Administer your storage VMs and data

AFX

NetApp
February 11, 2026

Table of Contents

Administer your storage VMs and data

Manage data

Prepare to manage your AFX storage system data

Before managing your AFX data, you should be familiar with the basic concepts and capabilities.

Because many of the concepts and administration procedures available on AFF and FAS systems are the same with AFX storage systems, reviewing the Unified ONTAP documentation can be helpful. Refer to the links in Related information for more information.

Terminology and options

There are several terms related to AFX storage you should be familiar with.

FlexVolume

A FlexVol is a type of logical container used in AFX storage systems. FlexVol volumes can be expanded, contracted, moved, and efficiently copied. They can also be partitioned into more manageable units using qtrees and resource usage can be limited using quotas.

FlexGroup

A FlexGroup volume is a scale-out NAS container that provides both high performance and automatic load distribution. Each consists of multiple volumes that share traffic transparently. FlexGroup volumes offer several benefits, including improved scalability and performance as well as simplified management.

FlexCache

FlexCache is an ONTAP caching technology that creates sparse, writable replicas of volumes on the same or different ONTAP clusters. It is designed to improve data access performance by bringing data closer to users, which can result in faster throughput with a smaller footprint. FlexCache is particularly useful for read-intensive workflows and helps to offload traffic from heavily accessed volumes.

S3 bucket

An S3 bucket is a storage container that holds objects or data in the cloud. With ONTAP, an S3 NAS bucket is a mapping between an S3 bucket name and a NAS path, allowing S3 access to any part of an SVM namespace with existing volumes and directory structure.

Data container

In the context of an AFX system, a data container is a generic term and can be either a volume or S3 bucket.

Qtree

A qtree is a logical subdivision within a volume that you can create to manage and organize data. It allows you to specify its properties and security style (NTFS or UNIX) and can inherit export policies from its parent volume or have its own. Qtrees can contain files and directories, and are often used to manage permissions and quotas more granularly within a volume.

Quota

A quota in ONTAP is a limit set on the amount of storage space or number of files that can be used by a

user, group, or qtree. Quotas are used to manage and control resource usage within a storage system, ensuring that no single user or application can consume an excessive amount of resources.

NFS session trunking

NFS trunking is a technology that enables NFS v4.1 clients to open multiple connections to different LIFs on the NFS server. This increases the data transfer speed and provides resilience through multiple paths when exporting volumes to trunking-capable clients. The LIFs must be on the same node to participate in the trunk.

To enable trunking, you need to have an SVM configured for NFS and NFSv4.1 should be enabled. It also requires remounting all the NFSv4.x clients after a configuration change which can be disruptive. Support and configuration procedures for NFS trunking are the same for all ONTAP systems. Learn more about NFS trunking

File system analytics

File System Analytics (FSA) is an ONTAP feature that provides real-time visibility into file usage and storage capacity trends within FlexGroup or FlexVol volumes. It eliminates the need for external tools by offering insights into storage utilization and optimization opportunities. FSA provides detailed views at various levels of a volume's file system hierarchy, including the SVM, volume, directory, and file levels.

Data migration options

There are several data migration options. The focus is on migrating external data into an AFX cluster.

Migrating data from AFF or FAS systems

A fully integrated migration path from AFF or FAS systems (which run the Unified ONTAP personality) to AFX is available using the following technologies:

- SnapMirror
- SVM Migrate
- SVM DR

In addition, FlexCache volumes can be attached between AFX and AFF or FAS systems in either direction.

Migrating data from a non-ONTAP source

Data migration from non-ONTAP systems can be performed using file-level copy operations. Fast copy utilities such as XCP or Copy and Sync can be used as well as standard utilities such as RoboCopy (for SMB) and rsync (for NFS) as well as third-party tools such as DataDobi.

Migration limitations

You can replicate data from AFF or FAS systems to AFX if the source data volume does not contain LUNs or NVMe namespaces. When replicating from AFX to AFF or FAS systems, the minimum supported ONTAP version for the AFF or FAS system is 9.16.1. This is the first ONTAP release that supports Advanced Capacity Balancing.

Display an overview of your storage

To get started managing your AFX data, you should display an overview of the storage.

About this task

You can access all the volumes and buckets defined for the AFX cluster. Each of these is considered to be a

data container.

