ONTAP® 9

Concepts

November 2018 | 215-11959_J0
doccomments@netapp.com

Updated for ONTAP 9.5
# Table of Contents

Deciding whether to use this guide ............................................................. 5  
**ONTAP platforms** .................................................................................. 6  
Cluster storage .......................................................................................... 7  
High-availability pairs .............................................................................. 8  
**Network architecture** ........................................................................... 9  
  Logical ports ............................................................................................ 9  
  Support for industry-standard network technologies .................................. 10  
**Disks and aggregates** .......................................................................... 11  
  Aggregates and RAID groups ................................................................. 11  
  Root-data partitioning ............................................................................ 12  
**Volumes, qtrees, files, and LUNs** ........................................................... 13  
**Storage virtualization** ........................................................................ 14  
  SVM use cases ........................................................................................ 15  
  Cluster and SVM administration ............................................................ 15  
  Namespaces and junction points .............................................................. 16  
**Path failover** ....................................................................................... 17  
  NAS path failover .................................................................................. 17  
  SAN path failover .................................................................................. 18  
**Load balancing** .................................................................................. 19  
**Replication** ......................................................................................... 21  
  Snapshot copies ...................................................................................... 21  
  SnapMirror disaster recovery and data transfer .......................................... 22  
  SnapVault archiving ............................................................................... 23  
  MetroCluster continuous availability ....................................................... 24  
**Storage efficiency** ............................................................................... 25  
  Thin provisioning ................................................................................... 25  
  Deduplication ......................................................................................... 25  
  Compression ............................................................................................ 26  
  FlexClone volumes, files, and LUNs ....................................................... 26  
**Security** ............................................................................................... 27  
  Client authentication and authorization .................................................... 27  
  Administrator authentication and RBAC ................................................... 28  
  Virus scanning ....................................................................................... 28  
  Encryption ............................................................................................... 29  
  WORM storage ...................................................................................... 30  
**Application aware data management** .................................................... 31  
**ONTAP release model** .......................................................................... 32  
Where to find additional information ....................................................... 33  
**Copyright information** .......................................................................... 36  
**Trademark information** ...................................................................... 37
Deciding whether to use the Concepts Guide

This guide describes the concepts that inform ONTAP data management software, including cluster storage, high-availability, virtualization, data protection, storage efficiency, and security. You should use this guide if you want to understand the full range of ONTAP features and benefits before you configure your storage solution.

If you want to create a basic storage configuration using best practices, you should choose the appropriate document from NetApp's library of express guides and power guides:

- Express guides describe how to complete key tasks quickly using OnCommand System Manager.
- Power guides describe how to complete advanced tasks quickly using the CLI.

If you need reference and configuration information about the ONTAP capabilities described in this guide, you should choose among the following documentation:

- High availability (HA) configuration
  High-availability configuration
- Cluster and SVM administration
  System administration
- Network and LIF management
  Network and LIF management
- Disks and aggregates
  Disk and aggregate management
- FlexVol volumes, FlexClone technology, and storage efficiency features
  Logical storage management
- SAN host provisioning
  SAN administration
- NAS file access
  - NFS management
  - SMB/CIFS management
- Disaster recovery and archiving
  Data protection
ONTAP platforms

ONTAP data management software offers unified storage for applications that read and write data over block- or file-access protocols, in storage configurations that range from high-speed flash, to lower-priced spinning media, to cloud-based object storage.

ONTAP implementations run on NetApp-engineered FAS or AFF appliances, on commodity hardware (ONTAP Select), and in private, public, or hybrid clouds (NetApp Private Storage or Cloud Volumes ONTAP). Specialized implementations offer best-in-class converged infrastructure (FlexPod Datacenter) and access to third-party storage arrays (FlexArray Virtualization).

Together these implementations form the basic framework of the NetApp data fabric, with a common software-defined approach to data management and fast, efficient replication across platforms.

About FlexPod Datacenter and FlexArray Virtualization

Although not represented in the illustration of the NetApp data fabric, FlexPod Datacenter and FlexArray Virtualization are key ONTAP implementations:

- FlexPod integrates best-in-class storage, networking, and compute components in a flexible architecture for enterprise workloads. Its converged infrastructure speeds the deployment of business-critical applications and cloud-based data center infrastructures.

- FlexArray is a front end for third-party and NetApp E-Series storage arrays, offering a uniform set of capabilities and streamlined data management. A FlexArray system looks like any other ONTAP system and offers all the same features.
Cluster storage

The current iteration of ONTAP was originally developed for NetApp's scale out cluster storage architecture. This is the architecture you typically find in datacenter implementations of ONTAP. Because this implementation exercises most of ONTAP's capabilities, it's a good place to start in understanding the concepts that inform ONTAP technology.

Datacenter architectures usually deploy dedicated FAS or AFF controllers running ONTAP data management software. Each controller, its storage, its network connectivity, and the instance of ONTAP running on the controller is called a node.

Nodes are paired for high availability (HA). Together these pairs (up to 12 nodes for SAN, up to 24 nodes for NAS) comprise the cluster. Nodes communicate with each other over a private, dedicated cluster interconnect.

Depending on the controller model, node storage consists of flash disks, capacity drives, or both. Network ports on the controller provide access to data. Physical storage and network connectivity resources are virtualized, visible to cluster administrators only, not to NAS clients or SAN hosts.

Nodes in an HA pair must use the same storage array model. Otherwise you can use any supported combination of controllers. You can scale out for capacity by adding nodes with like storage array models, or for performance by adding nodes with higher-end storage arrays.

Of course you can scale up in all the traditional ways as well, upgrading disks or controllers as needed. ONTAP’s virtualized storage infrastructure makes it easy to move data nondisruptively, meaning that you can scale vertically or horizontally without downtime.

---

**Scale out for capacity**

You can scale out for capacity by adding nodes with like controller models, or for performance by adding nodes with higher-end storage arrays, all while clients and hosts continue to access data.

---

**Single-node clusters**

A single-node cluster is a special implementation of a cluster running on a standalone node. You might want to deploy a single-node cluster in a branch office, for example, assuming the workloads are small enough and that storage availability is not a critical concern.

In this scenario, the single-node cluster would use SnapMirror replication to back up the site's data to your organization's primary data center. ONTAP Select, with its support for ONTAP running on commodity hardware, would be a good candidate for this type of implementation.
High-availability pairs

Cluster nodes are configured in high-availability (HA) pairs for fault tolerance and nondisruptive operations. If a node fails or if you need to bring a node down for routine maintenance, its partner can take over its storage and continue to serve data from it. The partner gives back storage when the node is brought back on line.

HA pairs always consist of like controller models. The controllers typically reside in the same chassis with redundant power supplies.

An internal HA interconnect allows each node to continually check whether its partner is functioning and to mirror log data for the other’s nonvolatile memory. When a write request is made to a node, it is logged in NVRAM on both nodes before a response is sent back to the client or host. On failover, the surviving partner commits the failed node’s uncommitted write requests to disk, ensuring data consistency.

Connections to the other controller’s storage media allow each node to access the other’s storage in the event of a takeover. Network path failover mechanisms ensure that clients and hosts continue to communicate with the surviving node.

To assure availability, you should keep performance capacity utilization on either node at 50% to accommodate the additional workload in the failover case. For the same reason, you may want to configure no more than 50% of the maximum number of NAS virtual network interfaces for a node.

On failover, the surviving partner commits the failed node’s uncommitted write requests to disk, ensuring data consistency.

