Administer your cluster

AFX

NetApp
February 11, 2026

Table of Contents

Administer your cluster

Monitor cluster processes

View the AFX storage system dashboard

You can sign in to System Manager to access the AFX dashboard and display the cluster status. This is a good first step before beginning your AFX administrative tasks or if you suspect an operational issue.

Before you begin

You'll need the following:

- IP address or domain name of the cluster management LIF
- Administrator account credentials

Steps

1. Connect to System Manager using a browser and the cluster management IP address:

   ```
   https://$FQDN_IPADDR/
   ```

   Example

   ```
   https://10.61.25.33/
   ```

2. Provide the username and password for the administrator account and select **Sign in**.
3. Select **Dashboard** in the left navigation pane and review the tiles on the page including the cluster **Health**.
4. In the navigation pane, select **Cluster** and then **Overview**.
5. Review the cluster name, version, ONTAP personality and the other details.
6. At the top of the overview page, select **Cabling** for a visual display of the cluster hardware and connections.
7. In the navigation pane, select **Events & Jobs** and then **System alerts** to display and review the system alerts.

View Insights to optimize your AFX storage system

You can use the *Insights* feature of ONTAP System Manager to display suggested configuration updates that align with NetApp best practices. These changes can optimize the security and performance of your AFX cluster.

For example, the Autonomous Ransomware Protection (ARP) feature is available with AFX and provides anti-ransomware protection. Insights will inform you if ARP is not configured.

About this task

Each of the insights is presented as a separate tile or card on the page that you can choose to implement or dismiss. You can also select the associated documentation link to learn more about a specific technology.

Steps

1. In System Manager, select **Analysis** and then **Insights**.
2. Review the available recommendations.

What's next

Perform any of the recommended actions to implement AFX configuration best practices.

Monitor AFX storage system cluster performance

You can display a high-level overview of the performance of your AFX cluster.

Storage capacity

The System Manager dashboard includes a high-level display of the storage utilization for the cluster.

Steps

1. In System Manager, select **Dashboard** in the navigation pane.
2. Locate the **Capacity** tile and view the physical storage available and used.
3. Select **History** to access Active IQ to view the historical data.

Cluster performance

System Manager provides a detailed overview of the AFX cluster performance.

Steps

1. In System Manager, select **Analysis** and then **Performance**.
2. Review the cluster performance summary at top including latency and throughput.
3. Under the **Top actors** tab, select the desired SVM and then **Enable activity tracking** as needed.
4. Under the **Volume performance** tab, view the performance details of a specific volume.

Related information

- Additional AFX cluster administration

View AFX storage system events and audit log

You can review the events and audit log messages generated by AFX to track internal processing and diagnose potential problems. The AFX system can be configured to forward this information, along with other related data, for additional processing and archival.

Events

The event messages provide a valuable record of system activity. Each event includes a description and unique identifier along with a recommended action.

1. In System Manager, select **Events & jobs** and then **Events**.
2. Review and respond to the recommended actions at the top of the page, such as enabling automatic update.

3. Select the **Events log** tab to display a list of the messages.
4. Select an event message to examine it in more detail, including the sequence number, description, event, and recommended action.
5. Optionally select the **Active IQ suggestions** tab and register with Active IQ to get detailed risk information for the cluster.

Audit log

The audit log includes a record of system activity based on the use of access protocols such as HTTP.

1. In System Manager, select **Events & jobs** and then **Audit logs**.
2. Select **Settings** to enable or disable the operations that are tracked.
3. Optionally select **Manage audit destinations**; review Manage notifications for more information.

Manage notifications

There are several types of notifications supported by AFX that you can forward.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Navigate to **Notification management** and select ⋮.
3. Select the appropriate action to view or configure the destinations used by AFX. For example, to configure:
   a. *Event destinations:* select **View event destinations**
   b. *Audit log destinations:* select **View audit destinations**
4. Select + Add as appropriate and provide the destination information.
5. Select **Save**.

