storage systems

Use ONTAP System Manager to monitor your storage utilization to ensure you have the storage capacity you need to serve current and future workloads.

Monitor cluster utilization

Regularly monitor the amount of storage consumed by your cluster to ensure that, if needed, you are prepared to expand the cluster capacity before running out of space.

Steps

1. In System Manager, select **Dashboard**.
2. Under **Capacity**, view the amount of physical used space and the amount of available space on your cluster.

   The data reduction ration represents the amount of space saved through storage efficiency.

What's next?

If your cluster is running low on space or if it doesn't have the capacity to meet a future demand, you should plan to add new drives to your ASA r2 system to increase your storage capacity.

Monitor storage unit utilization

Monitor the amount of storage consumed by a storage unit so that you can proactively increase the size of the storage unit based on your business needs.

Steps

1. In System Manager, select **Storage**.
2. Select the storage unit you want to monitor; then select **Overview**.
3. Under **Storage**, view the following:
   - Size of your storage unit
   - Amount of used space
   - Data reduction ratio

     The data reduction ratio represents the amount of space saved through storage efficiency

   - Snapshot used

     Snapshot used represents the amount of storage used by snapshots.

What's next?

If your storage unit is nearing capacity, you should modify the storage unit to increase its size.

Increase storage capacity on ASA r2 storage systems

Add drives to a node or shelf to increase the storage capacity of your ASA r2 system.

Use NetApp Hardware Universe to prepare for installation of a new drive

Before you install a new drive to a node or shelf, use the NetApp Hardware Universe to confirm that the drive you want to add is supported by your ASA r2 platform and to identify the correct slot for the new drive. The correct slots for adding drives vary depending on the platform model and ONTAP version. In some cases, you need to add drives to specific slots in sequence.

Steps

1. Go the NetApp Hardware Universe.
2. Under **Products**, select your hardware configurations.
3. Select your ASA r2 platform.
4. Select your ONTAP version; then select **Show Results**.
5. Beneath the graphic, select **Click here to see alternative views**; then choose the view that matches your configuration.
6. Use the view of your configuration to confirm that your new drive is supported and the correct slot for installation.

Result

You have confirmed that your new drive is supported and you know the appropriate slot for installation.

Install a new drive on the ASA r2

The minimum number of drives you should add in a single procedure is six. Adding a single drive might reduce performance.

About this task

You should repeat the steps in this procedure for each drive.

Steps

1. Properly ground yourself.
2. Gently remove the bezel from the front of the platform.
3. Insert the new drive into the correct slot.
   a. With the cam handle in the open position, use both hands to insert the new drive.
   b. Push until the drive stops.
   c. Close the cam handle so that the drive is fully seated into the mid plane and the handle clicks into place.

      Be sure to close the cam handle slowly so that it aligns correctly with the face of the drive.

4. Verify that the drive's activity LED (green) is illuminated.
   - IF the LED is solid, the drive has power.
   - If the LED is blinking, the drive has power and I/O is in progress. The LED will also blink if the drive firmware is being updated.

     Drive firmware is automatically updated (nondisruptively) on new drives that do not have current firmware versions.

5. If your node is configured for drive auto-assignment, you can wait for ONTAP to automatically assign the new drives to a node. If your node isn't configured for drive auto-assignment or if preferred, you can assign

the drives manually.

The new drives are not recognized until they are assigned to a node.

What's next?

After the new drives have been recognized, verify that they have been added and their ownership is specified correctly.

Update firmware on ASA r2 storage systems

ONTAP automatically downloads and updates firmware and system files on your ASA r2 system by default. If you want the flexibility of viewing recommended updates before they are downloaded and installed, you can use ONTAP System Manager to disable automated updates or to edit update parameters to show you notifications of available updates before any action is performed.

Enable automatic updates

Recommended updates for storage firmware, SP/BMC firmware and system files are automatically downloaded and installed on your ASA r2 system by default. If automatic updates have been disabled, you can enable them to reinstate the default behavior.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Automatic update** select ⋮, then select **Enable**.
3. Read and accept the EULA.
4. Accept the defaults to automatically update your firmware and system files. Optionally, select to show notifications or to automatically dismiss recommended updates.
5. Select to acknowledge that your update modifications will be applied to all current and future updates.
6. Select **Save**.

Result

Recommended updates are automatically downloaded and installed on your ASA r2 system based upon your update selections.