Steps

1. In System Manager, select **Storage** and then **Overview**
2. Next to **Volumes**, select → to display a list of volumes.
3. Next to **Buckets**, select → to display a list of buckets.
4. Update or create a data container as needed.

Related information

- Learn about ONTAP File System Analytics
- Additional AFX SVM administration
- Prepare to administer your AFX system
- Migrate an AFX system SVM
- NetApp Interoperability Matrix Tool

Create and configure a volume on an AFX storage system

You can create a volume and attach it to an SVM. Each volume can be exposed to clients using one of the access protocols supported by AFX.

About this task

When creating a volume, you need to provide a minimum amount of configuration details. Additional details can be provided during creation or afterwards by editing the volume. You need to select the SVM for the volume if you've created additional SVMs.

Steps

1. In System Manager, select **Storage** and then **Volumes**.
2. Select + Add and provide the basic configuration including name, capacity, and optimization.
3. Optionally select **More options** for additional configuration related to data protection, SnapLock, and NFS access.
4. Select **Save** to add the volume.

Manage the AFX storage system volumes

There are several administrative tasks you can perform as part of administering the volumes defined at your AFX cluster.

Create a qtree

A qtree is a logical subdivision within a volume that you can create to organize and administer data.

Steps

1. In System Manager, select **Storage** and then **Qtrees**.
2. Select + Add and provide the basic configuration including name, volume, and security style; optionally configure a quota.

3. Select **Save** to add the qtree.

Create a quota

A quota is a limit set on the amount of storage space or number of files that can be used by a user, group, or qtree. Quotas are used to manage and control resource usage within an AFX system.

Steps

1. In System Manager, select **Storage** and then **Quotas**.
2. Select the **Usage** tab to display a list of the active quotas across all volumes.
3. Select the **Volumes** tab to display a list of the volumes defined in the AFX cluster; select a specific volume to display additional information.
4. To define a quota, select the **Rules** tab.
5. Provide the configuration details, including the quota target, type and limits.
6. Select **Save** to add the quota.

Create and configure an S3 bucket on an AFX storage system

You can create a bucket and attach it to an SVM. Each bucket can be exposed to clients using the S3 access protocol supported by AFX.

About this task

When creating a bucket, you need to provide a minimum amount of configuration details. Additional details can be provided during creation or afterwards by editing the bucket. You need to select the SVM for the bucket if you've created additional SVMs.

Before you begin

You need to configure the S3 service for the SVM for clients to be able to access the bucket.

Steps

1. In System Manager, select **Storage** and then **Buckets**.
2. Select + Add and provide the basic configuration including name and capacity.
3. Optionally select **More options** for additional configuration related to data protection, locking, and permissions.
4. Select **Save** to add the bucket.

Manage the AFX storage system buckets

There are several administrative tasks you can perform as part of managing AFX S3 buckets and client access. S3 configuration and support in AFX is the same as provided with Unified ONTAP. Refer to the Unified ONTAP documentation for details.

Related information

Learn about ONTAP S3 configuration

Monitor and troubleshoot an AFX storage system

The AFX system includes several options to monitor the storage each cluster manages.

Display NAS clients

You can display a list of the NFS and SMB/CIFS clients currently connected to the AFX cluster.

Steps

1. In System Manager, select **Clients** in the navigation pane.
2. Select the tab **NFS** or **SMB/CIFS** as desired.
3. Customize the display as well as search and download the client information as needed.

Related information

- Prepare to manage your AFX data

Protect data

Prepare to protect your AFX storage system data

Before protecting your AFX data, you should be familiar with some of the key concepts and capabilities.

Because many of the concepts and administration procedures available on AFF and FAS systems are the same with AFX storage systems, reviewing the Unified ONTAP documentation for Data protection and disaster recovery can be helpful.

Terminology and options

There are several terms related to AFX data protection you should be familiar with.

Snapshot
: A snapshot is a read-only, point-in-time image of a volume. It is a foundational technology for ONTAP's replication and data protection services.

Consistency group
: A consistency group is a collection of volumes that are managed as a single unit. You can create consistency groups to simplify storage management and data protection for application workloads. For example, you can snapshot several volumes in one operation by using the consistency group instead of the individual volumes.