Related information

- ONTAP Event, performance, and health monitoring

View AFX storage system jobs

AFX includes an internal platform to run background jobs based on your configuration and administrative actions. These jobs can be long-running AFX components or short-lived processes executed in response to administrative tasks or REST API requests. You can display and monitor the jobs as needed.

Steps

1. In System Manager, select **Events & Jobs** and then **Jobs**.
2. Customize the display as well as search and download the job information as needed.

Manage networking and security

Manage AFX storage system cluster networking

You need to configure the network of your AFX storage system. The networking

environment supports several scenarios including clients accessing data at the SVMs and intercluster communication.

Creating a network resource is an important first step. You also need to perform additional administrative actions, such as editing or deleting network definitions, as needed.

Create a broadcast domain

A broadcast domain simplifies management of your cluster network by grouping ports that are part of the same layer two network. The storage virtual machines (SVMs) can then be assigned ports in the group for data or management traffic.

There are several broadcast domains created during cluster setup, including:

Default

This broadcast domain contains ports in the “Default” IPspace. These ports are used primarily to serve data. Cluster management and node management ports are also included.

Cluster

This broadcast domain contains ports in the “Cluster” IPspace. These ports are used for cluster communication and include all the 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) value of the ports defined for a broadcast domain are updated to the MTU value set in the broadcast domain.

Steps

1. In System Manager, select **Network** and then **Overview**.
2. Under **Broadcast domains**, select + Add .
3. Provide the name of the broadcast domain or accept the default.

   All broadcast domain names must be unique within an IPspace.

4. Provide the maximum transmission unit (MTU).

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

5. Choose the desired ports and select **Save**.

Create an IPspace

An IPspace is an administrative domain for IP addresses and related network configuration. These spaces can be used to support your SVMs through isolated administration and routing. For example, they are useful when clients have overlapping IP addresses from the same IP address and subnet range.

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

Steps

1. In System Manager, select **Network** and then **Overview**.
2. Under **IPspaces**, select + Add.
3. Provide the name of the IPspace or accept the default.

   All IPspace names must be unique within a cluster.

4. Select **Save**.

What's next

You can use the IPspace to create a subnet.

Create a subnet

A subnetwork or subnet enforces a logical division of the IP address space in your network. It enables you to allocate dedicated blocks of IP addresses for the creation of a network interface (LIF). Subnets simplify LIF creation by enabling you to use the subnet name instead of a specific IP address and network mask combination.

Before you begin

You must have a broadcast domain and IPspace where the subnet will be defined. Also note:

- All subnet names must be unique within a specific IPspace.
- The IP address range used for a subnet cannot overlap with the IP addresses of other subnets.

Steps

1. In System Manager, select **Network** and then **Overview**.
2. Under the **Subnets** tab, select + Add.
3. Provide the configuration details, including the name of the subnet, IP address details, and broadcast domain.
4. Select **Save**.

What's next

The new subnet will simplify the creation of your network interfaces.

Create a network interface

A logical network interface (LIF) consists of an IP address and related network configuration parameters. It can be associated with a physical or logical port and is typically used by the clients to access data provided by an SVM. LIFs provide resiliency in the event of a failure and can migrate among the node ports so communication is not interrupted.

Steps

1. In System Manager, select **Network** and then **Overview**.
2. Under the **Network interfaces** tab, select + Add.
3. Provide the configuration details, including the name of the interface, interface type, allowed protocols, and IP address details.
4. Select **Save**.

Related information

- Manage AFX Ethernet ports
- Learn about ONTAP broadcast domains
- Learn about ONTAP IPspace configuration
- Learn about subnets for the ONTAP network
- Network architecture overview

Manage AFX storage system Ethernet ports

The ports used by the AFX system provide a foundation for network connectivity and communication. There are several options available to customize the layer two configuration of your network.

Create a VLAN

A VLAN consists of switch ports grouped together into a broadcast domain. VLANs enable you to increase security, isolate potential 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

Note the following:

- You can't create a VLAN on an interface group port without any 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** and then **Ethernet ports**.
2. Select + VLAN.
3. Provide the configuration details, including the id, broadcast domain, and ports across the desired nodes.

