Administer and monitor

ASA r2

NetApp
February 11, 2026

Table of Contents

Administer and monitor

Upgrade and revert ONTAP

Upgrade ONTAP on ASA r2 storage systems

When you upgrade your ONTAP software on your ASA r2 system, you can take advantage of new and enhanced ONTAP features that can help you reduce costs, accelerate critical workloads, improve security, and expand the scope of data protection available to your organization.

ONTAP software upgrades for ASA r2 systems follow the same process as upgrades for other ONTAP systems. If you have an active SupportEdge contract for Active IQ Digital Advisor (also known as Digital Advisor), you should prepare to upgrade with Upgrade Advisor. Upgrade Advisor provides intelligence that helps you minimize uncertainty and risk by assessing your cluster and creating an upgrade plan specific to your configuration. If you don't have an active SupportEdge contract for Active IQ Digital Advisor, you should prepare to upgrade without Upgrade Advisor.

After you prepare for your upgrade, it is recommended that you perform upgrades using automated non-disruptive upgrade (ANDU) from System Manager. ANDU takes advantage of ONTAP's high-availability (HA) failover technology to ensure that clusters continue to serve data without interruption during the upgrade.

Learn more about ONTAP software upgrades.

Revert ONTAP on ASA r2 storage systems

ONTAP software reverts for ASA r2 systems follow the same process as reverts for other ONTAP systems.

Reverting an ONTAP cluster is disruptive. You must take the cluster offline for the duration of the reversion. You should not revert a production cluster without assistance from technical support. You can revert a new or test cluster without assistance. If the revert of a new or test system fails or if it finishes successfully, but you are not satisfied with the cluster performance in your production environment, you should contact technical support for assistance.

Revert an ONTAP cluster.

Revert requirements for ASA r2 systems

Certain ASA r2 cluster configurations require you to take specific actions before you begin an ONTAP software revert.

Reverting from ONTAP 9.17.1

If you are reverting from ONTAP 9.17.1 on an ASA r2 system, you should perform the following actions before you begin the revert:

> dynamic space balancing is enabled by default 14 days after either upgrading to ONTAP 9.17.1 or initializing a new ONTAP 9.17.1 ASA r2 cluster. You cannot revert from ONTAP 9.17.1 on your ASA r2 system after dynamic space balancing is enabled.

If you have…	Before you revert you should…
Hierarchical consistency groups in a SnapMirror active sync relationship	Delete the SnapMirror active sync relationship.
Active import relationships	Delete the active import relationships. Learn about import relationships.
Anti-ransomware protection enabled	Pause anti-ransomware protection.

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. Under **Software updates**, select **Enable**.
3. Read the EULA.
4. Accept the defaults to **Show notification** of recommended updates. Optionally, select to **Automatically update** 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 only if you want to manage updates entirely yourself. With automatic updates turned off, the system will not notify, download, or install updates. You are responsible for monitoring, downloading, scheduling, and installing all updates manually.

Steps

1. In System Manager, select **Cluster > Settings**.
2. Under **Software updates**, 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 **Software updates** 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 **Software updates** select →, then select **All other 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 **All other updates**.
3. Under **Manual Updates**, select **Add firmware files**; then select **Download from the server** or **Upload from the local client**.
4. Install the firmware update file.

Result

Your firmware is updated.

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 a storage VM

During cluster setup, your default data storage virtual machine (VM) is created. All new storage units are created inside your default data storage VM unless you create and select a different storage VM. You might want to can create an additional storage VM to segregate your storage units for different applications, departments or clients. For example, you might want to create a storage VM for your development environment and another storage VM for your production environment, or you might want to create a storage VM for your finance department and another storage VM for your marketing department.

Steps

1. Select **Cluster > Storage VMs**.
2. Select + Add.
3. Enter a name for the storage VM or accept the default name.
4. Under **Configure protocols**, select the protocols for the storage VM.

   Select **IP** for iSCSI and NVMe/TCP. Select **FC** for Fibre Channel or NVMe/FC.

5. Under **Storage VM administration**, select **Manage administrator account**; then enter the username and password for the administrator account.
6. Add a network interface for the storage VM.
7. Select **Save**.

What's next?

You have created a storage VM. You can now use the storage VM to provision storage.

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.

On an ASA r2 system, you can create IP, FC, and NVMe/FC LIFs. An IP data LIF can service both iSCSI and NVMe/TCP traffic by default. Separate data LIFs must be created for FC and NVMe/FC traffic.