Disable automatic updates

Disable automatic updates if you want the flexibility to view recommended updates before they are installed. If you disable automatic updates, you need to perform firmware and system file updates manually.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Automatic update** select ⋮, then select **Disable**.

Result

Automatic updates are disabled. You should regularly check for recommended updates and decide if you want to perform a manual installation.

View automatic updates

View a list of firmware and system file updates that have been downloaded to your cluster and are scheduled for automatic installation. Also view updates that have been previously automatically installed.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Automatic update** select ⋮, then select **View all automatic updates**.

Edit automatic updates

You can select to have recommended updates for your storage firmware, SP/BMC firmware and your system files automatically downloaded and installed on your cluster, or you can select to have recommended updates automatically dismissed. If you want to manually control installation or dismissal of updates, select to be notified when a recommended update is available; then you can manually select to install or dismiss it.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Automatic update** select ⋮, then select **Edit automatic updates**.
3. Update the selections for automatic updates.
4. Select **Save**.

Result

Automatic updates are modified based on your selections.

Update firmware manually

If you want the flexibility of viewing recommended updates before they are downloaded and installed, you can disable automated updates and update your firmware manually.

Steps

1. Download your firmware update file to a server or local client.
2. In System Manager, select **Cluster > Overview**, then select **Update**.
3. Select **Firmware update**; the select + Update firmware.

Result

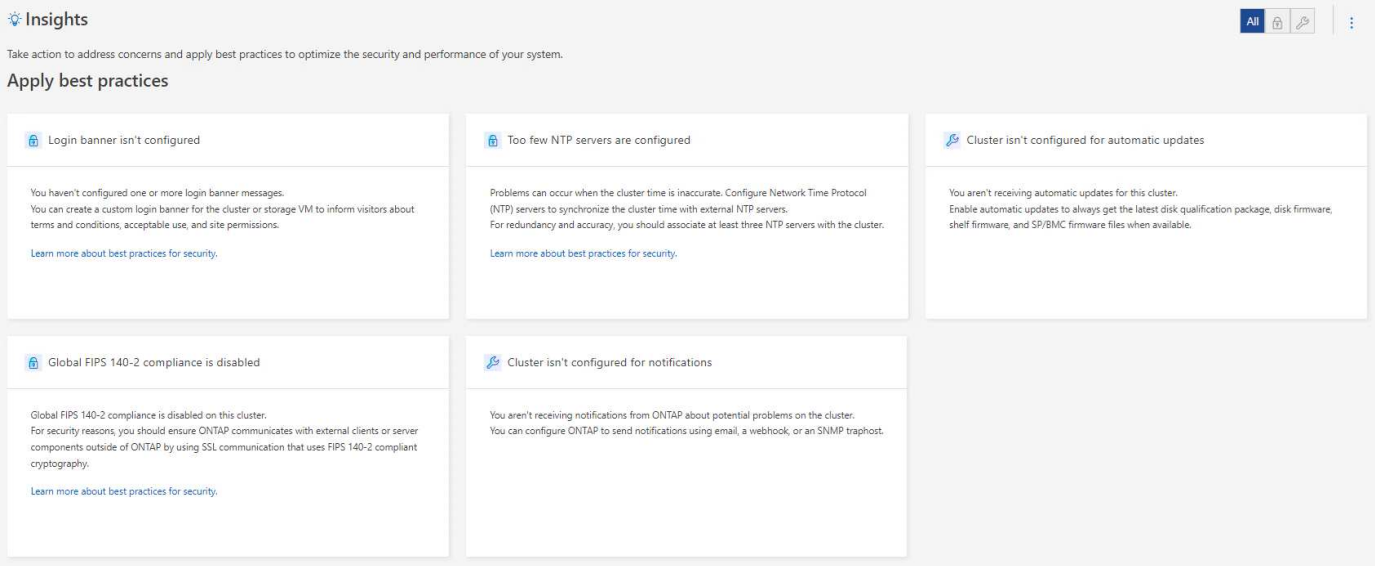
Your firmware is updated.

Optimize cluster security and performance with ASA r2 storage system insights

View *Insights* in ONTAP System Manager to identify best practices and configuration modifications that you can implement on your ASA r2 system to optimize cluster security and performance.

For example, suppose you have Network Time Protocol (NTP) servers configured for your cluster. However, you are unaware that you have less than the recommended number of NTP servers needed for optimal cluster time management. To help you prevent problems that can occur when the cluster time is inaccurate, Insights

will notify you that you have too few NTP servers configured and give you options to either learn more about this issue, fix it, or dismiss it.