Takeover and giveback in virtualized ONTAP implementations

Storage is not shared between nodes in virtualized “shared-nothing” ONTAP implementations like Cloud Volumes ONTAP or ONTAP Select. When a node goes down, its partner continues to serve data from a synchronously mirrored copy of the node’s data. It does not take over the node’s storage, only its data serving function.
Network architecture

The network architecture for an ONTAP datacenter implementation typically consists of a cluster interconnect, a management network for cluster administration, and a data network. NICs (network interface cards) provide physical ports for Ethernet connections. HBAs (host bus adapters) provide physical ports for FC connections.

Logical ports

In addition to the physical ports provided on each node, you can use logical ports to manage network traffic. Logical ports are interface groups or VLANs.

Interface groups

*Interface groups* combine multiple physical ports into a single logical “trunk port.” You might want to create an interface group consisting of ports from NICs in different PCI slots to ensure against a slot failure bringing down business-critical traffic.

An interface group can be single-mode, multimode, or dynamic multimode. Each mode offers differing levels of fault tolerance. You can use either type of multimode interface group to load-balance network traffic.

VLANs

*VLANs* separate traffic from a network port (which could be an interface group) into logical segments defined on a switch port basis, rather than on physical boundaries. The *end-stations* belonging to a VLAN are related by function or application.

You might group end-stations by department, such as Engineering and Marketing, or by project, such as release1 and release2. Because physical proximity of the end-stations is irrelevant in a VLAN, the end-stations can be geographically remote.
Support for industry-standard network technologies

ONTAP supports all major industry-standard network technologies. Key technologies include IPspaces, DNS load balancing, and SNMP traps.

Broadcast domains, failover groups, and subnets are described in *NAS path failover* on page 17.

**IPspaces**

You can use an *IPspace* to create a distinct IP address space for each virtual data server in a cluster. Doing so enables clients in administratively separate network domains to access cluster data while using overlapping IP addresses from the same IP address subnet range.

A service provider, for example, could configure different IPspaces for tenants using the same IP addresses to access a cluster.

**DNS load balancing**

You can use *DNS load balancing* to distribute user network traffic across available ports. A DNS server dynamically selects a network interface for traffic based on the number of clients that are mounted on the interface.

**SNMP traps**

You can use *SNMP traps* to check periodically for operational thresholds or failures. SNMP traps capture system monitoring information sent asynchronously from an SNMP agent to an SNMP manager.

---

**FIPS compliance**

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

**Aggregates** are containers for the disks managed by a node. You can use aggregates to isolate workloads with different performance demands, to tier data with different access patterns, or to segregate data for regulatory purposes.

- For business-critical applications that need the lowest possible latency and the highest possible performance, you might create an aggregate consisting entirely of SSDs.

- To tier data with different access patterns, you can create a hybrid aggregate, deploying flash as high-performance cache for a working data set, while using lower-cost HDDs or object storage for less frequently accessed data. A FlashPool consists of both SSDs and HDDs. A FabricPool consists of an all-SSD aggregate with an attached object store.

- If you need to segregate archived data from active data for regulatory purposes, you can use an aggregate consisting of capacity HDDs, or a combination of performance and capacity HDDs.

Aggregates and RAID groups

Modern RAID technologies protect against disk failure by rebuilding a failed disk's data on a spare disk. The system compares index information on a “parity disk” with data on the remaining healthy disks to reconstruct the missing data, all without downtime or a significant performance cost.

An aggregate consists of one or more RAID groups. The RAID type of the aggregate determines the number of parity disks in the RAID group and the number of simultaneous disk failures the RAID configuration protects against.

The default RAID type, RAID-DP (RAID-double parity), requires two parity disks per RAID group and protects against data loss in the event of two disks failing at the same time. For RAID-DP, the recommended RAID group size is between 12 and 20 HDDs and between 20 and 28 SSDs.

You can spread out the overhead cost of parity disks by creating RAID groups at the higher end of the sizing recommendation. This is especially the case for SSDs, which are much more reliable than capacity drives. For HDD aggregates, you should balance the need to maximize disk storage against countervailing factors like the longer rebuild time required for larger RAID groups.
Root-data partitioning

Every node must have a root aggregate for storage system configuration files. The root aggregate has the RAID type of the data aggregate.

A root aggregate of type RAID-DP typically consists of one data disk and two parity disks. That's a significant “parity tax” to pay for storage system files, when the system is already reserving two disks as parity disks for each RAID group in the aggregate.

*Root-data partitioning* reduces the parity tax by apportioning the root aggregate across disk partitions, reserving one small partition on each disk as the root partition and one large partition for data.

As the illustration suggests, the more disks used to store the root aggregate, the smaller the root partition. That's also the case for a form of root-data partitioning called *root-data-data partitioning*, which creates one small partition as the root partition and two larger, equally sized partitions for data.

Both types of root-data partitioning are part of the ONTAP Advanced Drive Partitioning (ADP) feature. Both are configured at the factory: root-data partitioning for entry-level FAS2xxx, FAS9000, FAS8200, FAS80xx and AFF systems, root-data-data partitioning for AFF systems only.
Volumes, qtrees, files, and LUNs

ONTAP serves data to clients and hosts from logical containers called *FlexVol volumes*. Because these volumes are only loosely coupled with their containing aggregate, they offer greater flexibility in managing data than traditional volumes.

You can assign multiple FlexVol volumes to an aggregate, each dedicated to a different application or service. You can expand and contract a FlexVol volume, move a FlexVol volume, and make efficient copies of a FlexVol volume. You can use *qtrees* to partition a FlexVol volume into more manageable units, and *quotas* to limit volume resource usage.

Volumes contain file systems in a NAS environment and LUNs in a SAN environment. A LUN (logical unit number) is an identifier for a device called a *logical unit* addressed by a SAN protocol. LUNs are the basic unit of storage in a SAN configuration. The Windows host sees LUNs on your storage system as virtual disks. You can nondisruptively move LUNs to different volumes as needed.

In addition to data volumes, there are a few special volumes you need to know about:

• A *node root volume* (typically “vol0”) contains node configuration information and logs.
• An *SVM root volume* serves as the entry point to the namespace provided by the SVM and contains namespace directory information.
• *System volumes* contain special metadata such as service audit logs.

You cannot use these volumes to store data.

**FlexGroup volumes**

In some enterprises a single namespace may require petabytes of storage, far exceeding even a FlexVol volume’s 100TB capacity.

A *FlexGroup volume* supports up to 400 billion files with 200 constituent member volumes that work collaboratively to dynamically balance load and space allocation evenly across all members.

There is no required maintenance or management overhead with a FlexGroup volume. You simply create the FlexGroup volume and share it with your NAS clients. ONTAP does the rest.
Storage virtualization

You use storage virtual machines (SVMs) to serve data to clients and hosts. Like a virtual machine running on a hypervisor, an SVM is a logical entity that abstracts physical resources. Data accessed through the SVM is not bound to a location in storage. Network access to the SVM is not bound to a physical port.

**Note:** SVMs were formerly called “vservers.” You will still see that term in the ONTAP command line interface (CLI).

An SVM serves data to clients and hosts from one or more volumes, through one or more network logical interfaces (LIFs). Volumes can be assigned to any data aggregate in the cluster. LIFs can be hosted by any physical or logical port. Both volumes and LIFs can be moved without disrupting data service, whether you are performing hardware upgrades, adding nodes, balancing performance, or optimizing capacity across aggregates.

The same SVM can have a LIF for NAS traffic and a LIF for SAN traffic. Clients and hosts need only the address of the LIF (IP address for NFS, SMB, or iSCSI; WWPN for FC) to access the SVM. LIFs keep their addresses as they move. Ports can host multiple LIFs. Each SVM has its own security, administration, and namespace.