If you want to enable automatic iSCSI LIF failover, you must create an IP LIF for iSCSI only traffic. When automatic iSCSI LIF failover is enabled, if a storage failover occurs, the IP iSCSI LIF is automatically migrated from its home node or port to its HA partner node or port and then back once the failover is complete. Or, if the port for an IP iSCSI LIF becomes unhealthy, the LIF is automatically migrated to a healthy port in its current home node and then back to its original port once the port is healthy again.

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.

What's next?

You can use the ONTAP command line interface (CLI) to create an iSCSI-only LIF with automatic failover.

Create a custom iSCSI-only LIF service policy

If you would like to create iSCSI-only LIFs with automatic LIF failover, you must first create a custom iSCSI-only LIF service policy.

You must use the ONTAP command line interface (CLI) to create the custom service policy.

Step

1. Set the privilege level to advanced:

```
set -privilege advanced
```

2. Create a custom iSCSI-only LIF service policy:

```
network interface service-policy create -vserver <storage_VM_name>
-policy <service_policy_name> -services data-core,data-iscsi
```

3. Verify that the service policy was created:

```
network interface service-policy show -policy <service_policy_name>
```

4. Return the privilege level to admin:

```
set -privilege admin
```

Create iSCSI-only LIFs with automatic LIF failover

If there are iSCSI LIFs on the storage VM that are not enabled for automatic LIF failover, your newly created LIFs will not be enabled for automatic LIF failover either. If automatic LIF failover is not enabled and there is a failover event your iSCSI LIFs will not migrate.

Before you begin

You must have created a custom iSCSI-only LIF service policy.

Steps

1. Create iSCSI-only LIFs with automatic LIF failover:

```
network interface create -vserver <storage_VM_name> -lif
<iscsi_lif_name> -service-policy <service_policy_name> -home-node
<home_node> -home-port <port_name> -address <ip_address> -netmask
<netmask> -failover-policy sfo-partner-only -status-admin up
```

   - It is recommended that you create two iSCSI LIFs on each node, one for fabric A and the other for fabric B. This provides redundancy and load balancing for your iSCSI traffic. In the following example, a total four iSCSI LIFs are created, two on each node, one for each fabric.

```
network interface create -vserver svm1 -lif iscsi-lif-01a -service
-policy custom-data-iscsi -home-node node1 -home-port e2b -address
<node01-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-01b -service
-policy custom-data-iscsi -home-node node1 -home-port e4b -address
<node01-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02a -service
-policy custom-data-iscsi -home-node node2 -home-port e2b -address
<node02-iscsi-a-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up

network interface create -vserver svm1 -lif iscsi-lif-02b -service
-policy custom-data-iscsi -home-node node2 -home-port e4b -address
<node02-iscsi-b-ip> -netmask 255.255.255.0 -failover-policy sfo-
partner-only -status-admin up
```

   - If you are using VLANs, adjust the `home-port` parameter to include the VLAN port information for the respective iSCSI fabric, for example, `-home-port e2b-<iSCSI-A-VLAN>` for iSCSI fabric A and `-home-port e4b-<iSCSI-B-VLAN>`.
   - If you are using interface groups (ifgroups) with VLANs, adjust the `home-port` parameter to include the appropriate VLAN port, for example, `-home-port a0a-<iSCSI-A-VLAN>` for iSCSI fabric A and

`-home-port a0a-<iSCSI-B-VLAN>` for iSCSI fabric B where `a0a` is the ifgroup and a0a-<iSCSI-A-VLAN> and a0a-<iSCSI-B-VLAN> are the respective VLAN ports for the iSCSI A fabric and the iSCSI B fabric.

2. Verify that the iSCSI LIFs were created:

```
network interface show -lif iscsi*
```

Modify a LIF (network interfaces)

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

About this task

ONTAP utilizes Network Time Protocol (NTP) to synchronize time across the cluster. After changing LIF IP addresses, you may need to update the NTP configuration to prevent synchronization failures. For more information, refer to the Knowledge Base article NTP synchronization fails after LIF IP change.

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 you 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 ratio 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 availability zone utilization

Each HA pair in an ASA r2 system uses a common pool of storage called a *storage availability zone*. The storage availability zone has access to all available disks in the storage system and is visible to both nodes in the HA pair.