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

4. Select **Save**.

Result

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

Create a LAG

A link aggregate group (LAG) is a technique that combines multiple physical network connections into a single

logical connection. You can use it to increase the bandwidth and provide redundancy between nodes.

Steps

1. In System Manager, select **Network** and then **Ethernet ports**.
2. Select **Link aggregate group**.
3. Provide the configuration details, including the node, broadcast domain, ports, mode, and load distribution.
4. Select **Save**.

Related information

- Manage AFX cluster networking
- Learn about ONTAP network port configuration
- Combine physical ports to create ONTAP interface groups

Prepare AFX storage system authentication services

You need to prepare the authentication and authorization services used by the AFX system to the user account and role definitions.

Configure LDAP

You can configure a Lightweight Directory Access Protocol (LDAP) server to maintain authentication information at a central location.

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** and then **Settings**.
2. Select ⚙ next to **LDAP**.
3. Select + Add and provide the name or IP address of the LDAP server.
4. Provide the necessary configuration information, including the schema, base DN, port, and binding.
5. Select **Save**.

Configure SAML authentication

Security Assertion Markup Language (SAML) authentication enables users to be authenticated by a secure identity provider (IdP) instead of providers using other protocols such as LDAP.

Before you begin

- The identity provider you plan to use for remote authentication must be configured. See the provider documentation for configuration details.
- You must have the URI of the identity provider.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Select ⚙ under **Security** next to **SAML authentication**.

3. Select **Enable SAML authentication**.
4. Provide the **IdP URL** and the **Host system** IP address and select **Save**.

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

5. Navigate to the IdP system you specified and copy the metadata from your clipboard to update the system metadata.
6. Return to the confirmation window in System Manager and 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.

Related information

- Manage AFX cluster users and roles
- Configure SAML authentication for remote ONTAP users
- Authentication and access control

Manage AFX storage system cluster users and roles

You can define user accounts and roles based on the authentication and authorization services available with AFX.

Each ONTAP user needs to have one role assigned. A role includes privileges and determines what actions the user is able to perform.

Create an account role

Roles for cluster administrators and storage VM administrators are automatically created when your AFX cluster is set up and initialized. You can 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** and then **Settings**.
2. In the **Security** section, next to **Users and roles**, select →.
3. Under **Roles**, select + Add.
4. Provide the name of the role and the attributes.
5. Select **Save**.

Create a cluster account

You can create a cluster-level account to use when performing cluster or SVM administration.

Steps

1. In System Manager, select **Cluster** and then **Settings**.

2. In the **Security** section, select → next to **Users and roles**.
3. Select + Add . under **Users**.
4. Enter a username and then select the role for the user.

   The role should be appropriate for the user. For example, the **admin** role is able to perform the full range of configuration tasks on your cluster.

5. Select the user login method and the authentication method; this will typically be **Password**.
6. Enter a password for the user.
7. Select **Save**.

Result

A new account is created and available for use with your AFX cluster.

Related information

- Prepare authentication services
- Additional AFX SVM administration

Manage certificates on an AFX storage system

Depending on your environment, you'll need to create and manage digital certificates as part of administering AFX. There are several related tasks you can perform.

Generate a certificate signing request

To get started using a digital certificate, you need to generate a certificate signing request (CSR). A CSR is used to request a signed certificate from a certificate authority (CA).As part of this, ONTAP creates a public/private key pair and includes the public key in the CSR.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Under **Security** and next to **Certificates**, select →
3. Select + Generate CSR.
4. Provide the subject common name and country; optionally provide the organization and organizational unit.
5. To change the default values which will define the certificate, select ↙↗ More options and make the desired updates.
6. Select **Generate**.

Result

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

Add a trusted certificate authority

ONTAP provides a default set of trusted root certificates for use with Transport Layer Security (TLS) and other protocols. You can add additional trusted certificate authorities as needed.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Under **Security** and next to **Certificates**, select →.
3. Select the tab **Trusted certificate authorities** and then select + Add.
4. Provide the configuration information, including the name, scope, common name, type, and certificate details; you can import the certificate instead by selecting **Import**.
5. Select **Add**.