Hierarchical consistency group
: Hierarchical consistency groups were introduced with ONTAP 9.16.1 and are available with AFX. With a hierarchical structure, one or more consistency groups can be configured as children under a parent. These hierarchical groups allow you to apply individual snapshot policies to child consistency groups and replicate the snapshots of all the children to a remote cluster as a single unit by replicating the parent.

SnapLock
: SnapLock is an ONTAP feature that allows you to protect your files by moving them to a write once read

many (WORM) state. This prevents modification or deletion for a specified retention period. SnapLock volumes are created cannot be converted from non-SnapLock volumes after creation based on the retention.

AFX data protection limitations

You should be aware of the ONTAP data protection limits and restrictions enforced by the AFX storage system.

SnapMirror synchronous (SM-S)

There is a scale limitation when using SM-S. You can have a maximum of 400 relationships across a single AFX system cluster.

Related information

- Additional AFX SVM administration
- Prepare to your administer AFX system

Create a consistency group on an AFX storage system

You can create consistency groups to simplify storage management and data protection for application workloads. A consistency group can be based on existing or new volumes.

Before you begin

If you plan to create one more more new volumes, you should become with the configuration options when creating a ne volume.

Steps

1. In System Manager, select **Protection** and then **Consistency groups**.
2. Select + Add and choose one of:
   - Using existing volumes
   - Using new NAS volumes
3. Provide the configuration details, including name, volumes, application type, and protection.
4. Select **Add**.

Related information

- Manage consistency groups
- Create and configure an AFX volume

Manage consistency groups on an AFX storage system

You can manage the consistency groups on an AFX system. This can streamline your storage administration.

Add snapshot data protection to a consistency group

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

Steps

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

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

Option	Steps
Select an existing snapshot policy	Select ⌄ next to the default policy; then select the existing policy that you want to use.
Create a new snapshot policy	a. Select + Add ; then enter the new policy name. b. Select the policy scope. c. Under **Schedules** select + Add . d. Select the name that appears under **Schedule name**; then select ⌄. e. Select the policy schedule. f. Under **Maximum snapshots**, enter the maximum number of snapshots that you want to retain of the consistency group. g. Optionally, under **SnapMirror label** enter a SnapMirror label. h. Select **Save**.

6. Select **Edit**.

Related information

- Learn about ONTAP consistency groups

Create a snapshot on an AFX storage system

To back up data on your AFX system, you need to create a snapshot. You can create a snapshot manually or schedule to be created automatically using a consistency group.

Before you begin

A snapshot is a local, read-only copy of your data that you can use to restore volumes to specific points in time. Snapshots can be created manually on demand or automatically at regular intervals based on a snapshot policy and schedule.

The snapshot policy and schedule specifies the details, including when to create the snapshots, how many copies to retain, how to name them, and how to label them for replication. For example, a system might create one snapshot every day at 12:10 a.m., retain the two most recent copies, name them “daily” (appended with a timestamp), and label them “daily” for replication.

Types of snapshots

You can create an on-demand snapshot of a single volume or a consistency group. You can also create automated snapshots of a consistency group containing multiple volumes. However you cannot create automated snapshots of a single volume.

- On-demand snapshots

  You can create an on-demand snapshot of a volume at any time. The volume does not need to be a member of a consistency group to be protected by an on-demand snapshot. If you create a snapshot of a volume that is a member of a consistency group, the other volumes in the consistency group are not included in the snapshot. When you create an on-demand snapshot of a consistency group, all the volumes in the consistency group are included.

- Automated snapshots

  Automated snapshots are created based on the snapshot policy definitions. To apply a snapshot policy to a volume for automated snapshot creation, the volumes needs to be a member of the same consistency group. If you apply a snapshot policy to a consistency group, all the volumes in the consistency group are protected.

Create a snapshot

Create a snapshot of a volume or consistency group.

Snapshot of a consistency group

Steps

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

   Local protection creates the snapshot on the same cluster containing the volume.

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

      The SnapMirror label is used by the remote destination.

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

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

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

6. If you want to replicate your snapshots to a remote cluster, under **Remote protection**, select **Replicate to a remote cluster**.
   a. Select the source cluster and storage VM; then select the replication policy.

      The initial data transfer for replication starts immediately by default.