In addition to data SVMs, ONTAP deploys special SVMs for administration:

- An **admin SVM** is created when the cluster is set up.
- A **node SVM** is created when a node joins a new or existing cluster.
- A **system SVM** is automatically created for cluster-level communications in an IPspace.

You cannot use these SVMs to serve data. There are also special LIFs for traffic within and between clusters, and for cluster and node management.

---

Why ONTAP is like middleware

The logical objects ONTAP uses for storage management tasks serve the familiar goals of a well-designed middleware package: shielding the administrator from low-level implementation details and insulating the configuration from changes in physical characteristics like nodes and ports. The basic idea is that the administrator should be able to move volumes and LIFs easily, reconfiguring a few fields rather than the entire storage infrastructure.
SVM use cases

Service providers use SVMs in secure multitenancy arrangements to isolate each tenant's data, to provide each tenant with its own authentication and administration, and to simplify chargeback. You can assign multiple LIFs to the same SVM to satisfy different customer needs, and you can use QoS to protect against tenant workloads “bullying” the workloads of other tenants.

Administrators use SVMs for similar purposes in the enterprise. You might want to segregate data from different departments, or keep storage volumes accessed by hosts in one SVM and user share volumes in another. Some administrators put iSCSI/FC LUNs and NFS datastores in one SVM and SMB shares in another.

Cluster and SVM administration

A cluster administrator accesses the admin SVM for the cluster. The admin SVM and a cluster administrator with the reserved name admin are automatically created when the cluster is set up.

A cluster administrator with the default admin role can administer the entire cluster and its resources. The cluster administrator can create additional cluster administrators with different roles as needed.

An SVM administrator accesses a data SVM. The cluster administrator creates data SVMs and SVM administrators as needed.

SVM administrators are assigned the vsadmin role by default. The cluster administrator can assign different roles to SVM administrators as needed.

Role-Based Access Control (RBAC)

The role assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.
Namespaces and junction points

A NAS namespace is a logical grouping of volumes joined together at junction points to create a single file system hierarchy. A client with sufficient permissions can access files in the namespace without specifying the location of the files in storage. Junctioned volumes can reside anywhere in the cluster.

Rather than mounting every volume containing a file of interest, NAS clients mount an NFS export or access an SMB share. The export or share represents the entire namespace or an intermediate location within the namespace. The client accesses only the volumes mounted below its access point.

You can add volumes to the namespace as needed. You can create junction points directly below a parent volume junction or on a directory within a volume. A path to a volume junction for a volume named “vol3” might be /vol1/vol2/vol3, or /vol1/dir2/vol3, or even /dir1/dir2/vol3. The path is called the junction path.

Every SVM has a unique namespace. The SVM root volume is the entry point to the namespace hierarchy.

Note: To ensure that data remains available in the event of a node outage or failover, you should create a load-sharing mirror copy for the SVM root volume on each node of the cluster, including the node on which the root volume is located.

Example

The following example creates a volume named “home4” located on SVM vs1 that has a junction path /eng/home:

```
cluster1::> volume create -vserver vs1 -volume home4 -aggregate aggr1 -size 1g -junction-path /eng/home
[Job 1642] Job succeeded: Successful
```
Path failover

There are important differences in how ONTAP manages path failover in NAS and SAN topologies. A NAS LIF automatically migrates to a different network port after a link failure. A SAN LIF does not migrate (unless you move it manually after the failure). Instead, multipathing technology on the host diverts traffic to a different LIF—on the same SVM, but accessing a different network port.

NAS path failover

A NAS LIF automatically migrates to a surviving network port after a link failure on its current port. The port to which the LIF migrates must be a member of the failover group for the LIF. The failover group policy narrows the failover targets for a data LIF to ports on the node that owns the data and its HA partner.

For administrative convenience, ONTAP creates a failover group for each broadcast domain in the network architecture. Broadcast domains group ports that belong to the same layer 2 network. If you are using VLANs, for example, to segregate traffic by department (Engineering, Marketing, Finance, and so on), each VLAN defines a separate broadcast domain. The failover group associated with the broadcast domain is automatically updated each time you add or remove a broadcast domain port.

It is almost always a good idea to use a broadcast domain to define a failover group to ensure that the failover group remains current. Occasionally, however, you may want to define a failover group that is not associated with a broadcast domain. For example, you may want LIFs to fail over only to ports in a subset of the ports defined in the broadcast domain.

Subnets

A subnet reserves a block of IP addresses in a broadcast domain. These addresses belong to the same layer 3 network and are allocated to ports in the broadcast domain when you create a LIF. It is usually easier and less error-prone to specify a subnet name when you define a LIF address than it is to specify an IP address and network mask.
**SAN path failover**

A SAN host uses ALUA (Asymmetric Logical Unit Access) and MPIO (multipath I/O) to reroute traffic to a surviving LIF after a link failure. Predefined paths determine the possible routes to the LUN served by the SVM.

In a SAN environment, hosts are regarded as *initiators* of requests to LUN *targets*. MPIO enables multiple paths from initiators to targets. ALUA identifies the most direct paths, called *optimized paths*.

You typically configure multiple optimized paths to LIFs on the LUN's owning node, and multiple non-optimized paths to LIFs on its HA partner. If one port fails on the owning node, the host routes traffic to the surviving ports. If all the ports fail, the host routes traffic over the non-optimized paths.

**Tip:** You can use ONTAP DSM technology to define a *load-balance policy* that determines how traffic is distributed over the optimized paths to a LUN.

ONTAP Selective LUN Map (SLM) limits the number of paths from the host to a LUN by default. A newly created LUN is accessible only through paths to the node that owns the LUN or its HA partner. You can also limit access to a LUN by configuring LIFs in a *port set* for the initiator.

---

**Moving volumes in SAN environments**

By default, ONTAP *Selective LUN Map (SLM)* limits the number of paths to a LUN from a SAN host. A newly created LUN is accessible only through paths to the node that owns the LUN or its HA partner, the *reporting nodes* for the LUN.

This means that when you move a volume to a node on another HA pair, you need to add reporting nodes for the destination HA pair to the LUN mapping. You can then specify the new paths in your MPIO setup. After the volume move is complete, you can delete the reporting nodes for the source HA pair from the mapping.
Load balancing

Performance of workloads begins to be affected by latency when the amount of work on a node exceeds the available resources. You can manage an overloaded node by increasing the available resources (upgrading disks or CPU), or by reducing load (moving volumes or LUNs to different nodes as needed).

You can also use ONTAP storage quality of service (QoS) to guarantee that performance of critical workloads is not degraded by competing workloads:

- You can set a QoS throughput ceiling on a competing workload to limit its impact on system resources (QoS Max).
- You can set a QoS throughput floor for a critical workload, ensuring that it meets minimum throughput targets regardless of demand by competing workloads (QoS Min).
- You can set a QoS ceiling and floor for the same workload.

Throughput ceilings

A throughput ceiling limits throughput for a workload to a maximum number of IOPS or MB/s. In the figure below, the throughput ceiling for workload 2 ensures that it does not “bully” workloads 1 and 3.

A policy group defines the throughput ceiling for one or more workloads. A workload represents the I/O operations for a storage object: a volume, file, or LUN, or all the volumes, files, or LUNs in an SVM. You can specify the ceiling when you create the policy group, or you can wait until after you monitor workloads to specify it.

Note: Throughput to workloads might exceed the specified ceiling by up to 10 percent, especially if a workload experiences rapid changes in throughput. The ceiling might be exceeded by up to 50% to handle bursts.