Result

You have added a trusted certificate authority to your AFX 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** and then **Settings**.
2. Under **Security** and next to **Certificates**, select →.
3. Select the tab **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 ⋮ and then select **Renew**. b. Enter or import the certificate information and select **Renew**.	a. Select ⋮ and then select **Delete**. b. Confirm that you want to delete and select **Delete**.

Result

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

Add a client/server certificate or local certificate authority

You can add a client/server certificate or a local certificate authority as part of enabling secure web services.

Steps

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

Result

You have added a new client/server certificate or local authorities to your AFX 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** and then **Settings**.
2. Under **Security** and next to Certificates, select →.
3. Select either **Client/server certificates** or **Local certificate authorities** as needed.
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 ⋮ and then select **Renew**. b. Enter or import the certificate information and select **Renew**.	Select ⋮ and then select **Delete**.

Result

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

Related information

- Generate and install a CA-signed server certificate in ONTAP
- Manage ONTAP certificates with System Manager

Manage storage VMs

Display the AFX storage system SVMs

You can display the data storage VMs defined in your AFX cluster. Each SVM provides an isolated environment for organizing your data and providing client access.

Steps

1. In System Manager, select **Cluster** and then **Storage VMs**.
2. Hover over the desired SVM and select ⋮ to view the primary administrative options including starting and stopping the SVM.
3. Optionally select a specific SVM to view more details including overview, settings, replication, and file system.

Related information

- Configure an AFX system SVM
- Understand storage virtual machines

Create an AFX storage system SVM

You can create an SVM to provide isolation and improve security. You might do this for different groups or projects within your organization.

About this task

When you create an SVM, you must provide a name and configure at least one protocol for client access. After selecting a client protocol, you will be prompted for the networking configuration as well. You can change the SVM configuration as needed after it has been created.

Before you begin

You'll need the following:

- A minimum of four IP addresses
- Name of an IPspace

Steps

1. In System Manager, select **Cluster** and then **Storage VMs**.
2. Select + Add .
3. Provide a name for the SVM.
4. Select a protocol for client access and provide the configuration details as appropriate.
5. Add a network interfaces for the SVM including the IP addresses and subnet mask.
6. Under **Storage VM administration**, optionally:
   a. Enable a maximum capacity and select a value
   b. Manage an administrator account for the SVM
7. Select **Save**.

Related information

- Configure an AFX system SVM
- Manage AFX system cluster networking

Configure an AFX storage system SVM

After you create an SVM, you can update the configuration based on your requirements and clients needs.

About this task

There are four access paths to the SVM configuration as reflected in the tabs on the landing page for a specific SVM. These include:

- Overview

  This provides a quick dashboard overview of the current configuration details related to network interfaces and services, protocols, storage, and protection.

- Settings

  You can access and update the entire SVM configuration as organized in several areas, such as protocols,

services, policies, and security.

- Replication

  This page provides a list of the current replication relationships defined for the SVM.

- File system

  You can track the activity and analytics for the SVM

Before you begin

You need to decide which SVM you are interested in displaying and updating.

Steps

1. In System Manager, select **Cluster** and then **Storage VMs**.
2. Select the desired SVM and then the **Settings** tab.
3. Review the configuration options on the page; select and update the settings as desired.

Migrate an AFX storage system SVM

You can migrate an SVM from one ONTAP cluster to another. SVM migration with AFX operates the same as with Unified ONTAP, although there are several interoperability considerations and restrictions. Refer to the Unified ONTAP documentation for details about performing an SVM migration.

Interoperability considerations

Before planning and performing an SVM migration, you should be aware of the interoperability considerations including capabilities and limitations.

Use cases

Cluster administrators can relocate an SVM from a source cluster to a destination cluster. You might do this as part of capacity management and load balancing, or to allow for equipment upgrades or data center consolidations. Because the AFX storage system does not support in-place upgrades from Unified ONTAP, SVM migration is an important use case.

You can move your application workloads from a Unified ONTAP cluster to AFX clusters without disruption. In addition, SVMs can be migrated in other ways including from an AFX cluster to a Unified ONTAP cluster as well as among AFX clusters.