7. Select **Save**.

Snapshot of a volume

Steps

1. In System Manager, select **Storage** and then **Volumes**.
2. Hover over the name of the volume you want to protect.
3. Select ⋮ ; then select **Protect**. If you want to create an immediate snapshot on-demand, under **Local protection**, select **Add a snapshot now**.

   Local protection creates the snapshot on the same cluster containing the volume.

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

   The SnapMirror label is used by the remote destination.

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

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

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

6. If you want to replicate your snapshots to a remote cluster, under **Remote protection**, select **Replicate to a remote cluster**.
   a. Select the source cluster and storage VM; then select the replication policy.

      The initial data transfer for replication starts immediately by default.
7. Select **Save**.

Related information

- Create an ONTAP snapshot policy

Manage snapshots on an AFX storage system

You can manage snapshots on your AFX system. Refer to the Unified ONTAP documentation for details.

Related information

- Create an ONTAP snapshot policy
- Protect ONTAP FlexGroup volumes using snapshots

Create an intercluster SVM peer relationship on an AFX storage system

A peer relationship defines network connections that enable clusters and storage virtual machine (VM) to exchange data securely. You can create a peer relationship between storage VMs on different clusters to enable data protection and disaster recovery using SnapMirror.

Before you begin

You must have established a cluster peer relationship between the local and remote clusters before you can create a storage VM peer relationship. Create a cluster peer relationship if you have not already done so.

Steps

1. In System Manager, select **Protection > Overview**.

2. Under **Storage VM peers** select **Add a storage VM peer**.
3. Select the storage VM on the local cluster; then select the storage VM on the remote cluster.
4. Select **Add a storage VM peer**.

Related information

- Learn more about peer relationships.

Manage snapshot replication on an AFX storage system

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

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

Step 1: Create a cluster peer relationship

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

Before you begin

The prerequisites for cluster peering are the same for AFX systems as for other ONTAP systems. Review the prerequisites for cluster peering.

Steps

1. On the local cluster, in System Manager, select **Cluster > Settings**.
2. Under **Intercluster Settings** next to **Cluster peers** select ⋮, then select **Add a cluster peer**.
3. Select **Lauch remote cluster**; this generates a passphrase you'll use to authenticate with the remote cluster.
4. After the passphrase for the remote cluster is generated, paste it under **Passphrase** on the local cluster.
5. Select + Add ; then enter the intercluster network interface IP address.
6. Select **Initiate cluster peering**.

What's next?

You have peered for local AFX cluster with a remote cluster. You can now create a replication relationship.

Step 2: Optionally, create a replication policy

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

Steps

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

3. Enter a name for the replication policy or accept the default name; then enter a description.
4. Select the **Policy scope**.

   If you want to apply the replication policy to the entire cluster, select **Cluster**. If you want the replication policy applied only to the volume in a specific storage VM, select **Storage VM**.

5. Select the **Policy type**.

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

6. Select **Save**.

What's next?

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

Step 3: Create a replication relationship

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

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

Before you begin

Create a replication relationship with or without locked destination snapshots.

With locked snapshots

Steps

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

   You must select a *vault* replication policy.

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

   The initial data transfer begins immediately by default.

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

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

11. Select **Save**.

Without locked snapshots

Steps

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

Option	Steps
Local destinations	1. Select **Local destinations**, then select Replicate. 2. Search for and select the source consistency group. The *source* consistency group refers to the consistency group on your local cluster that you want to replicate.

Option	Steps
Local sources	1. Select **Local sources**, then select Replicate . 2. Search for and select the source consistency group. The *source* consistency group refers to the consistency group on your local cluster that you want to replicate. 3. Under **Replication destination**, select the cluster to replicate to; then select the storage VM.

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

   The initial data transfer begins immediately by default.

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

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

6. Select **Save**.

What's next?

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

Step 4: Test replication failover

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

Steps

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

What's next?

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

Manage AFX storage system data protection policies and schedules

You can use snapshot policies to protect data in your consistency groups based on an automated schedule. The policy schedules within snapshot policies determine how often snapshots are taken.

Create a new protection policy schedule

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

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

Steps

1. Select **Protection** and then **Policies**; then select **Schedule**.
2. Select + Add .
3. Enter a name for the schedule; then select the schedule parameters.
4. Select **Save**.

What's next?

Now that you have created a new policy schedule, you can use the newly created schedule within your policies to define when snapshots are taken.

