Manage networking and security

AFX

NetApp
February 11, 2026

Table of Contents

Manage networking and security . . . 1
- Manage AFX storage system cluster networking . . . 1
  - Create a broadcast domain . . . 1
  - Create an IPspace . . . 1
  - Create a subnet . . . 2
  - Create a network interface . . . 2
  - Related information . . . 3
- Manage AFX storage system Ethernet ports . . . 3
  - Create a VLAN . . . 3
  - Create a LAG . . . 4
  - Related information . . . 4
- Prepare AFX storage system authentication services . . . 4
  - Configure LDAP . . . 4
  - Configure SAML authentication . . . 4
  - Related information . . . 5
- Manage AFX storage system cluster users and roles . . . 5
  - Create an account role . . . 5
  - Create a cluster account . . . 6
  - Related information . . . 6
- Manage certificates on an AFX storage system . . . 6
  - Generate a certificate signing request . . . 6
  - Add a trusted certificate authority . . . 7
  - Renew or delete a trusted certificate authority . . . 7
  - Add a client/server certificate or local certificate authority . . . 7
  - Renew or delete a client/server certificate or local certificate authorities . . . 8
  - Related information . . . 8

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

Copyright information

Trademark information