Throughput floors

A throughput floor guarantees that throughput for a workload does not fall below a minimum number of IOPS. In the figure below, the throughput floors for workload 1 and workload 3 ensure that they meet minimum throughput targets, regardless of demand by workload 2.

Tip: As the examples suggest, a throughput ceiling throttles throughput directly. A throughput floor throttles throughput indirectly, by giving priority to the workloads for which the floor has been set.
A workload represents the I/O operations for a volume, LUN, or, starting with ONTAP 9.3, file. A policy group that defines a throughput floor cannot be applied to an SVM. You can specify the floor when you create the policy group, or you can wait until after you monitor workloads to specify it.

**Note:** Throughput to a workload might fall below the specified floor if there is insufficient performance capacity (headroom) on the node or aggregate, or during critical operations like volume move trigger-cutover. Even when sufficient capacity is available and critical operations are not taking place, throughput to a workload might fall below the specified floor by up to 5 percent.

**Adaptive QoS**

Ordinarily, the value of the policy group you assign to a storage object is fixed. You need to change the value manually when the size of the storage object changes. An increase in the amount of space used on a volume, for example, usually requires a corresponding increase in the throughput ceiling specified for the volume.

*Adaptive QoS* automatically scales the policy group value to workload size, maintaining the ratio of IOPS to TBs|GBs as the size of the workload changes. That's a significant advantage when you are managing hundreds or thousands of workloads in a large deployment.

You typically use adaptive QoS to adjust throughput ceilings, but you can also use it to manage throughput floors (when workload size increases). Workload size is expressed as either the allocated space for the storage object or the space used by the storage object.

**Note:** Used space is available for throughput floors in ONTAP 9.5 and later. It is not supported for throughput floors in ONTAP 9.4 and earlier.

- An *allocated space* policy maintains the IOPS/TB|GB ratio according to the nominal size of the storage object. If the ratio is 100 IOPS/GB, a 150 GB volume will have a throughput ceiling of 15,000 IOPS for as long as the volume remains that size. If the volume is resized to 300 GB, adaptive QoS adjusts the throughput ceiling to 30,000 IOPS.

- A *used space* policy (the default) maintains the IOPS/TB|GB ratio according to the amount of actual data stored before storage efficiencies. If the ratio is 100 IOPS/GB, a 150 GB volume that has 100 GB of data stored would have a throughput ceiling of 10,000 IOPS. As the amount of used space changes, adaptive QoS adjusts the throughput ceiling according to the ratio.
Replication

Traditionally, ONTAP replication technologies served the need for disaster recovery (DR) and data archiving. With the advent of cloud services, ONTAP replication has been adapted to data transfer between endpoints in the NetApp data fabric. The foundation for all these uses is ONTAP Snapshot technology.

Snapshot copies

A Snapshot copy is a read-only, point-in-time image of a volume. The image consumes minimal storage space and incurs negligible performance overhead because it records only changes to files since the last Snapshot copy was made.

Snapshot copies owe their efficiency to ONTAP's core storage virtualization technology, its Write Anywhere File Layout (WAFL). Like a database, WAFL uses metadata to point to actual data blocks on disk. But, unlike a database, WAFL does not overwrite existing blocks. It writes updated data to a new block and changes the metadata.

It's because ONTAP references metadata when it creates a Snapshot copy, rather than copying data blocks, that Snapshot copies are so efficient. Doing so eliminates the “seek time” that other systems incur in locating the blocks to copy, as well as the cost of making the copy itself.

You can use a Snapshot copy to recover individual files or LUNs, or to restore the entire contents of a volume. ONTAP compares pointer information in the Snapshot copy with data on disk to reconstruct the missing or damaged object, without downtime or a significant performance cost.

A Snapshot policy defines how the system creates Snapshot copies of volumes. The policy specifies when to create the Snapshot copies, how many copies to retain, how to name them, and how to label them for replication. For example, a system might create one Snapshot copy 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.

![A Snapshot copy records only changes to the active file system since the last Snapshot copy.](image-url)
SnapMirror disaster recovery and data transfer

SnapMirror is disaster recovery technology, designed for failover from primary storage to secondary storage at a geographically remote site. As its name implies, SnapMirror creates a replica, or mirror, of your working data in secondary storage from which you can continue to serve data in the event of a catastrophe at the primary site.

Data is mirrored at the volume level. The relationship between the source volume in primary storage and the destination volume in secondary storage is called a data protection relationship. The clusters in which the volumes reside and the SVMs that serve data from the volumes must be peered. A peer relationship enables clusters and SVMs to exchange data securely.

Tip: You can also create a data protection relationship between SVMs. In this type of relationship, all or part of the SVM’s configuration, from NFS exports and SMB shares to RBAC, is replicated, as well as the data in the volumes the SVM owns.

The first time you invoke SnapMirror, it performs a baseline transfer from the source volume to the destination volume. The baseline transfer typically involves the following steps:

• Make a Snapshot copy of the source volume.
• Transfer the Snapshot copy and all the data blocks it references to the destination volume.
• Transfer the remaining, less recent Snapshot copies on the source volume to the destination volume for use in case the “active” mirror is corrupted.

Once a baseline transfer is complete, SnapMirror transfers only new Snapshot copies to the mirror. Updates are asynchronous, following the schedule you configure. Retention mirrors the Snapshot policy on the source. You can activate the destination volume with minimal disruption in case of a disaster at the primary site, and reactivate the source volume when service is restored.

Because SnapMirror transfers only Snapshot copies after the baseline is created, replication is fast and nondisruptive. As the failover use case implies, the controllers on the secondary system should be equivalent or nearly equivalent to the controllers on the primary system to serve data efficiently from mirrored storage.

Using SnapMirror for data transfer

You can also use SnapMirror to replicate data between endpoints in the NetApp data fabric. You can choose between one-time replication or recurring replication when you create the SnapMirror policy.
SnapVault archiving

SnapVault is archiving technology, designed for disk-to-disk Snapshot copy replication for standards compliance and other governance-related purposes. In contrast to a SnapMirror relationship, in which the destination usually contains only the Snapshot copies currently in the source volume, a SnapVault destination typically retains point-in-time Snapshot copies created over a much longer period.

You might want to keep monthly Snapshot copies of your data over a 20-year span, for example, to comply with government accounting regulations for your business. Since there is no requirement to serve data from vault storage, you can use slower, less expensive disks on the destination system.

As with SnapMirror, SnapVault performs a baseline transfer the first time you invoke it. It makes a Snapshot copy of the source volume, then transfers the copy and the data blocks it references to the destination volume. Unlike SnapMirror, SnapVault does not include older Snapshot copies in the baseline.

Updates are asynchronous, following the schedule you configure. The rules you define in the policy for the relationship identify which new Snapshot copies to include in updates and how many copies to retain. The labels defined in the policy (“monthly,” for example) must match one or more labels defined in the Snapshot policy on the source. Otherwise, replication fails.

Note: SnapMirror and SnapVault share the same command infrastructure. You specify which method you want to use when you create a policy. Both methods require peered clusters and peered SVMs.

NetApp Cloud Backup and support for traditional backups

SnapVault data protection relationships are disk-to-disk, ONTAP-to-ONTAP. Traditional backups, and now backup to the cloud with Cloud Backup, offer less expensive alternatives for long-term data retention.

A Cloud Backup appliance can back up any storage array to any cloud, and integrates with a wide range of backup software. Data that has been backed up to the cloud can be restored to any storage array in the fabric. Fast and easy retrieval from the cloud eliminates the requirement for tape-based backup in most use cases.