Create a snapshot policy

A snapshot policy defines how often snapshots are taken, the maximum number of snapshots allowed, and how long snapshots are retained.

Steps

1. In System Manager, select **Protection** and then **Policies**; then select **Snapshot policies**.
2. Select + Add .
3. Enter a name for the snapshot policy.
4. Select **Cluster** to apply the policy to the entire cluster. Select **Storage VM** to apply the policy to an individual storage VM.
5. Select **Add a schedule**; then enter the snapshot policy schedule.
6. Select **Add policy**.

What's next?

Now that you have created a snapshot policy, you can apply it to a consistency group. Snapshots will be taken of the consistency group based on the parameters you set in your snapshot policy.

Apply a snapshot policy to a consistency group

Apply a snapshot policy to a consistency group to automatically create, retain, and label snapshots of the

consistency group.

Steps

1. In System Manager, select **Protection** and then **Policies**; then select **Snapshot policies**.
2. Hover over the name of the snapshot policy you want to apply.
3. Select ⋮; then select **Apply**.
4. Select the consistency groups to which you want to apply the snapshot policy; then select **Apply**.

What's next?

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

Edit, delete, or disable a snapshot policy

Edit a snapshot policy to modify the policy name, maximum number of snapshots, or the SnapMirror label. Delete a policy to remove it and its associated back up data from your cluster. Disable a policy to temporarily stop the creation or transfer of snapshots specified by the policy.

Steps

1. In System Manager, select **Protection** and then **Policies**; then select **Snapshot policies**.
2. Hover over the name of the snapshot policy you want to edit.
3. Select ⋮; then select **Edit**, **Delete**, or **Disable**.

Result

You have modified, deleted or disabled the snapshot policy.

Edit a replication policy

Edit a replication policy to modify the policy description, transfer schedule, and rules. You can also edit the policy to enable or disable network compression.

Steps

1. In System Manager, select **Protection** and then **Policies**.
2. Select **Replication policies**.
3. Hover over the replication policy that you want to edit; then select ⋮.
4. Select **Edit**.
5. Update the policy; then select **Save**.

Secure data

Prepare to secure your AFX storage system data

Before managing your AFX data, you should be familiar with the major concepts and capabilities.

Terminology and options

There are several terms related to AFX data security you should be familiar with.

Ransomware

Ransomware is malicious software that encrypts files making them inaccessible to the user. There is typically some type of payment demanded to decrypt the data. ONTAP provides solutions to protect against ransomware through features like Autonomous Ransomware Protection (ARP).

Encryption

Encryption is the process of converting data into a secure format that cannot be easily read without proper authorization. ONTAP offers both software-based and hardware-based encryption technologies to protect data at rest. This ensures it cannot be read if the storage medium is repurposed, returned, misplaced, or stolen. These encryption solutions can be managed using either an external key management server or the Onboard Key Manager provided by ONTAP. Refer to Encrypt data at rest on an AFX storage system for more information.

Digital certificates and PKI

A digital certificate is an electronic document used to prove ownership of a public key. The public key and associated private key can be used in various ways, including to establish identity typically as part of a larger security framework such as TLS and IPsec. These keys, as well as the supporting protocols and formatting standards, form the basis for public key infrastructure (PKI). Refer to Manage certificates on an AFX storage system for more information.

Internet Protocol Security

IPsec is an Internet standard that provides in-flight data encryption, integrity, and authentication for traffic flowing among network endpoints at the IP level. It secures all IP traffic between ONTAP and clients including higher level protocols such as NFS and SMB. IPsec provides protection against malicious replay and man-in-the-middle attacks on your data. Refer to Secure IP connections on your AFX storage systems for more information.

Related information

- Additional AFX SVM administration
- Prepare to administer your AFX system

Encrypt data at rest on an AFX storage system

You can encrypt your data at the hardware and software level for dual-layer protection. When you encrypt data at rest, it can’t be read if the storage medium is repurposed, returned, misplaced, or stolen.

NetApp Storage Encryption (NSE) supports hardware encryption using self-encrypting drives (SEDs). SEDs encrypt data as it is written. Each SED contains a unique encryption key. Encrypted data stored on the SED can’t be read without the SED’s encryption key. Nodes attempting to read from an SED must be authenticated to access the SED’s encryption key. Nodes are authenticated by obtaining an authentication key from a key manager, then presenting the authentication key to the SED. If the authentication key is valid, the SED will give the node its encryption key to access the data it contains.