Steps

1. In System Manager, select **Insights**.
2. Review recommendations.

What's next

Perform any necessary actions to implement best practices and optimize your cluster security and performance.

View cluster events and jobs on ASA r2 storage systems

Use ONTAP System Manager to view a list of errors or alerts that have occurred in your system along with recommended corrective actions. You can also view system audit logs and a list of jobs that are active, completed, or failed.

Steps

1. In System Manager, select **Events & Jobs**.
2. View cluster events and jobs.

To view this…	Do this…
Cluster events	Select **Events**; then select **Event log**.
Active IQ suggestions	Select **Events**; then select **Active IQ suggestions**.
System alerts	a. Select **System alerts**. b. Select the system alert for which you want to take action. c. Acknowledge or suppress the alert.

To view this…	Do this…
Cluster jobs	Select **Jobs**.
Audit logs	Select **Audit logs**.

Send email notifications for cluster events and audit logs

Configure your system to send a notification to specific email addresses when there is a cluster event or audit log entry.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Next to **Notifications management** select ⋮.
3. To configure an event destination, select **View event destinations**; then select **Event destinations**. To configure an audit log destination, select **View audit destinations**; then select **Audit log destinations**.
4. Select + Add.
5. Enter the destination information; then select **Add**.

Result

The email address you added will now receive the specified email notifications for cluster events and audit logs.

Manage nodes

Reboot a node on an ASA r2 storage system

You might need to reboot a node for maintenance, troubleshooting, software updates or other administrative reasons. When a node is rebooted, its HA partner automatically executes a takeover. The partner node then performs an automatic giveback after the rebooted node comes back online.

Steps

1. In System Manager, select **Cluster > Overview**.
2. Select ⋮ next to the node you want to reboot; then select **Reboot**.
3. Enter the reason you are rebooting the node; then select **Reboot**.

   The reason you enter for the reboot is recorded in the system audit log.

What's next?

While the node is being rebooted, its HA partner performs a takeover so that there is no interruption in data service. When the reboot is complete, the HA partner performs a giveback.

Rename a node on an ASA r2 storage system

You can use ONTAP System Manager to rename a node on your ASA r2 system. You

might need to rename a node to align with the naming conventions of your organization or for other administrative reasons.

Steps

1. In System Manager, select **Cluster > Overview**.
2. Select ⋮ next to the node you want to rename; then select **Rename**.
3. Enter the new name for the node, then select **Rename**.

Result

The new name is applied to the node.

Manage user accounts and roles on ASA r2 storage systems

Use System Manager to configure active directory domain controller access, LDAP and SAML authentication for your user accounts. Create user account roles to define specific functions that users assigned to the roles can perform on your cluster.

Configure active directory domain controller access

Configure active directory (AD) domain controller access to your cluster or storage VM so that you can enable AD account access.

Steps

1. In System Manager, select **Cluster > Settings**.
2. In the **Security** section, under **Active Directory**, select **Configure**.

What's next?

You can now enable AD account access on your ASA r2 system.

Configure LDAP

Configure a Lightweight Directory Access Protocol (LDAP) server to centrally maintain user information for authentication.

Before you begin

You must have generated a certificate signing request and added a CA-signed server digital certificate.

Steps

1. In System Manager, select **Cluster > Settings**.
2. In the **Security** section, next to **LDAP**, select ⚙.
3. Enter the necessary LDAP server and binding information; then select **Save**.

What's next?

You can now use LDAP for user information and authentication.

Configure SAML authentication

Security Assertion Markup Language (SAML) authentication allows users to be authenticated by a secure identity provider (IdP) instead of the direct service providers such as Active Directory and LDAP.

Before you begin

- The IdP that you plan to use for remote authentication must be configured.

  See the IdP documentation for configuration.

- You must have the URI of the IdP.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Under **Security**, next to **SAML authentication**, select .
3. Select **Enable SAML authentication**.
4. Enter the IdP URL and the host system IP address; then select **Save**.

   A confirmation window displays the metadata information, which has been automatically copied to your clipboard.

5. Go to the IdP system you specified; then copy the metadata from your clipboard to update the system metadata.
6. Return to the confirmation window in System Manager; then select **I have configured the IdP with the host URI or metadata**.
7. Select **Logout** to enable SAML-based authentication.