If you have 4 or more nodes in your cluster, you can view the amount of space used by the storage availability zone for each HA pair. This metric is not available for 2-node clusters.

Steps

1. In System Manager, select **Cluster**; then select **Overview**.

   A summary of the storage availability zone utilization is displayed for each HA pair in the cluster.

2. If you want more detailed metrics, select a specific storage availability.

   Under **Overview**, the capacity of the storage availability zone, the amount of used space, and the data reduction ratio is displayed.

   Under **Storage units** a list of all the storage units in the storage availability zone is displayed.

What's next?

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

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 system and to identify the correct slot for the new drive. The correct slots for adding drives vary depending on the system 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 system.
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 system.
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.

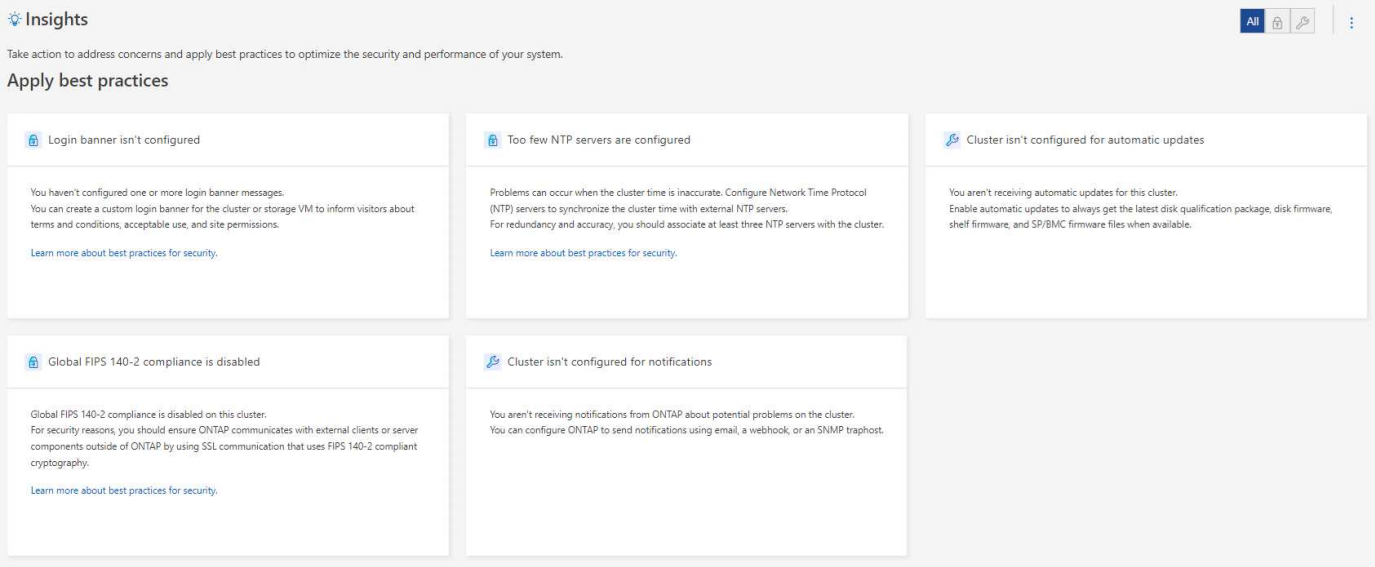
What's next?

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

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.
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

Add ASA r2 nodes to an ONTAP cluster

Beginning with ONTAP 9.16.1, ASA r2 storage systems support up to 12 nodes per cluster. After the new nodes of an HA pair have been cabled and powered on, you need to join them to the cluster.

Before you begin

Gather the following information:

- The node IP address
- The intercluster network interface IP address
- The intercluster network subnet mask

- The intercluster network gateway
- If you want to configure the onboard key manager (OKM), you need the OKM passphrase.

Steps

1. In System Manager, select **Cluster > Overview**.
2. Select ⋮ next to the node you want to join to the cluster; then select **Add node**
3. Enter the IP address for each node.
4. Enter the intercluster network interface IP address, subnet mask, and gateway.
5. If you want to configure the onboard key manager (OKM), enter the OKM passphrase.

   Configure onboard key manager for encryption is selected by default.

6. Select **Add**.

Result

The new HA pair is joined to the cluster.

What's next?

After you add the new HA pair to the cluster, you can enable data access from your SAN hosts to your new 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.

Copyright information

Trademark information