Version interoperability

The following table describes the allowable SVM migrations based on the ONTAP personality and release of the source and destination cluster.

Direction	Source version	Destination version
Unified to AFX	9.15.1 - 9.17.1	9.17.1
AFX to Unified	9.17.1	9.17.1
AFX to AFX	9.17.1	9.17.1

Prechecks

Unified ONTAP includes several prechecks that are also implemented with AFX. In addition, several new prechecks are added to flag features that aren't supported with AFX, including:

- FabricPool (volumes residing on composite aggregates)
- Thick provisioned volumes

Volume provisioning

The volumes are provisioned to balance their placement across the Storage Availability Zone (SAZ) of the AFX cluster.

Space guarantee

AFX does not support thick provisioning. A precheck is used to fail a migration if any volume in the SVM being migrated is thick provisioned.

Encryption

An AFX system supports NetApp volume encryption (NVE) but not NetApp aggregate encryption (NAE). Because of this, any NAE volumes at a Unified ONTAP cluster are converted to NVE volumes when migrated to AFX. The following table summarizes the compatibility and conversion.

Source volume	Destination volume
Plain text	Plain text
NVE	NVE
NAE	NVE

Additional restrictions

There are additional restrictions you should consider before migrating an SVM.

MetroCluster

The AFX storage system does not support NetApp MetroCluster. This creates a limitation when migrating an SVM. You cannot migrate an AFX SVM to or from an AFF or FAS system (or any NetApp system running the Unified ONTAP personality) that is configured to use MetroCluster. While these migration scenarios are not supported, they are also not explicitly blocked by the AFX prechecks and so you need to be careful not to attempt them.

Related information

- ONTAP SVM data mobility
- Compare AFX storage system to AFF and FAS systems
- FAQ for AFX storage systems

Support the cluster

Manage AutoSupport for an AFX storage system cluster

AutoSupport is a NetApp technology you can use to proactively monitor the health of your

AFX storage systems. It can automatically send messages to NetApp technical support, your internal support organization, or a support partner.

AutoSupport is enabled by default when you set up an AFX cluster and messages will be send to NetApp technical support. To send messages to your internal support organization, you need to properly configure your cluster and provide a valid email host. AFX begins sending AutoSupport messages 24 hours after it is active.

You need to sign in to System Manager using a cluster administrator account to manage AutoSupport.

Test AutoSupport connectivity

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

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Next to **AutoSupport** select ⋮ and then **Test connectivity**.
3. Enter a subject for the AutoSupport message and select **Send test AutoSupport message**.

Add AutoSupport recipients

You can optionally add members of your internal support organization to the list of email addresses that receive AutoSupport messages.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Next to **AutoSupport** select ⋮ and then **More options**.
3. Next to **Email**, select ✎ and then + Add .
4. Provide the email address for the recipient; for the recipient category, select:
   - **Partner** for your partners
   - **General** for members of your internal support organization
5. Select **Save**.

Result

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

Send AutoSupport data

If a problem occurs with your AFX system, you should manually send the AutoSupport data. This can significantly decrease the amount of time it takes to identify and resolve the issue.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Next to **AutoSupport** select ⋮ and then **Generate and send**.
3. Provide a subject for the AutoSupport message.

4. Select **Send**.

Result

Your AutoSupport data is sent to technical support.

Suppress support case generation

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

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Next to **AutoSupport** select ⋮ and then **Suppress support case generation**.
3. Specify the number of hours to suppress the generation of support cases and the nodes you don't want cases generated for.
4. Select **Send**.

Result

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** and then **Settings**.
2. Next to **AutoSupport** select ⋮ and then **Resume support case generation**.
3. Select the nodes for which you want to resume AutoSupport case generation.
4. Select **Send**.

Result

AutoSupport cases will be autogenerated for your AFX system as needed.

Related information

- Learn about ONTAP AutoSupport
- Prepare to use ONTAP AutoSupport

Submit and view support cases for an AFX storage system

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 in progress or closed.

