Learn more

ASA r2

NetApp
February 01, 2026

Table of Contents

Learn more

ASA r2 for ONTAP power users

Compare ASA r2 systems to other ONTAP systems

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

The following are classified as ASA r2 systems:

- ASA A1K
- ASA A90
- ASA A70
- ASA A50
- ASA A30
- ASA A20
- ASA C30

Personality differences

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 ASA systems is identified as the *ASA ONTAP personality*. ONTAP running on AFF and FAS ONTAP systems 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: `system node show -personality -is-disaggregated`

For ASA r2 systems, the *personality* is *ASA r2* and the status of *is-disaggregated* is *true*.

The personality of your ONTAP storage system cannot be changed.

Storage layer differences

ASA r2 systems use a simplified storage layer that is different from the storage layer used by FAS, AFF, and ASA systems.

FAS, AFF, and ASA systems

The storage layer for FAS, AFF, and ASA systems use 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. With these systems, ONTAP users can create and modify aggregates, volumes, LUNs and namespaces.

ASA r2 systems

Instead of aggregates, the storage layer in ASA r2 systems uses storage availability zones. A storage availability zone is a common pool of storage available to both nodes of a single HA pair. Both nodes in the HA pair have access to all available disks in their shared storage availability zone. For example, in a 2-node ASA r2 system ONTAP cluster, there is one storage availability zone, accessible by both nodes in the cluster. In a 4-node ASA r2 system ONTAP cluster, there are two storage availability zones. Each HA pair in the cluster has access to one of the storage availability zones.

When a storage unit (based on either a LUN or an NVMe namespace) is created, ONTAP automatically creates a volume in the appropriate storage availability zone to house the storage unit. The newly created volume is automatically placed within the storage availability zone for optimal performance and balanced capacity utilization. Capacity utilization is balanced within the storage availability zone based on your version of ONTAP. Learn about capacity balancing in an ASA r2 cluster.

Summary of ASA r2 system differences

ASA r2 systems differ from FAS, AFF, and ASA systems in the following ways:

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

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. Learn more about unsupported ASA r2 commands.

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 storage VM creation with protocol services

New clusters automatically contain a default data storage virutal machine (VM) 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 are always thinly provisioned on ASA r2 storage systems. Thick provisioning is not supported.

Changes to data compression

Temperature-sensitive storage efficiency is not applied on ASA r2 systems. On ASA r2 systems, compression is not based on *hot* (frequently accessed) data or *cold* (infrequently accessed) data. Compression begins without waiting for data to become cold.

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.

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:

- Default automatic iSCSI LIF failover

  In ASA r2 systems, the default networking LIF is shared between NVMe and SCSI hosts, so doesn't support automatic failover. To enable automatic iSCSI LIF failover, you must create an iSCSI only LIF. Automatic failover is enabled on iSCSI only LIFS by default.

  When automatic iSCSI LIF failover is enabled, if a storage failover occurs, the 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 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.

- FabricPool
- LUN thick provisioning
- MetroCluster
- Object protocols
- ONTAP S3 SnapMirror and S3 APIs

ASA r2 systems support the following:

- Snaplock

  Learn how to lock snapshots on your ASA r2 system.

- Dual-layer encryption

  Learn how to apply dual-layer encryption to data on your ASA r2 system.

Support for SnapMirror replication

SnapMirror replication is supported on ASA r2 systems with the following limitations:

- SnapMirror synchronous replication is not supported.
- SnapMirror active sync is supported only between two ASA r2 systems.

  Learn more about SnapMirror active sync on ASA r2 systems.

- SnapMirror asynchronous replication is supported only between two ASA r2 systems. SnapMirror asynchronous replication is not supported between an ASA r2 system and an ASA, AFF or FAS system or the cloud.

  Learn more about SnapMirror replication policies supported on ASA r2 systems.

For more information

- See the NetApp Hardware Universe for more information on ASA r2 hardware support and limitations.