Numerous vendors offer traditional backup for ONTAP-managed data. Veeam, Veritas, Syncsort, and Commvault, among others, all offer integrated backup for ONTAP systems.
MetroCluster continuous availability

MetroCluster configurations protect data by implementing two physically separate, mirrored clusters. Each cluster synchronously replicates the data and SVM configuration of the other. In the event of a disaster at one site, an administrator can activate the mirrored SVM and begin serving data from the surviving site.

- Fabric-attached MetroCluster configurations support metropolitan-wide clusters.
- Stretch MetroCluster configurations support campus-wide clusters.

Clusters must be peered in either case.

MetroCluster uses an ONTAP feature called SyncMirror to synchronously mirror aggregate data for each cluster in copies, or plexes, in the other cluster's storage. If a switchover occurs, the remote plex on the surviving cluster comes online and the secondary SVM begins serving data.

Using SyncMirror in non-MetroCluster implementations

You can optionally use SyncMirror in a non-MetroCluster implementation to protect against data loss if more disks fail than the RAID type protects against, or if there is a loss of connectivity to RAID group disks. The feature is available for HA pairs only.

Aggregate data is mirrored in plexes stored on different disk shelves. If one of the shelves becomes unavailable, the unaffected plex continues to serve data while you fix the cause of the failure.

Keep in mind that an aggregate mirrored using SyncMirror requires twice as much storage as an unmirrored aggregate. Each plex requires as many disks as the plex it mirrors. You would need 2,880 GB of disk space, for example, to mirror a 1,440 GB aggregate, 1,440 GB for each plex.

Note: SyncMirror is also available for FlexArray Virtualization implementations.
Storage efficiency

ONTAP offers a wide range of storage efficiency technologies in addition to Snapshot copies. Key technologies include thin provisioning, deduplication, compression, and FlexClone volumes, files, and LUNs. Like Snapshot copies, all are built on ONTAP’s Write Anywhere File Layout (WAFL).

Thin provisioning

A thin-provisioned volume or LUN is one for which storage is not reserved in advance. Instead, storage is allocated dynamically, as it is needed. Free space is released back to the storage system when data in the volume or LUN is deleted.

Suppose that your organization needs to supply 5,000 users with storage for home directories. You estimate that the largest home directories will consume 1 GB of space.

In this situation, you could purchase 5 TB of physical storage. For each volume that stores a home directory, you would reserve enough space to satisfy the needs of the largest consumers.

As a practical matter, however, you also know that home directory capacity requirements vary greatly across your community. For every large user of storage, there are ten who consume little or no space.

Thin provisioning allows you to satisfy the needs of the large storage consumers without having to purchase storage you might never use. Since storage space is not allocated until it is consumed, you can “overcommit” an aggregate of 2 TB by nominally assigning a size of 1 GB to each of the 5,000 volumes the aggregate contains.

As long as you are correct that there is a 10:1 ratio of light to heavy users, and as long as you take an active role in monitoring free space on the aggregate, you can be confident that volume writes won’t fail due to lack of space.

Deduplication

Deduplication reduces the amount of physical storage required for a volume (or all the volumes in an AFF aggregate) by discarding duplicate blocks and replacing them with references to a single shared block. Reads of deduplicated data typically incur no performance charge. Writes incur a negligible charge except on overloaded nodes.

As data is written during normal use, WAFL uses a batch process to create a catalog of block signatures. After deduplication starts, ONTAP compares the signatures in the catalog to identify duplicate blocks. If a match exists, a byte-by-byte comparison is done to verify that the candidate blocks have not changed since the catalog was created. Only if all the bytes match is the duplicate block discarded and its disk space reclaimed.

Deduplication reduces the amount of physical storage required for a volume by discarding duplicate data blocks.
Compression

Compression reduces the amount of physical storage required for a volume by combining data blocks in compression groups, each of which is stored as a single block. Reads of compressed data are faster than in traditional compression methods because ONTAP decompresses only the compression groups that contain the requested data, not an entire file or LUN.

You can perform inline or postprocess compression, separately or in combination:

- **Inline compression** compresses data in memory before it is written to disk, significantly reducing the amount of write I/O to a volume, but potentially degrading write performance. Performance-intensive operations are deferred until the next postprocess compression operation, if any.
- **Postprocess compression** compresses data after it is written to disk, on the same schedule as deduplication.

**Inline data compaction**

Small files or I/O padded with zeros are stored in a 4 KB block whether or not they require 4 KB of physical storage. **Inline data compaction** combines data chunks that would ordinarily consume multiple 4 KB blocks into a single 4 KB block on disk. Compaction takes place while data is still in memory, so it is best suited to faster controllers.

FlexClone volumes, files, and LUNs

FlexClone technology references Snapshot metadata to create writable, point-in-time copies of a volume. Copies share data blocks with their parents, consuming no storage except what is required for metadata until changes are written to the copy. FlexClone files and FlexClone LUNs use identical technology, except that a backing Snapshot copy is not required.

Where traditional copies can take minutes or even hours to create, FlexClone software lets you copy even the largest datasets almost instantaneously. That makes it ideal for situations in which you need multiple copies of identical datasets (a virtual desktop deployment, for example) or temporary copies of a dataset (testing an application against a production dataset).

You can clone an existing FlexClone volume, clone a volume containing LUN clones, or clone mirror and vault data. You can split a FlexClone volume from its parent, in which case the copy is allocated its own storage.

FlexClone copies share data blocks with their parents, consuming no storage except what is required for metadata.
Security

ONTAP uses standard methods to secure client and administrator access to storage and to protect against viruses. Advanced technologies are available for encryption of data at rest and for WORM storage.

Client authentication and authorization

ONTAP authenticates a client machine and user by verifying their identities with a trusted source. ONTAP authorizes a user to access a file or directory by comparing the user's credentials with the permissions configured on the file or directory.

Authentication

You can create local or remote user accounts:

- A local account is one in which the account information resides on the storage system.
- A remote account is one in which account information is stored on an Active Directory domain controller, an LDAP server, or a NIS server.

ONTAP uses local or external name services to look up host name, user, group, netgroup, and name mapping information. ONTAP supports the following name services:

- Local users
- DNS
- External NIS domains
- External LDAP domains

A name service switch table specifies the sources to search for network information and the order in which to search them (providing the equivalent functionality of the /etc/nsswitch.conf file on UNIX systems). When a NAS client connects to the SVM, ONTAP checks the specified name services to obtain the required information.

Kerberos support

Kerberos is a network authentication protocol that provides “strong authentication” by encrypting user passwords in client-server implementations. ONTAP supports Kerberos 5 authentication with integrity checking (krb5i) and Kerberos 5 authentication with privacy checking (krb5p).

Authorization

ONTAP evaluates three levels of security to determine whether an entity is authorized to perform a requested action on files and directories residing on an SVM. Access is determined by the effective permissions after evaluation of the security levels:

- Export (NFS) and share (SMB) security
  Export and share security applies to client access to a given NFS export or SMB share. Users with administrative privileges can manage export and share-level security from SMB and NFS clients.

- Storage-Level Access Guard file and directory security
  Storage-Level Access Guard security applies to SMB and NFS client access to SVM volumes. Only NTFS access permissions are supported. For ONTAP to perform security checks on UNIX users for access to data on volumes for which Storage-Level Access Guard has been applied, the UNIX user must map to a Windows user on the SVM that owns the volume.

- NTFS, UNIX, and NFSv4 native file-level security
Native file-level security exists on the file or directory that represents the storage object. You can set file-level security from a client. File permissions are effective regardless of whether SMB or NFS is used to access the data.