   The IdP system will display an authentication screen.

What's next?

You can now use SAML authentication for your user accounts.

Create user account roles

Roles for cluster administrators and storage VM administrators are automatically created when your cluster is initialized. Create additional user account roles to define specific functions that users assigned to the roles can perform on your cluster.

Steps

1. In System Manager, select **Cluster > Settings**.
2. In the **Security** section, next to **Users and roles**, select .
3. Under **Roles**, select + Add .
4. Select the role attributes.

   To add multiple attributes, select + Add .

5. Select **Save**.

Result

A new user account is created and available for use on your ASA r2 system.

Create an administrator account

Create an administrator user account to enable the account user to perform specific actions on your cluster based on the role assigned to the account. To enhance account security, set up multi-factor authentication (MFA) when you create the account.

Steps

1. In System Manager, select **Cluster > Settings**.
2. In the **Security** section, next to **Users and roles**, select →.
3. Under **Users**, select + Add .
4. Enter a username; then select a role to assign to the user.
5. Select the user login method and the authentication method.
6. To enable MFA, select + Add ; then select a secondary login method and authentication method
7. Enter a password for the user.
8. Select **Save**.

Result

A new administrator account is created and available for use on your ASA r2 cluster.

Manage security certificates on ASA r2 storage systems

Use digital security certificates to verify the identity of remote servers.

Online Certificate Status Protocol (OCSP) validates the status of digital certificate requests from ONTAP services using SSL and Transport Layer Security (TLS) connections.

Generate a certificate signing request

Generate a certificate signing request (CSR) to create a private key which can be used to generate a public certificate.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Under **Security**, next to **Certificates**, select →; then select + Generate CSR.
3. Enter the subject common name; then select the country.
4. If you want to change the GSR defaults, select extended key usage, or add subject alternative names, select ↙↗ More options; then make the desired updates.
5. Select **Generate**.

Result

You have generated a CSR to which can be used to generate a public certificate.

Add a trusted certificate authority

ONTAP provides a default set of trusted root certificates for applications using Transport Layer Security (TLS). You can add additional trusted certificate authorities as needed.

Steps

1. Select **Cluster > Settings**.
2. Under **Security**, next to **Certificates**, select →.
3. Select **Trusted certificate authorities**.
4. Enter or import the certificate details; then select + Add.

Result

You have added a new trusted certificate authority to your ASA r2 system.

Renew or delete a trusted certificate authority

Trusted certificate authorities must be renewed annually. If you do not want to renew an expired certificate, you should delete it.

Steps

1. Select **Cluster > Settings**.
2. Under **Security**, next to **Certificates**, select →.
3. Select **Trusted certificate authorities**.
4. Select the trust certificate authority that you want to renew or delete.
5. Renew or delete the certificate authority.

To renew the certificate authority, do this…	To delete the certificate authority, do this…
a. Select ⋮; then select **Renew**. b. Enter or import the certificate information; then select **Renew**.	a. Select ⋮; then select **Delete**. b. Confirm that you want to delete; then select **Delete**.

Result

You have renewed or deleted an existing trusted certificate authority on your ASA r2 system.

Add a client/server certificate or local certificate authorities

Add a client/server certificate or local certificate authorities to enable secure web services.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Under **Security**, next to **Certificates**, select →.
3. Select **Client/server certificates** or **Local certificate authorities**.
4. Add the certificate information; then select + Add.

Result

You have added a new client/server certificate or local authorities to your ASA r2 system.

Renew or delete a client/server certificate or local certificate authorities

Client/server certificates and local certificate authorities must be renewed annually. If you do not want to renew

an expired certificate or local certificate authorities, you should delete them.

Steps

1. Select **Cluster > Settings**.
2. Under **Security**, next to Certificates, select →.
3. Select **Client/server certificates**, or **Local certificate authorities**.
4. Select the certificate you want to renew or delete.
5. Renew or delete the certificate authority.

To renew the certificate authority, do this…	To delete the certificate authority, do this…
a. Select ⋮; then select **Renew**. b. Enter or import the certificate information; then select **Renew**.	Select ⋮; then select **Delete**.

Result

You have renewed or deleted an existing client/server certificate or local certificate authority on your ASA r2 system.

Verify host connectivity on your ASA r2 storage system

If there is an issue with host data operations, you can use ONTAP System Manager to verify that the connection from your host to your ASA r2 storage system is active.