ONTAP CLI support for ASA r2 storage systems

Instead of aggregates, the storage layer in ASA r2 systems use storage availability zones. A storage availability zone is a common pool of storage available to a single HA pair. Both nodes in the HA pair have access to all available disks in their shared storage availability zone. When a storage unit (LUN or NVMe namespace) is created, ONTAP automatically creates a volume in the appropriate 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`, `storage` 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 maxsize`
- `lun move`
- `lun move-in-volume`

  > The `lun move-in-volume` command is replaced with the `lun rename` and the `vserver nvme namespace rename` commands.

- `lun transition`

Unsupported `storage` commands

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

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 `volume` commands and parameters

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

  The `volume modify` 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`

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**.

Common ONTAP features supported on ASA r2 systems

Because ASA r2 systems run a streamlined version of ONTAP, many common ONTAP tasks and System Manager functions are performed the same way on ASA r2 systems as on other ONTAP systems.

For more information about common features and functions, see the following ONTAP documentation.

Data protection

Learn more about common data protection features supported on ASA r2 systems.

Clustered external key servers

You can configure connectivity to clustered external key management servers on a storage VM. With clustered key servers, you can designate primary and secondary key servers on a storage VM. When registering keys, ONTAP will first attempt to access a primary key server before sequentially attempting to access secondary servers until the operation completes successfully, preventing duplication of keys.

Learn to configure clustered external key servers.

External key management for encryption at rest

You can use one or more KMIP servers to secure the keys the cluster uses to access encrypted data.

- Enable external key management.
- Enable external key management (NVE).

Data security

Learn more about common data security features supported on ASA r2 systems.

Administrator access management

The role assigned to an administrator determines which functions the administrator can perform. Predefined roles for cluster administrators and storage VM administrators are provided by System Manager. You assign the role when you create the administrator's account, or you can assign a different role later.

- Learn to manage administrator access with System Manager.

Client authentication and authorization

ONTAP uses standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage. ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

Learn about client authentication and authorization.

OAuth 2.0 authentication

You can use the Open Authorization (OAuth 2.0) framework to control access to your ONTAP clusters. OAuth 2.0 restricts and controls access to protected resources using signed access tokens.

Learn about OAuth 2.0 authentication.

SAML authentication and administrator access

You can configure and enable Security Assertion Markup Language (SAML) authentication for web services. SAML authenticates users by an external Identity Provider (IdP) instead of the directory service providers such as Active Directory and LDAP.

Learn to Configure SAML authentication.

Networking

Learn more about common networking features supported on ASA r2 systems.

FIPS compliance

ONTAP is compliant in the Federal Information Processing Standards (FIPS) 140-2 for all SSL connections. You can turn SSL FIPS mode on and off, set SSL protocols globally, and turn off any weak ciphers such as RC4 within ONTAP.

Beginning with ONTAP 9.18.1 postquantum computing cryptographic algorithms are supported for SSL. These algorithms provide additional protection against potential future quantum computing attacks, and are available when SSL FIPS mode is disabled.

- Learn to configure FIPS for all SSL connections.

Link Aggregation Groups (LAGs)

An interface group, also known as a Link Aggregation Group (LAG), is created by combining two or more physical ports on the same node into a single logical port. The logical port provides increased resiliency, increased availability, and load sharing.

Learn about Link Aggregation Groups.

SAN Protocols

ASA r2 systems support all SAN protocols (iSCSI, FC, NVMe/FC, NVMe/TCP).

- Learn more about the iSCSI protocol.
- Learn more about the Fibre Channel (FC) protocol.
- Learn about the NVMe protocol .
  - Learn to configure NVMe copy offload.

    Beginning with ONTAP 9.18.1, NVMe copy offload is supported. NVMe copy offload enables an NVMe host to offload copy operations from its CPU to the CPU of the ONTAP storage controller. The host can copy data from one NVMe namespace to another while reserving its CPU resources for application workloads.

- Learn more about space allocation (unmap) for NVMe.

  Beginning with ONTAP 9.16.1, space deallocation (also called “hole punching” and “unmap”) is enabled for NVMe namespaces by default. Space deallocation allows a host to deallocate unused blocks from namespaces to reclaim space.

System Manager

You can search for various actions, objects,and information topics in System Manager. You can also search table data for specific entries.

Learn to search, filter and sort information in System Manager.

Copyright information

Trademark information