**Administrator authentication and RBAC**

Administrators use local or remote login accounts to authenticate themselves to the cluster and SVM. Role-Based Access Control (RBAC) determines the commands to which an administrator has access.

**Authentication**

You can create local or remote cluster and SVM administrator accounts:

- A local account is one in which the account information, public key, or security certificate resides on the storage system.
- A remote account is one in which account information is stored on an Active Directory domain controller, an LDAP server, or a NIS server.

Except for DNS, ONTAP uses the same name services to authenticate administrator accounts as it uses to authenticate clients.

**RBAC**

The *role* assigned to an administrator determines the commands to which the administrator has access. You assign the role when you create the account for the administrator. You can assign a different role or define custom roles as needed.

**Virus scanning**

You can use integrated antivirus functionality on the storage system to protect data from being compromised by viruses or other malicious code. ONTAP virus scanning, called *Vscan*, combines best-in-class third-party antivirus software with ONTAP features that give you the flexibility you need to control which files get scanned and when.

Storage systems offload scanning operations to external servers hosting antivirus software from third-party vendors. The *ONTAP Antivirus Connector*, provided by NetApp and installed on the external server, handles communications between the storage system and the antivirus software.

- You can use *on-access scanning* to check for viruses when clients open, read, rename, or close files over SMB. File operation is suspended until the external server reports the scan status of the file. If the file has already been scanned, ONTAP allows the file operation. Otherwise, it requests a scan from the server.
- You can use *on-demand scanning* to check files for viruses immediately or on a schedule. You might want to run scans only in off-peak hours, for example. The external server updates the scan status of the checked files, so that file-access latency for those files (assuming they have not been modified) is typically reduced when they are next accessed over SMB. You can use on-demand scanning for any path in the SVM namespace, even for volumes that are exported only through NFS.

You typically enable both scanning modes on an SVM. In either mode, the antivirus software takes remedial action on infected files based on your settings in the software.

**Virus scanning in disaster recovery and MetroCluster configurations**

For disaster recovery and MetroCluster configurations, you must set up separate Vscan servers for the local and partner clusters.
Encryption

ONTAP offers both software- and hardware-based encryption technologies for ensuring that data at rest cannot be read if the storage medium is repurposed, returned, misplaced, or stolen.

**NetApp Volume Encryption**

NetApp Volume Encryption (NVE) is a software-based technology for encrypting data at rest one volume at a time. An encryption key accessible only to the storage system ensures that volume data cannot be read if the underlying device is separated from the system.

Both data, including Snapshot copies, and metadata are encrypted. Access to the data is given by a unique XTS-AES-256 key, one per volume. A built-in Onboard Key Manager secures the keys on the same system with your data.

You can use NVE on any type of aggregate (HDD, SSD, hybrid, array LUN), with any RAID type, and in any supported ONTAP implementation, including ONTAP Select. You can also use NVE with NetApp Storage Encryption (NSE) to “double encrypt” data on NSE drives, provided that you use the NSE Onboard Key Manager option.

**NetApp Storage Encryption**

NetApp Storage Encryption (NSE) supports "self-encrypting" disks (SEDS) that encrypt data as it is written. The data cannot be read without an encryption key stored on the disk. The encryption key, in turn, is accessible only to an authenticated node.

On an I/O request, a node authenticates itself to an SED using an authentication key retrieved from an external key management server or Onboard Key Manager:

- The external key management server is a third-party system in your storage environment that serves authentication keys to nodes using the Key Management Interoperability Protocol (KMIP).
- The Onboard Key Manager is a built-in tool that serves authentication keys to nodes from the same storage system as your data.
NSE supports self-encrypting HDDs and SSDs. You can use NetApp Volume Encryption with NSE to “double encrypt” data on NSE drives, provided that you use the Onboard Key Manager.

### When to use KMIP servers

Although it is less expensive and typically more convenient to use the Onboard Key Manager, you should set up KMIP servers if any of the following are true:

- Your encryption key management solution must comply with Federal Information Processing Standards (FIPS) 140-2 or the OASIS KMIP standard.
- You need a multi-cluster solution. KMIP servers support multiple clusters with centralized management of encryption keys.
- Your business requires the added security of storing authentication keys on a system or in a location different from the data. KMIP servers stores authentication keys separately from your data.

### WORM storage

*SnapLock* is a high-performance compliance solution for organizations that use write once, read many (WORM) storage to retain critical files in unmodified form for regulatory and governance purposes.

A single license entitles you to use SnapLock in strict *Compliance mode*, to satisfy external mandates like SEC Rule 17a-4, and a looser *Enterprise mode*, to meet internally mandated regulations for the protection of digital assets. SnapLock uses a tamper-proof *ComplianceClock* to determine when the retention period for a WORM file has elapsed.

You can use *SnapLock for SnapVault* to WORM-protect Snapshot copies on secondary storage. You can use SnapMirror to replicate WORM files to another geographic location for disaster recovery and other purposes.
Application aware data management

Application aware data management enables you to describe the application that you want to deploy over ONTAP in terms of the application, rather than in storage terms. The application can be configured and ready to serve data quickly with minimal inputs by using OnCommand System Manager and REST APIs.

The application aware data management feature provides a way to set up, manage, and monitor storage at the level of individual applications. This feature incorporates relevant ONTAP best practices to optimally provision applications, with balanced placement of storage objects based on desired performance service levels and available system resources.

The application aware data management feature includes a set of application templates, with each template consisting of a set of parameters that collectively describe the configuration of an application. These parameters, which are often preset with default values, define the characteristics that an application administrator could specify for provisioning storage on an ONTAP system, such as database sizes, service levels, protocol access elements such as LIFs as well as local protection criteria and remote protection criteria. Based on the specified parameters, ONTAP configures storage entities such as LUNs and volumes with appropriate sizes and service levels for the application.

You can perform the following tasks for your applications:

- Create applications by using the application templates
- Manage the storage associated with the applications
- Modify or delete the applications
- View applications
- Manage Snapshot copies of the applications
ONTAP release model

The ONTAP release model delivers feature releases twice every calendar year, typically in the second and fourth quarters. It delivers service update releases every one to two months as necessary. It offers debug releases on an emergency basis.

Release types

- A feature release includes a set of new market-driven features, as well as fixes for bugs that customers encountered in earlier releases. Each feature release is numbered “ONTAP x.y”, for example, “ONTAP 9.0” or “ONTAP 9.1”.
- A service update release delivers timely fixes for critical bugs encountered in the field, for customers who cannot wait for the next feature release. Each service update is numbered “ONTAP x.yPz”, for example, “ONTAP 9.0P1” or “ONTAP 9.0P2”.
- A debug release is a hot-fix release delivered on an exception basis to a specific customer. These releases are not normally planned and are provided only in case of extraordinary need. Each debug release is numbered “ONTAP x.yPzDa”, for example, “ONTAP 9.0P1D1” or “ONTAP 9.0P2D2”.

Service update and debug releases are referred to as “P-release patches.”

A feature release is made available as a Release Candidate (RC), then as a General Availability (GA) release:

- The Release Candidate designation indicates that NetApp completed internal testing as well as early customer validation of the release.
- The General Availability designation indicates that a Release Candidate performed extraordinarily well across multiple deployments, enabling customers to achieve 99.999% availability or better in production environments.

Any configuration qualified for an ONTAP GA release is automatically qualified for all P-release patches of that release. If support is introduced in a patch release, subsequent patch releases maintain that support.

For complete information, see ONTAP release model.