Steps

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

   The host connectivity status is indicated next to name of the host group as follows:

   - **OK**: Indicates all initiators are connected to both nodes.
   - **Partially Connected**: Indicates that some of the initiators are not connected both nodes.
   - **None Connected**: Indicates that no initiators are connected.

What's next?

Make updates on your host to correct connectivity issues. ONTAP will recheck the connection status every fifteen minutes.

Maintain your ASA r2 storage system

Go to the ASA r2 maintain documentation to learn how to perform maintenance procedures on your ASA r2 system components.

Learn more

ASA r2 for ONTAP power users

Compare ASA r2 systems to other ONTAP systems

ASA r2 systems offer a unified hardware and software solution for SAN-only environments built on all flash platforms. ASA r2 systems vary from other ONTAP systems (ASA, AFF, and FAS) in the implementation of its storage layer, supported protocols, and ONTAP personality.

On an ASA r2 system, ONTAP software is streamlined to provide support for essential SAN functionality while limiting the visibility and availability of non-SAN related features and functions. For example, System Manager running on an ASA r2 system does not display options to create home directories for NAS clients. This streamlined version of ONTAP is identified as the *ASA r2 personality*. ONTAP running on all other ONTAP systems (ASA, AFF, FAS) is identified as the *unified ONTAP personality*. The differences between ONTAP personalities are referenced in the ONTAP command reference (man pages), REST API specification, and EMS messages where applicable.

You can verify the personality of your ONTAP storage from System Manager or from the ONTAP CLI.

- From the System Manager menu, select **Cluster > Overview**.
- From the CLI, enter: `san config show`

The personality of your ONTAP storage system cannot be changed.

The storage layer for ONTAP systems running the unified ONTAP personality uses aggregates as the base unit of storage. An aggregate owns a specific set of the disks available in a storage system. The aggregate allocates space on the disks it owns to volumes for LUNs and namespaces. A unified ONTAP user can use the command line interface (CLI) to create and modify aggregates, volumes, LUNs and namespaces.

The storage layer in ASA r2 systems uses a storage availability zone instead of aggregates. A storage availability zone is a common pool of storage that has access to all available disks in the storage system. The storage availability zone is visible to both nodes in an ASA r2 HA pair. When a storage unit (based on either a LUN or an NVMe namespace) is created, ONTAP automatically creates a volume containing a storage virtual machine (VM) in the storage availability zone to house the storage unit. Because of this automated and simplified approach to storage management, certain System Manager options, ONTAP commands, and REST API endpoints are not available or have limited usage on an ASA r2 system. For example, because volume creation and management is automated for ASA r2 systems, the **Volumes** menu does not appear in System Manager and the `volume create` command is not supported.

ASA r2 storage compares to other ONTAP storage systems in the following ways:

	ASA r2	**ASA**	**AFF**	**FAS**
ONTAP personality	ASA r2	ASA	Unified	Unified

	ASA r2	ASA	AFF	FAS
SAN protocol support	Yes	Yes	Yes	Yes
NAS protocol support	No	No	Yes	Yes
Storage layer support	Storage availability zone	Aggregates	Aggregates	Aggregates

The following ASA platforms are classified as ASA r2 systems:

- ASA A1K
- ASA A70
- ASA A90

For more information

- Learn more about ONTAP hardware systems.
- See full configuration support and limitations for ASA and ASA r2 systems in NetApp Hardware Universe.
- Learn more about the NetApp ASA.

Summary of ASA r2 system differences

The major differences between ASA r2 systems and FAS, AFF, and ASA systems relevant to the ONTAP command line interface (CLI) and REST API are described below.

Default SVM creation with protocol services

New clusters automatically contain a default data SVM with the SAN protocols enabled. IP data LIFs support iSCSI and NVMe/TCP protocols and use the `default-data-blocks` service policy by default.

Automatic volume creation

Creating a storage unit (LUN or namespace) automatically creates a volume from the storage availability zone. This results in a simplified and common namespace. Deleting a storage unit automatically deletes the associated volume.

Changes to thin and thick provisioning

Storage units for are always thinly provisioned on ASA r2 storage systems. Thick provisioning is not supported.

ONTAP software support and limitations for ASA r2 storage systems

While ASA r2 systems offers a wide range of support for SAN solutions, certain ONTAP software features are not supported.