Before you begin

You need to be registered with Active IQ to view support cases for your AFX storage system.

Steps

1. To create and submit a new support case, in System Manager select:
   a. **Cluster** and then **Support**
   b. **Go to NetApp Support**
2. To view a previously submitted case, in System Manager select:
   a. **Cluster** and then **Support**
   b. **View my cases**

Related information

- View and submit support cases with ONTAP System Manager

Upgrade and maintain the cluster

Expand an AFX storage system cluster

You can expand the compute capacity of an AFX cluster independent of the storage capacity. The expansion is performed without disruption and increases performance linearly as volumes are rebalanced across the nodes. This feature is a significant benefit as you adjust to the ongoing needs of your AFX system users.

Prepare to expand a cluster

Before expanding an AFX cluster, you should be familiar with the basic requirements and general approach to troubleshooting.

Requirements

You need the credentials for a cluster administrator account and be able to connect to the ONTAP CLI using SSH. When expanding a cluster, you must add an even number of nodes and adhere to the size limitations of your AFX system based on the release.

Troubleshooting

There are a few concepts and troubleshooting scenarios you should be aware of as you perform the cluster expansion.

Automatic volume rebalancing

Automated Topology Management (ATM) is in internal AFX system component that detects allocation imbalances and rebalances volumes across the cluster nodes. It relies on the Zero Copy Volume Move (ZCVM) technology to relocate volumes using metadata updates instead of copying the data. ZCVM is the default volume move technology available with AFX storage systems.

Possible troubleshooting scenarios

There are several scenarios you might need to investigate during the volume moves associated with the expansion of an AFX cluster.

Volumes are not being moved by ATM

This can occur when the cluster is already in balance or when there are no eligible volumes to move.

Confusion about how or when ATM should be active

It may appear that volumes aren't distributed as quickly as expected. ATM attempts to detect and respond to hardware events every five minutes. In the worst case, a rebalance operation is launched 40 minutes after the last one completed.

CLI commands

There are several commands you can use to monitor a cluster expansion operation.

- `volume move show`
- `volume move show -instance`

You should contact NetApp support for additional assistance as needed.

Add nodes to expand a cluster

This procedure describes how to add a pair of nodes to an existing cluster and can be adapted to other deployment environments. You'll need to use both the ONTAP CLI and System Manager administrative interfaces.

Steps

1. Connect to the ONTAP CLI and set advanced privilege level:

   ```
   afx> set advanced
   ```

2. Display the volume locations of the current nodes; note the number of volumes per node:

   ```
   afx> vol show -fields node,size,constituent-count -is-constituent true -node *
   ```

3. Display the cluster interconnect IP addresses and save for use in later steps:

   ```
   afx> net int show -role cluster
   ```

4. Log into the service processor of each node you wish to add to the cluster.
5. From the prompt, type **system console** to access the node's console.
6. Boot the node to display the boot menu prompt:

   ```
   LOADER> boot_ontap menu
   ```

   If the menu does not load, use the **Ctrl+C** technique to access the boot menu.

7. Select one of the boot options from the menu as appropriate; if prompted type **yes** to continue.

   If you get sent back to LOADER from here, type **boot_ontap** at the LOADER prompt.

8. Use the cluster setup wizard to configure a node management LIF, subnet, and gateway.

   This configuration will be used by System Manager to detect the node to be added to the cluster. Enter the values as prompted, including port, IP address, netmask, and default gateway.

9. Press **CTL+C** to access the CLI.
10. Modify the cluster interconnect addresses so they're routable in your network; use the configuration appropriate for your environment:

    ```
    afx> net int show -role cluster

    afx> net int modify -vserver Cluster -lif clus1 -address 192.168.100.201

    afx> net int modify -vserver Cluster -lif clus2 -address 192.168.100.202
    ```

    This step is only needed if the other interfaces do not use the 169.254.x.x addresses that ONTAP auto creates.