Software version support

NetApp adheres to a software product version lifecycle management policy. The objective of this policy is to enable customers to predictably manage IT infrastructure.

The following table shows the available support levels:

<table>
<thead>
<tr>
<th>Support level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full support</td>
<td>Includes technical support, root cause analysis, online documentation, online software, maintenance, and P-release patches.</td>
</tr>
<tr>
<td>Limited support</td>
<td>Includes technical support, root cause analysis, online documentation, and online software. Does not include maintenance and P-release patches.</td>
</tr>
<tr>
<td>Self-service support</td>
<td>Provides online documentation only.</td>
</tr>
</tbody>
</table>

For complete information, see Software version support.
Where to find additional information

You can learn more about the technologies described in this guide in NetApp's extensive library of user documentation, technical reports, and white papers. References are organized by the section of this guide in which the technology is discussed. References are repeated if they pertain to more than one section.

ONTAP platforms

- *NetApp Data Fabric Architecture Fundamentals*
  Describes how the NetApp Data Fabric unifies data management across distributed resources.

- *NetApp Cloud Volumes ONTAP and Cloud Manager Resources*
  Lists Cloud Volumes ONTAP and Cloud Manager resources.

- *NetApp ONTAP Select Resources*
  Lists ONTAP Select resources.

Cluster storage

- *System administration*
  Describes cluster and SVM administration.

- *NetApp Hardware Universe*
  Contains support information for NetApp storage controllers and related hardware.

- *NetApp Interoperability Matrix Tool*
  Contains support information for ONTAP software.

High-availability pairs

- *High-availability configuration*
  Describes how to configure HA pairs.

  Describes best practices for HA pair configuration.

Network architecture

- *Network and LIF management*
  Describes network management and LIF configuration.

- *SNMP express configuration*
  Describes how to quickly configure SNMP in a cluster.

  Describes how ONTAP network architectures are implemented.

Disks and aggregates

- *Disk and aggregate management*
  Describes how to create and expand aggregates and how to manage disks and RAID groups.

  Describes how to configure storage systems for maximum data availability.
Volumes, qtrees, files, and LUNs

- **Logical storage management**
  Describes how to manage FlexVol volumes, qtrees, files, and LUNs.

- **FlexGroup volumes management**
  Describes how to set up, manage, and protect FlexGroup volumes.

- **SAN administration**
  Describes how to configure and manage LUNs, igroups, and targets for SAN protocols.

Storage virtualization

- **SMB/CIFS configuration express**
  Describes how to quickly configure CIFS/SMB client access.

- **NFS express configuration**
  Describes how to quickly configure NFS client access.

- **FC express configuration for Windows**
  Describes how to quickly configure FC access for Windows hosts.

- **iSCSI express configuration for Windows**
  Describes how to quickly configure iSCSI access for Windows hosts.

- **Volume move express management**
  Describes how to quickly move a volume to another node.

Path failover

- **Network and LIF management**
  Describes network management and LIF configuration.

- **NetApp Documentation: Data ONTAP DSM for Windows MPIO**
  Describes how to use ONTAP DSM technology to manage traffic to LUNs.

- **NetApp Technical Report 3441: Windows Multipathing Options with Data ONTAP: Fibre Channel and iSCSI**
  Describes multipathing options available for iSCSI and Fibre Channel SAN.

Load balancing

- **Logical storage management**
  Describes how to manage FlexVol volumes, qtrees, files, and LUNs.

- **Performance management**
  Describes how to use QoS to guarantee workload performance.

Replication

- **Volume disaster recovery express preparation**
  Describes how to quickly configure a SnapMirror destination volume.

- **Volume disaster express recovery**
  Describes how to quickly activate a SnapMirror destination volume after a disaster, and how to reactivate the source volume after its recovery.

- **Data protection**
  Describes how to manage Snapshot copies on a local ONTAP system, and how to replicate Snapshot copies to a remote system using SnapMirror.
• **NetApp Documentation: MetroCluster in ONTAP 9**
  Provides links to MetroCluster documentation.

  Describes SnapMirror best practices.

  Describes SnapVault best practices.

  Describes MetroCluster best practices.

**Storage efficiency**

• **Logical storage management**
  Describes how to manage FlexVol volumes, qtrees, files, and LUNs.

• **NetApp Technical Report 3563: NetApp Thin Provisioning Increases Storage Utilization With On Demand Allocation**
  Introduces ONTAP thin provisioning.

  Describes ONTAP deduplication and compression.

• **NetApp Technical Report 3742: Using FlexClone to Clone Files and LUNs**
  Describes how to use FlexClone to create space efficient copies of files and LUNs.

**Security**

• **NFS management**
  Provides reference information for NFS file access.

• **SMB/CIFS management**
  Provides reference information for CIFS file access.

• **Administrator authentication and RBAC**
  Describes how to enable login accounts for cluster and SVM administrators, and how to use role-based access control (RBAC) to define the capabilities of administrators.

• **Antivirus configuration**
  Describes how to configure ONTAP virus scanning.

• **Encryption of data at rest**
  Describes how to encrypt data at rest with software-based NetApp Volume Encryption or hardware-based NetApp Storage Encryption.

• **Archive and compliance using SnapLock technology**
  Describes how to use SnapLock to WORM-protect data.

  Describes name services best practices.

• **NetApp Technical Report 4073: Secure Unified Authentication**
  Describes how to configure Kerberos authentication for NFS clients.
Copyright information

Copyright © 2018 NetApp, Inc. All rights reserved. Printed in the U.S.

No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

Data contained herein pertains to a commercial item (as defined in FAR 2.101) and is proprietary to NetApp, Inc. The U.S. Government has a non-exclusive, non-transferrable, non-sublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b).
Trademark information

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

How to send comments about documentation and receive update notifications

You can help us to improve the quality of our documentation by sending us your feedback. You can receive automatic notification when production-level (GA/FCS) documentation is initially released or important changes are made to existing production-level documents.

If you have suggestions for improving this document, send us your comments by email.

doccomments@netapp.com

To help us direct your comments to the correct division, include in the subject line the product name, version, and operating system.

If you want to be notified automatically when production-level documentation is released or important changes are made to existing production-level documents, follow Twitter account @NetAppDoc.

You can also contact us in the following ways:

• NetApp, Inc., 1395 Crossman Ave., Sunnyvale, CA 94089 U.S.

• Telephone: +1 (408) 822-6000

• Fax: +1 (408) 822-4501

• Support telephone: +1 (888) 463-8277
Index

A

admin role
  and cluster administrator 15
admin SVM
  concepts 14, 15, 28
ADP
  concepts 12
Advanced Data Partitioning (ADP)
  concepts 12
aggregate
  and disk partitioning 12
  and disks 11
  and RAID groups 11
  and volumes 13
  concepts 11
  use cases 11
ALUA
  concepts 18
application aware data management
  overview 31
archiving
  characteristics of SnapVault 23
  concepts 30
Asymmetric Logical Unit Access (ALUA)
  concepts 18
authentication
  concepts 27, 28
authorization
  concepts 27, 28
Storage-Level Access Guard 27

B

baseline transfer
  concepts 22
broadcast domain
  and VLANs 17
  concepts 17

C

CIFS share
  concepts 16
cloud storage
  with Cloud Volumes ONTAP 6
cluster
  administrator 15, 28
  concepts 7, 8
  interconnect 7, 9
  peering 22
comments
  how to send feedback about documentation 38
commodity hardware
  and ONTAP Select 6
compaction
  concepts 26
compression
  concepts 26