ASA r2 systems do not support the following:

- iSCSI LIF failover

- FabricPool
- LUN thick provisioning
- MetroCluster
- Object protocols
- ONTAP S3 SnapMirror and S3 APIs
- SnapMirror to Cloud
- SnapMirror to non-ASA r2 systems
- Selective LUN Map (SLM)

ASA r2 systems support the following:

- Snaplock
- Dual-layer encryption

For more information

- See the NetApp Hardware Universe for more information on ASA r2 hardware support and limitations.
- Learn how to lock snapshots on your ASA r2 system.
- Learn how to apply dual-layer encryption to data on your ASA r2 system.

ONTAP CLI support for ASA r2 storage systems

Instead of traditional aggregates, which own a specific set of the disks available in a storage system, ASA r2 systems use a *storage availability zone*. A storage availability zone is a common pool of storage that has access to all available disks in the storage system. The storage availability zone is visible to both nodes in an ASA r2 HA pair. When a storage unit (LUN or NVMe namespace) is created, ONTAP automatically creates a volume containing a storage virtual machine (VM) in the storage availability zone to house the storage unit.

Because of this simplified approach to storage management, `storage aggregate` commands are not supported on ASA r2 systems. Support for certain `lun` and `volume` commands and parameters is also limited.

The following commands and command sets are not supported on ASA on r2:

Unsupported `lun` commands

- `lun copy`
- `lun geometry`
- `lun import`
- `lun mapping add-reportng-nodes`
- `lun mapping-remove-reporting-nodes`
- `lun maxsize`
- `lun move`
- `lun move-in-volume`

  This command is replaced with lun rename/vserver nvme namespace rename.

- `lun transition`

Unsupported `volume` commands and parameters

- `volume autosize`
- `volume create`
- `volume delete`
- `volume expand`
- `volume modify`

  This command is not available when used in conjunction with the following parameters:

  - `-anti-ransomware-state`
  - `-autosize`
  - `-autosize-mode`
  - `-autosize-shrik-threshold-percent`
  - `-autosize-reset`
  - `-group`
  - `-is-cloud-write-enabled`
  - `-is-space-enforcement-logical`
  - `-max-autosize`
  - `-min-autosize`
  - `-offline`
  - `-online`
  - `-percent-snapshot-space`
  - `-qos*`
  - `-size`
  - `-snapshot-policy`
  - `-space-guarantee`
  - `-space-mgmt-try-first`
  - `-state`
  - `-tiering-policy`
  - `-tiering-minimum-cooling-days`
  - `-user`
  - `-unix-permisions`
  - `-vserver-dr-protection`
- `volume make-vsroot`
- `volume mount`

- `volume move`
- `volume offline`
- `volume rehost`
- `volume rename`
- `volume restrict`
- `volume transition-prepare-to-downgrade`
- `volume unmount`

Unsupported `volume clone` commands

- `volume clone create`
- `volume clone split`

Unsupported `volume snaplock` commands

- `volume snaplock modify`

Unsupported `volume snapshot` commands

- `volume snapshot`
- `volume snapshot autodelete modify`
- `volume snapshot policy modify`

Unsupported `volume` command sets

- `volume activity-tracking`
- `volume analytics`
- `volume conversion`
- `volume file`
- `volume flexcache`
- `volume flexgroup`
- `volume inode-upgrade`
- `volume object-store`
- `volume qtree`
- `volume quota`
- `volume reallocation`
- `volume rebalance`
- `volume recovery-queue`
- `volume schedule-style`

Unsupported `storage` commands

- `storage failover show-takeover`
- `storage failover show-giveback`
- `storage aggregate relocation`
- `storage disk assign`
- `storage disk partition`
- `storage disk reassign`

For more information

See the ONTAP command reference for a full list of supported commands

Set up an ONTAP ASA r2 cluster using the CLI

It is recommended that you use System Manager to set up your ONTAP ASA r2 cluster. System Manager offers a quick and easy guided workflow to get your cluster up and running. However, if you are accustomed to working with ONTAP commands, the ONTAP command line interface (CLI) can optionally be used for cluster setup. Cluster set up using the CLI offers no additional options or advantages than cluster set up using System Manager.

During cluster setup, your default data storage virtual machine (VM) is created, an initial storage unit is created, and your data LIFs are automatically discovered. Optionally, you can enable the Domain Name System (DNS) to resolve host names, set your cluster to use the Network Time Protocol (NTS) for time

synchronization, and enable encryption of data at rest.