11. Repeat the above steps on the other AFX node controller.
12. Access the System Manager using the cluster management IP address.
13. In System Manager, select **Cluster** and then **Overview**; select the **Nodes** tab.
14. Locate the section **Not part of this cluster**; select + Add.
    - If the nodes were discovered before the cluster interconnect IP addresses are changed, you'll need to re-discover the nodes by exiting the window and navigating back.
    - You can optionally use the CLI to add the nodes instead of System Manager; see the command `cluster add-node`.
15. Provide the configuration details in the **Add nodes** menu; you can add management IP addresses manually or using a subnet.
16. Connect to the ONTAP CLI to monitor the status of the node add operation:

    ```
    afx> add-node-status
    ```

17. After the operations have completed, confirm the volume placement across all nodes; issue the command once for each node using the appropriate node name:

    ```
    afx> set advanced

    afx> vol show -fields node,size,constituent-count -is-constituent true -node
    NODE_NAME
    ```

Result

- Adding new nodes to the cluster is nondisruptive.
- Volume moves should happen automatically.
- Performance will scale linearly.

Related information

- Prepare to administer your AFX system
- FAQ for ONTAP AFX storage systems
- NetApp Support Site

Upgrade ONTAP on an AFX storage system

When you upgrade your ONTAP software on your AFX 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.

AFX storage systems do not support ONTAP revert operations.

ONTAP software upgrades for AFX storage 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.

Related information

- Learn about ONTAP upgrade.

Update firmware on an AFX storage system

ONTAP automatically downloads and updates firmware and system files on your AFX storage system by default. If you want to view the recommended updates before they are downloaded and installed, you can disable automated updates. You can also edit update parameters to show you notifications of available updates before any action is performed.

Enable automatic updates

When you enable automatic updates for your AFX cluster, recommended updates for storage firmware, SP/BMC firmware and system files are automatically downloaded and installed by default.

Steps

1. In System Manager, select **Cluster** and then **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 ONTAP AFX 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. 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 → and 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.

ONTAP revert unsupported with AFX storage systems

Reverting an ONTAP cluster is the process of moving all the nodes to the previous major ONTAP release.

NetApp AFX storage systems do not support ONTAP revert. Attempting a revert operation with AFX can result in cluster instability and data loss. You should not attempt a revert operation on an AFX system.

Additional administration for an AFX storage system cluster

In addition to the typical AFX cluster administration, there may be other tasks you need to perform based on your environment. Most of the additional tasks can be performed using System Manager, although in some cases you may need to use the CLI.

> The ONTAP features and administration described are common to AFX storage systems and AFF or FAS systems running Unified ONTAP. Links to the relevant Unified ONTAP documentation are included as appropriate.

Licensing

AFX systems are licensed in a similar way as Unified ONTAP AFF and FAS systems. An AFX cluster includes most features by default for the protocols supported.

ONTAP license management

An ONTAP license is a record of one or more software entitlements. All licenses are defined and provided using a NetApp license file (NLF). Refer to ONTAP licensing overview for more information.

Install a license on an AFX system

You can install license files to activate additional features as needed for your AFX storage system.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. Next to **Licenses**, select →.
3. Select the **Features** tab to display the available ONTAP features.
4. To optionally install a licenses, select the **Installed licenses** tab.
5. Select + Add.
6. Select a local license file and select **Add**.

Security

There are several optional security features you can configure and use with your AFX deployment.

ONTAP security and data encryption

It's important to protect the security and priacy of your AFX storage system. Refer to Security and data encryption

ONTAP authentication and access control

The AFX storage system provides several options for configuring authentication and access control services. Refer to Authentication and access control for more information.

Administer OAuth 2.0 on an AFX system

OAuth 2.0 is the industry standard authorization framework used to restrict and control access to protected resources using signed access tokens.

Steps

1. In System Manager, select **Cluster** and then **Settings**.
2. In the **Security** section, next to **OAuth 2.0 authorization**, select →.
3. Enable OAuth 2.0
4. Select **Add configuration** and provide the configuration details.
5. Select **Save**.

Related information

- FAQ for AFX storage systems
- Overview of the ONTAP OAuth 2.0 implementation
- Additional administration for AFX SVMs

Copyright information

Trademark information