D

data fabric
  concepts 6
data protection
  concepts 22, 30
  MetroCluster continuous availability 24
  SnapMirror disaster recovery 22
  Snapshot copies 21
data SVM
  concepts 14
data transfer
  concepts 22
debug release
  ONTAP 32
deduplication
  concepts 25
disaster recovery
  concepts 22, 24
disk
  and aggregates 11
  and RAID groups 11, 12
disk encryption
  concepts 29
disk partitioning
  concepts 12
DNS load balancing
  concepts 10
documentation
  how to receive automatic notification of changes to 38
  how to send feedback about 38
DSM
  concepts 18

E

encryption
  disk encryption 29
  volume encryption 29
export
  NFS 16

F

FabricPool
  concepts 11
failover
  HA pairs 8
  network path 17, 18
failover group
  concepts 17
fault tolerance
  concepts 8
feature release
  ONTAP 32
Federal Information Processing Standards (FIPS) and encryption 29
feedback how to send comments about documentation 38
FIPS compliance and encryption 29 concepts 10
FlashPool concepts 11
FlexClone copies and Snapshot technology 26
FlexGroup volume concepts 13
FlexVol volume concepts 13

G
General Availability ONTAP 32
giveback
HA pairs 8

H
HA interconnect 8, 9
HA pairs concepts 7, 8 failover 8 giveback 8 takeover 8
high availability (HA) pairs concepts 7, 8 failover 8 giveback 8 takeover 8
hybrid aggregate concepts 11

I
information how to send feedback about improving documentation 38
interconnect cluster 7, 9
HA 8, 9
interface group concepts 9
IPSpaces concepts 10

J
junction point and volumes 16 concepts 16

K
Kerberos support in ONTAP 27
Key Management Interoperability Protocol (KMIP) and disk encryption 29
KMIP and disk encryption 29

L
LIF and path failover 17, 18 concepts 14 moving 14
load balancing concepts 19
load-sharing mirror requirement for root volume 16
logical interface (LIF) and path failover 17, 18 concepts 14
logical ports concepts 9
LUN concepts 13

M
MetroCluster disaster recovery concepts 24
MPIO concepts 18
multipath I/O (MPIO) concepts 18
multitenancy concepts 15

N
namespace and volumes 16 concepts 16
NAS path failover concepts 17
NetApp data fabric concepts 6
network architecture ONTAP 9, 10
network path failover in NAS 17 in SAN 18
NFS export concepts 16
node concepts 7, 8 in HA pair 7, 8
node root volume concepts 13
node SVM concepts 14
non-optimized path
Index

A

concepts 18
nondisruptive operations
  concepts 8

O

Onboard Key Manager and encryption 29

ONTAP
  administrator authentication and authorization 28
  ADP support 12
  Advanced Data Partitioning (ADP) 12
  aggregates 11
  ALUA 18
  and MPIO 18
  and namespaces 16
  broadcast domain 17
  client authentication and authorization 27
  cluster storage 7, 15
  compaction 26
  compression 26
  data protection 24
  data transfer 22
  debug release 32
  deduplication 25
  disaster recovery 22, 24
  DSM 18
  encryption 29
  FabricPool 11
  failover group 17
  fault tolerance 8
  feature release 32
  FIPS compliance 10, 29
  FlashPool 11
  FlexClone copies 26
  General Availability 32
  high availability (HA) pairs 8
  high availability (HA) pairs 7
  Kerberos support 27
  LIF 17, 18
  load balancing 19
  logical interface 14, 15
  logical interface (LIF 17, 18
  logical ports 9
  LUNs 13
  MetroCluster continuous availability 24
  NAS path failover 17
  network architecture 9, 10
  nondisruptive operations 8
  platform support 6
  port set 18
  protocol support 6
  QoS 19
  qtree 13
  RAID groups 11
  RBAC 15, 28
  Release Candidate 32
  release model 32
  Role-Based Access Control (RBAC) 15, 28
  root-data partitioning 12
  root-data-data partitioning 12
  SAN path failover 18
  scale out architecture 7
  Selective LUN Map (SLM 18
  service update 32
  SnapLock archiving and compliance 30
  SnapMirror replication 22
  Snapshot copies 21
  software version support 32
  storage quality of service (QoS 19
  Storage Virtual Machine (SVM) 14, 15
  subnets 17
  support for cloud storage 6
  support for commodity hardware 6
  support for WORM storage 30
  supported platforms 6
  SyncMirror 24
  thin provisioning 25
  virtualization 7, 14–17
  volumes 13
  WAFL 21, 25, 26
  Write Anywhere File Layout (WAFL) 21, 25, 26

ONTAP Antivirus Connector
  role in virus scanning 28
  optimized path
  concepts 18

P

parity disk
  concepts 11, 12
  path failover
    in SAN 18
  peered clusters and SVMs
    concepts 22
  platform support
    ONTAP 6
  port set
    concepts 18
  protocol support
    ONTAP 6

Q

QoS
  concepts 19
  multitenancy use case 19
  qtree
    concepts 13

R

RAID group
  concepts 11, 12
  sizing recommendations 11, 12
RAID-DP
  concepts 11
RBAC
  concepts 15, 28
Release Candidate
  ONTAP 32
release model
  ONTAP 32
replication
  MetroCluster continuous availability 24
SnapMirror disaster recovery and data transfer 22
Snapshot copies 21
role
concepts 15, 28
Role-Based Access Control (RBAC)
concepts 15, 28
root aggregate
concepts 12
root volume
requirement for load-sharing mirror copy 16
root-data-data partitioning
concepts 12
root-data-partitioning
concepts 12
S
SAN path failover
concepts 18
scale out architecture
concepts 7
security
administrator authentication and authorization 28
client authentication and authorization 27
encryption 29
Kerberos support 27
Storage-Level Access Guard 27
WORM storage 30
Selective LUN Map (SLM)
concepts 18
self-encrypting disk (SED)
concepts 29
service update
ONTAP 32
share
CIFS 16
SMB 16
SLM
concepts 14, 18
SMB share
concepts 16
SnapLock archiving and compliance
concepts 30
SnapLock for SnapVault
concepts 30
SnapMirror disaster recovery and data transfer
concepts 22
Snapshot copies
concepts 21, 22, 26
SnapVault archiving
characteristics of 23
SNMP traps
concepts 10
software version support
ONTAP 32
storage efficiency
compaction 26
compression 26
deduplication 25
thin provisioning 25
storage encryption
concepts 29
storage quality of service (QoS)
concepts 19
multitenancy use case 19
Storage Virtual Machine (SVM)
administrators 15, 28
and namespace 16
concepts 14
root volume 16
use cases 15
Storage-Level Access Guard
concepts 27
subnet
concepts 17
SVM
administrators 15, 28
and multitenancy 15
and namespace 16
concepts 14
disaster recovery 22
root volume 16
use cases 15
SVM peering
concepts 22
SVM root volume
concepts 13
SyncMirror
concepts 24
system volume
concepts 13
T
takeover
HA pairs 8
thin provisioning
concepts 25
throughput ceiling (QoS Max)
concepts 19
throughput floor (QoS Min)
concepts 19
Twitter
how to receive automatic notification of
documentation changes 38
V
virtualization
ONTAP 7
VLAN
and broadcast domain 17
concepts 9
volume
and junction points 16
and namespaces 16
concepts 13
moving 14
volume encryption
concepts 29
vsadmin role
and SVM administrators 15
Vscan
antivirus scanning functionality in ONTAP 28

W

WORM storage
ONTAP support for 30
Write Anywhere File Layout (WAFL)
concepts 21, 25, 26