Before you begin

Gather the following information:

- Cluster management IP address

  The cluster management IP address is a unique IPv4 address for the cluster management interface used by the cluster administrator to access the admin storage VM and manage the cluster. You can obtain this IP address from the administrator responsible for assigning IP addresses in your organization.

- Network subnet mask

  During cluster setup, ONTAP recommends a set of network interfaces appropriate for your configuration. You can adjust the recommendation if necessary.

- Network gateway IP address
- Partner node IP address
- DNS domain names
- DNS name server IP addresses
- NTP server IP addresses
- Data subnet mask

Steps

1. Power on both nodes of the HA pair.
2. Show the nodes discovered on the local network:

   ```
   system node show-discovered -is-in-cluster false
   ```

3. Start the cluster setup wizard:

   ```
   cluster setup
   ```

4. Acknowledge the AutoSupport statement.
5. Enter values for the node management interface port, IP address, netmask and default gateway.
6. Press **Enter** to continue setup using the command line interface; then enter **create** to create a new cluster.
7. Accept the system defaults or enter your own values.
8. After setup on the first node is complete, log into the cluster.
9. Verify that the cluster is active and the first node is healthy:

   ```
   system node show-discovered
   ```

10. Add the second node to the cluster:

```
cluster add-node -cluster-ip <partner_node_ip_address>
```

11. Optionally, synchronize the system time across the cluster

Synchronize without symmetric authentication	`cluster time-service ntp server create -server <server_name>`
Synchronize with symmetric authentication	`cluster time-service ntp server create -server <server_ip_address> -key-id <key_id>`

a. Verify that the cluster is associated with an NTP server:

```
Cluster time-service ntp show
```

12. Optionally, download and run ActiveIQ Config Advisor to confirm your configuration.

What's next?

You are ready to set up data access from your SAN clients to your system.

REST API support for ASA r2

The ASA r2 REST API is based on the REST API provided with the unified ONTAP personality, with a number of changes adapted to the unique characteristics and capabilities of the ASA r2 personality.

Types of API changes

There are several types of differences between the ASA r2 system REST API and the unified ONTAP REST API available with FAS, AFF, and ASA systems. Understanding the types of changes will help you better utilize the online API reference documentation.

New ASA r2 endpoints not supported in unified ONTAP

Several endpoints have been added to the ASA r2 REST API which are not available with unified ONTAP.

For example, a new block-volume endpoint has been added to the REST API for ASA r2 systems. The block-volume endpoint provides access to both LUN and NVMe namespace objects, enabling an aggregated view of the resources. This is only available through the REST API.

As another example, the **storage-units** endpoints provide an aggregated view of the LUNs and NVMe namespaces. There are several endpoints and they're all based on or derived from `/api/storage/storage-units`. You should also review `/api/storage/luns` and

`/api/storage/namespaces`.

Restrictions on the HTTP methods used for some endpoints

Several endpoints available with ASA r2 have restrictions on which HTTP methods can be used as compared with unified ONTAP. For example, POST and DELETE are not allowed when using the endpoint `/api/protocols/nvme/services` with ASA r2 systems.

Property changes for an endpoint and HTTP method

Some ASA r2 system endpoint and method combinations do not support all the defined properties available in the unified ONTAP personality. For example, when using PATCH with the endpoint `/api/storage/volumes/{uuid}`, several properties are not supported with ASA r2, including:

- `autosize.maximum`
- `autosize.minimum`
- `autosize.mode`

Changes to internal processing

There are several changes to how ASA r2 processes certain REST API requests. For example, a DELETE request with the endpoint `/api/storage/luns/{uuid}` is processed asynchronously.

Enhanced security with OAuth 2.0

OAuth 2.0 is the industry standard authorization framework. It's used to restrict and control access to protected resources based on signed access tokens. You can configure OAuth 2.0 using System Manager to protect ASA r2 system resources.

After OAuth 2.0 is set up with System Manager, access by the REST API clients can be controlled. You need to first obtain an access token from an authorization server. The REST client then passes the token to the ASA r2 cluster as a bearer token using the HTTP authorization request header. See Authentication and authorization using OAuth 2.0 for more information.

Access the ASA r2 API reference documentation through the Swagger UI

You can access the REST API reference documentation through the Swagger UI at your ASA r2 system.