Before you begin

Use the AFX onboard key manager or an external key manager to serve authentication keys to your nodes. In addition to NSE, you can also enable software encryption to add another layer of security to your data.

Steps

1. In System manager, select **Cluster** and then **Settings**.
2. In the **Security** section, under **Encryption**, select **Configure**.
3. Configure the key manager.

Option	Steps
Configure the Onboard key Manager	a. Select **Onboard Key Manager** to add the key servers. b. Enter a passphrase.
Configure an external key manager	a. Select **External key manager** to add the key servers. b. Select + Add to add the key servers. c. Add the KMIP server CA certificates. d. Add the KMIP client certificates.

4. Select **Dual-layer encryption** to enable software encryption.
5. Select **Save**.

Related information

- Encryption

Secure IP connections on your AFX storage systems

IP Security (IPsec) is an Internet protocol standard that provides data encryption, integrity, and authentication for traffic flowing among network endpoints at the IP level. You can use IPsec to enhance the security of the front-end network between an AFX cluster and the clients.

Configuring IPsec on an AFX system

The IPsec configuration procedures for AFX storage systems are the same as AFF and FAS systems, with the exception of the supported network interface controller (NIC) cards used with the hardware offload feature. Refer to Prepare to configure IP security for the ONTAP network for more information.

Hardware offload feature

Several of the IPsec cryptographic operations, such as encryption and integrity checks, can be offloaded to a supported NIC card on your AFX system. This can significantly improve the performance and throughput of the network traffic protected by IPsec.

Beginning with ONTAP 9.18.1, the IPsec hardware offload feature is extended to support IPv6 traffic.

The following NIC cards are supported for the IPsec hardware offload feature on AFX storage systems beginning with ONTAP 9.17.1:

- X50130B (2p, 40G/100G Ethernet controller)
- X50131B (2p, 40G/100G/200G/400G Ethernet controller)

Refer to the NetApp Hardware Universe for more information about the supported cards for the ONTAP release running on your AFX system.

Related information

- Prepare to configure IP security for the ONTAP network
- NetApp Hardware Universe

Additional administration for an AFX storage system SVM

In addition to the typical AFX SVM 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.

Storage management and performance

There are several optional storage management and performance features you can configure and use with your AFX deployment.

ONTAP NAS storage management

Network Attached Storage (NAS) provides dedicated file storage which can be accessed by multiple clients in the network. ONTAP supports several NAS protocols. Refer to NAS storage management for more information.

ONTAP FlexCache volumes

FlexCache is an ONTAP remote caching feature. It brings data closer to clients which improves access performance and reduces costs. Creating a FlexCache volume, which initially copies only the metadata from the origin file system, simplifies file distribution and reduces WAN traffic. Refer to Learn about ONTAP FlexCache volumes for more information.

ONTAP FlexGroup volumes

A FlexGroup volume consists of several member volumes that share the traffic automatically and transparently. FlexGroup volumes offer several benefits, including high performance and simplified management. Refer to FlexGroup volume setup for more information.

Data protection

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

Consistency groups

A consistency group is a collection of volumes that are managed as a single unit. Refer to Learn about ONTAP

consistency groups for more information.

SnapLock

You can protect your files by converting them to a write once read many (WORM) state at a volume level. SnapLock supports two modes. Compliance mode ensures the files cannot be deleted until their retention period expires which addresses government or industry-specific mandates. Enterprise mode allows privileged users to delete files before their retention period expires. Refer to Learn about ONTAP SnapLock for more information.

Security

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

FPolicy

FPolicy is a file access notification framework used to monitor and manage file access events on storage virtual machines (SVMs). You can use FPolicy to create policies that define which file operations to monitor, and optionally block, based on criteria you define. FPolicy is commonly used for security auditing, compliance, and data governance. Refer to Learn about ONTAP FPolicy solutions for more information.

ONTAP event and performance monitoring

You can monitor the health and performance of a cluster. This includes setting up alerts for events and managing notifications for system health alerts. Refer to Event, performance, and health monitoring for more information.

Related information

- FAQ for AFX storage systems
- Additional administration for AFX clusters

Copyright information

Trademark information