About this task

You should access the ASA r2 reference documentation page for details about the REST API. As part of this, you can search for the string **Platform Specifics** to find details about ASA r2 system support for the API calls and properties.

Before you begin

You must have the following:

- IP address or host name of the ASA r2 system's cluster management LIF
- User name and password for an account with authority to access the REST API

Steps

1. Type the URL in your browser and press **Enter**:

   `https://<ip_address>/docs/api`

2. Sign in using your administrator account.

   The ASA r2 API documentation page is displayed with the API calls organized in major resource categories.

3. To see an example of an API call that's specifically applicable only to ASA r2 systems, scroll down to the **SAN** category and click **GET /storage/storage-units**.

Get help

Manage AutoSupport on ASA r2 storage systems

AutoSupport is a mechanism that proactively monitors the health of your system and automatically sends messages to NetApp technical support, your internal support organization, and a support partner.

AutoSupport messages to technical support are enabled by default when you set up your cluster. You must set the correct options and have a valid mail host to have messages sent to your internal support organization. ONTAP begins sending AutoSupport messages 24 hours after it is enabled.

Before you begin

You must be a cluster administrator to manage AutoSupport.

Test AutoSupport connectivity

After you have set up your cluster, you should test your AutoSupport connectivity to verify that technical support will receive messages generated by AutoSupport.

Steps

1. In system manager, select **Cluster >Settings**.
2. Next to **AutoSupport** select ⋮; then select **Test connectivity**.
3. Enter a subject for the AutoSupport message; then select **Send test AutoSupport message**.

What's next?

Your have verified that technical support can receive AutoSupport messages from your ASA r2 system and will have data needed to assist you should you experience a problem.

Add AutoSupport recipients

Add members of your internal support organization to the list of email addresses that receive AutoSupport messages.

Steps

1. In system manager, select **Cluster >Settings**.
2. Next to **AutoSupport** select ⋮; then select **More options**.
3. Next to **Email**, select ✎; then select + Add .
4. Enter the email address for the recipient; then the the recipient category.

   For partners, select **Partner** for the recipient category. Select **General** for members of your internal support organization.

5. Select save.

What's next?

The email addresses you have added will receive new AutoSupport messages for their specific recipient category.

Send AutoSupport data

Should a problem occur on your ASA r2 system, AutoSupport data can significantly decrease the time it takes to identify and resolve issues.

Steps

1. In system manager, select **Cluster >Settings**.
2. Next to **AutoSupport** select ⋮; then select **Generate and send**.
3. Enter a subject for the AutoSupport message; then select **Send**.

What's next?

Your AutoSupport data is sent to technical support.

Suppress support case generation

If you are performing an upgrade or maintenance on your ASA r2 system, you might want to suppress AutoSupport generation of support cases until your upgrade or maintenance is complete.

Steps

1. In system manager, select **Cluster >Settings**.
2. Next to **AutoSupport** select ⋮; then select **Suppress support case generation**.
3. Specify the number of hours to suppress the generation of support cases; then select the nodes for which you do not want cases generated.
4. Select **Send**.

What's next?

AutoSupport cases will not be generated during the time you specified. If you complete your upgrade or maintenance before the specified time expires, you should resume support case generation immediately.

Resume support case generation

If you have suppressed the generation of support cases during an upgrade or maintenance window, you should resume support case generation immediately after your upgrade or maintenance is complete.

Steps

1. In system manager, select **Cluster >Settings**.
2. Next to **AutoSupport** select ⋮; then select **Resume support case generation**.
3. Select the nodes for which you want to resume AutoSupport cases generated.
4. Select **Send**.

Result

AutoSupport cases are autogenerated for your ASA r2 system as needed.

Submit and view support cases for ASA r2 storage systems

If you have an issue that requires assistance, you can use ONTAP System Manager to submit a case to technical support. You can also use ONTAP System Manager to view cases that are closed or in progress.

You must be registered with Active IQ to view support cases for your ASA r2 system.

Steps

1. To submit a support case, in System Manager, select **Cluster >Support**; then select **Go to NetApp Support**.
2. To view a previously submitted case, in System Manager, select **Cluster >Support**; then select **View my cases**.

Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

https://www.netapp.com/company/legal/copyright/

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

https://www.netapp.com/company/legal/trademarks/

Patents

A current list of NetApp owned patents can be found at:

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Privacy policy

https://www.netapp.com/company/legal/privacy-policy/

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

Copyright information

Trademark information